# INTERNATIONAL JOURNAL OF INTELLIGENT COMMUNICATION AND COMPUTER SCIENCE

ISSN: 3048-7285

VOL. 2, NO. 2

**Pages: 96**


## TABLE OF CONTENT


A comparative analysis of Machine Learning based algorithms for diagnosis of Alzheimer's Disease.
Tamoghna Mukherjee, Anirban Mitra, Pronaya Bhattacharya, Debolina Nath and Pragya Mukherjee (Pages: 1-16)

Enhancing Security with a Distributed Honeypot System Based on Blockchain: A Mathematical Attack Analysis.
Neharika Nishad and Rahul Singh (Pages: 17-26)

Blockchain-Enabled Wireless Sensor Networks: A Paradigm Shift in Security and Data Integrity.
Amit Yadav and Manish Jain (Pages: 27-38)

Integrating Visible Light Communication into Vehicle-to-Vehicle Systems: A Detailed Overview.
Avanish Kumar Dixit and Rohitashwa Pandey (Pages: 39-56)

Underwater Rescue Management in Flooded Areas Using Wireless Sensor Networks: An Overview.
Sangeeta Ranjan and Atul Mathur (Pages: 57-76)

Leveraging ECG Biometrics for Enhanced Security and Health Monitoring.
Sandeep Tripathi and Rohitashwa Pandey (Pages: 77-96)



Contact:
editor@ijiccs.in
ijiccs@gmail.com

**International Journal of Intelligent Communication and Computer Science**
**Vol. 2, No. 2, 2024, Pages 1-16.**

# A comparative analysis of Machine Learning based algorithms for diagnosis of Alzheimer's Disease

**Tamoghna Mukherjee[1], Anirban Mitra[1], Pronaya Bhattacharya[1], Debolina Nath[1] and Pragya Mukherjee[1]**

[1]Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Kolkata-700135, West Bengal, India

**Research Paper**

Email: pbhattacharya@kol.amity.edu,
Received: 11 Jul 2024, revised: 1 Aug 2024 Accepted: 1 Aug 2024

**Abstract:**

Alzheimer's disease (AD) is one of the most prevalent types of dementia, a term used to describe a deterioration in memory along with various other mental and behavioural skills in people. The rate of the affected individuals is increasing at an alarming rate and is ultimately affecting a huge section of the population. The OASIS (Open Access Series of Imaging Studies) longitudinal dataset has been used in this study's comparative analysis of various classification algorithms for the diagnosis of AD. Since the accuracy of the obtained results is of utmost importance in the case of highly sensitive medical data, the aim is to achieve high prediction accuracy. Among the applied classification algorithms such as Random Forest (RF), Logistic Regression (LR), Gradient Boosting Classifier (GBC), Naive Bayes Classifier (NBC), and Support Vector Machine (SVM), it was found that NBC provides the most stable results with a high accuracy of 97.33% on our dataset. Hence, NBC was chosen for the creation of our prediction model and deployed to operate as the underlying algorithm for the UI of our web application. The developed UI accepts patient-oriented data inputs from the user and displays whether the patient is demented or non-demented.

**Keywords:** Alzheimer's disease, Logistic Regression, Random Forrest, Gradient Boosting, Naive Bayes, Support Vector Machine.

## 1. Introduction

Dementia [1] is the general term associated with the loss of memory, language and other thinking capabilities that severely affects daily functioning in human beings. As reported by World Health Organization (WHO), dementia is currently the seventh leading cause of death and one of the major causes of disability and dependency among the aged population. With 60–70% of cases, Alzheimer's disease (AD) [2] is the most prevalent type of dementia. At present, more than 55 million people across the globe are affected by AD and the number is on continuous rise. Statistics indicate that it will increase to 78 million by 2030 and 139 million by 2050 [3]. The disease also has a major economic impact on the nations, and it is accessed that its total estimated cost is over 1.3 trillion USD across the globe. Though there is no such curative method for this neurodegenerative disease, its early detection can slow down the progressive degeneration in the patient through supporting medication. The initiation of proper medication at an early stage can prevent the neurons from getting damaged to a greater extent within a shorter time frame.

The World Alzheimer Report [4], released every year, suggests the different developments with respect to the disease diagnosis and its prevention and post diagnosis treatment process. The early detection of AD using modern technology is one of its main focuses. Several studies are being conducted in this domain and efforts are being made to predict as well as identify symptoms of AD with accuracy. The detection of AD requires thorough medical analysis under the supervision of an expert professional. This makes it a costly as well as time-consuming affair. The diagnosis of the disease is mostly based on the analysis of MRI scans conducted over a period on the patients. As the cost of the medical assessments is continuously on rise, often it is beyond the capacity of the masses to afford it. Moreover, the demand for such medical assessments is so high that it leads to long waiting periods before undergoing the assessment and obtaining the test results. This leads to unwanted delays in the diagnosis and initiation of the treatment. Thus, automating the detection process can reduce both the time and the cost of treatment. Artificial Intelligence and ML have emerged as one of the most used approaches for the detection of AD[5]. In this study, we aim to apply different supervised learning algorithms to classify patients as demented or non-demented and use the best-performing algorithm to develop a prediction model for AD. For this purpose, the OASIS longitudinal dataset was chosen since it is a labeled dataset suitable for the application of classification algorithms. The following were applied after data preprocessing as discussed in detail under the proposed mechanism: LR [6], RF [7], GBC [8], NBC [9], and SVM [10]. Each of them performed well on the pre-processed data, however, NBC showed the best and most stable results with an accuracy of 97.33%. Thus, it was chosen to develop the prediction model. The working model seemed to classify the patients with great accuracy. A UI interface was also created by deploying the NBC-based prediction model at the backend to make it easier to predict the results by giving the patient-specific data as input.

**Motivation, contribution and limitations**

The motivation behind this study is rooted in the significant impact that dementia, particularly Alzheimer's disease (AD), has on the global population. Dementia is a major cause of disability and dependency among the elderly, with AD being the most prevalent form. The current methods of diagnosing AD are costly, time-consuming, and often lead to delays in treatment initiation due to the high demand and associated expenses of medical assessments like MRI scans. This study aims to address these challenges by leveraging Artificial Intelligence (AI) and Machine Learning (ML) to develop an automated and cost-effective method for early detection of AD. Early detection can significantly slow the progression of the disease through timely intervention, thus improving patient outcomes and reducing the economic burden on healthcare systems.
The methods for analysis was chosen meticulously based on certain traits matching with the desired outcome. Logistic Regression is a straightforward and interpretable algorithm that was applied to classify patients as demented or non-demented. Its use helps in understanding the influence of individual features on the probability of a patient being demented, providing valuable insights into the relationships between the input variables and the outcome. In terms of Random Forest, an ensemble learning method, was used to improve classification performance by combining multiple decision trees. It helps in handling a large number of input variables and managing missing data effectively. A equally competitive method Gradient Boosting Classifier was applied to enhance predictive accuracy by sequentially building models to correct the errors of previous models. This method is effective in capturing complex patterns in the data. To judge more we used Naive Bayes Classifier, based on Bayes' theorem. It was found to perform best with an accuracy of 97.33%. It was selected for the final prediction model due to its simplicity, efficiency, and surprisingly robust performance despite its strong independence assumptions. Lastly Support Vector Machine was used to classify patients by finding the optimal hyperplane that separates the data into different classes. SVM is effective in high-dimensional spaces and with datasets where the number of dimensions exceeds the number of samples.
The accuracy and performance of the model are highly dependent on the quality and comprehensiveness of the OASIS longitudinal dataset. Any biases or limitations in the dataset can directly affect the model's reliability and generalizability. While NBC performed best in this study, its effectiveness is contingent on the assumption that features are independent. In real-world scenarios, this assumption may not always hold true, potentially affecting the model's accuracy in different contexts. The model's ability to generalize to diverse populations or datasets outside of the OASIS dataset is not established. The effectiveness of the model across different demographic and clinical settings needs further validation. Developing a prediction model and user interface is one aspect, but integrating this tool into existing healthcare systems and ensuring its adoption by healthcare

providers presents additional challenges. Issues related to interoperability, user training, and system acceptance need to be addressed. Using patient data for training and deploying AI models raises ethical and privacy concerns. Ensuring data security, patient consent, and compliance with regulations such as HIPAA is crucial.

Each method contributed uniquely to the study, offering insights into their strengths and limitations. The Naive Bayes Classifier's outstanding performance led to its selection for the final prediction model, which was integrated into a user-friendly interface for practical use in early detection of AD. Overall, while the study makes significant contributions towards automating the early detection of AD using AI and ML, further work is needed to address these limitations and ensure the model's broader applicability and integration into healthcare practice.

The remainder of the paper is organized as follows: Section II discusses the previous studies conducted in this domain, Section III focuses on the Proposed Mechanism, Section IV contains the Experimentation Results, and Section V which suggests the Conclusion and Future Works, followed by the set of References used in this paper.

## 2. Literature Review

Several studies have been conducted over the years using different datasets as well as different approaches for developing an efficient clinical system to predict Alzheimer's disease. Numerous strategies have been applied to detect and predict the disease, particularly in the fields of ML and deep learning. Some of the pre-existing works conducted in this field have been discussed below.

Both supervised and unsupervised learning algorithms have been extensively employed in ML for disease diagnosis as well as prediction. In [11], generalized linear models (GLM), decision trees (DT), Rule induction, NBC, k-nearest neighbors (k-NN), and deep learning techniques were all applied to the Alzheimer's Disease Neuroimaging Initiative (ADNI) dataset, collected through the TADPOLE (The Alzheimer's Disease Prediction Of Longitudinal Evolution) challenge [12]. The objective was to categorize the five distinct phases of AD and to determine the most distinctive characteristic for each stage of AD within the ADNI dataset. The obtained results showed that GLM outperformed the rest with the highest accuracy of 88.24%. In another study [13], ADNI was used as a part of the early detection analysis of AD where a sophisticated hybrid cognitive classification mechanism was applied using 2-layer model stacking. The procedure outperformed other popular classification techniques. The algorithm showed 3 experiments with the ultimate highest accuracy of 95.12% using hybrid modeling. In [14], a neural network architecture was proposed along with a novel preprocessing algorithm for the prediction of AD. Data from the ADNI was preprocessed using a novel technique named as "All-Pairs" technique to produce the training dataset. In the "All-Pairs" technique the comparison of all possible pairs of temporal data points for each patient was considered. The trained model was capable of correlating clinical data obtained from patients at a particular instance of time with the progression of AD in the future. The model was found to be effective at predicting AD with an average mAUC score of 0.866. An in-depth examination of various deep learning approaches under the generative and discriminative architecture of deep learning has been performed in [15]. Data from OASIS has been used in [16] for the prediction of AD by SVM, LR, DT, and RF. After running the developed model before as well as after fine-tuning, it was found that SVM yielded the best results with an accuracy of 91.8% among the applied algorithms. A similar approach was used for detection in [17] by employing LR, SVM, RF, Extra Trees, and GBC. Extensive research work has been done using the data obtained from OASIS concentrating more on feature selection and feature extraction using ML algorithms in [18].

In [19], SVM, NBC, XGBoost, DT, LR, RF, Bagging and AdaBoost were applied on The Korean Brain Aging Study for the Early diagnosis and prediction of Alzheimer's disease dataset to classify patients under examination into the following three categories: individuals with cognitively normal control, individuals with mild cognitive impairment and individuals suffering from AD. XGBoost performed best on this dataset showing an accuracy of 82.09%.

Since RF has been proven to be effective at reducing high-dimensional and multi-source data, it has been widely employed for the prediction of AD. For instance, [20] examines the most recent RF implementations on single and multimodal neuroimaging data for the diagnosis and prognosis of AD. The use of Next Generation Sequencing (NGS) techniques has been applied in [21] to develop high-throughput screening methods for identifying the biomarkers and variants that assist in the early diagnosis of a disease. It suggests a model called VEPAD that relies on the use of cross-validation-based recursive feature elimination, which is then followed by a forward feature selection to choose key features to distinguish between deleterious and neutral variants.

**Table 1: Summarized literature survey**

| Study | Dataset | Methods | Key Findings |
|---|---|---|---|
| Shahbaz et al. [11] | ADNI (TADPOLE) | GLM, DT, NBC, k-NN, Deep Learning | GLM outperformed other methods in classifying AD stages |
| Khan et al. [13] | ADNI | Hybrid Cognitive Classification (2-layer model stacking) | Hybrid model stacking outperformed popular classification techniques |
| Soliman et al. [14] | ADNI | Neural Network with "All-Pairs" technique for preprocessing | Novel preprocessing technique improved prediction accuracy |
| Shastry et al. [15] | Not specified | Various Deep Learning Approaches | In-depth examination of generative and discriminative DL architectures |
| Antor et al. [16] | OASIS | SVM, LR, DT, RF | SVM performed best after fine-tuning |
| Varun et al. [17] | OASIS | LR, SVM, RF, Extra Trees, GBC | Emphasis on feature selection and extraction |
| Hosseinzadeh Kasani et al. [19] | Korean Brain Aging Study | SVM, NBC, XGBoost, DT, LR, RF, Bagging, AdaBoost | XGBoost performed best among applied algorithms |
| Sarica et al. [20] | Various | Random Forest | Systematic review of RF implementations for AD diagnosis |
| Rangaswamy et al. [21] | NGS data | VEPAD Model, cross-validation-based recursive feature elimination | High-throughput screening for biomarkers and variants |
| Kishore et al. [22] | Not specified | SVM | SVM with linear kernel outperforms other ML algorithms |
| Khan et al. [23] | MRI data | Transfer Learning (VGG architecture) | Layer-by-layer fine-tuning with real MRI data |
| Liu et al. [24] | MRI images | Multiple kernels combining edge and node features | Effective categorization of AD |
| Huang et al. [25] | Not specified | Longitudinal monitoring, hierarchical classification | Addressed high feature dimensionality and added spatial information for better accuracy |

The study conducted in [22] shows that the SVM algorithm with linear kernel outperforms other ML algorithms in detecting AD, although initial research studies proved lesser accuracy with the SVM algorithm in the detection of the said disease. In [23], transfer learning using a VGG architecture has been developed where the network has been fine-tuned layer-by-layer while also feeding a predefined group of such layers with real MRI data. The use of multiple kernels to combine edge characteristics and node features for the categorization of AD, as well as the evaluation of 710 MRI images using 10-fold cross-validation, have been proven to be effective [24]. Longitudinal monitoring of MCI brain imaging and a hierarchical classification strategy for predicting AD have been applied in [25] to deal with high feature dimensionality difficulties and adding spatial information for increasing prediction accuracy. Table1 describes the summarized literature survey.

These are a few to name and several other notable works have been conducted in this field. Hence, gaining insights from the above-discussed studies, our aim in this study is to apply classification techniques on our

chosen dataset post-preprocessing and develop a predictive model that can predict AD with high accuracy. A supporting UI will also be developed to make the developed model easy to use by all.

## 3. Proposed Mechanism

To develop a model for predicting and analyzing Alzheimer's Disease (AD), we followed a systematic workflow as illustrated in Fig. 1. This workflow outlines the step-by-step process used to build and evaluate each machine learning (ML) algorithm applied in our study. The process begins with data collection, where we gather and prepare datasets that include relevant clinical and imaging features associated with AD. This step ensures that the data used for training and testing the models are comprehensive and representative of various aspects of the disease. Next, we perform data preprocessing, which involves cleaning the data, handling missing values, and normalizing or standardizing features to improve model performance. Feature selection is then conducted to identify and retain the most informative variables, reducing dimensionality and enhancing the relevance of the data for the model. Following preprocessing, we split the data into training and testing sets. The training set is used to build and tune the ML models, while the testing set is reserved for evaluating their performance. This split helps ensure that the models are both trained on a representative subset and validated on unseen data. We then apply a range of machine learning algorithms, including supervised and unsupervised learning techniques, as specified in our study. Each algorithm is trained using the training data, and hyperparameters are optimized to achieve the best possible performance.

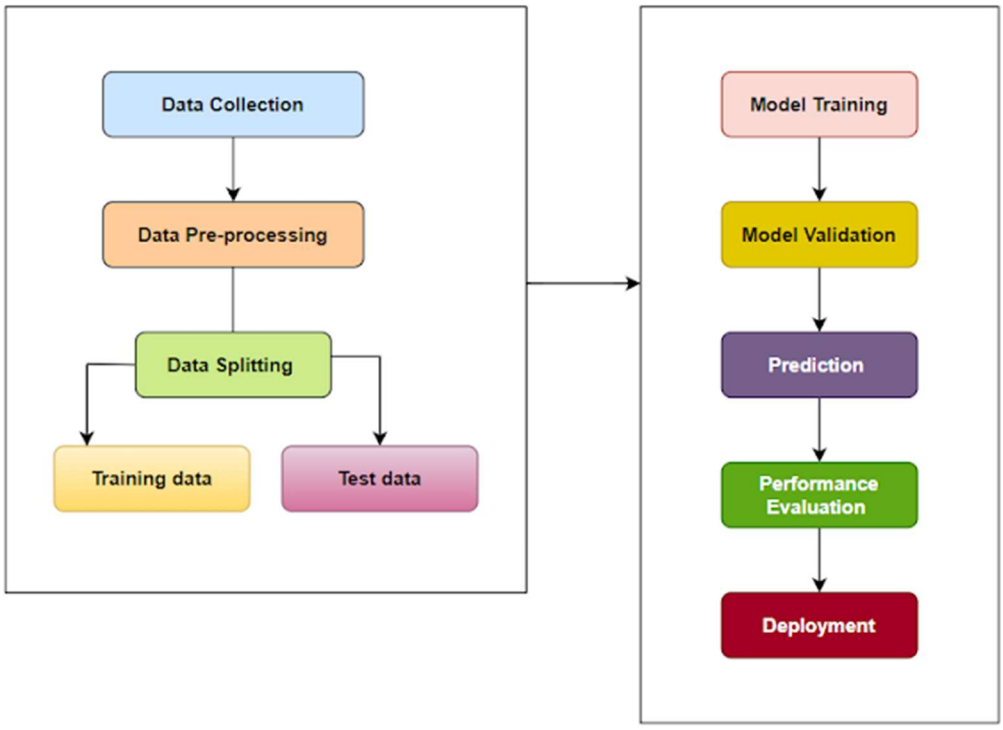


**Figure 1: Overall workflow of the proposed mechanism**

### 3.1 Dataset Description

In this study, the data used has been obtained from the OASIS longitudinal dataset available in Kaggle [37]. This dataset which was released in 2010 contains details of MRI scans of 150 participants, elderly males as well as females, in the age group of 60 to 96 collected over a course of 373 imaging sessions. Thus, OASIS-LD is a labelled dataset on which supervised learning algorithms are applicable for prediction purposes, Table 2.

**Table 2: OASIS-LD Attributes**

| Sl.No. | Attributes | Description |
|---|---|---|
| 1 | Subject ID | Subject Identification |
| 2 | MRI ID | MRI Exam Identification |
| 3 | Group | Class or type of patients |
| 4 | Visit | Visit Order |
| 5 | MR Delay | MR delay time |
| 6 | M/F | Gender |
| 7 | Hand | Hand |
| 8 | Age | Age of patients |
| 9 | EDUC | Years of Education |
| 10 | SES | Socioeconomic Status |
| 11 | MMSE | Mini Mental State Examination |
| 12 | CDR | Clinical Dementia Rating |
| 13 | eTIV | Estimated total intracranial volume |
| 14 | nWBV | Normalize Whole Brain Volume |
| 15 | ASF | Atlas Scaling Factor |

### 3.2 Data Preprocessing

Data preprocessing is an important step before evaluating any ML algorithm. Several steps have been taken into consideration to remove data inconsistency and redundancy from the raw dataset, such as data scaling, removal of features having lesser to least relation to the target variable, handling missing values, conversion of textual data to numeric data, etc. The chosen dataset required preprocessing without which the algorithms could not be applied it satisfactorily. Hence the following preprocessing steps were carried out to make the dataset ready for further processing:

1. The columns namely -**Subject ID, MRIID, Hand,** and **Visit** were dropped from the dataset as they were not significant parameters for model creation.
2. The null values present in the **SES** and **MMSE** fields were replaced by the mean values of the respective columns.
3. The column labelled **M/F** was renamed as **Gender**.
4. Since it is easier to deal with numeric values compared to characters, the values **M** and **F** present in the **Gender** column, signifying male and female respectively, were converted to 0 and 1.
5. Similarly, the values **Non-Demented** and **Demented** were replaced by 0 and 1 respectively.

Some ML algorithms show better performance when the input variables with numeric values are scaled to a standard range. Standardization scales the individual input variable by subtracting the mean from the data point and dividing by the standard deviation. This ensures the mean of the data values to be 0 and the standard deviation to be 1. As a part of our analysis, Standard scalar has been used to scale the input data. It was found that the algorithms considered, especially SVC significantly improved the performances and showed higher accuracy once the dataset was scaled using the standardization technique. The dataset was divided into a training dataset (containing 80% of the data) and a testing dataset (containing 20% of the data) following pre-processing and scaling. The testing data was used to evaluate the model's accuracy after it had been trained using ML techniques utilizing the training data.

### 3.3 Classification Algorithms

As a part of the comparative study of several classification techniques of ML algorithms for the prediction of AD in an individual, this paper focuses on the following algorithms:

#### 3.3.1: Logistic Regression (LR):

Logistic regression is a fundamental and widely-used statistical method for binary classification tasks, where the goal is to predict the probability of an outcome belonging to one of two distinct categories. The relationship between the independent features and the dependent variable, which has two alternative outcomes (e.g.: 0/1), is shown via logistic regression [26] [27]. The general function for logistic regression, used for the predictive analysis of the dependent binary variable (in our case it is *demented/non-demented*) is sigmoid function denoted by-

$$f(x) = 1/1+e^{-x} \quad (1)$$

The function $f(x)$ in Eq. 1 converts a real value to a probability between 0 and 1. The class probability is taken to be 0 if it lies below the threshold value (0.5), else 1 in Fig. 2.

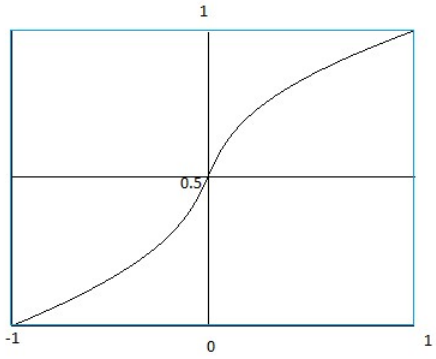


**Figure 2: Logistic function for deciding class label**

**Key Points:**

1. **Binary Classification:** Primarily used for binary outcomes (0/1, true/false, yes/no), but can be extended to multiclass classification.
2. **Linear Model:** Assumes a linear relationship between the input features and the log-odds of the output.
3. **Sigmoid Function:** Uses the logistic sigmoid function to convert the linear combination of inputs into a probability.
4. **Interpretability:** The coefficients (weights) provide insight into the influence of each feature on the prediction.
5. **Regularization:** Can incorporate L1 (Lasso) or L2 (Ridge) regularization to prevent overfitting.

#### 3.3.2: Random Forest Classifier (RF):

Random Forest is a versatile and robust ensemble learning technique primarily used for classification and regression tasks. It builds upon the concept of decision trees by creating a "forest" of multiple decision trees, which collectively contribute to the final prediction. The process begins with generating a multitude of decision trees using a technique called bootstrap aggregating, or "bagging." In this method, different subsets of the

training data are sampled with replacement to train each tree, which introduces diversity among the trees and helps reduce overfitting.
In nutshell RF classifier [28] [29] takes the average of the outcomes from every decision tree and the most voted prediction result is chosen. This provides accurate and more precise prediction results.
The algorithm goes like –

1. Start by selecting random instances from the training data.
2. Build decision trees with the selected data.
3. Choose the number of decision trees.
4. Repeat steps 1 and 2
5. For testing data points, assign the category with majority votes from the created sub trees.

The visual flow of the algorithm has been demonstrated below in Fig. 3.

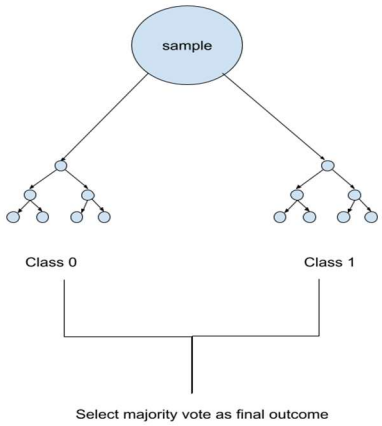


**Figure 3: Majority voting in RF**

The first decision tree for the RF model trained on the considered dataset has been visualized in Fig.4.

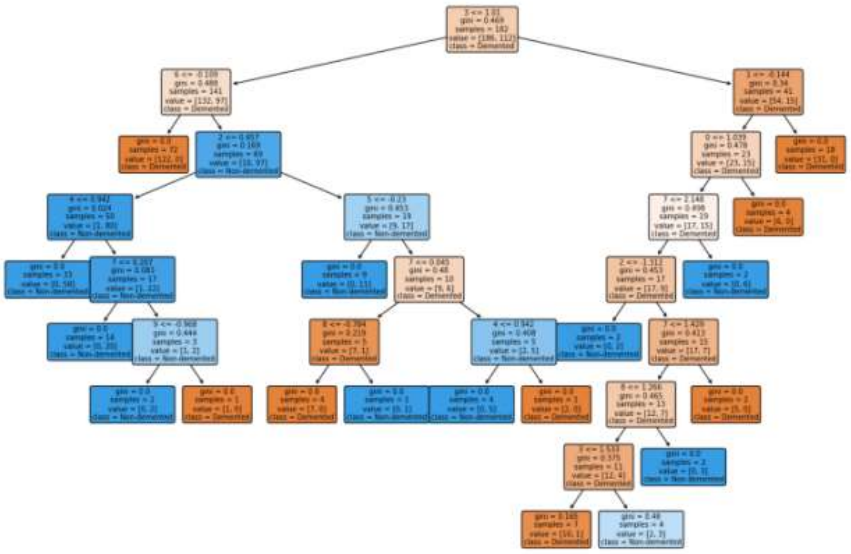

**Figure 4: DT structure in classifying demented and non-demented individual.**

**Key Points:**

1. **Ensemble Method**: Combines multiple decision trees to improve predictive performance and control overfitting.
2. **Bootstrap Aggregation (Bagging)**: Each tree is trained on a random subset of the data (with replacement) to create diversity among the trees.
3. **Random Feature Selection**: At each split in the tree, a random subset of features is considered for splitting, which helps reduce correlation between trees.
4. **Non-linear**: Capable of capturing complex interactions between features.
5. **Robustness**: Generally robust to overfitting and performs well on a variety of tasks.
6. **Feature Importance**: Provides an estimate of feature importance by measuring the impact of each feature on the accuracy of the model.

**3.3.3: Gradient Boosting Classifier (GBC):**

The GBC is a powerful and flexible ensemble learning technique used for classification tasks. It builds models incrementally by combining the outputs of several weak learners, typically decision trees, to create a strong predictive model. The fundamental idea behind GBC is to improve the performance of the model by addressing the errors made by previous models in the ensemble. GBC [30] moves ahead with repeated functions that keep on minimizing the loss function. In other words, it is a type of ensemble learning mechanism which makes sure to improvise at every iteration [31].

The skeleton of the GBC algorithm works as follows-

1. Initialize the model with log(odds) as the constant value.
2. Calculate the residuals of the predictor.
3. Create the decision trees.
4. Update the residual errors in the next iteration.
5. Continue steps 2-4 until the loss function is minimized.

**Key Points:**

1. **Ensemble Method**: Builds an ensemble of weak learners (usually decision trees) sequentially.
2. **Boosting**: Each subsequent tree is trained to correct the errors of the previous trees by focusing on the residual errors.
3. **Additive Model**: Combines the predictions of multiple trees by adding them together, typically with a learning rate to control the contribution of each tree.
4. **Gradient Descent**: Uses gradient descent to minimize a loss function by iteratively adding trees that reduce the overall error.
5. **Flexibility**: Can optimize various loss functions and is suitable for both classification and regression tasks.
6. **Hyperparameters**: Involves several hyperparameters such as the number of trees, tree depth, and learning rate, which need careful tuning to avoid overfitting and achieve optimal performance.

**3.3.4. Naive Bayes Classifier (NBC):**

The Naive Bayes Classifier (NBC) is a probabilistic machine learning algorithm based on Bayes' Theorem with an assumption of independence among features. It is widely used for classification tasks due to its simplicity, efficiency, and effectiveness in handling large datasets. NBC uses a probabilistic framework for solving classification problems [32] [33]. It is based on the use of the Bayes Theorem (Eq. 2) [34] which follows:

$$P(C / A) = (P( A / C).P(C)) / P(A) \quad (2)$$

where P(C) is the prior probability and P(C|A) is the posterior probability with respect to the occurrence of event A. In NBC, the relationship between input features and class expressed as probabilities and a naïve assumption is made the features/ attributes are independent of each other.

The algorithm follows as –

1. Get the frequency table based on the target class.
2. Calculate the respective likelihood.
3. Calculate posterior probability using Bayes Theorem [34].

### 3.3.5 Support Vector Machine (SVM)/ Support Vector Classifier (SVC)

The SVM is a powerful supervised learning algorithm used for classification and regression tasks. It is known for its effectiveness in high-dimensional spaces and its ability to create complex decision boundaries. The foundation of SVC[35] [36] is based on the idea of building a decision boundary or hyperplane that can divide n-dimensional space into classes so that fresh input points can be classified correctly. To create the hyperplane, SVM selects the extreme points or vectors, also referred to as support vectors.

The SVM works as follows:

1. SVM tries to find the best fit boundary to separate the classes.
2. The distance between the hyperplane and the support vector is known as margin, and the main motive is to maximize the margin for linear data points.
3. In case of non-linear data points, the concept of 3D is implemented.

## 4. Result and Discussion

The models have been developed and implemented using Python 3.9.1 using various standard libraries available. The results obtained after the implementation of the discussed mechanism are presented in this section.

### 4.1 Dataset Visualization

A thorough visual analysis of the dataset reveals several significant conclusions that provide valuable insights into its characteristics and underlying patterns. This analysis involves using various visualization techniques to explore and understand the data more deeply.

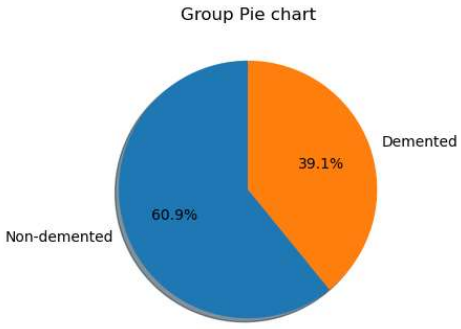


**Figure 5: Group distribution**

The OASIS longitudinal dataset reveals that among 373 of the total individuals under consideration, 227 of them are found to be non-demented (60.9%) while 146 of the total are demented (39.1%) according to Fig. 5. This indicates that the dataset is somewhat imbalanced, with a higher proportion of non-demented cases.

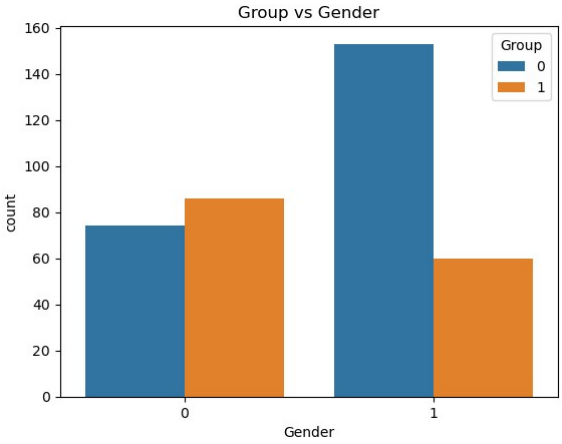


**Figure 6: Group vs. Gender distribution**

Men have higher chances of dementia as compared to female (0 for male and 1 for female as demonstrated in Fig. 6). This distribution provides additional context for evaluating model performance, as it shows the imbalance not only in the target variable (Demented vs. Non-demented) but also in the gender distribution.

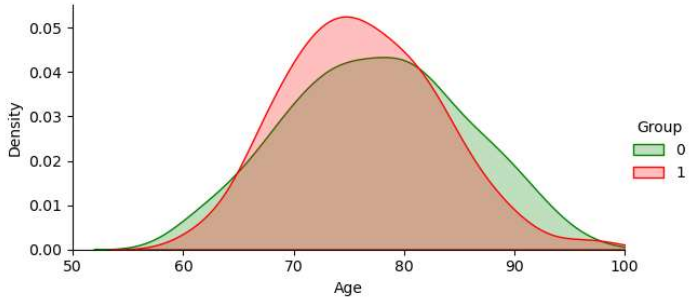


**Figure 7: Group vs. Age distribution**

Dementia is highly probable within the age span of 70-80 years according to Fig. 7. The plot suggests that the Demented group tends to have a higher peak density around the age of 75. The Non-demented group has a more spread out age distribution, with a peak density slightly lower than the Demented group.

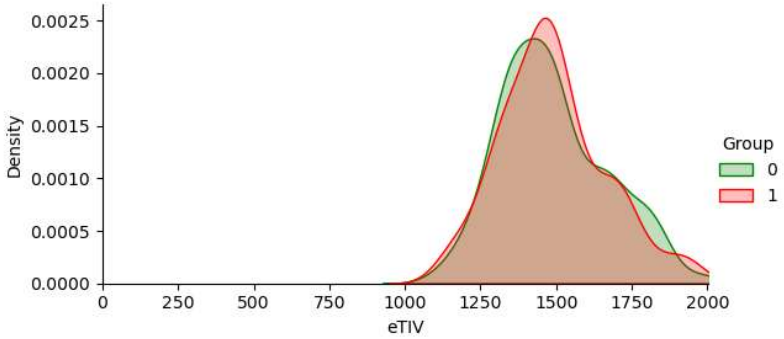


**Figure 8: Group vs. eTIV distribution**

Fig. 8 shows both groups have a similar distribution pattern, with a peak around the same eTIV value. Group 1 (red line) appears to have a slightly higher peak density than Group 0 (green line), indicating a higher concentration of data points around the peak eTIV value.The distribution tails off similarly for both groups on either side of the peak, but Group 1 shows a bit more spread towards higher eTIV values.

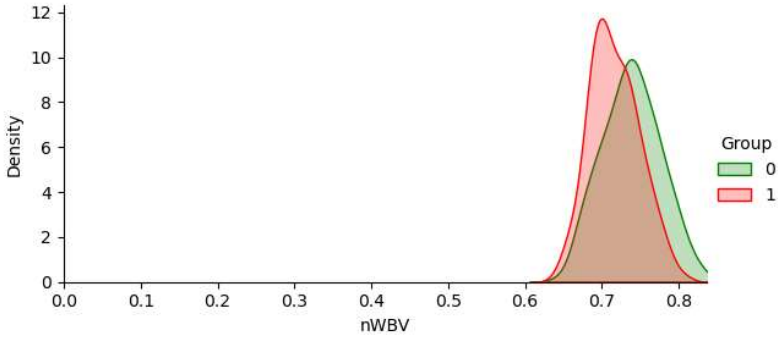


**Figure 9: Group vs. nWBV distribution**

Fig. 9 shows the distributions of both groups are narrower and more peaked compared to the eTIV plot. Group 1 (red line) has a higher peak density than Group 0 (green line), indicating a higher concentration of data points around the peak nWBV value. The peak for Group 1 is slightly shifted to the left of the peak for Group 0, indicating that Group 1 tends to have lower nWBV values compared to Group 0. Both groups have a very tight distribution, with most of the values falling between 0.6 and 0.8.

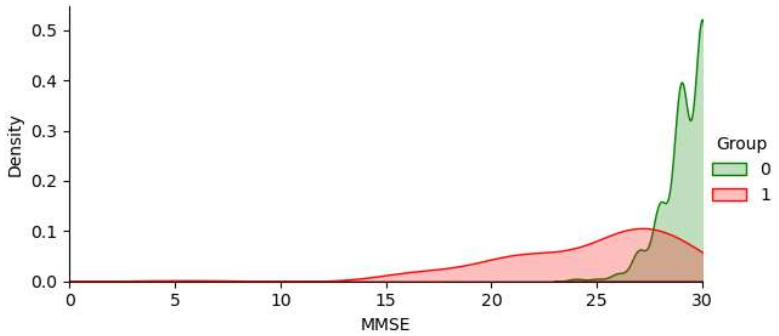


**Figure 10: Group vs. MMSE distribution**

In Fig. 10. Group 0 (green line) shows a significant peak at an MMSE score of 30, indicating a high concentration of individuals with the highest possible MMSE score. Group 1 (red line) has a more spread-out distribution, with a notable peak around an MMSE score of 25, but also showing a wider range of lower scores. The density for Group 0 increases sharply around the maximum MMSE score, while Group 1 shows a gradual increase and decrease in density across the score range.
This suggests that individuals in Group 0 generally perform better on the MMSE, clustering around the highest score, whereas individuals in Group 1 have more variability in their MMSE scores, with many scoring below the maximum.

### 4.2 Model Results

The confusion matrices for the four classification models—Random Forest (RF), Logistic Regression (LR), Gradient Boosting Classifier (GBC), and Support Vector Classifier (SVC)—reveal detailed insights into their performance in predicting positive and negative classes.
For the Random Forest (RF) model, the confusion matrix shows a total of 484 true positives (TP) and 16 false negatives (FN). This indicates that the model effectively identified positive instances while misclassifying a relatively small number. The false positive (FP) count is also 16, with 484 true negatives (TN), demonstrating a high level of accuracy in distinguishing negative cases (Table 3). The RF model performs robustly with a high number of correct predictions and a low rate of misclassifications.

**Table 3: Confusion Matrix for Random Forest (RF)**

| | Predicted Positive | Predicted Negative |
|---|---|---|
| **Actual Positive** | 484 (TP) | 16 (FN) |
| **Actual Negative** | 16 (FP) | 484 (TN) |

In the case of Logistic Regression (LR), the model correctly predicted 480 positives (TP) but missed 20 positive instances (FN). It also incorrectly classified 20 negatives as positives (FP) while correctly identifying 480 negatives (TN) (Table 4). Compared to the Random Forest model, the Logistic Regression model shows a slight increase in both false negatives and false positives, though it still maintains a strong overall performance.

**Table 4: Confusion Matrix for Logistic Regression (LR)**

| | Predicted Positive | Predicted Negative |
|---|---|---|
| **Actual Positive** | 480 (TP) | 20 (FN) |
| **Actual Negative** | 20 (FP) | 480 (TN) |

The Gradient Boosting Classifier (GBC) exhibits similar performance to Logistic Regression, with 480 true positives and 20 false negatives. It also recorded 20 false positives and 480 true negatives (Table 5). The results from GBC are consistent with those of the Logistic Regression model, indicating its effectiveness in classification tasks.

**Table 5: Confusion Matrix for Gradient Boosting Classifier (GBC)**

| | Predicted Positive | Predicted Negative |
|---|---|---|
| **Actual Positive** | 480 (TP) | 20 (FN) |
| **Actual Negative** | 20 (FP) | 480 (TN) |

The Support Vector Classifier (SVC) shows some variations in its performance metrics. It achieved 473 true positives and 27 false negatives, suggesting that it missed a higher number of positive instances compared to the other models. The SVC also had 26 false positives and 474 true negatives (Table 6). While the model still performs well, it demonstrates slightly more difficulty in balancing precision and recall compared to the others.

**Table 6: Confusion Matrix for Support Vector Classifier (SVC)**

| | Predicted Positive | Predicted Negative |
|---|---|---|
| **Actual Positive** | 473 (TP) | 27 (FN) |
| **Actual Negative** | 26 (FP) | 474 (TN) |

The Naive Bayes Classifier (NBC) has a high rate of true positives (43) and very low false positives (0), suggesting it is effective at identifying positive cases without misclassifying negatives as positives (Table 7). However, its overall performance is lower compared to other classifiers, such as Random Forest, Logistic Regression, Gradient Boosting Classifier, and Support Vector Classifier, which exhibit higher accuracy and better overall classification metrics. The Naive Bayes approach might be suitable in scenarios where computational simplicity is prioritized, but it does not match the robustness and accuracy of the more complex models like RF, LR, GBC, and SVC.

The performance analysis of various algorithms applied to the pre-processed data reveals that the Naive NBC outperforms all other models with an impressive accuracy of 97.33%. This accuracy surpasses that of the RF classifier, which achieved an accuracy of 96.8%, and both LR and GBC, which both recorded accuracies of 96.00%. The SVC lagged slightly behind with an accuracy of 94.67%. Given these results, NBC was selected for developing the prediction model due to its superior performance.

**Table 7: Confusion Matrix for Naive Bayes Classifier (NBC)**

| | Predicted Positive | Predicted Negative |
|---|---|---|
| **Actual Positive** | 43 (TP) | 2 (FN) |
| **Actual Negative** | 0 (FP) | 29 (TN) |

The Table 4, presents a comprehensive comparison of various machine learning models based on several performance metrics, including Accuracy, Precision, Recall, and F1 Score.

**Table 4: Comparative analysis of the results**

| Model | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| **RF [16]** | 96.8% | 96.8% | 96.8% | 96.8% |
| **LR [17]** | 96.00% | 96.0% | 96.0% | 96.0% |
| **GBC [17]** | 96.00% | 96.0% | 96.0% | 96.0% |
| **SVC [22]** | 94.67% | 94.67% | 94.67% | 94.67% |
| **NBC (Proposed)** | **97.33%** | **94.1%** | **100%** | **97.0%** |

**Accuracy:** The NBC model achieved the highest accuracy at 97.33%, surpassing the RF, LR, GBC, and SVC models. This indicates that NBC is more effective in making correct predictions overall compared to the other classifiers. RF, LR, and GBC followed closely with accuracies of 96.8% and 96.00%, respectively, while SVC had the lowest accuracy at 94.67%.
**Precision:** Precision measures the proportion of true positive predictions among all positive predictions made by the model. The NBC model exhibited a precision of 94.1%, which is lower than that of RF, LR, and GBC, each achieving 96.0%. However, this trade-off in precision is compensated by NBC's perfect Recall.
**Recall:** Recall indicates the model's ability to correctly identify all relevant positive cases. NBC outperformed all other models with a perfect recall of 100%. This demonstrates NBC's superior ability to minimize false negatives and accurately detect all positive instances, an essential attribute for applications where missing a positive case could be critical.
**F1 Score:** The F1 Score, which balances precision and recall, was highest for the NBC model at 97.0%, reflecting its overall robustness in handling positive cases. The RF, LR, and GBC models had an F1 Score of 96.0%, while the SVC model's F1 Score was the lowest at 94.67%.

Overall, the NBC model not only provides the highest accuracy and F1 Score but also excels in Recall, making it the most effective model among those evaluated for the task at hand.

## 5. Conclusion and Future works

AD is a major health concern affecting a large part of the aged population across the globe. Thus, it is more important to diagnose early symptoms of the disease accurately to reduce risk and provide early medical intervention in cases of such diseases that do not have a cure. As seen in previous works, several ML models have been developed to diagnose AD at an early stage; however, the challenge lies in achieving accurate results. In this study, we have addressed this challenge and aimed to achieve high prediction accuracy with our developed model. We presented a comparative analysis of the performance among five state-of-art classification algorithms on the chosen dataset and developed the prediction model using the one with the highest accuracy. Following the application of each algorithm to the preprocessed data, the findings show that NBC has the best performance with the maximum accuracy of 97.33%, followed by other applied algorithms like - RF (96.8%), LR (96.00%), GBC (96.00%), and SVC (94.67%). In comparison to previous works, we

achieved an appreciably high accuracy. As part of our originality, we attempted to fit our models with as many relevant features from the dataset as feasible after thorough data cleaning and pre-processing. Apart from that, it was evident that efficient data cleaning and pre-processing resulted in better performances on the considered algorithms. Such high prediction accuracy is of immense significance, especially in cases of medical data and disease prediction where a patient's life is at stake.

This research can be expanded in the future by applying neural networks for prediction methods that will aid in disease detection and analysis of new features in the dataset. In addition, we will focus on improving the accuracy of the prediction in the future scope of the study, which will boost its significance in medical disciplines.

## References


1. Geldmacher, D.S., and P.J. Whitehouse. "Evaluation of Dementia." The New England Journal of Medicine (1996). https://doi.org/10.1056/NEJM199608013350507.
2. Scheltens, Phillip, Bart de Strooper, Miia Kivipelto, Helene Holstege, Gael Chételat, C.E. Teunissen, J. Cummings, and W. Flier. "Alzheimer's Disease." The Lancet 397, no. 10284 (2021): 1577-1590.
3. Wang, X., J. Qi, Y. Yang, and P. Yang. "A Survey of Disease Progression Modelling Techniques for Alzheimer's Diseases." IEEE International Conference on Industrial Informatics (2019): 1237-1242.
4. Flemming, Richard, John Zeisel, and Kirsty Bennett. World Alzheimer Report 2020. Alzheimer's Disease International, September 2020.
5. Yang, Kuo, and Emad A. Mohammed. "A Review of Artificial Intelligence Technologies for Early Prediction of Alzheimer's Disease." Electrical Engineering and Systems Science (2020). https://doi.org/10.48550/arXiv.2101.01781.
6. Wright, R. E. "Logistic Regression." In Reading and Understanding Multivariate Statistics, edited by L. G. Grimm and P. R. Yarnold, 217–244. Washington, DC: American Psychological Association, 1995.
7. Chaudhary, Archana, Savita Kolhe, and Raj Kamal. "An Improved Random Forest Classifier for Multi-Class Classification." Information Processing in Agriculture 3, no. 4 (2016): 215-222.
8. Bahad, P., and P. Saxena. "Study of AdaBoost and Gradient Boosting Algorithms for Predictive Analytics." In International Conference on Intelligent Computing and Smart Communication 2019, edited by G. Singh Tomar, N. S. Chaudhari, J. L. V. Barbosa, and M. K. Aghwariya, 22. Algorithms for Intelligent Systems. Singapore: Springer, 2020. https://doi.org/10.1007/978-981-15-0633-8_22.
9. Rish, I. "An Empirical Study of the Naive Bayes Classifier." In IJCAI, vol. 3, 2001.
10. Evgeniou, T., and M. Pontil. "Support Vector Machines: Theory and Applications." In Machine Learning and Its Applications: Advanced Lectures, 249-257. Berlin: Springer, 2001. https://doi.org/10.1007/3-540-44673-7_12.
11. Shahbaz, Muhammad, Shahzad Ali, Aziz Guergachi, Aneeta Niaz, and Amina Umer. "Classification of Alzheimer's Disease using ML Techniques." In ICDS19, vol. 2, 296-303. https://doi.org/10.5220/0007949902960303.
12. Marinescu, Razvan V., Neil P. Oxtoby, Alexandra L. Young, Esther E. Bron, Arthur W. Toga, Michael W. Weiner, Frederik Barkhof, Nick C. Fox, Stefan Klein, Daniel C. Alexander, and the EuroPOND Consortium. "TADPOLE Challenge: Prediction of Longitudinal Evolution in Alzheimer's Disease." Quantitative Biology (2018).
13. Khan, Afreen, and Swaleha Zubair. "Development of a Three Tiered Cognitive Hybrid ML Algorithm for Effective Diagnosis of Alzheimer's Disease." Journal of King Saud University - Computer and Information Sciences 34, no. 10, Part A (2022).
14. Soliman, Sarah A., El-Sayed A. El-Dahshan, and Abdel-Badeeh M. Salem. "Predicting Alzheimer's Disease with 3D Convolutional Neural Networks." International Journal of Applications of Fuzzy Sets and Artificial Intelligence 1 (2020): 125-146.
15. Shastry, K.A., V. Vijayakumar, M.K.M. V, M. B A, and C. B N. "Deep Learning Techniques for the Effective Prediction of Alzheimer's Disease: A Comprehensive Review." Healthcare 10 (2022): 1842. https://doi.org/10.3390/healthcare10101842.
16. Antor, Morshedul Bari, A. H. M. Shafayet Jamil, Maliha Mamtaz, Mohammad Monirujjaman Khan, Sultan Aljahdali, Manjit Kaur, Parminder Singh, and Mehedi Masud. "A Comparative Analysis of ML

Algorithms to Predict Alzheimer's Disease." Journal of Healthcare Engineering (2021). https://doi.org/10.1155/2021/9917919.
17. Varun, Krishna Kumar, Shankar Hamritha, and Mavuthanahalli Channabasavegowda Vinay. "Prediction of Alzheimer's Disease Using ML." In Proceedings of Third International Conference on Communication, Computing and Electronics Systems, Lecture Notes in Electrical Engineering, vol. 844. Singapore: Springer. https://doi.org/10.1007/978-981-16-8862-1_50.
18. Sivakani, R., and G. A. Ansari. "ML Framework for Implementing Alzheimer's Disease." 2020 International Conference on Communication and Signal Processing (ICCSP) (2020): 588-592. https://doi.org/10.1109/ICCSP48568.2020.9182220.
19. Hosseinzadeh Kasani, Payam, Sara Hosseinzadeh Kasani, Yeshin Kim, Cheol-Heui Yun, Seong Hye Choi, and Jae-Won Jang. 2021 International Conference on Information and Communication Technology Convergence (ICTC). Jeju Island, Republic of Korea, October 2021.
20. Alessia, Sarica, Antonio Cerasa, and Aldo Quattrone. "Random Forest Algorithm for the Classification of Neuroimaging Data in Alzheimer's Disease: A Systematic Review." Frontiers in Aging Neuroscience 9 (2017). https://doi.org/10.3389/fnagi.2017.00329.
21. Rangaswamy, Uday, S. Akila Parvathy Dharshini, Dhanusha Yesudhas, and M. Michael Gromiha. "VEPAD - Predicting the Effect of Variants Associated with Alzheimer's Disease Using ML." Computers in Biology and Medicine 124 (2020): 103933. https://doi.org/10.1016/j.compbiomed.2020.103933.
22. Kishore, P., Ch. Usha Kumari, M.N.V.S.S. Kumar, and T. Pavani. "Detection and Analysis of Alzheimer's Disease Using Various ML Algorithms." Materials Today: Proceedings 45, Part 2 (2021).
23. Khan, N. M., N. Abraham, and M. Hon. "Transfer Learning With Intelligent Training Data Selection for Prediction of Alzheimer's Disease." IEEE Access 7 (2019): 72726-72735. https://doi.org/10.1109/ACCESS.2019.2920448.
24. Liu, J., J. Wang, B. Hu, F.-X. Wu, and Y. Pan. "Alzheimer's Disease Classification Based on Individual Hierarchical Networks Constructed With 3-D Texture Features." IEEE Transactions on NanoBioscience 16, no. 6 (2017): 428-437. https://doi.org/10.1109/TNB.2017.2707139.
25. Huang, M., W. Yang, Q. Feng, et al. "Longitudinal Measurement and Hierarchical Classification Framework for the Prediction of Alzheimer's Disease." Scientific Reports 7 (2017): 39880. https://doi.org/10.1038/srep39880.
26. Austin, J. T., R. A. Yaffee, and D. E. Hinkle. "Logistic Regression for Research in Higher Education." In Higher Education: Handbook of Theory and Research, vol. 8, 379–410. New York: Agathon Press, 1992.
27. Cabrera, A. F. "Logistic Regression Analysis in Higher Education: An Applied Perspective." In Higher Education: Handbook of Theory and Research, vol. 10, 225–256. New York: Agathon Press, 1994.
28. Biau, Gerard. "Analysis of a Random Forests Model." Journal of Machine Learning Research 13 (2012): 1063-1095.
29. Kulkarni, Vrushali Y., and Pradeep K. Sinha. "Effective Learning and Classification using Random Forest Algorithm." International Journal of Engineering and Innovative Technology (IJEIT) 3, no. 11 (2014).
30. Friedman, Jerome H. "Greedy Function Approximation: A Gradient Boosting Machine." Annals of Statistics 29, no. 5 (2001): 1189-1232. https://doi.org/10.1214/aos/1013203451.
31. Natekin, A., and A. Knoll. "Gradient Boosting Machines, a Tutorial." Frontiers in Neurorotics 7 (2013).
32. Yang, F.-J. "An Implementation of Naive Bayes Classifier." 2018 International Conference on Computational Science and Computational Intelligence (CSCI) (2018): 301-306. https://doi.org/10.1109/CSCI46756.2018.00065.
33. Nagarani, V., A. Karpagam, B. Vasuki, and N. Sundarakannan. "Real Life Applications of Bayes Theorem." JAC: A Journal Of Composition Theory XIV, no. II (2022).
34. Puga, J. L., and M. Krzywinski. "Bayes' Theorem." Nature Methods (2015): 277–278. https://doi.org/10.1038/nmeth.3335.
35. Vishwanathan, S. V. M., and M. Narasimha Murty. "SSVM: A Simple SVM Algorithm." In Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02, vol. 3, 2393-2398. Honolulu, HI, USA, 2002. https://doi.org/10.1109/IJCNN.2002.1007516.
36. Pisner, Derek A., and David M. Schnyer. "Support Vector Machine." In Machine Learning, Methods and Applications to Brain Disorders, 101-121. 2020. https://doi.org/10.1016/B978-0-12-815739-8.00006-7.
37. Oasis longitudinal dataset : https://www.kaggle.com/datasets/ninadaithal/imagesoasis

**International Journal of Intelligent Communication and Computer Science**
**Vol. 2, No. 2, 2024, Pages 17-26.**

# Enhancing Security with a Distributed Honeypot System Based on Blockchain: A Mathematical Attack Analysis

**Neharika Nishad[1] and Rahul Singh[2]**

[1]Research Scholar, Department of Computer Science and Engineering, Kanpur Institute of Technology, Affiliated to AKTU, Lucknow
[2]Department of Computer Science and Engineering, Kanpur Institute of Technology, Affiliated to AKTU, Lucknow

**Research Paper**

Email: nehariikanishad1@gmail.com
Received: 14 Mar 2024, Revised: 21 Aug 2024 Accepted: 20 Sep 2024

**Abstract:**

As cyber threats continue to evolve, the need for robust security measures becomes paramount. In this study, we propose a novel approach to enhance cybersecurity through the implementation of a distributed honeypot system built on blockchain technology. This system leverages the inherent security features of blockchain to create a resilient network of honeypots, capable of detecting and deterring malicious activities effectively. We conduct a comprehensive mathematical analysis of potential attacks targeting this distributed honeypot system, providing insights into its resilience and effectiveness against various cyber threats. Our findings underscore the potential of blockchain-based distributed honeypot systems as a proactive defense mechanism in the ever-evolving landscape of cybersecurity threats**.**

**Keywords:** Honeypot, Distributed system, Blockchain

## 1. Introduction

In the contemporary digital landscape, cybersecurity has emerged as a critical concern, with the proliferation of sophisticated cyber threats posing significant challenges to individuals, organizations, and nations alike [1]. As cyber attacks continue to evolve in complexity and scale, there is an urgent need for innovative and robust security solutions to safeguard against potential breaches and intrusions. Among the myriad of cybersecurity approaches, honeypot systems have gained prominence as an effective tool for detecting, monitoring, and mitigating malicious activities [2].

Traditionally, honeypots are decoy systems designed to lure cyber attackers into interacting with simulated vulnerabilities, thereby providing valuable insights into their tactics, techniques, and procedures (TTPs) [3]. However, the effectiveness of conventional honeypots is often limited by their centralized nature, making them susceptible to evasion and detection by sophisticated adversaries. To address these shortcomings, there is a growing interest in the development of distributed honeypot systems that leverage decentralized architectures, such as blockchain technology, to enhance resilience and scalability [4].

Blockchain, originally devised as the underlying technology powering cryptocurrencies like Bitcoin, has garnered widespread attention for its potential applications beyond financial transactions [5]. By employing cryptographic principles and distributed consensus mechanisms, blockchain enables the creation of tamper-proof and transparent ledgers, fostering trust and accountability in decentralized environments. Leveraging

these attributes, researchers have begun exploring the integration of blockchain into cybersecurity frameworks, including distributed honeypot systems, to bolster their security and reliability.
Motivated by the need for innovative cybersecurity solutions, this paper proposes a distributed honeypot system based on blockchain technology. Our approach aims to harness the inherent security features of blockchain to create a resilient network of honeypots capable of detecting and mitigating cyber threats effectively. By distributing the honeypot infrastructure across multiple nodes within a blockchain network, we seek to enhance its robustness against evasion and detection by adversaries.
In this paper, we provide a comprehensive analysis of our proposed distributed honeypot system, focusing on its architecture, functionality, and security implications. Additionally, we conduct a mathematical analysis to evaluate its efficacy in detecting and deterring various cyber attacks, including reconnaissance, infiltration, and exfiltration attempts. Furthermore, we discuss the potential challenges and limitations of our approach and propose avenues for future research and development.

## 2. Honeypot and Blockchain

### 2.1 Honeypot System

In the realm of cybersecurity, honeypots have emerged as a valuable tool for detecting and analyzing malicious activities [6]. Honeypots are decoy systems designed to mimic legitimate assets or services within a network, enticing cyber attackers to interact with them. By monitoring and analyzing the activities directed at these decoy systems, security practitioners can gain valuable insights into the tactics, techniques, and procedures employed by adversaries. Traditional honeypots are typically deployed as standalone entities, often centralized within a network, which can make them susceptible to evasion and detection by sophisticated attackers. However, the evolution of cyber threats has spurred the development of more advanced honeypot architectures, including distributed honeypot systems.

**Notable Papers**

**Li, Yang et. al [7]** This paper presents a game-theoretic analysis of distributed honeypots, focusing on strategic interactions between attackers and defenders in a cybersecurity context. By modeling the interaction as a game, the authors investigate optimal strategies for both attackers attempting to evade detection and defenders seeking to detect and mitigate attacks. The study provides insights into the effectiveness of distributed honeypots in deterring malicious activities and highlights the importance of game theory in understanding and mitigating cyber threats.

**Shi, Leyi et.al [8]** This paper proposes a dynamic distributed honeypot system based on blockchain technology to enhance cybersecurity defenses. The authors leverage blockchain's decentralized and immutable ledger to distribute honeypot instances across a network, enabling real-time updates and adaptability to evolving threats. The study demonstrates the effectiveness of the blockchain-based approach in detecting and mitigating cyber-attacks, highlighting its potential for improving the resilience of honeypot systems.

**H. Arun [9]** This paper introduces Honeymesh, a novel approach for preventing distributed denial of service (DDoS) attacks using virtualized honeypots. The author presents a virtualized honeypot architecture capable of dynamically scaling and adapting to mitigate DDoS attacks effectively. Through extensive experimentation and evaluation, the study demonstrates the efficacy of Honeymesh in thwarting DDoS attacks and protecting network infrastructure from disruptions caused by malicious actors.

**Wang et. al.** [10] This paper proposes a strategic honeypot game model specifically tailored for mitigating distributed denial of service (DDoS) attacks in smart grid environments. The authors analyze the strategic interactions between attackers and defenders within the context of the smart grid infrastructure, considering the unique challenges and requirements of this domain. Through theoretical modeling and simulation studies, the study provides insights into effective defense strategies against DDoS attacks in smart grid deployments.

**Miao and Wang [11]** This paper presents an SDN-enabled pseudo-honeypot strategy for mitigating distributed denial of service (DDoS) attacks in the industrial Internet of Things (IIoT) environment. The authors leverage software-defined networking (SDN) principles to dynamically deploy pseudo-honeypots and divert malicious traffic away from critical IIoT infrastructure. Through experimental validation and analysis, the study demonstrates the effectiveness of the proposed strategy in enhancing the resilience of IIoT systems against DDoS attacks.

**Huang et. al [12]** This paper introduces a distributed cloud honeypot architecture designed to detect and mitigate cyber threats in cloud computing environments. The authors propose a scalable and resilient architecture leveraging distributed cloud resources to deploy and manage honeypot instances. Through experimental evaluation and performance analysis, the study demonstrates the effectiveness of the distributed cloud honeypot architecture in detecting and responding to various types of cyber attacks targeting cloud infrastructure.

### 2.2 Blockchain System

Blockchain technology, originally devised as the backbone of cryptocurrencies like Bitcoin, has expanded its reach beyond finance. At its core, blockchain serves as a decentralized and immutable ledger, recording transactions across a network of nodes transparently and securely. Leveraging cryptographic principles and consensus mechanisms, blockchain ensures data integrity and builds trust in distributed environments. Its security properties, including immutability, transparency, and decentralization, make it attractive for bolstering cybersecurity solutions such as honeypot systems. Incorporating blockchain into cybersecurity strategies enhances resilience against evolving threats. Blockchain's decentralized architecture reduces reliance on single points of failure and centralized control, mitigating risks in distributed ecosystems. The immutability of blockchain records ensures tamper-proof transaction histories, enabling accurate attribution of malicious activities within honeypot systems. Additionally, blockchain's transparency facilitates real-time monitoring and auditing, empowering organizations to detect and respond to security breaches swiftly. Furthermore, blockchain-enabled honeypots offer secure platforms for collaborative threat intelligence sharing. By securely recording and sharing attack data on the blockchain, organizations can enhance their collective defense posture against sophisticated adversaries. This collaborative approach fosters a stronger, more unified response to cyber threats, ultimately contributing to a safer digital landscape.

**Notable Papers**

**Liu et.al [13]** This paper introduces B4SDC, a blockchain-based system designed for secure data collection in Mobile Ad-Hoc Networks (MANETs). The authors propose a novel approach to leverage blockchain technology for securely collecting and storing security-related data in MANETs, addressing the challenges of data integrity, reliability, and privacy. Through experimental evaluation and performance analysis, the study demonstrates the effectiveness of B4SDC in enhancing the security and reliability of data collection in MANETs.

**Sun et.al [14]** This paper presents a blockchain-based IoT access control system designed to enhance security, lightweight, and cross-domain compatibility in IoT environments. The authors propose a novel access control mechanism leveraging blockchain technology to ensure secure and decentralized access management for IoT devices across diverse domains. Through experimental validation and analysis, the study demonstrates the feasibility and effectiveness of the proposed blockchain-based access control system in addressing security challenges in IoT deployments.

**Leng et. al. [15]** This paper provides a comprehensive survey of blockchain security techniques and research directions, focusing on addressing security challenges and vulnerabilities in blockchain systems. The authors present an overview of existing security mechanisms and explore emerging research directions for enhancing the security and resilience of blockchain networks. Through a systematic review of literature, the study offers insights into the current state-of-the-art in blockchain security and identifies future research directions in this rapidly evolving field.

**Berdik et. al. [16]** This paper presents a survey on the use of blockchain technology for information systems management and security. The authors review existing literature and discuss the applications of blockchain in various domains, including data management, authentication, and access control. Through a comprehensive analysis, the study highlights the potential benefits and challenges of integrating blockchain into information systems and offers insights into future research directions in this area.

**Huaqun, and Yu [17]** This paper provides a survey of blockchain technology and its security aspects, covering fundamental concepts, architectures, security mechanisms, and challenges. The authors review existing literature on blockchain security and discuss potential solutions to address security vulnerabilities and threats. Through a systematic analysis, the study offers a comprehensive overview of blockchain technology and its implications for security in various applications and domains.

**Singh et. al. [18]** This paper discusses blockchain security attacks, challenges, and solutions in the context of future distributed Internet of Things (IoT) networks. The authors examine potential security threats and vulnerabilities in blockchain-based IoT deployments and propose solutions to mitigate these risks. Through a comprehensive analysis, the study offers insights into the security implications of blockchain technology for distributed IoT networks and presents strategies to enhance their security posture.

In this paper, we explore the convergence of honeypot technology and blockchain to create a novel approach for bolstering cyber defenses. Our proposed distributed honeypot system leverages blockchain's decentralized architecture to distribute honeypot instances across a network of nodes, thereby enhancing their resilience against evasion and detection by adversaries. Through theoretical analysis and practical insights, we elucidate the potential benefits and challenges of integrating blockchain technology into honeypot-based cybersecurity frameworks.

## 3. Proposed Method

In Figure 1, the network portrayal illustrates the allocation of keys and states to individual nodes, distinguishing between Normal (N) and Honeypot (H) nodes. Each node possesses a unique key and is assigned a state based on its function within the network, either as a standard operational node or as a honeypot intended to entice and monitor malicious activities. This differentiation plays a pivotal role in the network's effective operation by enabling the identification and segregation of honeypot nodes from regular operational nodes.

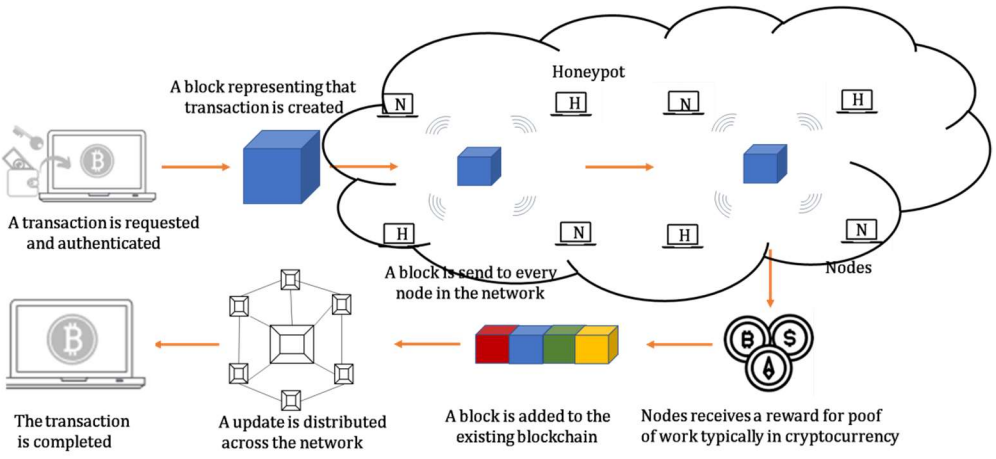


**Figure 1: Schematic of Decentralized Honeypot system based on Blockchain Networks**

During the initial operational phase, a symmetric key technique is employed to encrypt the records of each node within the network. This encryption process defines the cryptographic algorithm utilized to secure the

node records. Symmetric key encryption entails the utilization of a single key for both data encryption and decryption, ensuring that only authorized parties possessing the key can access the encrypted information.
By leveraging symmetric key encryption in the initial phase, the network guarantees the confidentiality and integrity of node records, thereby safeguarding sensitive information against unauthorized access or tampering. This cryptographic technique introduces an additional layer of security to the network, effectively mitigating the risks associated with data breaches and unauthorized disclosures. Furthermore, the adoption of symmetric key encryption facilitates efficient and seamless communication between nodes, thereby enhancing the overall robustness and reliability of the network infrastructure.
In our system architecture, each node, whether classified as a Normal node or a Honeypot node, has the capability to participate in the same blockchain or different blockchains. It is a noteworthy observation that the resilience and security of a blockchain network tend to improve as the number of participating nodes increases. Consequently, in our proposed framework, we incorporate both Normal and Honeypot nodes within the same blockchain network to leverage this inherent property.
By integrating both types of nodes into a unified blockchain network, we aim to enhance the overall robustness and security posture of the system. The inclusion of Honeypot nodes within the blockchain not only contributes to the detection and monitoring of malicious activities but also strengthens the integrity and consensus mechanisms of the blockchain itself. Moreover, the coexistence of Normal and Honeypot nodes within the same blockchain fosters a collaborative environment where both types of nodes contribute to the network's collective resilience against cyber threats.
This approach offers several advantages, including increased transparency, fault tolerance, and immutability, which are fundamental properties of blockchain technology. Additionally, it enables seamless interoperability and communication between Normal and Honeypot nodes, facilitating the exchange of valuable information and insights to enhance cybersecurity defenses. Overall, the integration of both node types within the same blockchain network represents a strategic decision aimed at maximizing the effectiveness and efficiency of our system architecture in combating evolving cyber threats.

### 3.1 Mathematical Modeling for Attack Prediction

Let us assume a intruder start a attack then the likelihood of the intruder achieving success is represented by the probability of

$$s_c(a) = ps_c(a+1) + qs_c(a-1) \quad (1)$$

where $a$ and $c$ are bounded such that $0 \le a \le c$,
In the above given equation, p defines the winning probability, while $q = 1 - p$ is the loosing probability of a person. Due to the fact that equation (1) is a second order linear ordinary differential equation. Hence, initially a solution form $s_c(a) = z^a$ has to be assumed for some unknown base value $z$. Now, on substituting the form into (1), we have:

$$z^a = pz^{a+1} + qz^{a-1} \quad (2)$$

It must be noted here that the value of $z$ should not be equal to 0.As a result, the equation (2) can factor out a common $z^{a-1}$. Now,

$$pz^2 - z + q = 0 \quad (3)$$

So $z = 1$ and $z = \frac{1}{p} - 1 = \frac{q}{p}$. Consequently, the solution of (1) is

$$s_c(a) = C_1(1)^a + C_2\left(\frac{q}{p}\right)^a \quad (4)$$

It begins when the attack transaction becomes part of the blockchain. During this phase, the honest chain extends by $z$ blocks, denoted as $z \in \mathrm{N}$, while the attacker's chain extends by $k$ blocks, where $k \in \mathrm{N}$. Notably, $k$ can range from 0 to positive infinity. If $k$ exceeds $z$, the attack succeeds; otherwise, if $k$ is less than or equal to $z$, the attack fails. However, the scenario remains precarious even if the number of blocks the attacker is behind, denoted as *z*, is less than or equal to the number of blocks *k* mined by the honest network.

In such cases, the attacker still maintains the opportunity to catch up. The process of determining the probability of the attacker eventually catching up from z blocks behind closely resembles a classical problem in probability theory known as the Gambler's Ruin Problem. This parallel leads to the derivation of equation (5) as outlined in reference [19]. This equation encapsulates the likelihood of the attacker successfully overtaking the honest network despite starting from a disadvantaged position *z* blocks behind. By drawing parallels to the Gambler's Ruin Problem, researchers can better understand and model the dynamics of blockchain security in scenarios where attackers seek to overcome the honest network's lead and assert control over the network's consensus mechanism.

$$q_z = \begin{cases} 1 & if\ p \le q \\ \left(\frac{q}{p}\right)^2 & if\ p > q \end{cases} \tag{5}$$

In this given equation, *p* represents the probability of an honest node discovering the next block, while *q* indicates the probability of the attacker finding the next block. Furthermore, $q_z$ denotes the probability of the attacker eventually catching up from bb blocks behind. These parameters play crucial roles in determining the dynamics of blockchain consensus mechanisms, particularly in scenarios where the attacker seeks to overcome a disadvantageous position and assert control over the network. Considering the range of possibilities for $k$ from 0 to positive infinity—there are infinite scenarios where the attack succeeds. Hence, we opt to compute ( $1 - P_{attack\ failure}$ ) instead.

The Poisson distribution serves as a fundamental probability distribution in statistics, particularly in scenarios involving the occurrence of rare events or events happening randomly over time or space. Formally, it expresses the probability of a specified number of events occurring within a fixed interval, under the assumption that these events happen independently and at a constant average rate known as the mean rate. The extension of the honest chain by $z$ blocks represents a $fixed\ time\ interval$ , while each instance of the attacker chain extending by one block constitutes an individual event. Consequently, the probability of each distinct value of $k$ occurring is represented as:

$$P_{every\ different\ k\ appears} = \frac{\lambda^k e^{-\lambda}}{k!} \tag{6}$$

The variable $k$ is the expected value. Let's suppose that the honest chain aims to extend by $z$ blocks with a probability of *p*. In this scenario, the total duration required for the honest chain to extend by $z$ blocks is governed by a Poisson distribution with a mean of $z / p$ . Within this same time frame of $z / p$ , the attacker chain can generate, on average $\lambda = z / p.q = \frac{zq}{p}$ blocks.

If $z$ exceeds *k*, it indicates that the attacker's chain extends more blocks than the honest chain. Consequently, the attack on the chain is deemed successful, resulting in $(1 - P_{attack\ failure})$ being equal to 1.

However, when $z$ is less than or equal to k, the probability that the attacker's chain can still bridge the gap from $z - k$ blocks behind is given by $\left(\frac{z}{p}\right)^{(z-k)}$ , while the probability that the attacker's chain cannot catch up is

$$P_{can't\ catch\ up} = 1 - \left(\frac{q}{p}\right)^{(z-k)} \tag{7}$$

As per (5) and (6), we have

$$P_{every\ different\ k\ attack\ failure} = P_{every\ different\ k\ appears} \cdot P_{can't\ catch\ up}$$

$$= \frac{\lambda^k e^{-\lambda}}{k!} \cdot \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \tag{8}$$

Now,

$$P_{attack\ failure} = \sum_{k=0}^{z} P_{every\ different\ k\ attack\ failure} = \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \tag{9}$$

At last, we have

$$P_{attack\ successful} = 1 - P_{attack\ failure} = \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \tag{10}$$

## 4. Results

The results presented in the Figure 2 show the relationship between the number of nodes in a network and the corresponding attack probability with $q$= 0.1. As the number of nodes increases, the attack probability decreases exponentially. This trend suggests that larger networks with more nodes are significantly more resilient to attacks compared to smaller networks. For instance, when there are only 5 nodes in the network, the attack probability is relatively high at $9.13\times10^{-4}$. However, as the number of nodes increases to 10, the attack probability decreases drastically to $1.24\times10^{-6}$. This pattern continues as the number of nodes further increases, with the attack probability diminishing exponentially. By the time the network reaches 25 nodes, the attack probability is extremely low at $3.3\times10^{-15}$, indicating a highly secure and robust network configuration. These results highlight the importance of network scalability and size in mitigating the risk of attacks. Larger networks offer greater diversity and redundancy, making them inherently more resilient to malicious activities.

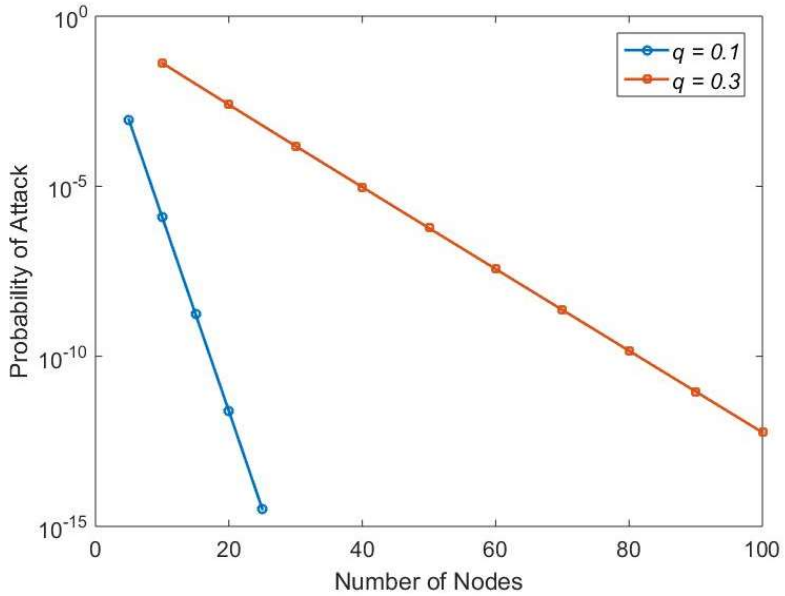


**Figure 2: Probability of attack vs. number of nodes**

The results presented in the Figure 2, demonstrate a clear correlation between the number of nodes in a network and the associated attack probability, assuming a fixed probability of attack at $q$ = 0.3. As the number

of nodes increases, the likelihood of a successful attack decreases exponentially. This inverse relationship underscores the significance of network size and scalability in enhancing security against malicious activities.
For instance, with only 10 nodes in the network, the attack probability is relatively high at 0.042. However, as the network expands to 100 nodes, the attack probability diminishes significantly to $5.81\times10^{-13}$, indicating a highly secure network configuration. This substantial decrease in attack probability highlights the resilience of larger networks, which offer greater diversity and redundancy, thereby making it more challenging for attackers to exploit vulnerabilities.
Furthermore, the exponential decrease in attack probability as the number of nodes increases underscores the importance of network scalability in mitigating security risks. Larger networks not only provide more potential targets for attackers but also distribute the impact of attacks more widely, minimizing the likelihood of successful breaches.
Overall, these results emphasize the critical role of network size and scalability in bolstering cybersecurity defenses. By understanding and leveraging the relationship between network size and attack probability, organizations can design and deploy resilient networks capable of withstanding a wide range of cyber threats.

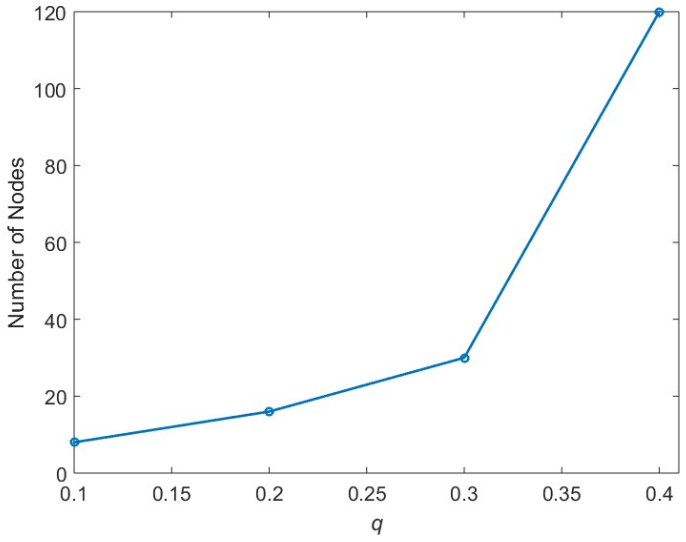


**Figure 3: Number of Nodes vs. Probability of attack**

The Figure 3 presents the relationship between the probability of attack and the corresponding number of nodes required to maintain the attack probability below a threshold of 0.0001. As the probability of attack increases, the number of nodes needed to achieve this threshold also rises, demonstrating the escalating security challenge posed by higher probabilities of attack.
For instance, with a relatively low probability of attack at 0.1, only 8 nodes are needed to ensure that the attack probability remains below 0.0001. However, as the probability of attack doubles to 0.2, the required number of nodes also doubles to 16. This trend continues, with higher probabilities of attack necessitating larger networks to maintain the desired level of security.
At a probability of attack of 0.3, the required number of nodes increases further to 30, indicating the significant impact of higher probabilities on network security requirements. This result underscores the importance of considering not only the likelihood but also the severity of potential attacks when designing and securing network infrastructures.
The exponential increase in the required number of nodes becomes more pronounced as the probability of attack reaches 0.4, where a substantial network size of 120 nodes is needed to maintain the attack probability below the specified threshold. This emphasizes the critical importance of proactive security measures and robust network defenses in mitigating the risks associated with higher probabilities of attack.
In summary, the results highlight the escalating security challenges posed by higher probabilities of attack, underscoring the need for organizations to implement comprehensive cybersecurity strategies and allocate resources accordingly to safeguard against potential threats.

## 5. Conclusion

In conclusion, our study emphasizes the critical importance of robust security measures in addressing the evolving landscape of cyber threats. Through the implementation of a distributed honeypot system built on blockchain technology, we propose a novel approach to enhancing cybersecurity. By leveraging the inherent security features of blockchain, our system creates a resilient network of honeypots capable of effectively detecting and deterring malicious activities.

Our comprehensive mathematical analysis of potential attacks targeting the distributed honeypot system provides valuable insights into its resilience and effectiveness against various cyber threats. The results demonstrate a clear correlation between the number of nodes in the network and the corresponding attack probability, highlighting the importance of network scalability in mitigating security risks. As evidenced by our findings, blockchain-based distributed honeypot systems offer significant potential as proactive defense mechanisms against cyber threats. By integrating blockchain technology into honeypot frameworks, organizations can enhance their cybersecurity posture and mitigate the risks associated with evolving threats.

## References


1. Bécue, Adrien, Isabel Praça, and João Gama. "Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities." *Artificial Intelligence Review* 54, no. 5 (2021): 3849-3886.
2. Tsiknas, Konstantinos, Dimitrios Taketzis, Konstantinos Demertzis, and Charalabos Skianis. "Cyber threats to industrial IoT: a survey on attacks and countermeasures." *IoT* 2, no. 1 (2021): 163-186.
3. Javadpour, Amir, Forough Ja'fari, Tarik Taleb, Mohammad Shojafar, and Chafika Benzaïd. "A Comprehensive Survey on Cyber Deception Techniques to Improve Honeypot Performance." *Computers & Security* (2024): 103792.
4. Franco, Javier, Ahmet Aris, Berk Canberk, and A. Selcuk Uluagac. "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2351-2383.
5. Gorkhali, Anjee, Ling Li, and Asim Shrestha. "Blockchain: A literature review." *Journal of Management Analytics* 7, no. 3 (2020): 321-343.
6. Franco, Javier, Ahmet Aris, Berk Canberk, and A. Selcuk Uluagac. "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2351-2383.
7. Li, Yang, Leyi Shi, and Haijie Feng. "A game-theoretic analysis for distributed honeypots." *Future Internet* 11, no. 3 (2019): 65.
8. Shi, Leyi, Yang Li, Tianxu Liu, Jia Liu, Baoying Shan, and Honglong Chen. "Dynamic distributed honeypot based on blockchain." *IEEE Access* 7 (2019): 72234-72246.
9. Deshpande, Hrishikesh Arun. "Honeymesh: Preventing distributed denial of service attacks using virtualized honeypots." *arXiv preprint arXiv:1508.05002* (2015).
10. Wang, Kun, Miao Du, Sabita Maharjan, and Yanfei Sun. "Strategic honeypot game model for distributed denial of service attacks in the smart grid." *IEEE Transactions on Smart Grid* 8, no. 5 (2017): 2474-2482.
11. Du, Miao, and Kun Wang. "An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of Things." *IEEE Transactions on Industrial Informatics* 16, no. 1 (2019): 648-657.
12. Huang, Jason Xiaojun, Shikun Zhou, Nick Savage, and Weicong Zhang. "A distributed cloud Honeypot architecture." In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp. 1176-1181. IEEE, 2021.
13. Liu, Gao, Huidong Dong, Zheng Yan, Xiaokang Zhou, and Shohei Shimizu. "B4SDC: A blockchain system for security data collection in MANETs." *IEEE transactions on big data* 8, no. 3 (2020): 739-752.
14. Sun, Shuang, Rong Du, Shudong Chen, and Weiwei Li. "Blockchain-based IoT access control system: towards security, lightweight, and cross-domain." *IEEE Access* 9 (2021): 36868-36878.

15. Leng, Jiewu, Man Zhou, J. Leon Zhao, Yongfeng Huang, and Yiyang Bian. "Blockchain security: A survey of techniques and research directions." *IEEE Transactions on Services Computing* 15, no. 4 (2020): 2490-2510.
16. Berdik, David, Safa Otoum, Nikolas Schmidt, Dylan Porter, and Yaser Jararweh. "A survey on blockchain for information systems management and security." *Information Processing & Management* 58, no. 1 (2021): 102397.
17. Guo, Huaqun, and Xingjie Yu. "A survey on blockchain technology and its security." *Blockchain: research and applications* 3, no. 2 (2022): 100067.
18. Singh, Saurabh, ASM Sanwar Hosen, and Byungun Yoon. "Blockchain security attacks, challenges, and solutions for the future distributed iot network." *IEEE Access* 9 (2021): 13938-13959.
19. Moravec, Jiří. "Financial Aspects of Global Payment Systems." (2023).

International Journal of Intelligent Communication and Computer Science
Vol. 2, No. 2, 2024, Pages 27-38.

# Blockchain-Enabled Wireless Sensor Networks: A Paradigm Shift in Security and Data Integrity

**Amit Yadav[1] and Manish Jain[2]**

[1]PSIT College of Higher Education, Kanpur, INDIA
[2]Allenhouse Business School, Kanpur, INDIA

Email: amityadav.mnnit@gmail.com

**Research Paper**

Received: 23 May 2024, Revised: 13 Sep. 2024 Accepted: 22 Sep 2024

**Abstract:**

This paper explores the integration of blockchain technology with wireless sensor networks (WSNs) to enhance security, data integrity, and operational efficiency. WSNs are increasingly deployed in various applications, including smart cities, environmental monitoring, and healthcare, where the security of sensitive data is paramount. Traditional centralized approaches to data management in WSNs pose significant vulnerabilities to attacks and data tampering. By implementing blockchain, a decentralized and immutable ledger, we aim to create a more robust framework for data transmission and storage. This study discusses the potential benefits of blockchain in WSNs, including enhanced trust through transparency, improved fault tolerance, and the facilitation of secure peer-to-peer communication among sensors. We also address the challenges of integrating blockchain with existing WSN architectures, such as energy consumption, scalability, and latency. Through theoretical and simulation analysis this paper highlights innovative solutions and future directions for research, ultimately demonstrating that the fusion of blockchain technology and wireless sensor networks can significantly improve the resilience and functionality of smart systems.

**Keywords:** Blockchain, Wireless Sensor Networks, Data Security, Decentralization, Smart Systems, Data Integrity, Peer-to-Peer Communication, Scalability, Fault Tolerance, IoT Applications.

## 1. Introduction

Wireless Sensor Networks (WSNs) consist of spatially distributed autonomous sensors that monitor physical or environmental conditions [1]. These sensors collect data and transmit it wirelessly to a central processing unit or sink for analysis and decision-making. The inherent advantages of WSNs such as flexibility, ease of deployment, and low installation costs have led to their widespread adoption in various applications, including environmental monitoring, smart cities, healthcare, military surveillance, and industrial automation [2]. Typically, a WSN comprises sensor nodes equipped with sensing, computation, and communication capabilities that collaborate to gather and relay data, often forming a mesh network to enhance reliability and coverage [3]. Despite these benefits, WSNs face significant security challenges due to their unique characteristics. The wireless nature of communication makes them vulnerable to attacks such as eavesdropping, data tampering, and denial-of-service (DoS) attacks [4]. Additionally, the limited computational power and battery resources of sensor nodes constrain the implementation of robust security measures.

Key security issues in WSNs include ensuring data confidentiality to protect sensitive information from unauthorized access and maintaining data integrity to guarantee that information remains accurate and untampered during transmission [5]. Authentication is critical to verify the identities of sensor nodes and prevent unauthorized access, yet the lightweight nature of these nodes complicates the use of traditional

authentication mechanisms [6]. The potential for node compromise poses another risk, as sensor nodes deployed in remote environments can be physically attacked, leading to disruptions in network operations or unauthorized data collection. Furthermore, security protocols often consume additional computational resources, which can drain the limited battery life of sensor nodes, necessitating a balance between security and energy efficiency [7]. Scalability is also a concern, as WSNs may consist of hundreds or thousands of nodes, requiring security solutions that can adapt to changing network sizes and topologies. Lastly, WSNs are particularly susceptible to DoS attacks, which can overwhelm nodes with traffic or target critical components to disrupt service.

This paper presents the concept of integrating blockchain technology into WSNs, exploring how this innovative fusion can enhance data security, reliability, and transparency within these networks. The discussion begins with a comprehensive overview of the proposed system architecture, outlining the roles and interactions of various components involved in the integration process. By delineating the architecture, we aim to clarify how sensor nodes, communication protocols, and blockchain elements can work together to create a cohesive system that addresses existing challenges in WSNs. Additionally, introductory results from preliminary blockchain implementations are presented, showcasing their potential impact on data integrity and accessibility.

## 2. Introduction to WSN and Blockchain

### 2.1 Wireless Sensor Network

The general layout of a WSN consists of several key components that work together to monitor and transmit environmental data effectively [8]. At the top of this architecture is the User Interface, which allows end-users to access and analyze the processed data collected by the network (Figure 1). Users can interact with the system through web applications, mobile apps, or dedicated software, enabling them to make informed decisions based on real-time data.

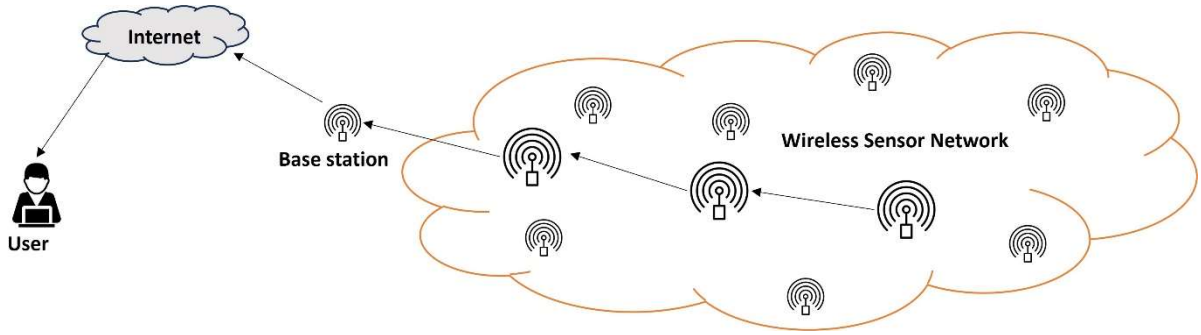


**Figure 1: Schematic of the WSN architecture**

Beneath the user interface lies the Base Station, which serves as a crucial bridge between the sensor nodes and external networks. The base station is responsible for aggregating data from multiple sensor nodes, ensuring efficient data management and transmission. It plays a vital role in coordinating communication within the network and relaying information to users.
Connected to the base station are the Sensor Nodes, the fundamental units of the WSN. Each sensor node is equipped with sensing capabilities to monitor specific environmental conditions, such as temperature, humidity, light, or motion. These nodes generate unique identifiers (Node IDs) to distinguish themselves within the network. The sensor nodes periodically collect data and transmit it to the base station for further processing.
Additionally, the layout includes a Data Processing Center, which provides enhanced computational resources for data analysis and storage. This center can perform advanced analytics, leveraging cloud services or other computing resources to handle large volumes of data generated by the sensor nodes.

Overall, the integration of these components allows for effective monitoring, data collection, and analysis, ensuring that the WSN operates efficiently and meets the needs of its users.

### 2.2 Blockchain System

Applying blockchain technology to traditional wireless sensor networks represents a novel and innovative research approach. One of the key advantages of blockchain technology is its decentralization, which eliminates the reliance on a single server. Traditional sensor networks often require data to be aggregated and processed in a central location, which can be a potential point of failure. By utilizing a blockchain-based approach for data distribution, the risks associated with centralized data repositories are significantly reduced [9]. This research proposes an integration of blockchain technology into the structure of WSNs. The blockchain-based method demonstrated in this study has proven to be reliable and holds the potential to be a groundbreaking technique in the Internet of Things (IoT) domain [10].

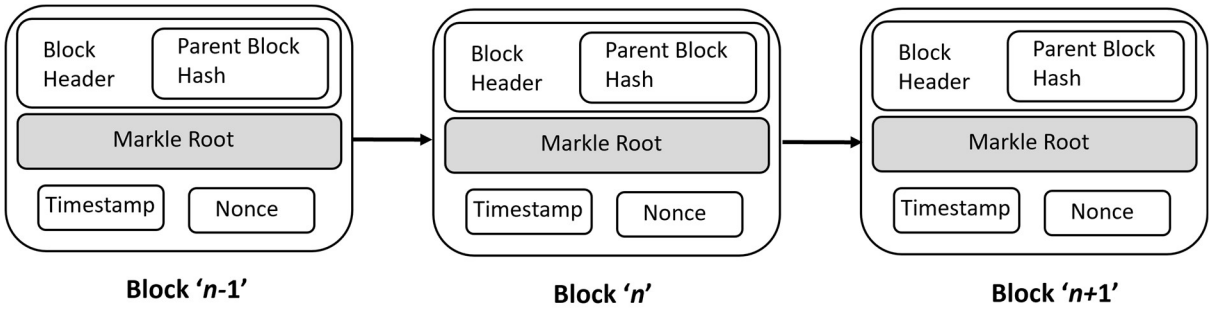


**Figure 2: Schematic of the Block in Blockchain**

This study leverages several key advantages of blockchain technology. The most significant benefit is its decentralized nature, which ensures that transmitted messages are difficult to alter or tamper with. By utilizing distributed ledger technology and decentralized storage, the system eliminates the need for centralized control by a single device or administrative organization. Instead, all nodes in the network share equal rights and responsibilities. The integrity and security of the block data are maintained collectively by the nodes, which also perform encryption functions [11], [12].

Once sensor data is verified and appended to the blockchain in the proposed system, it is stored permanently and securely within the distributed ledger [13]– [15]. A critical vulnerability arises only if a malicious actor gains control of more than 51% of the nodes simultaneously, which could potentially compromise the operation of the blockchain-based system. However, in the absence of such a scenario, altering data on a single node has no impact on the overall system, ensuring that blockchain data remains highly stable and trustworthy. As a result, the sensor data managed by the proposed blockchain-based approach is consistently secure, complete, and accessible at any time and from anywhere. This makes the system resilient to tampering and ensures the integrity of the sensor data in real-time applications [16]– [18].

### 2.3 Challenges in WSN and Blockchain Integration

Integrating blockchain technology into wireless sensor networks (WSNs) offers a promising avenue for enhancing data security, integrity, and transparency. However, this integration is not without its challenges. WSNs, characterized by their numerous, resource-constrained sensor nodes, face unique hurdles when adopting blockchain's decentralized architecture [19]. The details are as below

#### 2.3.1 Scalability

Wireless sensor networks often consist of thousands, or even millions, of nodes. When integrating blockchain, the challenge arises in managing the increased volume of transactions generated by these numerous nodes. Traditional blockchain architectures can struggle to maintain high throughput as more transactions are added,

leading to bottlenecks. Solutions must consider scalability strategies such as sharding or off-chain processing, but these introduce complexity in ensuring data consistency and integrity across the network.

### 2.3.2 Energy Consumption

Energy efficiency is paramount in WSNs due to the limited battery life of sensor nodes. The consensus mechanisms typically used in blockchain, such as Proof of Work or even Proof of Stake, can be energy-intensive, requiring substantial computational resources. Implementing lighter consensus algorithms, such as Practical Byzantine Fault Tolerance or Delegated Proof of Stake, may alleviate some energy demands, but these approaches often come with trade-offs in terms of security and decentralization. Finding a balance that allows for effective blockchain operations without draining node batteries is a critical challenge.

### 2.3.3 Data Privacy

While blockchain provides a transparent and tamper-resistant ledger, the public nature of most blockchain implementations can conflict with the need for data privacy in certain applications. Sensitive information collected by sensors may be exposed on the blockchain, making it vulnerable to unauthorized access. Implementing privacy-preserving technologies, such as zero-knowledge proofs or encryption techniques, is essential but adds complexity to the architecture. Striking a balance between transparency and confidentiality is crucial to ensure that the integration of blockchain does not compromise sensitive data.

### 2.3.4 Latency

The requirement for consensus in blockchain networks can introduce significant latency, which is detrimental in time-sensitive applications typical of WSNs, such as environmental monitoring or industrial automation. Each transaction may require multiple confirmations from various nodes, leading to delays that can impact the system's responsiveness. Exploring solutions such as asynchronous consensus algorithms or hybrid architectures that combine blockchain with traditional centralized approaches may help mitigate latency issues, but they must be carefully designed to maintain the integrity and security of the data.

### 2.3.5 Network Reliability

WSNs are often exposed to environmental factors that can lead to node failures, such as extreme weather conditions or physical obstructions. These failures can disrupt communication and data collection, complicating the reliability of both the WSN and the blockchain. Ensuring that the blockchain can function effectively even when certain nodes are offline or unreachable is essential. Techniques like node redundancy, data replication, and robust recovery protocols must be integrated into the design to maintain a resilient network that can handle real-world conditions.

### 2.3.6 Complexity of Integration

Merging blockchain protocols with existing WSN architectures involves significant technical challenges. WSNs have diverse hardware and software platforms, each with different capabilities and constraints. Integrating blockchain requires careful consideration of how data is collected, transmitted, and recorded on the blockchain. The added complexity may necessitate new middleware solutions, protocols, or APIs to facilitate communication between sensor nodes and the blockchain network. This complexity can lead to increased development time and costs, requiring collaboration among multidisciplinary teams.

### 2.3.7 Interoperability

In a world where multiple blockchain platforms and WSN protocols coexist, ensuring interoperability between different systems is a major challenge. Various blockchains may implement different standards, consensus mechanisms, and data formats, making it difficult for sensor data from one network to be recognized or utilized by another. Developing standardized protocols and APIs that enable seamless interaction between different blockchain and WSN systems is crucial for fostering collaboration and enhancing the overall functionality of integrated solutions.

### 2.3.8 Regulatory Compliance

With the increasing focus on data protection regulations, such as GDPR or CCPA, ensuring compliance when using decentralized, immutable ledgers poses significant challenges. Data stored on a blockchain may be subject to regulations requiring the ability to delete or anonymize personal data, which conflicts with the

inherent characteristics of blockchain technology. Organizations must navigate these regulatory landscapes by implementing data management strategies that respect legal requirements while still leveraging the benefits of blockchain, potentially involving hybrid solutions that store sensitive data off-chain.

### 2.3.9 Limited Processing Power

Many sensor nodes in WSNs are designed for low power and low-cost operation, which often limits their processing capabilities. These constraints can make it challenging to implement complex blockchain functionalities, such as executing smart contracts or maintaining a full node. To address this, lightweight blockchain protocols and specialized hardware designs must be explored. This could involve offloading certain computational tasks to more powerful edge devices or using simpler consensus algorithms that require less processing power, thereby enabling effective blockchain integration without overwhelming the sensor nodes.

### 2.3.10 Consensus Mechanism Selection

Choosing the right consensus mechanism for blockchain integration in WSNs is crucial to achieving a balance between security, efficiency, and resource consumption. Traditional mechanisms like Proof of Work may provide high security but are not suitable for resource-constrained environments. Alternative mechanisms such as Proof of Authority, which relies on a limited number of trusted nodes, or federated consensus approaches can offer more efficiency but may sacrifice some degree of decentralization. Carefully evaluating the trade-offs of various consensus mechanisms in the context of specific applications is necessary to ensure optimal performance and security in integrated systems.

## 3. Proposed Method

The architecture of a WSN is designed to facilitate efficient data collection, aggregation, and transmission through a collaborative framework of nodes as shown in Figure 3. At the core of this architecture are normal nodes, also known as sensor nodes, which serve as the fundamental building blocks of the network. These nodes are equipped with sensors to monitor various parameters. They continuously sample their surroundings, gathering relevant data that may require preliminary processing to filter out noise and anomalies. Once this initial processing is complete, normal nodes communicate their findings to aggregator nodes using wireless protocols like Zigbee or LoRa, enabling efficient transmission over short to medium distances.

Aggregator nodes play a critical role as intermediaries between normal nodes and the base station. Their primary function is to collect, process, and consolidate data from multiple normal nodes before forwarding the aggregated information to the base station for further analysis or storage. By applying aggregation techniques such as averaging or summation, aggregator nodes reduce data redundancy and minimize transmission costs, conserving bandwidth and energy in the process. After aggregation, these nodes transmit the processed data to the base station, which serves as the central hub for the WSN.

At the base station, the aggregated data undergoes further analysis using statistical methods or machine learning algorithms to extract meaningful insights or detect anomalies. This centralized processing capability allows for generating reports, visualizations, and alerts based on the analyzed data, which can be crucial for decision-making. Additionally, the base station coordinates network operations, sending commands back to normal nodes for reconfiguration or data retrieval as conditions change. Overall, the communication flow in a WSN involves normal nodes collecting data, sending it to aggregator nodes for processing, and ultimately forwarding the aggregated information to the base station. This layered approach not only optimizes resource use and conserves energy but also enhances the overall effectiveness of the network, supporting a wide range of applications from environmental monitoring to smart city initiatives.

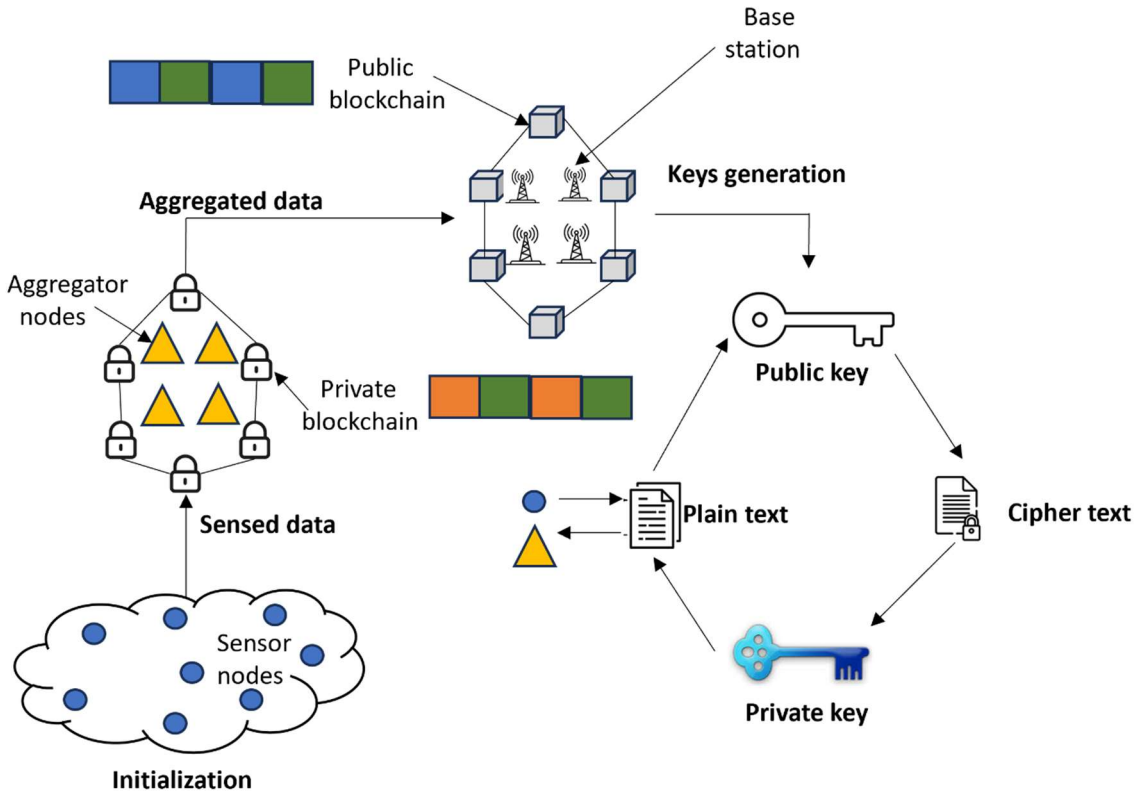


**Figure 3: Schematic of the Blockchain enabled WSN**

Private blockchains are ideal for normal nodes in a WSN because they ensure secure data management and privacy. Each normal node, such as an individual sensor, can operate within a private blockchain that restricts access to authorized participants only. This setup allows for confidential communication between nodes, protecting sensitive data from unauthorized access. The consensus mechanism can be streamlined for efficiency, enabling faster transaction validations crucial for real-time data processing in sensor networks. Additionally, private blockchains can be tailored to meet the specific needs of the WSN, optimizing resource usage, which is vital for battery-operated sensors. By maintaining data integrity and enhancing communication security, private blockchains significantly improve the operational reliability of normal nodes.

In contrast, public blockchains serve an important role for aggregator nodes in WSNs, offering transparency and broad accessibility. Aggregator nodes collect data from multiple normal nodes and publish aggregated information on a public blockchain, ensuring that this data is available to all stakeholders, including researchers and the general public. The transparency inherent in public blockchains fosters trust, as anyone can verify the data's authenticity and source. Furthermore, the decentralized nature of public blockchains eliminates single points of failure, enhancing data resilience against manipulation. By utilizing public blockchains, aggregator nodes can also implement incentive mechanisms, encouraging participation from users and data providers alike, thus enhancing collaboration and the overall value of the data collected within the network.

In blockchain technology, key generation is a fundamental process that establishes secure user interactions through a pair of cryptographic keys: a public key and a private key. The generation typically begins with the creation of a private key, which is a randomly selected number generated using a secure random number generator. This private key must be kept secret, as it is crucial for signing transactions and proving ownership of assets within the blockchain. Once the private key is established, the corresponding public key is derived using a mathematical function, specifically elliptic curve multiplication in the case of Elliptic Curve Cryptography (ECC), which is commonly employed in many blockchain systems. The public key, which can be freely shared, serves as an address to which others can send transactions or assets.

In operation, when a user wants to initiate a transaction, they utilize their private key to sign the transaction data, which creates a unique digital signature. This signature not only verifies the authenticity of the transaction but also ensures that it has not been tampered with. The public key allows others to verify this signature, confirming that it was generated by the corresponding private key without revealing the private key itself. This asymmetric encryption mechanism provides a robust level of security, making it computationally infeasible for anyone to derive the private key from the public key. By employing this system of key generation and management, blockchains enable secure, transparent, and decentralized transactions, empowering users to maintain control over their assets while ensuring the integrity of the entire network.

## 4. RSA and ECC Keys description

**RSA**

RSA is one of the first public-key cryptosystems and is widely used for secure data transmission [20]. Its security is based on the difficulty of factoring the product of two large prime numbers.

**Key Generation**

1. Select two distinct large prime numbers p and q.
2. Compute: n=p×q
   This n is used as the modulus for both the public and private keys.
3. Calculate Euler's Totient: $\phi(n) = (p-1)(q-1)$
4. Choose Public Exponent e: Select an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$
   Common choices for e include 3, 17, or 65537.
5. Compute Private Exponent d: Calculate d as the modular multiplicative inverse of $e$ modulo $\phi(n)$
   $d = e^{-1} \bmod(\phi(n))$
6. The public key is (e,n), and the private key is (d,n).

**Encryption**

To encrypt a message M (where M<n):

$C = M^e \bmod(n)$

Here, C is the ciphertext.

**Decryption**

To decrypt the ciphertext C:

$M = C^d \bmod(n)$

This retrieves the original message M.

**ECC**

ECC is a public-key cryptosystem based on the mathematics of elliptic curves over finite fields [20]. It offers similar security to RSA but with smaller key sizes, making it more efficient.

**Key Generation**

1. Choose an Elliptic Curve: Define an elliptic curve E over a finite field Fp. The curve is usually expressed in the form:
   $y^2 = x^3 + ax + b$
2. Choose a point G on the curve, which serves as the generator point.
3. Choose a random integer d (the private key) in the range [1,n−1], where n is the order of the point G.
4. Calculate the public key Q by multiplying the base point G by the private key d:
   Q=dG

**Encryption**

1. Select a random integer k.
2. Calculate the points $P_1$ and $P_2$:

   $P_1 = k.G$ (shared point)

   $P_2 = k.Q$ (shared secret)
3. Derive a symmetric key from $P_2$
4. Use the symmetric key to encrypt the plaintext message M into ciphertext C.

**Decryption**

1. The receiver computes the shared secret using their private key d:

   $P_2 = k.Q$

   where *k* is the same random integer used during encryption.
2. Use the symmetric key derived from the shared secret to decrypt the ciphertext C back into the plaintext message M.

## 5. Results

The Table 1, presents a comparison between ECC and RSA in terms of key lengths, time for key generation, and time for signature verification. For ECC, the key lengths start at 163 bits, requiring 0.08 seconds for key generation and 0.23 seconds for signature verification. As the key length increases to 233 bits, the key generation time rises to 0.18 seconds and signature verification time to 0.51 seconds. With a key length of 283 bits, these times increase further to 0.27 seconds and 0.86 seconds, respectively. At 409 bits, the key generation time reaches 0.64 seconds, while signature verification takes 1.8 seconds. The largest ECC key length listed is 571 bits, with key generation taking 1.44 seconds and signature verification requiring 4.53 seconds.

**Table 1: Comparison of RSA and ECC Keys**

| ECC | | | RSA | | |
|---|---|---|---|---|---|
| **Key Length** | **Time (Key Generation)** | **Time (Signature Verification)** | **Key Length** | **Time (Key Generation)** | **Time (Signature Verification)** |
| 163 | 0.08 | 0.23 | 1024 | 0.16 | 0.01 |
| 233 | 0.18 | 0.51 | 2240 | 7.74 | 0.01 |
| 283 | 0.27 | 0.86 | 3072 | 9.80 | 0.01 |
| 409 | 0.64 | 1.8 | 7680 | 113.90 | 0.01 |
| 571 | 1.44 | 4.53 | 15,360 | 679.06 | 0.03 |

In comparison, RSA starts with a key length of 1024 bits, which has a key generation time of 0.16 seconds and a very quick signature verification time of 0.01 seconds. As RSA key lengths increase to 2048 bits, the key generation time significantly rises to 0.62 seconds, but signature verification remains low at 0.02 seconds. At 2240 bits, the key generation time jumps to 7.74 seconds, while verification time remains constant at 0.01 seconds. For a 3072-bit key, the generation time is 9.80 seconds, with signature verification still at 0.01 seconds. At the highest RSA key length of 15,360 bits, key generation takes a substantial 679.06 seconds, while signature verification takes slightly longer at 0.03 seconds. Overall, the data illustrates that while ECC offers shorter key lengths with competitive performance, RSA requires longer keys and considerably more time for key generation as the key length increases.

The block structure of the blockchain is illustrated in Figure 4, providing a clear representation of the key components that comprise each block within the chain. Each block contains several essential elements, starting with index numbers, which serve as unique identifiers for the blocks, allowing for easy reference and retrieval.

Following this, the data section holds the actual information recorded in the block, which, in the context of a WSN, include sensor readings, timestamps, and other relevant metadata.
Another critical component is the previous hash, which links each block to its predecessor, thereby ensuring the integrity and chronological order of the blockchain. This cryptographic hash not only confirms the identity of the previous block but also protects against tampering; any alteration in the data of a prior block would change its hash, invalidating all subsequent blocks. The current hash is generated from the block's content, including the previous hash, and serves as a digital fingerprint for that block, reinforcing its authenticity.
Additionally, the block structure includes a nonce, a number used in the mining process to help achieve the proof-of-work consensus. The nonce is essential for validating the block, as it must satisfy specific cryptographic requirements, adding a layer of security to the blockchain. Together, these components form a robust structure that not only enhances security but also supports the transparency and traceability of data within the network, making the blockchain a powerful tool for managing information in wireless sensor networks.

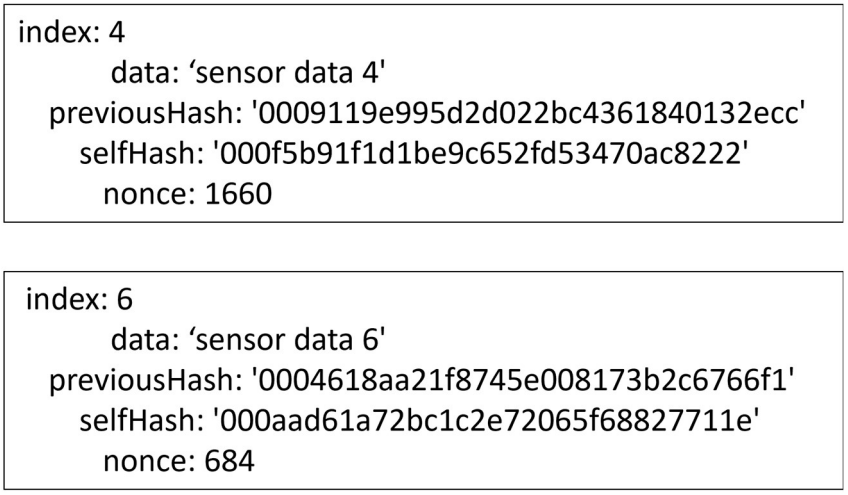


**Figure 4: Schematic of the Blocks in Blockchain**

Figure 5 illustrates the relationship between the number of mined blocks and time, providing a visual representation of the mining activity within the blockchain network. The x-axis represents time, measured in specific intervals, while the y-axis denotes the cumulative number of blocks successfully mined during those intervals. As depicted in the figure, the graph shows a generally upward trend, indicating that as time progresses, an increasing number of blocks are being mined. This trend is expected in a well-functioning blockchain environment, where miners continuously participate in the mining process, competing to solve cryptographic puzzles and validate transactions. Several key observations can be made from the graph. Initially, there may be a slower rate of block generation, particularly if the network is newly established or if the difficulty level for mining is set high. Over time, as more miners join the network and become familiar with the mining process, the rate of block creation tends to increase. This increase may also correlate with adjustments in mining difficulty, which can be dynamically modified based on the total computational power of the network, ensuring that blocks are generated at a consistent rate.

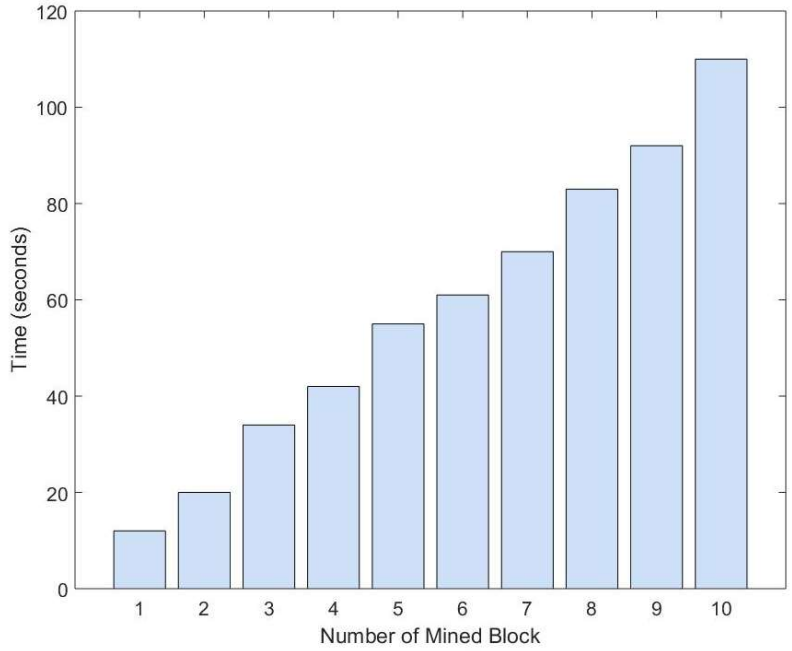


**Figure 5: Number of Mined Block vs. Time (Seconds)**

Figure 6 presents the relationship between the number of transactions per block and time, with specific parameters indicating that the number of peer-to-peer (P2P) nodes is set at 10 and a total of 30 blocks have been mined.

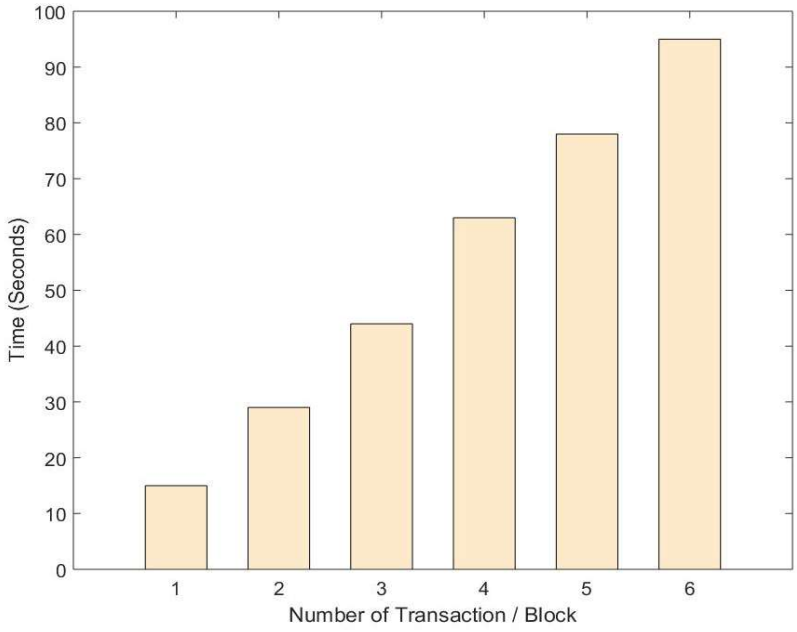


**Figure 6: Number of transaction/Block vs. Time (Seconds)**

The x-axis of the figure represents time intervals, while the y-axis indicates the number of transactions included in each mined block. As shown, the graph illustrates the variation in the number of transactions that are packed into each block over time.

Initially, the number of transactions per block may be low, reflecting the early stages of mining when the network is still establishing itself. As the blockchain evolves and more transactions are generated by users interacting with the network, the number of transactions per block is expected to increase. The presence of 10 active P2P nodes facilitates this process, as these nodes collaboratively contribute to transaction generation and block formation.

Throughout the timeline depicted in the figure, there may be noticeable fluctuations in the number of transactions per block due to varying user activity. For instance, periods of high activity, such as during promotional events or market spikes, may lead to a significant increase in the number of transactions being processed. Conversely, during quieter periods, the number of transactions per block may decrease, reflecting reduced user engagement.

With a total of 30 mined blocks, the data suggests a growing trend in transaction inclusion as the network matures. This growth not only enhances the efficiency of the blockchain but also demonstrates its capacity to handle increased transaction loads over time. The effective management of transactions per block is crucial for maintaining network performance and ensuring timely validation of transactions.

## 6. Conclusion

In conclusion, this paper highlights the transformative potential of integrating blockchain technology with WSNs to enhance security, data integrity, and operational efficiency across various applications, including smart cities, environmental monitoring, and healthcare. By addressing the vulnerabilities inherent in traditional centralized data management systems, the proposed decentralized and immutable blockchain framework offers significant improvements in data protection against tampering and unauthorized access. The study elucidates the numerous benefits of this integration, such as increased transparency, enhanced trust, improved fault tolerance, and secure peer-to-peer communication among sensors. While we acknowledge the challenges related to energy consumption, scalability, and latency, our theoretical and simulation analyses provide innovative solutions and outline promising future research directions. Ultimately, this work demonstrates that the fusion of blockchain and WSNs not only enhances the resilience of smart systems but also lays the groundwork for more secure and efficient data management in an increasingly interconnected world.

## References


1. Prabhu, Boselin, N. Balakumar, and A. Antony. "Wireless sensor network based smart environment applications." *Wireless Sensor Network Based Smart Environment Applications (January 31, 2017). IJIRT* 3, no. 8 (2017).
2. Fahmy, Hossam Mahmoud Ahmad. "WSNs applications." In *Concepts, applications, experimentation and analysis of wireless sensor networks*, pp. 67-242. Cham: Springer Nature Switzerland, 2023.
3. Nurlan, Zhanserik, Tamara Zhukabayeva, Mohamed Othman, Aigul Adamova, and Nurkhat Zhakiyev. "Wireless sensor network as a mesh: Vision and challenges." *IEEE Access* 10 (2021): 46-67.
4. Singh, Rahul Sourav, Ajay Prasad, Roselina Maria Moven, and Hiren Kumar Deva Sarma. "Denial of service attack in wireless data network: A survey." In *2017 Devices for Integrated Circuit (DevIC)*, pp. 354-359. IEEE, 2017.
5. Alotaibi, Bandar. "Utilizing blockchain to overcome cyber security concerns in the internet of things: A review." *IEEE Sensors Journal* 19, no. 23 (2019): 10953-10971.
6. Rao, Patruni Muralidhara, and Bakkiam David Deebak. "A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions." *Ad Hoc Networks* 146 (2023): 103159.
7. Alghamdi, Abdullah, Ali M. Al Shahrani, Sultan Sughair AlYami, Ihtiram Raza Khan, PSG Aruna Sri, Papiya Dutta, Ali Rizwan, and Prashanth Venkatareddy. "Security and energy efficient cyber-physical systems using predictive modeling approaches in wireless sensor network." *Wireless Networks* 30, no. 6 (2024): 5851-5866.

8. Raghavendra, Cauligi S., Krishna M. Sivalingam, and Taieb Znati, eds. *Wireless sensor networks*. Springer, 2006.
9. Feng, Qi, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. "A survey on privacy protection in blockchain system." *Journal of network and computer applications* 126 (2019): 45-58.
10. Nofer, Michael, Peter Gomber, Oliver Hinz, and Dirk Schiereck. "Blockchain." *Business & information systems engineering* 59 (2017): 183-187.
11. Hassan, Muneeb Ul, Mubashir Husain Rehmani, and Jinjun Chen. "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions." *Future Generation Computer Systems* 97 (2019): 512-529.
12. Truong, Hien Thi Thu, Miguel Almeida, Ghassan Karame, and Claudio Soriente. "Towards secure and decentralized sharing of IoT data." In *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 176-183. IEEE, 2019.
13. Moin, Sana, Ahmad Karim, Zanab Safdar, Kalsoom Safdar, Ejaz Ahmed, and Muhammad Imran. "Securing IoTs in distributed blockchain: Analysis, requirements and open issues." *Future Generation Computer Systems* 100 (2019): 325-343.
14. Hsiao, Sung-Jung, and Wen-Tsai Sung. "Employing blockchain technology to strengthen security of wireless sensor networks." *IEEE Access* 9 (2021): 72326-72341.
15. Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, Alireza Jolfaei, and AKM Najmul Islam. "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system." *Journal of Parallel and Distributed Computing* 172 (2023): 69-83.
16. Machado, Caciano, and Antônio Augusto Medeiros Fröhlich. "IoT data integrity verification for cyber-physical systems using blockchain." In *2018 IEEE 21st international symposium on real-time distributed computing (ISORC)*, pp. 83-90. IEEE, 2018.
17. Abosata, Nasr, Saba Al-Rubaye, Gokhan Inalhan, and Christos Emmanouilidis. "Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications." *Sensors* 21, no. 11 (2021): 3654.
18. Liang, Xueping, Juan Zhao, Sachin Shetty, and Danyi Li. "Towards data assurance and resilience in IoT using blockchain." In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, pp. 261-266. IEEE, 2017.
19. Ismail, Shereen, Diana W. Dawoud, and Hassan Reza. "Securing wireless sensor networks using machine learning and blockchain: A review." *Future Internet* 15, no. 6 (2023): 200.
20. Ma, Mingxuan. "Comparison between RSA and ECC." In *2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*, pp. 642-645. IEEE, 2021.

**International Journal of Intelligent Communication and Computer Science**
**Vol. 2, No. 2, 2024, Pages 39-56.**

# Integrating Visible Light Communication into Vehicle-to-Vehicle Systems: A Detailed Overview

**Avanish Kumar Dixit[1] and Rohitashwa Pandey[2]**

[1]Research Scholar, Department of Computer Science and Engineering, Bansal Institute of Engineering and Technology, Lucknow, Affiliated to AKTU, Lucknow
[2]Department of Computer Science and Engineering Bansal Institute of Engineering and Technology, Lucknow,, Affiliated to AKTU, Lucknow

**Review Paper**

Email: avanishkumar15@gmail.com
Received: 24 Apr 2024, Revised: 17 Sep. 2024 Accepted: 11 Oct 2024

**Abstract:**

Vehicle-to-Vehicle (V2V) communication is a cornerstone technology for achieving safer, more efficient transportation systems, particularly in the context of autonomous and semi-autonomous vehicles. Traditional V2V communication systems predominantly rely on radio frequency (RF) technologies like Dedicated Short-Range Communications (DSRC) and cellular networks. However, these systems face challenges such as interference, congestion, and limited bandwidth. Visible Light Communication (VLC), leveraging the visible spectrum of light, has emerged as a promising alternative due to its high bandwidth, secure communication, and minimal interference. This review paper explores the potential of VLC for V2V communication, covering the technical aspects, challenges, applications, and future directions.

**Keywords:** Vehicle-to-Vehicle Communication, Visible Light Communication, V2V, Autonomous Vehicles, Communication Systems, Safety, Traffic Management

## 1. Introduction

V2V communication is a transformative technology that enables direct, wireless communication between vehicles, facilitating the exchange of real-time data to enhance road safety, optimize traffic flow, and support the development of autonomous driving systems (Figure 1) [1]. By enabling vehicles to share information about their location, speed, direction, and other critical data points, V2V communication allows for a more cooperative driving environment, where vehicles can anticipate and respond to each other's actions [2]. This seamless exchange of information not only enhances the situational awareness of drivers but also helps in preventing accidents, reducing congestion, and improving overall traffic efficiency. As the automotive industry moves toward increased automation and the realization of fully autonomous vehicles (AVs) [3], V2V communication becomes an essential component of a connected transportation ecosystem. It acts as the backbone for advanced driver-assistance systems (ADAS) [4], autonomous vehicle coordination, and smart traffic management, fostering a more intelligent, safer, and sustainable future of transportation. However, the implementation of V2V communication faces significant challenges, such as limited communication range, data security concerns, and the need for real-time, high-bandwidth exchanges in dynamic driving conditions. This paper explores one promising solution to address these challenges, Visible Light Communication (VLC) [5] as

an alternative to traditional radio frequency (RF)-based systems [6], outlining its potential advantages, challenges, and future role in the evolution of V2V communication systems.

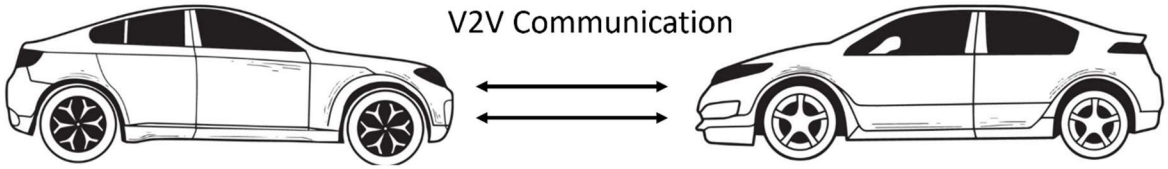


**Figure 1: Schematic diagram for V2V communication**

The key aspects of the V2V communications are:

## Cooperative Driving

Cooperative driving, enabled by V2V communication, represents a significant leap forward in creating a more synchronized and efficient transportation environment [7]. Through V2V communication, vehicles can share vital data with one another in real-time, such as their speed, direction, position, and even the status of their brakes or turn signals. This exchange of information allows vehicles to "talk" to each other, creating a dynamic network where driving decisions are informed by the actions of surrounding vehicles. In environments where multiple vehicles interact, such as intersections, highways, or urban roads, this coordination becomes especially crucial. For instance, V2V communication can enable vehicles to adjust their speed to maintain safe distances, facilitate smoother lane changes, and even prevent accidents in situations where drivers might not have full visibility of other vehicles, such as around blind corners or in dense traffic [8]. On highways, cooperative driving can also support platooning, where vehicles travel in tight formation, reducing drag and improving fuel efficiency. In urban environments, cooperative driving can help optimize traffic flow, reduce congestion, and enhance pedestrian safety [9]. Ultimately, the synergy between vehicles created by V2V communication is fundamental to transforming traditional, reactive driving into a proactive, cooperative driving system that prioritizes safety, efficiency, and coordination.

## Collision Avoidance

By sharing real-time data on their location, speed, and trajectory, vehicles equipped with V2V communication can effectively anticipate and avoid potential collisions, significantly reducing accidents and fatalities [10]. This constant flow of information allows vehicles to "see" beyond their immediate surroundings, enhancing their situational awareness. For instance, when a vehicle detects sudden braking or an unexpected stop ahead, it can immediately transmit this information to following vehicles, alerting them to reduce speed or take evasive action. This early warning system helps prevent rear-end collisions, which are one of the most common types of accidents [11]. Additionally, V2V communication enables vehicles to predict the actions of other road users. For example, a vehicle approaching an intersection can communicate with others in the vicinity, allowing it to anticipate whether another vehicle might run a red light or fail to yield. This predictive capability extends to autonomous vehicles (AVs) as well, allowing them to make real-time decisions based on the behaviour of other road users, further enhancing overall road safety [12]. By integrating real-time data into driving decisions, V2V communication transforms traditional reactionary driving into a proactive safety system, effectively reducing accidents, improving traffic flow, and saving lives.

## Improved Traffic Flow

V2V communication can significantly enhance the flow of traffic by enabling vehicles to coordinate their actions in real time, creating a more streamlined and efficient transportation system [13] (Figure 2). One of the primary ways V2V systems optimize traffic flow is by coordinating speeds and lane changes. Vehicles can adjust their speed to match the flow of traffic, ensuring smoother transitions between different road sections, reducing

sudden braking, and preventing traffic bottlenecks [14]. For example, if a traffic jam or congestion is detected ahead, vehicles can communicate this to others, allowing them to adjust their speed or take alternate routes, avoiding the buildup of traffic and reducing congestion.

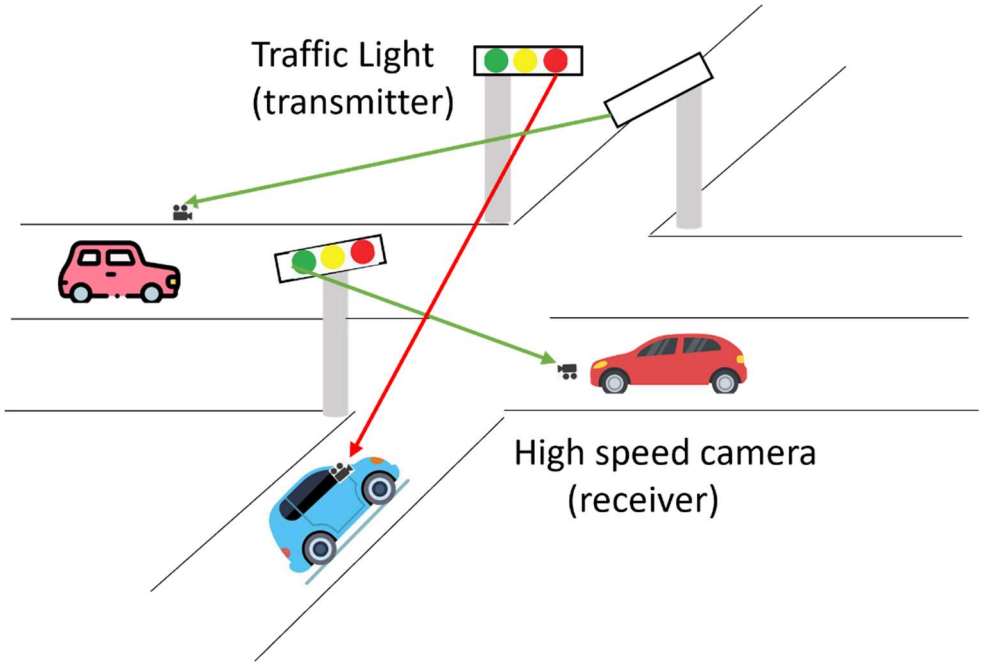


**Figure 2: Schematic diagram for traffic control using V2V communication**

Another major benefit of V2V communication is the ability for vehicles to operate in platoons—groups of vehicles that travel in close formation. This concept, known as platooning, is especially effective on highways and can reduce the amount of space between vehicles without compromising safety. In a platoon, vehicles are controlled through V2V systems that allow them to synchronize their movements, maintaining optimal distances between one another. This formation reduces air resistance (drag) for the entire group, leading to improved fuel efficiency and lower emissions, while also increasing road capacity by reducing the space traditionally required between vehicles.

Furthermore, by smoothing the transitions during lane merges, ensuring optimal spacing on the road, and adapting to real-time traffic conditions, V2V communication helps to minimize stop-and-go driving and traffic jams, contributing to a more fluid traffic flow [15]. This not only reduces overall congestion but also improves fuel consumption and environmental impact, as vehicles operating in more coordinated and efficient patterns burn less fuel and produce fewer emissions. Ultimately, V2V systems hold the potential to transform transportation networks into more intelligent, responsive, and sustainable systems, where vehicles and infrastructure work together to enhance the overall driving experience.

## Autonomous Vehicle Support

In the context of AVs, V2V communication becomes even more critical, as it enables AVs to share essential information with other vehicles in real time, empowering them to make split-second decisions without human intervention [16]. Unlike human drivers, autonomous vehicles rely on a combination of sensors, algorithms, and external communication systems like V2V to navigate the road safely and efficiently. V2V allows AVs to exchange critical data such as their position, speed, trajectory, and the status of their sensors, which are essential for maintaining situational awareness.

For instance, if an AV detects an obstacle in its path or an unexpected traffic condition ahead, it can share this information with nearby vehicles, which can then adjust their behaviour accordingly. This collaborative awareness is particularly important for AVs, as they may not always have the same level of environmental perception as a human driver [17]. Through V2V, AVs can "see" around corners, beyond obstacles, or through

blind spots, allowing them to anticipate the actions of other road users and make pre-emptive decisions to avoid potential collisions. For example, if one AV detects sudden braking or an emergency stop in traffic, it can quickly notify following vehicles, enabling them to decelerate in time and prevent a chain reaction crash. Furthermore, V2V communication enhances the ability of AVs to merge, turn, and interact with other vehicles more smoothly and safely. By knowing the intent and movement of surrounding vehicles, autonomous vehicles can make more informed decisions about when to change lanes or navigate complex driving situations like intersections or roundabouts [18]. This communication helps eliminate the uncertainties that typically arise in traffic scenarios, particularly in environments with complex or unpredictable human driver behaviour.

## 2. Traditional RF-Based V2V Communication

RF communication systems have long been the cornerstone of V2V communication technologies. These systems utilize electromagnetic waves in the radio frequency spectrum to transmit and receive data, facilitating communication between vehicles over both short and long distances [19]. RF-based V2V communication is integral to enabling a wide range of safety, efficiency, and connectivity applications, allowing vehicles to share critical information such as location, speed, and direction. Over the years, several RF-based technologies have emerged as key enablers of V2V communication. Some of the most widely adopted RF technologies for V2V systems include:

### 2.1 Dedicated Short-Range Communications (DSRC)

DSRC is a widely recognized standard for V2V and Vehicle-to-Infrastructure (V2I) communication, originally designed for the intelligent transportation systems (ITS) market [20]. It operates in the 5.9 GHz band and provides low-latency, secure communication over short distances (typically up to 1,000 meters). DSRC is used for various safety applications, such as collision avoidance, intersection management, and emergency vehicle alerts.

**Limitations:**

**Limited Bandwidth:** The 5.9 GHz spectrum allocated for DSRC is limited in bandwidth, which can cause congestion when a large number of vehicles are on the road, especially in high-density urban areas.

**Vulnerability to Interference:** Since the DSRC spectrum is shared with other wireless technologies, it is susceptible to interference from devices like Wi-Fi routers, mobile phones, and other RF-based systems. This can degrade the performance of V2V communication.

### 2.2 5G Communication

The advent of 5G technology marks a significant leap forward in the development of V2V communication systems, offering capabilities that go beyond what current communication technologies (such as 4G and Wi-Fi) can provide. 5G offers a high-speed, high-bandwidth network with the capacity to support massive numbers of connected devices, all while ensuring ultra-low latency a critical feature for real-time communication in dynamic environments like roadways [21]. With latency as low as under 1 millisecond (ms), 5G has the potential to fundamentally transform how vehicles communicate with each other and with surrounding infrastructure.

**Limitations:**

**Network Dependency:** 5G communication is network-based, meaning vehicles rely on cellular towers or base stations for communication. In rural or sparsely populated areas, the signal coverage may be insufficient for reliable communication.

**Congestion and Latency:** While 5G offers high bandwidth and low latency, network congestion—particularly in highly dense urban areas—can still cause delays or dropped connections, reducing the effectiveness of V2V communication in critical situations.

**Security Risks:** 5G relies on a centralized infrastructure, which makes it vulnerable to cyberattacks, hacking, or data breaches. These risks are particularly concerning for safety-critical applications like autonomous driving.

### 2.3 Wi-Fi (IEEE 802.11p)

Wi-Fi-based communication, specifically the IEEE 802.11p standard, is another key technology used in vehicular networks for short-range communication [22]. Similar to DSRC, IEEE 802.11p operates in the 5 GHz frequency band and provides a solution for vehicles to exchange data in real-time over short distances, typically within a range of a few hundred meters. While it shares some characteristics with DSRC in terms of data rates and range, IEEE 802.11p is generally considered a more flexible and lower-cost alternative, particularly suitable for non-safety-critical applications.

**Limitations:**

**Interference and Range:** Like DSRC, Wi-Fi systems are susceptible to interference from other RF devices. Additionally, its communication range is typically limited to a few hundred meters, which is insufficient for many real-time safety applications, especially in high-speed scenarios.

**Limited Channel Capacity:** Wi-Fi can become congested when many vehicles are transmitting simultaneously, leading to delays or data loss.

## 3. Drawbacks of RF-Based V2V Communication

While RF-based technologies such as DSRC, 5G, and Wi-Fi have proven to be effective in enabling V2V communication and have shown promise for a variety of applications, they each face several significant limitations that can hinder their performance, particularly in high-speed, dynamic driving environments. These challenges can significantly reduce the overall effectiveness of V2V systems, especially in critical applications like collision avoidance, real-time traffic management, and autonomous vehicle coordination. Below are some of the key challenges these RF-based technologies face:

### 3.1 Limited Bandwidth

**Challenge:** RF-based communication systems operate within predefined frequency bands, which are limited in bandwidth. For example, DSRC operates in the 5.9 GHz band, which is shared with other wireless technologies such as Wi-Fi and Bluetooth. As the number of connected vehicles increases, the demand for bandwidth increases, leading to network congestion and slower data transmission rates.

**Impact:** This congestion limits the ability of V2V systems to handle large amounts of data in real-time, especially when it comes to complex applications like real-time video streaming from cameras, high-resolution sensor data, or other bandwidth-intensive tasks necessary for autonomous driving.

### 3.2 Interference from Other RF Devices

**Challenge:** RF signals are highly susceptible to interference from other devices operating in the same or adjacent frequency bands. In urban areas, where there are many devices (e.g., smartphones, Wi-Fi routers, industrial equipment), the RF spectrum becomes crowded, leading to signal degradation and data loss.

**Impact:** In high-traffic environments, interference can disrupt communication between vehicles, reducing the reliability of safety-critical systems like collision avoidance. This is especially problematic in urban areas, where vehicle density and communication requirements are high.

### 3.3 Security Concerns

**Challenge:** RF-based communication is inherently vulnerable to various types of security threats, including eavesdropping, jamming, and spoofing. Since RF signals can travel large distances, malicious actors can potentially intercept, modify, or disrupt communication between vehicles.

**Impact:** Security is a major concern for V2V communication because any tampering with critical safety data (such as vehicle position, speed, or intent) could lead to catastrophic accidents. Additionally, a lack of robust encryption and authentication mechanisms in existing RF-based systems could allow unauthorized access to vehicle communication networks, raising privacy concerns.

### 3.4 Challenges in High-Speed, Dynamic Environments

**Challenge:** RF-based communication systems often struggle to maintain consistent and reliable communication in high-speed, dynamic environments like highways or urban areas with complex traffic patterns. The speed and unpredictable nature of moving vehicles can cause signal degradation, time delays, and packet loss.

**Impact:** For applications like real-time collision avoidance and autonomous driving, even a small delay or loss of data can lead to accidents or loss of control. The reliance on RF systems also makes it difficult to achieve the necessary levels of precision and reliability for these critical tasks.

## 4. Visible Light Communication

Visible Light Communication (VLC) is an emerging communication technology that leverages the visible spectrum of light to transmit data. In contrast to traditional RF-based communication systems, VLC uses light waves (typically emitted by light-emitting diodes (LEDs)) to enable wireless communication between devices [23]. The visible spectrum, which spans wavelengths from approximately 380 nm to 750 nm, offers a much larger bandwidth compared to the traditional RF spectrum, making VLC a promising solution for next-generation Vehicle-to-Vehicle (V2V) communication. V2V communication is essential for facilitating cooperative driving, enhancing traffic management, improving safety, and supporting the development of AVs [24]. Traditional RF-based communication systems, while widely deployed, have several limitations in terms of bandwidth, interference, latency, and security, especially in high-density environments and at high speeds. VLC, with its high data rates, low latency, and inherent security advantages, has the potential to overcome many of these challenges, making it a promising alternative or complement to RF-based V2V systems.

### 4.1 Principles of VLC for V2V Communication

VLC represents a transformative approach to wireless communication, particularly for V2V communication, leveraging the visible light spectrum (approximately 380 nm to 750 nm) for high-speed data transmission. VLC offers several advantages over traditional RF communication, such as higher data rates, improved security, and low interference [25-28]. Understanding the core principles of VLC is essential for appreciating its potential in V2V communication systems. Below, we explore the fundamental principles that underpin VLC technology in the context of V2V applications.

### 4.2 Light Emitting Diodes (LEDs) as the Primary Source

VLC relies heavily on LEDs [29] as the source of light for data transmission. LEDs have become the dominant light source for VLC for several reasons [30]:

**High Efficiency:** LEDs are energy-efficient and have a high luminous output, making them ideal for applications where both energy efficiency and brightness are required. They also have a fast-switching time, which is essential for high-speed data transmission in VLC systems.

**Durability and Longevity:** LEDs have a long lifespan and are robust against environmental factors, making them suitable for both vehicle and infrastructure applications (e.g., headlights, brake lights, traffic signals, street lamps).

In V2V communication, vehicle-mounted LEDs (headlights, taillights, and turn signals) can be modulated to transmit data to nearby vehicles or infrastructure. These LEDs are already a part of the vehicle's lighting system, meaning that adding communication functionality to existing components can significantly reduce the cost and complexity of implementing VLC.

### 4.3 Line-of-Sight (LOS) Communication

VLC operates under a LOS [31] communication model, meaning that for successful data transmission, there must be a direct optical path between the transmitter (LED light source) and the receiver (photodetector or camera) (Figure 3).

**LOS Advantages:** The line-of-sight requirement enhances security by limiting the distance over which signals can be intercepted or jammed. Since light cannot travel through opaque objects like walls, unauthorized interception or eavesdropping is much harder compared to RF systems. This makes VLC more secure and less prone to attacks like signal jamming or eavesdropping.

**LOS Challenges:** On the other hand, the requirement for line-of-sight can be a limitation in certain dynamic scenarios (e.g., in heavy traffic, when vehicles are obstructed by other vehicles, or in complex urban environments with obstacles such as buildings or trees). To overcome this, VLC systems may need to incorporate multi-vehicle communication and relays to ensure continuity of communication in cases where direct line-of-sight is temporarily unavailable.
One potential solution to the LOS challenge is the use of reflective surfaces (such as road signs or adjacent vehicles) to bounce the light signal, allowing for indirect communication paths, although this may reduce the reliability and speed of the connection.


**Figure 3: Schematic of LoS and NLoS configurations**

### 4.4 Photodetectors for Signal Reception

At the receiver end, photodetectors are used to detect the light signals that carry the data. The most common photodetectors in VLC systems are [32]:

**Photodiodes:** These devices convert light into an electrical current and are commonly used in VLC systems due to their high sensitivity and fast response time [33]. Photodiodes can detect the modulated light signal from the vehicle's headlights, taillights, or infrastructure lights and convert it into a readable electrical signal for processing.

**Phototransistors:** These are also used for VLC systems and offer higher amplification compared to photodiodes, making them useful for longer-range applications [34]. They provide the necessary gain to detect low-intensity light signals in noisy environments.

For V2V communication, the photodetector must be capable of quickly and accurately interpreting the modulated light signals sent by other vehicles or infrastructure. Camera-based systems can also be employed to detect light changes, although they are typically more complex and slower than direct photodetectors.

### 4.5 Communication Range and Data Rate Considerations

The communication range of a VLC system is influenced by factors like the power of the light source, the sensitivity of the photodetector, and environmental conditions such as ambient light [35]. The visible light spectrum has limited propagation distance compared to RF communication, as light typically travels in straight lines and is more easily blocked by obstacles.

**Range:** While VLC's range is limited, it is usually sufficient for short-range communication required in V2V applications, such as exchanging data between vehicles that are in close proximity (e.g., within 100–200 meters). Advanced techniques, like beamforming and relays, can help extend the range.

**Data Rates:** VLC systems can achieve high data rates, often reaching gigabit-per-second speeds due to the broad available bandwidth in the visible light spectrum. This makes VLC ideal for data-intensive V2V applications such as video streaming, sensor data exchange, and real-time road hazard detection.

Although the range of VLC might not be as extensive as RF communication systems (like 5G), its high data throughput makes it suitable for short-range, high-bandwidth communication needs, which are common in V2V communication.

### 4.6 Ambient Light and Interference Management

Ambient light (sunlight, streetlights, etc.) can interfere with the VLC signal, particularly in outdoor or urban environments. However, VLC systems can manage this challenge by employing various techniques [36]:

**Signal Processing Algorithms:** Advanced digital signal processing (DSP) techniques are used to filter out noise from ambient light, enabling reliable communication even in bright conditions. This can include using adaptive filtering, modulation schemes like OFDM, and spatial diversity to minimize the impact of ambient light on data transmission [37].

**Color and Intensity Modulation**: Modulation schemes such as Color Shift Keying (CSK) and Pulse Amplitude Modulation (PAM) can help mitigate ambient light interference by encoding information in multiple colors or light intensities, making the signal more resilient to external disturbances [38].

**Time-Division Multiplexing (TDM):** In some cases, VLC systems use TDM, where different communication channels operate at different times, ensuring that ambient light does not interfere with signal reception at a specific time [39].

### 4.7 Energy Efficiency and Cost-Effectiveness

LEDs, which are widely used in vehicle headlights, taillights, and traffic signals, provide a highly energy-efficient means of communication. VLC can leverage these existing LED light sources for data transmission without the need for additional, power-hungry communication devices. This makes VLC an attractive option for electric vehicles (EVs), where energy efficiency is a key consideration [40].
By using modulation of existing vehicle lights, VLC provides a cost-effective communication solution, avoiding the need for specialized hardware and infrastructure that would be required by traditional RF systems [41]. Since vehicle-mounted LEDs are already part of the vehicle's system, the additional cost for communication functionality is relatively minimal.

## 5. Advantages of VLC in V2V Communication

VLC offers several distinct advantages over traditional RF-based communication systems. These advantages are particularly important for enabling high-performance V2V communication, where high data rates, low latency, security, energy efficiency, and spectrum availability are essential. Below are some of the key benefits of VLC that make it an ideal candidate for V2V communication.

V2N (Vehicle-to-Network) [42], V2V (Vehicle-to-Vehicle) [43], V2I (Vehicle-to-Infrastructure) [44], and V2P (Vehicle-to-Pedestrian) [45] are key components of the intelligent transportation systems that enable safer, more efficient, and connected roadways. V2V communication allows vehicles to exchange information such as speed, location, and road conditions, helping to prevent accidents by providing real-time warnings about potential collisions. V2I communication connects vehicles with infrastructure like traffic signals and road sensors, enabling smoother traffic flow, reducing congestion, and enhancing safety through timely alerts about traffic conditions or signal changes (Figure 4). V2N extends these interactions to the broader network, linking vehicles with cloud-based services for traffic management, navigation, and updates, ensuring the vehicle is informed of the latest conditions. Finally, V2P communication improves pedestrian safety by enabling vehicles to detect pedestrians and alert drivers when pedestrians are in danger, thus preventing accidents. Together, these technologies pave the way for the development of autonomous driving and smarter cities.

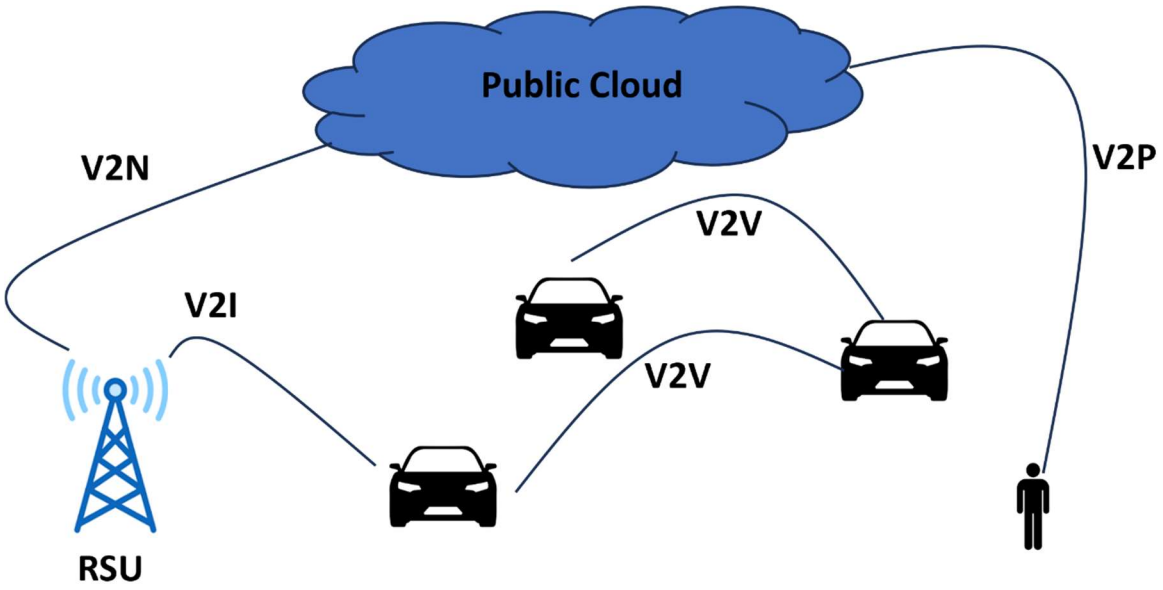


**Figure 4: Schematic of Vehicle Communication**

### 5.1 High Data Rates and Low Latency

The ability of VLC to support high data rates is one of its most significant advantages over RF communication. The visible light spectrum, which spans from approximately 380 nm to 750 nm, provides a vast bandwidth that can support extremely fast data transmission speeds. Compared to traditional RF-based communication systems, which are often constrained by limited frequency ranges, VLC's broader spectrum allows for much higher data throughput [46].

**High Data Rates:** With the large bandwidth available in the visible light spectrum, VLC can achieve data rates up to 10 Gbps or more. In contrast, RF-based systems like DSRC (Dedicated Short-Range Communications) typically operate at data rates of around 6 Mbps, and Wi-Fi can reach 1-2 Gbps at best. This large capacity is especially beneficial for high-bandwidth applications in V2V communication, such as the transmission of real-time video from cameras, LiDAR data, and sensor information used for autonomous driving.

**Low Latency:** In addition to high data rates, VLC offers very low latency (the time it takes for data to be transmitted from one vehicle to another). Latency is crucial in safety-critical applications, where a delay in communication could result in accidents. For instance, in collision avoidance systems, vehicles must quickly exchange data on their speed, location, and trajectory to make real-time decisions. Since VLC signals propagate at the speed of light (around 300,000 km/s), the delay in transmission is almost negligible, which makes VLC ideal for time-sensitive applications such as adaptive cruise control, automated lane merging, and emergency vehicle prioritization.

**Real-Time Communication:** The combination of high bandwidth and low latency in VLC ensures that real-time communication is possible in dynamic driving environments. Vehicles can quickly react to sudden changes in traffic conditions, such as a vehicle abruptly braking or a pedestrian crossing the road, by receiving and processing information almost instantaneously.

### 5.2 Low Interference and Security

VLC operates on a LOS basis, which means the signals can only be transmitted effectively between two devices (such as two vehicles or a vehicle and an infrastructure node) if there is an unobstructed path between them. This LOS requirement has important implications for interference and security in V2V communication systems [47].

**Reduced Interference:** One of the major challenges with RF communication is the susceptibility to interference from other RF devices operating in the same frequency range. In densely populated environments, such as urban areas, Wi-Fi networks, cellular networks, and other RF transmitters can cause signal congestion and interference, reducing the reliability of V2V communication. In contrast, VLC is immune to this type of interference because it operates in the visible light spectrum, which is separate from the crowded RF bands.

**Security:** VLC offers significant security benefits due to its reliance on direct line-of-sight communication. Unlike RF signals, which can easily pass through walls and obstacles, VLC signals are constrained by physical barriers. This makes it much more difficult for a potential attacker to intercept the signal from a distance. In the case of RF communication, hackers or eavesdroppers can potentially access communication signals by simply being within range, even if they are not within direct line-of-sight. With VLC, however, the signal can be "contained" within the environment, and interception requires direct access to the optical path, which is much harder to achieve without being physically near the vehicles involved.

**Enhanced Privacy:** Since VLC signals are confined to the LOS between devices, there is a much lower risk of unauthorized access or eavesdropping on the communication. This makes VLC an ideal candidate for V2V applications in autonomous vehicles or smart transportation systems, where privacy and confidentiality are crucial for maintaining safe and secure interactions between vehicles and infrastructure.

### 5.3 Energy Efficiency

VLC also offers energy efficiency advantages over traditional RF communication systems. This efficiency is especially important in the context of vehicles, where energy consumption directly impacts battery life and fuel economy, especially for electric and hybrid vehicles.

**Leveraging Existing Light Sources:** One of the most significant advantages of VLC is its ability to use existing light sources in vehicles and infrastructure. For example, vehicle [48] headlights, taillights, brake lights, and even streetlights can be repurposed to transmit data, significantly reducing the need for additional power-hungry communication devices. Vehicles already rely on LED lighting for visibility, and these LEDs can be used for VLC without the need for separate power-hungry transmitters.

**Energy-Efficient LEDs:** LEDs are inherently low-power and long-lasting, making them an ideal choice for VLC systems. By using energy-efficient LEDs, VLC systems can minimize power consumption while still providing

high-performance communication. This helps to reduce the overall energy demands of a vehicle's communication system and can contribute to sustainable transportation by decreasing the environmental impact.

**Reduction in Hardware Costs:** Since VLC can utilize existing components like vehicle lights and street lamps for data transmission, there is no need to add additional, energy-draining communication hardware to the vehicle. This not only makes VLC an energy-efficient option but also helps to lower the overall cost of V2V communication systems.

### 5.4 Reduced Congestion and Spectrum Efficiency

As demand for wireless communication grows, the RF spectrum has become increasingly congested, particularly in urban areas where multiple devices are competing for bandwidth. VLC, by operating in the visible light spectrum, provides a valuable alternative to RF-based communication systems [49].

**Reduced Spectrum Congestion:** The visible light spectrum is largely untapped and remains underutilized compared to RF bands, which are becoming crowded with Wi-Fi, cellular networks, satellite communications, and other wireless technologies. By using VLC, the demand for RF spectrum can be alleviated, reducing the burden on the overused RF spectrum and improving the overall efficiency of the wireless communication environment.

**Efficient Spectrum Use:** Since the visible light spectrum is vast, VLC has significant potential for high-spectrum efficiency. By using techniques like modulation and encoding tailored for the visible spectrum, VLC can maximize the use of the available bandwidth to transmit large amounts of data without impacting the performance of other wireless technologies.

**Complementing RF Systems:** VLC does not necessarily need to replace RF communication; rather, it can work in conjunction with RF-based systems. In scenarios where RF communication is constrained (e.g., in highly congested urban areas), VLC can provide additional capacity and resilience, helping to offload data and improve the overall network performance of V2V communication systems.

**Future of Smart Cities:** With the development of smart cities and autonomous vehicle networks, VLC can be integrated into the infrastructure, such as smart streetlights and traffic signals, to create a seamless communication network that enhances traffic management, road safety, and vehicle coordination. The ability to transmit data over longer distances without causing congestion will be a significant benefit to future V2V systems in urban environments.

## 6. Challenges and Limitations of VLC in V2V Communication

While VLC presents a compelling solution for V2V communication with numerous benefits, several challenges and limitations must be addressed for it to be widely adopted in real-world applications. These challenges are primarily related to the physical properties of light, environmental factors, and the infrastructure requirements needed for large-scale deployment. Below are the key challenges that need to be overcome for VLC to reach its full potential in V2V communication.

### 6.1 Line-of-Sight Requirement

A fundamental characteristic of VLC is its LOS dependency, which presents both advantages and challenges for V2V communication.

**Obstructions:** VLC communication relies on a direct visual path between the transmitter (e.g., a vehicle's headlights or tail-lights) and the receiver (e.g., another vehicle or infrastructure). This means that any physical obstruction—such as other vehicles, buildings, or road infrastructure—can block or attenuate the VLC signal, rendering communication unreliable or even impossible. In dense urban environments, where vehicles are

often parked in tight spaces or traffic congestion leads to frequent close vehicle formations, maintaining a clear line of sight becomes a significant challenge.

**Non-Linear Vehicle Alignment:** For effective communication, vehicles must generally be in a straight line with one another. In real-world scenarios, vehicles may not always be aligned in such a manner, especially in complex traffic situations (e.g., at intersections or during lane changes). If the vehicles are misaligned, the LOS requirement may not be met, and communication could fail or be severely degraded.

**Impact on Dynamic Driving:** In dynamic driving environments where vehicles are constantly changing speed, direction, and lane position, maintaining a stable LOS for VLC communication could be difficult, especially at higher speeds or in challenging road conditions. This issue could affect the scalability of VLC in systems like autonomous vehicle fleets, where coordination and data sharing between vehicles are key to safe operation.

**Mitigation:** Potential solutions could include the integration of additional sensors, such as infrared or millimeter-wave sensors, to assist VLC when LOS is disrupted. Additionally, hybrid systems that combine VLC with RF communication could provide a fallback mechanism for maintaining connectivity in LOS-blocked situations.

## 6.2 Limited Range

Another significant limitation of VLC for V2V communication is its relatively short communication range, especially when compared to RF communication systems.

**Outdoor Environment Limitations:** The range of VLC is generally constrained to about 100-200 meters, which can be a limitation in situations where longer-distance communication is needed, such as on highways or in rural areas. This range is significantly shorter than RF-based systems like 5G (which can support coverage over kilometers) or DSRC (typically ranging up to 1 km in optimal conditions).

**Vehicle Speed:** The limited range of VLC also poses challenges in high-speed environments, like highways, where vehicles may quickly move out of range of one another before the communication can take effect. In such environments, RF communication systems may be more suitable due to their longer range and ability to maintain communication at high speeds.

**Scaling Issues:** In densely packed urban environments, maintaining effective communication between multiple vehicles may be harder due to the short range of VLC systems. In large-scale deployments with many vehicles on the road, there would be a need for multiple communication channels to ensure inter-vehicle communication coverage, which could add to the complexity of VLC systems.

**Mitigation:** To address this issue, smart infrastructure like LED-equipped traffic signals or streetlights could act as relay stations, helping extend the effective communication range by transmitting signals to a wider area. Additionally, hybrid systems that switch between VLC and RF communication, depending on range and environmental factors, may provide greater flexibility.

## 6.3 Vulnerability to Environmental Factors

VLC communication systems are highly sensitive to environmental conditions, which can affect their reliability and performance in real-world driving scenarios.

**Ambient Light Conditions:** The performance of VLC systems can be significantly degraded by strong ambient light, such as direct sunlight during the day. Sunlight in particular can create interference in the visible spectrum, making it difficult for the photodetectors in receiving vehicles to distinguish the modulated VLC signal from background light. This is particularly problematic during the daytime when sunlight is strong, and the contrast between the communication signal and the background light becomes minimal.

**Weather and Atmospheric Conditions**: Inclement weather (such as fog, rain, or snow) can also impact the propagation of visible light. In adverse weather, the scattering or absorption of light by water droplets or particulates in the air can reduce the effectiveness of VLC, leading to signal attenuation or complete communication failure. This is particularly true in conditions such as heavy fog or rainstorms, where visibility is severely reduced.

**Low Light Conditions:** While VLC is effective in well-lit conditions (such as at night or under streetlights), its performance may be compromised in environments with insufficient ambient light. This could affect situations such as late-night driving or in poorly lit areas where there may be insufficient illumination for communication to occur effectively.

**Mitigation:** To address these environmental challenges, adaptive modulation techniques could be used, where the VLC system automatically adjusts the signal to compensate for changing lighting conditions. Infrared-based communication systems could also be integrated as a backup in low-light or obstructed environments. Additionally, the use of multi-modal communication systems that combine VLC with RF communication could ensure reliable data transmission under various environmental conditions.

### 6.4 Infrastructure Dependency

For widespread deployment of VLC for V2V communication, there is a significant dependency on infrastructure, which introduces both logistical and economic challenges.

**Need for Smart Infrastructure:** To achieve optimal performance, VLC relies on smart infrastructure that is equipped with LED-based light sources. This includes LED-equipped traffic lights, street lamps, traffic signs, and vehicle-mounted LEDs. Upgrading existing infrastructure to support VLC communication would require significant investment from both public and private sectors. Cities would need to retrofit their streetlights and other infrastructure with the appropriate lighting technology and communication modules.

**Vehicle Integration:** Vehicles themselves must be equipped with the necessary VLC transceivers (light sources and photodetectors) to send and receive signals. This would require manufacturers to integrate these systems into their vehicles, which could increase production costs and complexity. Additionally, retrofitting older vehicles with VLC communication technology could be cost-prohibitive for many car owners, limiting the adoption of the technology in the short term.

**Urban vs. Rural Deployment:** While smart cities are more likely to have the infrastructure necessary to support VLC communication, rural or less-developed areas may lack the necessary infrastructure. This could result in uneven coverage, where VLC-based V2V communication may work well in urban environments but be unreliable or unavailable in rural settings.

**High Initial Costs:** The deployment of VLC-based infrastructure requires a large upfront investment in new streetlight systems, VLC communication modules for vehicles, and associated hardware. Governments and cities must allocate resources for this infrastructure upgrade, and there may be resistance due to the high initial costs.

**Mitigation:** Governments, municipalities, and private sectors could collaborate on the development of public-private partnerships to fund infrastructure upgrades. Additionally, modular and scalable solutions for VLC communication infrastructure could be developed, allowing for phased deployment to reduce the financial burden. Hybrid solutions that combine VLC with RF communication could be used to provide partial V2V coverage until more extensive VLC infrastructure is developed.

## 7. Future Directions and Research Opportunities

While VLC shows great promise as a solution for V2V communication, several challenges remain that must be addressed to enable its widespread adoption in real-world applications. To overcome these limitations, future

research should focus on several key areas that would enhance the robustness, scalability, and interoperability of VLC-based V2V systems. Below are some important directions for future exploration.

### 7.1 Hybrid Communication Systems

One of the most promising ways to overcome the limitations of VLC in V2V communication is to develop hybrid communication systems that combine VLC with other communication technologies such as radio frequency (RF), radar, or LiDAR.

**Complementary Strengths**: While VLC offers high data rates and low latency, its reliance on line-of-sight and its vulnerability to environmental factors (e.g., fog, direct sunlight, or obstacles) can limit its effectiveness. By integrating VLC with RF communication technologies such as DSRC or 5G, the system can leverage the wide coverage and range of RF communication, while benefiting from the high-speed, high-capacity transmission of VLC in situations where line-of-sight is maintained.

**Multi-Sensor Integration**: Radar and LiDAR technologies, which are already commonly used in autonomous vehicles, can be integrated into VLC systems to enhance situational awareness and provide redundant sensing in environments where VLC alone might be insufficient. For example, when VLC communication is obstructed due to vehicle misalignment or weather conditions, radar or LiDAR can provide alternative means of detecting obstacles, helping vehicles to maintain safe distances and avoid collisions.

**Dynamic Switching**: Developing intelligent algorithms that can dynamically switch between VLC, RF, radar, or LiDAR depending on the communication environment (e.g., whether line-of-sight is maintained or whether adverse weather is present) can help create a more reliable and fault-tolerant V2V communication system.

### 7.2 Signal Processing Advancements

To fully realize the potential of VLC in V2V communication, significant advancements in signal processing techniques are required to overcome the challenges posed by environmental factors, interference, and data transmission reliability.

**Error Correction and Robust Modulation**: Developing error correction algorithms specifically tailored for VLC systems is essential to address the loss of signal integrity caused by environmental factors such as ambient light interference and atmospheric conditions. Advanced modulation schemes and error correction techniques, like Turbo codes, LDPC (Low-Density Parity-Check codes), or Polar codes, could be used to ensure that data is transmitted reliably over long distances despite signal degradation.

**Adaptive Signal Processing**: In dynamic driving environments, the communication conditions for VLC can change rapidly (e.g., when a vehicle enters a tunnel, or if sunlight directly hits the sensor). Research into adaptive signal processing techniques that adjust modulation parameters, transmit power, and error correction schemes based on real-time environmental conditions could improve VLC system performance.

**Interference Mitigation**: Even though VLC is less prone to interference from other wireless devices compared to RF, it is still susceptible to interference from ambient light sources (e.g., sunlight, street lamps). Research into techniques for interference mitigation, such as the use of polarized light or time-division multiplexing, could help reduce the impact of such interference on the reliability of VLC communication in V2V systems.

### 7.3 Autonomous Vehicle Integration

As the development of AVs continues to advance, the integration of VLC into AV systems will play a key role in enhancing the situational awareness and coordination between vehicles, especially in complex, multi-vehicle scenarios.

**Vehicle-to-Vehicle Coordination**: In autonomous driving scenarios, vehicles need to communicate with one another to predict each other's intentions, such as whether a vehicle is about to change lanes, slow down, or

stop. VLC can enable real-time communication between autonomous vehicles, ensuring that they are aware of each other's location, speed, and trajectory. This level of cooperation is vital for ensuring the safe and efficient operation of AV fleets, particularly in dense traffic conditions.

**Advanced Driving Maneuvers**: Research into cooperative driving and platooning will benefit significantly from VLC. In platooning, multiple vehicles travel in close formation to reduce fuel consumption and improve traffic flow. VLC can provide the high-speed, low-latency communication needed to synchronize the movements of multiple vehicles in real time.

**Enhanced Perception and Decision Making**: Autonomous vehicles rely on various sensors (e.g., cameras, radar, and LiDAR) for perception. Integrating VLC as a communication channel between vehicles can help augment the decision-making process by providing additional data such as the status of surrounding vehicles, road conditions, or traffic signals, which can enhance the vehicle's situational awareness and improve its decision-making capabilities.

### 7.4 Infrastructure and Standardization

For VLC-based V2V communication systems to become widely adopted, there is a need for the establishment of industry standards and the development of a robust infrastructure that supports the technology on a global scale.

**Global Standards for VLC**: To ensure interoperability between different vehicles, manufacturers, and infrastructures, it is essential to develop common standards for VLC technology. These standards should address key issues such as data formats, communication protocols, modulation techniques, and security measures. By establishing unified standards, VLC systems can ensure that vehicles and infrastructure from different manufacturers and regions can communicate seamlessly with one another.

**Smart Infrastructure Deployment**: Widespread adoption of VLC requires the installation of smart infrastructure, such as LED-equipped traffic lights, streetlights, and smart road signs, that are capable of transmitting and receiving data. Governments and private companies will need to collaborate on the development and funding of such infrastructure. Additionally, research into scalable deployment models that allow for gradual integration of VLC into existing transportation networks is needed.

**Interoperability with Existing Communication Systems**: VLC should be able to work in conjunction with existing RF-based communication systems (e.g., DSRC, 5G, Wi-Fi). Research into interoperability between VLC and RF systems is essential to ensure that mixed-modal communication can occur in real-world scenarios.

## 8. Conclusion

VLC represents a promising frontier for V2V communication, offering significant advantages over traditional radio frequency (RF) systems, such as high data rates, low latency, and enhanced security. VLC's ability to utilize the visible light spectrum—a largely untapped bandwidth allows for faster and more efficient data transmission, making it an ideal candidate for improving vehicle safety, optimizing traffic flow, and facilitating the development of autonomous driving systems. The key strengths of VLC lie in its ability to provide high-speed, real-time communication, which is essential for safety-critical applications like collision avoidance and adaptive cruise control. Its inherent line-of-sight communication mechanism reduces the risk of interference from other wireless systems, thus providing secure and reliable communication channels between vehicles. Moreover, VLC's energy efficiency, particularly by leveraging existing infrastructure like LED-equipped streetlights and headlights, positions it as a sustainable solution for smart transportation systems. However, while VLC presents considerable advantages, it also comes with inherent challenges, such as the line-of-sight requirement and limited communication range. These challenges can hinder its deployment in certain environments, especially in urban areas with complex traffic conditions and physical obstructions. Environmental factors, such as ambient light interference, weather conditions, and nighttime visibility, further complicate VLC's effectiveness under certain conditions. Despite these limitations, ongoing research and technological advancements are making strides to address these concerns. Innovations in signal processing

techniques, such as error correction and adaptive modulation, are being developed to improve VLC's resilience to environmental factors. Additionally, hybrid communication systems that combine VLC with RF technologies, LiDAR, and radar are being explored to enhance system reliability in dynamic and diverse driving conditions. These hybrid systems will allow VLC to operate in synergy with other communication technologies, providing a robust and flexible solution for V2V communication in varying environments. The development of smart infrastructure that supports VLC communication, such as smart streetlights and LED-based traffic signals, will also play a crucial role in enabling the widespread adoption of VLC. Collaborative efforts between governments, automotive manufacturers, and tech companies will be essential to build the necessary infrastructure and set global standards for VLC-based communication.

## References


1. Darbha, Swaroop, Shyamprasad Konduri, and Prabhakar R. Pagilla. "Benefits of V2V communication for autonomous and connected vehicles." *IEEE Transactions on Intelligent Transportation Systems* 20, no. 5 (2018): 1954-1963.
2. El Zorkany, Mohamed, Ahmed Yasser, and Ahmed I. Galal. "Vehicle to vehicle "V2V" communication: scope, importance, challenges, research directions and future." *The Open Transportation Journal* 14, no. 1 (2020).
3. Duarte, Fábio, and Carlo Ratti. "The impact of autonomous vehicles on cities: A review." *Journal of Urban Technology* 25, no. 4 (2018): 3-18.
4. Shaout, Adnan, Dominic Colella, and Selim Awad. "Advanced driver assistance systems-past, present and future." In *2011 Seventh International Computer Engineering Conference (ICENCO'2011)*, pp. 72-82. IEEE, 2011.
5. Matheus, Luiz Eduardo Mendes, Alex Borges Vieira, Luiz FM Vieira, Marcos AM Vieira, and Omprakash Gnawali. "Visible light communication: concepts, applications and challenges." *IEEE Communications Surveys & Tutorials* 21, no. 4 (2019): 3204-3237.
6. Hossain, Eftekhar, Nursadul Mamun, and Md Fahim Faisal. "Vehicle to vehicle communication using RF and IR technology." In *2017 2nd international conference on electrical & electronic engineering (ICEEE)*, pp. 1-5. IEEE, 2017.
7. Caveney, Derek, and William B. Dunbar. "Cooperative driving: Beyond V2V as an ADAS sensor." In *2012 IEEE Intelligent Vehicles Symposium*, pp. 529-534. IEEE, 2012.
8. Cao, Jiayu, Supeng Leng, Lei Zhang, Muhammad Imran, and Haoye Chai. "A V2V empowered consensus framework for cooperative autonomous driving." In *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 5729-5734. IEEE, 2022.
9. Dubey, Rohit K., Javier Argota Sánchez–Vaquerizo, Damian Dailisan, and Dirk Helbing. "Cooperative adaptable lanes for safer shared space and improved mixed-traffic flow." *Transportation Research Part C: Emerging Technologies* 166 (2024): 104748.
10. Fahmy, Hazem M., Gerd Baumann, Mohamed A. Abd El Ghany, and Hassan Mostafa. "V2V-based vehicle risk assessment and control for lane-keeping and collision avoidance." In *2017 29th International Conference on Microelectronics (ICM)*, pp. 1-5. IEEE, 2017.
11. Jahnavi, Maudhoo, Neha Yadav, Krishanu Griyagya, Mahendra Singh Meena, and Ved Prakash. "Vehicle to vehicle communication for collision avoidance." *International Journal for Research in Applied Science and Engineering Technology* 6, no. 5 (2018): 1380-1386.
12. Huang, Chung-Ming, and Shih-Yang Lin. "An early collision warning algorithm for vehicles based on V2V communication." *International Journal of Communication Systems* 25, no. 6 (2012): 779-795.
13. Lee, Euntak, Bongsoo Son, and Wongil Kim. "Automated Driving Control in Mixed Traffic Flow Using V2V Communication." *IEEE Transactions on Intelligent Vehicles* (2024).
14. Wang, Runmin, Zhigang Xu, Xiangmo Zhao, and Jinchao Hu. "V2V-based method for the detection of road traffic congestion." *IET Intelligent Transport Systems* 13, no. 5 (2019): 880-885.

15. Benzaman, Ben, and Deepak Sharma. "Discrete event simulation of a road intersection integrating V2V and V2I features to improve traffic flow." In *2017 Winter Simulation Conference (WSC)*, pp. 3054-3065. IEEE, 2017.
16. Darbha, Swaroop, Shyamprasad Konduri, and Prabhakar R. Pagilla. "Benefits of V2V communication for autonomous and connected vehicles." *IEEE Transactions on Intelligent Transportation Systems* 20, no. 5 (2018): 1954-1963.
17. Liu, Changliu, Chung-Wei Lin, Shinichi Shiraishi, and Masayoshi Tomizuka. "Improving efficiency of autonomous vehicles by v2v communication." In *2018 Annual American Control Conference (ACC)*, pp. 4778-4783. IEEE, 2018.
18. Feng, Shuo, and Simon Haykin. "Cognitive risk control for anti-jamming V2V communications in autonomous vehicle networks." *IEEE Transactions on Vehicular Technology* 68, no. 10 (2019): 9920-9934.
19. Singh, Gurinder, Anand Srivastava, Vivek Ashok Bohara, Zilong Liu, and Dirk Pesch. "Towards 6G-V2X: Aggregated RF-VLC for Ultra-Reliable and Low-Latency Autonomous Driving." *IEEE Communications Standards Magazine* (2024).
20. Nguyen, Tien Viet, Patil Shailesh, Baghel Sudhir, Gulati Kapil, Libin Jiang, Zhibin Wu, Durga Malladi, and Junyi Li. "A comparison of cellular vehicle-to-everything and dedicated short range communication." In *2017 IEEE Vehicular Networking Conference (VNC)*, pp. 101-108. IEEE, 2017.
21. Roger, Sandra, David Martín-Sacristán, David Garcia-Roger, Jose F. Monserrat, Apostolos Kousaridas, Panagiotis Spapis, and Serkan Ayaz. "5G V2V communication with antenna selection based on context awareness: Signaling and performance study." *IEEE transactions on intelligent transportation systems* 23, no. 2 (2020): 1044-1057.
22. Singh, Anjali, and Brahmjit Singh. "A study of the IEEE802. 11p (WAVE) and LTE-V2V technologies for vehicular communication." In *2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, pp. 157-160. IEEE, 2020.
23. Matheus, Luiz Eduardo Mendes, Alex Borges Vieira, Luiz FM Vieira, Marcos AM Vieira, and Omprakash Gnawali. "Visible light communication: concepts, applications and challenges." *IEEE Communications Surveys & Tutorials* 21, no. 4 (2019): 3204-3237.
24. Pathak, Parth H., Xiaotao Feng, Pengfei Hu, and Prasant Mohapatra. "Visible light communication, networking, and sensing: A survey, potential and challenges." *IEEE communications surveys & tutorials* 17, no. 4 (2015): 2047-2077.
25. Rehman, Saeed Ur, Shakir Ullah, Peter Han Joo Chong, Sira Yongchareon, and Dan Komosny. "Visible light communication: A system perspective—Overview and challenges." *Sensors* 19, no. 5 (2019): 1153.
26. Haas, Harald. "Visible light communication." In *2015 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1-72. IEEE, 2015.
27. O'brien, Dominic C., Lubin Zeng, Hoa Le-Minh, Grahame Faulkner, Joachim W. Walewski, and Sebastian Randel. "Visible light communications: Challenges and possibilities." In *2008 IEEE 19th international symposium on personal, indoor and mobile radio communications*, pp. 1-5. IEEE, 2008.
28. Khan, Latif Ullah. "Visible light communication: Applications, architecture, standardization and research challenges." *Digital Communications and Networks* 3, no. 2 (2017): 78-88.
29. Schmid, Stefan, Giorgio Corbellini, Stefan Mangold, and Thomas R. Gross. "LED-to-LED visible light communication networks." In *Proceedings of the fourteenth ACM international symposium on Mobile ad hoc networking and computing*, pp. 1-10. 2013.
30. Komine, Toshihiko, and Masao Nakagawa. "Fundamental analysis for visible-light communication system using LED lights." *IEEE transactions on Consumer Electronics* 50, no. 1 (2004): 100-107.
31. Cui, Kaiyun, Gang Chen, Zhengyuan Xu, and Richard D. Roberts. "Line-of-sight visible light communication system design and demonstration." In *2010 7th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP 2010)*, pp. 621-625. IEEE, 2010.

32. Morales-Céspedes, Máximo, Borja Genovés Guzmán, Alejandro López Barrios, and Víctor P. Gil Jiménez. "Colored Reconfigurable Photodetectors for Aligning the Light in Vehicular VLC." *IEEE Transactions on Vehicular Technology* (2024).
33. Vieira, M. A., Manuela Vieira, Paula Louro, and Pedro Vieira. "Vehicular Visible Light Communication: a road-to-vehicle proof of concept." In *Optical Sensing and Detection V*, vol. 10680, pp. 95-104. SPIE, 2018.
34. Anbalagan, R., M. Zahir Hussain, D. Jayabalakrishnan, DB Naga Muruga, and M. Prabhahar. "Vehicle to vehicle data transfer and communication using LI-FI technology." *Materials Today: Proceedings* 45 (2021): 5925-5933.
35. El Zorkany, Mohamed, Ahmed Yasser, and Ahmed I. Galal. "Vehicle to vehicle "V2V" communication: scope, importance, challenges, research directions and future." *The Open Transportation Journal* 14, no. 1 (2020).
36. Alam, Mohammad Rakibul, and Saleh Faruque. "Prospects of differential optical receiver with ambient light compensation in vehicular visible light communication." In *2016 IEEE Vehicular Networking Conference (VNC)*, pp. 1-4. IEEE, 2016.
37. Memedi, Agon, and Falko Dressler. "Vehicular visible light communications: A survey." *IEEE Communications Surveys & Tutorials* 23, no. 1 (2020): 161-181.
38. Kassir, Saadallah, Jean Abou Rahal, and Zaher Dawy. "On the performance of camera receivers for V2V visible light communication systems." In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1-7. IEEE, 2017.
39. Omar, Hassan Aboubakr, and Weihua Zhuang. *Time division multiple access for vehicular communications*. Springer, 2014.
40. Shurrab, Mohammed, Shakti Singh, Hadi Otrok, Rabeb Mizouni, Vinod Khadkikar, and Hatem Zeineldin. "An efficient vehicle-to-vehicle (V2V) energy sharing framework." *IEEE Internet of Things Journal* 9, no. 7 (2021): 5315-5328.
41. Qin, Peng, Yang Fu, Xu Feng, Xiongwen Zhao, Shuo Wang, and Zhenyu Zhou. "Energy-efficient resource allocation for parked-cars-based cellular-V2V heterogeneous networks." *IEEE Internet of Things Journal* 9, no. 4 (2021): 3046-3061.
42. Elagin, Vasiliy, Anastasia Spirkina, Mikhail Buinevich, and Andrei Vladyko. "Technological aspects of blockchain application for vehicle-to-network." *Information* 11, no. 10 (2020): 465.
43. Zeadally, Sherali, J. Guerrero, and Juan Contreras. "A tutorial survey on vehicle-to-vehicle communications." *Telecommunication Systems* 73, no. 3 (2020): 469-489.
44. Miller, Jeffrey. "Vehicle-to-vehicle-to-infrastructure (V2V2I) intelligent transportation system architecture." In *2008 IEEE intelligent vehicles symposium*, pp. 715-720. IEEE, 2008.
45. Anaya, José Javier, Pierre Merdrignac, Oyunchimeg Shagdar, Fawzi Nashashibi, and José E. Naranjo. "Vehicle to pedestrian communications for protection of vulnerable road users." In *2014 IEEE Intelligent Vehicles Symposium Proceedings*, pp. 1037-1042. IEEE, 2014.
46. Khan, Latif Ullah. "Visible light communication: Applications, architecture, standardization and research challenges." *Digital Communications and Networks* 3, no. 2 (2017): 78-88.
47. Albayrak, Cenk, Sinasi Cetinkaya, Kadir Turk, and Huseyin Arslan. "Physical layer security for visible light communication in reflected indoor environments with inter-symbol interference." *IEEE Transactions on Information Forensics and Security* 18 (2023): 2709-2722.
48. Teixeira, Lucas, Felipe Loose, Carlos Henrique Barriquello, Vitalio Alfonso Reguera, Marco Antônio Dalla Costa, and J. Marcos Alonso. "On energy efficiency of visible light communication systems." *IEEE Journal of Emerging and Selected Topics in Power Electronics* 9, no. 5 (2021): 6396-6407.
49. Mustapha, Mahmud, and Ibrahim Develi. "Visible Light Communication: A Tool For Addressing Radio Frequency Spectrum Congestion." In *International conference on advances and innovations in engineering (ICAIE 2017) Elazig Turkey, May*, pp. 10-12. 2020.

**International Journal of Intelligent Communication and Computer Science**
**Vol. 2, No. 2, 2024, Pages 57-76.**

# Underwater Rescue Management in Flooded Areas Using Wireless Sensor Networks: An Overview

**Sangeeta Ranjan[1] and Atul Mathur[2]**

[1]Research Scholar, Department of Computer Science and Engineering, Naraina College of Engineering and Technology, Kanpur, Affiliated to AKTU, Lucknow
[2]Department of Computer Science and Engineering, Naraina College of Engineering and Technology, Affiliated to AKTU, Lucknow

**Review Paper**

Email: sangeeta.ranjan2@gmail.com
Received: 16 Apr 2024, Revised: 13 Sep. 2024 Accepted: 10 Oct 2024

**Abstract:**

Floods are among the most destructive natural disasters, causing extensive loss of life, property damage, and displacement of populations. Traditional search and rescue (SAR) operations in flood-affected areas face significant challenges due to adverse conditions such as deep waters, fast-moving currents, low visibility, and lack of communication infrastructure. To address these challenges, this paper explores the potential of Wireless Sensor Networks (WSNs) in enhancing underwater rescue management in flooded environments. WSNs, consisting of distributed sensor nodes that collect and transmit real-time environmental data, offer unique advantages for monitoring and coordinating rescue efforts in disaster-stricken areas. By deploying various sensors such as acoustic, pressure, temperature, and motion detectors, WSNs can provide continuous situational awareness, track victims, assess flood dynamics, and support real-time decision-making. However, the deployment of WSNs in underwater rescue operations is not without challenges, including communication limitations, sensor node durability, and energy constraints. This paper discusses these challenges and highlights technological innovations that can improve the reliability and effectiveness of WSNs, such as hybrid communication systems, energy harvesting, and autonomous underwater vehicles (AUVs). Ultimately, the integration of WSNs into flood rescue operations has the potential to significantly improve response times, enhance rescue efficiency, and reduce the risks to human rescuers, offering a promising approach for disaster management in flooded regions.

**Keywords:** Flood Rescue, Wireless Sensor Networks (WSNs), Underwater Rescue, Search and Rescue (SAR), Disaster Management, Acoustic Sensors, Autonomous Underwater Vehicles (AUVs)

## 1. Introduction

Floods are among the most frequent and catastrophic natural disasters globally, capable of causing widespread destruction in a matter of hours or days [1]. The impacts of flooding are multifaceted, leading to not only significant loss of life but also severe economic, social, and environmental consequences. Floods often displace thousands of people, submerge homes and critical infrastructure, and disrupt essential services such as healthcare, education, and transportation. In the most severe cases, floods can result in the collapse of bridges, roads, dams, and buildings, further complicating rescue and recovery efforts [2]. The aftermath of a flood often leaves affected areas isolated, with limited access to emergency services or external support.

In such catastrophic events, the need for rapid and efficient search and rescue (SAR) operations becomes paramount [3]. Time is of the essence when lives are at risk, and the window of opportunity for successful rescues can be narrow. The challenges faced by rescue teams are compounded by the very nature of flood-affected environments. These include deep and fast-moving waters, submerged debris, and often unpredictable currents [4]. The visibility in these environments is typically poor, making it difficult for rescuers to locate survivors or navigate safely [5]. Traditional SAR methods that rely on human rescuers, helicopters, boats, and divers, while effective in certain situations, are often hindered by these adverse conditions, slowing down response times and reducing the overall effectiveness of the mission [6].

In recent years, advancements in technology have provided new avenues for improving SAR operations. One of the most promising innovations in this space is the use of WSNs. WSNs consist of spatially distributed sensor nodes that collect data from their environment and communicate wirelessly with each other or to a central command center. These networks have been successfully deployed in a wide range of applications, including environmental monitoring, disaster management, and industrial monitoring, among others [7]. What makes WSNs particularly well-suited for flood rescue operations is their ability to function in challenging environments, providing continuous monitoring and data collection in real-time. WSNs offer a variety of benefits in the context of flood rescue operations. They provide a means to monitor a flood-affected area in a way that is not possible with traditional methods. WSNs can be used to track water levels, monitor water quality, detect underwater currents, and even detect the presence of survivors or rescuers [8]. Equipped with a range of sensors, such as temperature, pressure, motion, and acoustic sensors, these networks can capture critical data about the underwater environment. This data can then be transmitted wirelessly to a central command center, where it can be analyzed and used to make informed decisions in real-time, thus enhancing the speed and accuracy of rescue operations.

For example, during a flood, WSNs could help locate survivors by detecting acoustic signals from distress calls or monitoring motion in the water to identify areas where individuals may be trapped. Additionally, these networks can provide detailed information about the flood's behaviour, such as the rise and fall of water levels, current velocities, and the potential for further flooding, which would allow rescue teams to adapt and respond more effectively. Moreover, WSNs enable remote monitoring of underwater environments, which can reduce the need for human rescuers to enter dangerous or submerged areas [9]. This reduces the risk to human lives and makes it possible to gather valuable information without endangering rescue personnel [10].

The integration of WSNs into underwater rescue management is a relatively novel approach and promises to revolutionize the way disaster response is handled. However, despite their potential, several challenges remain in deploying WSNs effectively in flooded areas. These challenges include issues related to the communication infrastructure in underwater environments, the energy limitations of sensor nodes, and the difficulty of maintaining network stability in a dynamic and often harsh physical environment [11]. For instance, acoustic waves, which are commonly used for communication between nodes in underwater WSNs, face significant limitations in terms of range, bandwidth, and susceptibility to interference from water noise or other sources. Additionally, sensor nodes need to be robust enough to withstand the harsh conditions of a flooded area, including high pressure, corrosion, and the risk of physical damage from debris [12].

Despite these challenges, ongoing advancements in sensor technologies, energy-efficient systems, and communication protocols continue to make WSNs more viable for underwater rescue operations. Researchers are developing new approaches to address the limitations of underwater communication, such as hybrid communication systems that combine acoustic and optical methods, and energy harvesting techniques that can prolong the life of sensor nodes. In addition, the use of autonomous vehicles (e.g., drones or autonomous underwater vehicles - AUVs) equipped with WSNs is becoming an increasingly popular solution for deploying and maintaining sensor networks in flood-affected areas. These vehicles can autonomously navigate through hazardous environments and deploy sensors at strategic locations to monitor key data points.

This paper aims to explore the role of WSNs in enhancing underwater rescue management during floods. It will examine the potential applications of WSNs in flood rescue, discuss the challenges that must be addressed for their effective implementation, and highlight the technological innovations that can overcome these challenges. Through a comprehensive analysis, this paper seeks to demonstrate how WSNs can provide critical support in improving the speed, safety, and effectiveness of flood rescue operations, ultimately contributing to saving lives and mitigating the impact of flooding on communities around the world.

## 2. Background and Motivation

Flooded areas present one of the most challenging environments for search and rescue (SAR) operations. These areas are typically characterized by unpredictable and dynamic water conditions, which include varying depths, fast-moving currents, fluctuating water levels, poor visibility, and the presence of debris such as fallen trees, buildings, and other obstructions. Such conditions make it extremely difficult for human rescuers to navigate and perform their tasks effectively [13]. In addition to these environmental challenges, flood-prone regions often lack adequate infrastructure, such as roads, power supplies, and communication networks, further complicating rescue efforts. In many cases, traditional SAR teams rely on boats, helicopters, or divers, all of which can be hindered by the murky waters, hazardous debris, and unpredictable behaviour of the floodwaters [14].

Given the high risks to human life in flood zones, there is a clear need for innovative technologies that can support and augment SAR operations. Traditional methods, while valuable, are often limited in their effectiveness under such harsh conditions. As such, there is a growing interest in utilizing WSNs to assist in rescue operations in these environments.

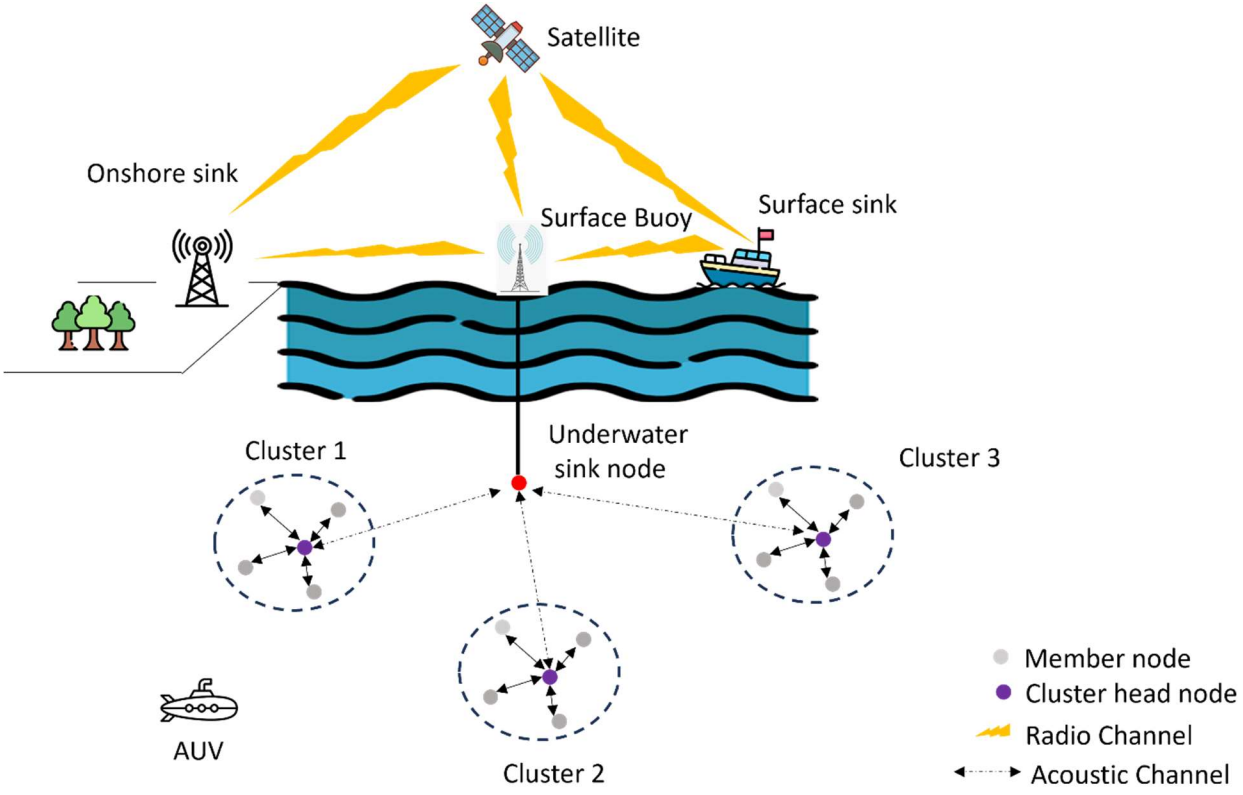


**Figure 1: Schematic of underwater WSN system**

WSNs consist of networks of distributed sensor nodes, each equipped with various sensing devices such as temperature, pressure, depth, acoustic, and motion sensors. These sensor nodes can be deployed in the flood-affected areas to gather data about the environment and communicate wirelessly with a central processing unit or command center [15]. The key advantage of WSNs is their ability to provide real-time environmental monitoring and data collection, even in challenging conditions where human intervention might be too risky or impractical.

The motivation behind deploying WSNs in underwater rescue operations is multifaceted. By providing continuous monitoring, these networks can help assess water conditions, track the movement of victims, and identify potential hazards that rescuers might face. This capability can significantly enhance decision-making and operational efficiency during SAR missions.

## 3. Advantages of Using WSNs in Underwater Rescue Operations

### 3.1 Real-time Monitoring:

WSNs enable the continuous tracking of environmental conditions such as water levels, temperature variations, and flow rates. This data can help identify changes in conditions that might pose risks to rescuers or victims [16]. For instance, sudden increases in water flow or a rise in water levels can trigger early warnings, enabling rescue teams to adjust their strategies or evacuate certain areas. Continuous monitoring can also help track the progress of the floodwaters, providing valuable information for long-term recovery efforts.

### 3.2 Autonomous Deployment:

One of the primary challenges of rescue operations in flooded environments is the difficulty and danger of deploying personnel into such areas. WSNs can be deployed autonomously via robotic vehicles or drones, including Autonomous Underwater Vehicles (AUVs) [17]. These vehicles can navigate through the floodwaters, placing sensor nodes in key locations without putting human lives at risk. Autonomous deployment also reduces the time and effort required for initial setup, allowing the rescue operation to begin much faster.

### 3.3 Data Fusion and Communication:

WSNs integrate data from a variety of sensors, creating a comprehensive understanding of the underwater environment [18]. For example, combining depth sensor data with acoustic sensor data can provide more accurate localization of survivors or submerged objects. This fused data can be transmitted wirelessly to command centers or rescue teams, ensuring that all involved parties have access to up-to-date, accurate information. The ability to transmit data in real-time via wireless communication reduces the dependency on traditional communication infrastructure, which may be damaged or absent in flood-affected areas.

### 3.4 Improved Decision-Making and Resource Allocation:

By providing accurate and real-time data, WSNs enable better situational awareness, allowing SAR teams to make informed decisions quickly [19]. This data can assist in prioritizing areas for rescue operations, directing teams to the most critical locations based on water conditions, potential victim locations, and hazards. The real-time feedback allows for more agile decision-making, ensuring that resources are allocated effectively and efficiently. This rapid decision-making can be the difference between life and death during a flood disaster.

### 3.5 Reducing Human Risk:

Perhaps one of the most important advantages of integrating WSNs into rescue operations is the reduction in risk to human rescuers. Deploying sensor networks, drones, and AUVs into flooded areas reduces the need for human personnel to enter hazardous conditions [20]. For example, sensors placed in strategic locations can monitor areas that are too dangerous for human intervention, such as rapidly moving waters or submerged structures, thereby minimizing the exposure of rescuers to extreme risks.

### 3.6 Long-term Monitoring for Recovery:

Beyond the immediate rescue phase, WSNs can continue to play an essential role during the recovery and rehabilitation phases [21]. Continuous monitoring can assess the impact of the flood on local infrastructure, track water quality, and help identify areas still at risk of further flooding or landslides. This data is invaluable for long-term recovery planning and ensures that the area is fully assessed before rebuilding efforts are launched.

## 4. Key Components of WSNs for Underwater Rescue

WSNs have become an invaluable tool for enhancing underwater rescue operations in flood-affected areas. These networks comprise several critical components that work synergistically to gather, process, and

communicate real-time data from dynamic and often hazardous environments [22]. The following sections describe the key components of WSNs that make them effective for underwater rescue operations:

### 4.1 Sensor Nodes

Sensor nodes are the foundational elements of any WSN. They are responsible for capturing data about the underwater environment, processing it locally, and transmitting relevant information to the network for further analysis [23]. In an underwater rescue scenario, these sensor nodes need to be specifically designed to endure the extreme conditions present in flooded areas, including high-pressure environments, temperature fluctuations, and high humidity. They are typically equipped with various types of sensors tailored to monitor environmental parameters critical for rescue missions. Some common sensors include:

- **Acoustic Sensors**: Acoustic sensors detect underwater sounds, which can include human distress signals, the noise produced by moving objects, or the vocalizations of survivors [24]. These sensors can help identify the presence of trapped victims or distinguish between different sources of sound, providing valuable insight into the state of the rescue operation. Since sound travels well in water, acoustic sensors are commonly used for communication and detection in underwater environments.
- **Pressure and Depth Sensors**: These sensors monitor the depth of the water and the surrounding pressure conditions. Rapid changes in water depth could indicate potential hazards such as a sudden surge in water level or the collapse of structures [25]. Monitoring pressure also helps to understand the structural integrity of submerged areas, alerting rescuers to areas where there may be a risk of collapse or flooding.
- **Temperature and Humidity Sensors**: These sensors monitor changes in water temperature and humidity levels [26]. Temperature fluctuations can influence the behavior of floodwaters, while changes in humidity levels may be indicative of environmental instability or contamination. In rescue operations, such data is important for assessing the safety of divers, the condition of survivors, and planning appropriate rescue strategies.
- **Motion Sensors**: Motion detection is crucial for tracking both rescuers and victims [27]. These sensors can detect movement within a given range, helping to pinpoint the location of individuals in need of assistance or to monitor the movement of rescuers in dangerous zones. They can also detect the presence of underwater debris, which could pose a danger to both rescuers and victims.

### 4.2 Data Processing Unit (DPU)

The Data Processing Unit (DPU) is a central component that aggregates and processes data collected from the various sensor nodes. In an underwater environment, where communication with surface units can be challenging due to signal attenuation, the DPU helps filter and process the raw data in real time [28]. By performing initial data analysis locally on the sensor nodes or at the DPU, unnecessary data can be discarded, and only the most relevant information is transmitted to the command center.
The DPU is responsible for:

- Filtering noise from the data.
- Aggregating data from multiple sensor nodes.
- Performing basic analysis to detect anomalies (e.g., rapid changes in water depth, sudden temperature shifts, or distress signals).
- Sending relevant processed data to the command center for further decision-making.

By reducing the amount of data transmitted and focusing on actionable insights, the DPU enhances the efficiency of the network and ensures faster, more accurate decision-making.

### 4.3 Wireless Communication Network

In flooded areas, traditional communication infrastructure is often disrupted or non-functional due to water damage or the absence of reliable connectivity. This is where the wireless communication network within a WSN becomes critical. WSNs primarily rely on two types of communication methods in underwater environments: acoustic communication and radio frequency (RF) communication [29]. These methods are tailored to the specific constraints of underwater environments, where sound and electromagnetic waves behave differently than in air.

- **Acoustic Communication**: Acoustic signals are the most commonly used method for wireless communication in underwater networks. They can transmit data over relatively long distances, especially in shallow or moderately deep waters. Acoustic communication is highly effective for real-time data transfer between sensor nodes and the central system [30]. However, it has limitations such as low bandwidth, high signal attenuation with increasing depth, and interference from environmental noise. Despite these drawbacks, acoustic waves remain the most reliable option for underwater communication.
- **Radio Frequency (RF) Communication**: RF communication is typically used for shorter distances, such as within nodes closer to the water surface or in shallow areas [31]. RF waves can suffer from significant attenuation in water, limiting their usefulness in deeper or murkier waters. However, they are useful in applications where the sensor nodes are closer to the surface or where hybrid communication systems (using both RF and acoustic methods) are employed.

A robust communication network ensures the continuous flow of real-time data between sensors, rescue robots, and the command center, despite the challenges of underwater signal transmission.

## 5. Rescue Robots/Autonomous Underwater Vehicles (AUVs)

Rescue robots and Autonomous Underwater Vehicles (AUVs) are critical technological tools that play an essential role in improving the efficiency and safety of underwater rescue operations in flood-affected areas [32]. These vehicles are designed to operate autonomously or be remotely controlled, providing a means to conduct complex tasks in hazardous and submerged environments where human intervention is either too dangerous or impractical [33]. AUVs are increasingly deployed in flood scenarios due to their ability to perform tasks with precision, flexibility, and speed, all while minimizing the risks to human rescuers [34].
Here are several key roles that AUVs play in underwater rescue operations:

### 5.1 Deploying Sensor Nodes

One of the primary functions of AUVs in rescue missions is the autonomous deployment of sensor nodes in strategically important areas. The ability to autonomously place sensors in flood-affected zones, including deep or fast-moving waters, provides several advantages:

- **Reduced Risk to Human Rescuers:** Traditional methods of sensor deployment often require human divers or operators to venture into hazardous floodwaters, which exposes them to significant risks, including strong currents, submerged debris, and poor visibility. AUVs eliminate the need for direct human involvement in such environments, thereby enhancing safety.

- **Accelerated Setup Process:** In many rescue operations, time is of the essence. AUVs can swiftly navigate floodwaters and deploy sensors in pre-determined or dynamically chosen locations. This reduces the setup time for the sensor network, allowing for quicker initiation of monitoring and real-time data collection.

- **Strategic Placement:** AUVs can be equipped with advanced navigation systems and algorithms that allow them to identify optimal locations for sensor deployment. For example, they may choose areas with high survivor likelihood, such as pockets of calm water or near buildings or infrastructure that are submerged but still intact.

## 5.2 Surveying the Environment

AUVs are also crucial for surveying the environment in flooded areas, particularly when human access to certain locations is impossible or too risky [35]. These vehicles are often equipped with an array of sensors that allow them to gather detailed data about the state of the floodwaters and submerged structures.

- **Real-Time Imaging:** AUVs can be outfitted with cameras, sonar systems, or LiDAR sensors to provide real-time imaging of submerged areas. This gives rescue teams a visual representation of the flood's impact, such as detecting the locations of survivors, identifying submerged debris, and assessing the integrity of underwater structures.
- **Detailed Mapping:** In addition to visual imaging, AUVs can produce detailed maps of the flooded areas, capturing data such as the topography of the underwater landscape, water depth, and flow patterns. This data is invaluable for understanding the flood dynamics, planning effective rescue strategies, and identifying safe routes for human rescuers to follow.
- **Hard-to-Reach Areas:** AUVs are especially valuable in hard-to-reach or dangerous zones. For example, they can access deep or narrow crevices where human divers might struggle or where physical obstacles prevent access. These vehicles can provide a thorough survey of areas that would otherwise remain unexplored, thereby improving the overall situational awareness of the command center.

## 5.3 Supporting Data Collection

Beyond deploying sensors, AUVs are essential for ongoing data collection during rescue operations. They are capable of retrieving data from submerged or remote sensors, ensuring that the network remains operational and up-to-date throughout the mission [36].

- **Data Retrieval:** In flood situations, sensors may become displaced, malfunction, or lose power over time. AUVs can be dispatched to retrieve data from these sensors, relocate them, or replace them with new ones if necessary. This ensures that the sensor network remains effective and that rescue teams continue to receive accurate, real-time information.
- **Data Integration:** AUVs can also assist in integrating the data gathered from various sensors across the flood-affected area. This data can include information from temperature sensors, motion detectors, pressure sensors, and acoustic devices. AUVs can help compile and transmit this data back to the command center, where it can be analyzed and used for decision-making.
- **Remote Locations**: Certain areas may be too dangerous for humans to reach, such as locations where the water is contaminated or the risk of structural collapse is high. AUVs can navigate these hazardous zones, ensuring that vital data from these hard-to-reach locations is still collected and communicated back to the rescue teams.

## 5.4 Enhancing Safety and Speed of Rescue Operations

The primary advantage of integrating AUVs into underwater rescue missions is their ability to reduce the need for human intervention in dangerous environments, thus significantly improving the safety of rescue operations [37].

- **Minimized Human Exposure to Danger:** By utilizing AUVs to perform tasks like sensor deployment, environmental surveying, and data collection, human rescuers are kept out of harm's way. In the event of a submerged or unstable building, for example, AUVs can inspect the structure before humans enter, alerting teams to potential risks such as collapse, submerged electrical hazards, or hazardous materials.

- **Faster Data Collection and Analysis:** AUVs can operate around the clock, providing continuous data collection without the need for rest or recovery. This constant flow of real-time information allows for faster analysis by the command center, which can then deploy rescue teams more effectively based on the most current information.
- **Increased Operational Efficiency:** The autonomous nature of AUVs allows them to work efficiently in hazardous areas that would be difficult or dangerous for humans to access. As a result, they can cover a larger area in a shorter amount of time, thereby improving the overall efficiency of the rescue mission.

## 5.5 Command Center

The Command Center serves as the central hub in any underwater rescue operation, especially in flood-affected areas [38]. It is where data from various sources such as sensor networks, Autonomous Underwater Vehicles (AUVs), and rescue robots is aggregated, analyzed, and utilized to coordinate all rescue efforts. Equipped with advanced data analysis, visualization tools, and real-time communication systems, the command center plays a crucial role in ensuring that rescue operations are carried out effectively, efficiently, and with minimal risk to human personnel.

The command center's core function is to act as the decision-making and operational nerve center for the entire rescue mission. It not only monitors the ongoing situation in real-time but also provides critical insights into flood dynamics, victim location, and environmental hazards. The integration of real-time data feeds, predictive algorithms, and machine learning models empowers the command center to make informed decisions that can significantly impact the outcome of the rescue operation.

**Key Functions of the Command Center**

1. **Real-time Monitoring**

The command center provides continuous monitoring of the situation, keeping track of real-time updates from all deployed sensor nodes, AUVs, and other environmental monitoring devices [39]. Real-time data includes information such as:

- **Water depth:** Monitoring the changing levels of floodwaters to assess flood dynamics.
- **Current speeds:** Tracking the velocity of moving water, which helps determine areas that may be at greater risk or harder to reach.
- **Temperature and environmental data:** Keeping an eye on water temperatures, humidity, and environmental conditions that could impact both rescuers and survivors.
- **Motion and detection of distress signals:** Identifying the movement of victims, or tracking distress signals from survivors using acoustic or motion sensors.

The continuous monitoring of these parameters allows operators to stay updated on the status of the operation and adapt quickly to changing conditions. Operators can pinpoint high-risk areas where immediate rescue actions are necessary, adjusting strategies in real-time based on the most current data.

2. **Data Analysis**

The command center is equipped with powerful data processing and analysis tools. As data is collected by the sensor network, it undergoes real-time processing to detect patterns, trends, and anomalies. This analysis helps in making crucial decisions regarding rescue operations. Key aspects of data analysis include:

- **Water dynamics analysis:** Real-time monitoring of water flow, depth, and temperature helps in predicting potential hazards such as water surges, submerged structures, or blocked pathways.
- **Survivor detection:** Data from acoustic sensors and motion detectors can be analyzed to locate the position of survivors. Machine learning algorithms can be used to predict areas where people are likely to be trapped based on sensor data patterns.
- **Trend identification:** Continuous analysis of environmental data helps identify trends such as rising water levels or increasing current speeds. By tracking these trends, the command center can forecast future conditions, which aids in planning rescue operations.
- **Predictive algorithms:** Advanced algorithms, including machine learning models, can be deployed to anticipate dangerous conditions, such as the likelihood of floodwaters reaching certain critical areas or predicting the movement of survivors in the water. Predictive models can also assist in estimating the best time window for rescue missions, taking into account factors such as weather forecasts and water flow patterns.

Data analysis not only assists in identifying immediate risks but also helps the command center anticipate future challenges, allowing the rescue teams to stay one step ahead in the mission.

### 3. Mission Coordination

The command center coordinates all aspects of the rescue mission based on the analysis of incoming data. The center's operational responsibility includes the strategic allocation of resources and deployment of rescue teams to the most critical areas. Key functions related to mission coordination include:

- **Resource Allocation:** Based on the data received from sensors and AUVs, the command center makes real-time decisions on the allocation of rescue teams and equipment. This involves directing personnel to areas with the highest likelihood of finding survivors, focusing on zones with the most urgent needs, or clearing paths that are obstructed by debris.
- **Team Deployment:** The command center oversees the deployment of human rescuers, drones, and AUVs. By continuously analyzing environmental data, the center can ensure that rescue teams are deployed to areas that are not only most likely to have survivors but also those that are safe from imminent threats (e.g., rising water levels or debris).
- **Directing AUVs and Robots:** The command center can communicate directly with AUVs and other autonomous robots, providing them with new tasks or directing them to specific areas that require attention. For example, it can instruct AUVs to survey flooded structures, deploy additional sensors, or retrieve data from malfunctioning sensor nodes.
- **Real-time Communication:** The command center maintains communication with all deployed teams whether they are human rescuers in boats or underwater, or autonomous vehicles. This ensures that all units are working toward the same objectives, with the latest information available at every step.

Mission coordination ensures that rescue efforts are not only efficient but also optimized for the most critical needs of the situation, maximizing the chances of saving lives.

### 4. Situational Awareness

Situational awareness is the ability to understand and interpret the environment in which rescue operations are unfolding. The command center is tasked with integrating and analyzing a variety of data sources to maintain a comprehensive understanding of the situation at all times. Key aspects of situational awareness include:

- **Environmental Mapping:** The integration of real-time data from AUVs, sensors, and rescue robots allows the command center to create detailed environmental maps. These maps can highlight flooded zones, submerged infrastructure, potential obstacles, and the locations of survivors.
- **Continuous Data Integration:** Data from sensor nodes, AUVs, motion sensors, and cameras are continuously integrated and updated. This creates a dynamic picture of the operational environment, with situational changes being detected and responded to quickly.
- **Risk Assessment:** The command center assesses the risks posed to both rescuers and survivors based on real-time environmental data. It can evaluate factors such as water current strength, the stability of submerged structures, the likelihood of water surges, and more. This real-time analysis helps make critical safety decisions for human rescuers and assets.

Effective situational awareness helps operators make the right decisions quickly, ensuring the safety of rescuers, optimizing resource deployment, and improving the chances of successful rescues.

## 6. Applications of WSNs in Underwater Rescue Management

WSNs have found critical applications in underwater rescue management, especially in flood-affected areas where traditional rescue methods are often inefficient, dangerous, or impractical. By providing real-time monitoring, hazard detection, and enhanced situational awareness, WSNs enable rescue teams to work more efficiently, safely, and effectively [40]. Below are key applications of WSNs in underwater rescue operations:

### 6.1 Search and Rescue Operations

Search and rescue (SAR) operations in flooded areas face significant challenges due to poor visibility, strong currents, and the vast coverage area often involved. Traditional methods often require human rescuers to manually search through these conditions, which is both time-consuming and risky. WSNs, however, can significantly enhance the efficiency and effectiveness of these operations by:

- **Continuous Monitoring of Target Areas:** WSNs can be deployed in areas with high chances of containing trapped victims, such as buildings, submerged vehicles, or narrow water channels. The sensor nodes collect real-time data on environmental conditions and movement within these zones, alerting rescuers to potential locations where survivors may be found.
- **Data Analysis for Victim Localization:** Data collected from sensors, such as acoustic sensors, motion detectors, and temperature sensors, can be analyzed to identify areas of high activity or distress signals, helping to pinpoint the exact locations of victims. By combining this data with known flood patterns and environmental conditions, WSNs provide valuable insights that assist rescue teams in narrowing down search areas.
- **Reduced Search Time:** By focusing efforts on the most likely victim locations identified through sensor data, SAR teams can reduce the overall search time, allowing for faster rescues and more lives saved.

### 6.2 Hazard Monitoring and Risk Assessment

Flooded areas pose numerous risks, including the collapse of infrastructure, underwater currents, hazardous debris, and toxic chemical exposure. The dynamic and unpredictable nature of floodwaters makes real-time hazard monitoring essential for ensuring the safety of both victims and rescue teams. WSNs contribute to hazard monitoring and risk assessment in the following ways:

- **Continuous Hazard Detection:** WSNs can be equipped with a range of sensors (e.g., pressure, motion, and temperature sensors) to monitor environmental conditions, such as changes in water pressure,

water flow velocity, and the presence of submerged obstacles. These sensors can detect dangerous fluctuations in water levels or fast-moving currents that might pose risks to rescuers or survivors.

- **Structural Integrity Monitoring:** In flood situations, the risk of infrastructure collapse such as the failure of bridges, dams, or buildings increases significantly. WSNs can be used to assess the structural health of critical infrastructure by deploying sensors that monitor for signs of stress, cracks, or material failure. These sensors can detect minute changes in the structure that may signal imminent collapse, enabling the command center to prioritize rescue efforts based on the structural integrity of various areas.

- **Early Warning Systems:** By integrating data from multiple sensors, WSNs can identify emerging hazards and provide early warnings to rescuers, enabling them to take appropriate actions before a situation becomes life-threatening. For example, if an underwater sensor detects unusual pressure shifts indicating the potential collapse of a building, the system can alert nearby rescue teams to evacuate or avoid certain zones.

### 6.3 Environment and Infrastructure Monitoring

The environmental impact of floods extends beyond the immediate threat to human lives. Floodwaters can cause significant damage to infrastructure, leading to long-term complications for recovery efforts. WSNs can be applied to monitor both environmental conditions and the health of key infrastructure in flooded areas. Some specific use cases include:

- **Monitoring Flooded Infrastructure:** Many critical infrastructures, such as bridges, dams, and power stations, are vulnerable to damage during floods. WSNs can be used to assess the structural integrity of these facilities by deploying sensors that monitor vibrations, stress, and strain on the structures. This helps determine which structures are safe to access and which ones pose a significant risk of collapse.

- **Environmental Data Collection:** WSNs can also gather important environmental data, such as water quality, temperature, and pH levels. This data helps rescue teams assess whether floodwaters are contaminated with hazardous chemicals or pollutants, and it can inform decisions about when and where to deploy human rescuers to reduce exposure to dangerous substances.

- **Waterway Monitoring:** In addition to monitoring infrastructure, WSNs can track water levels in rivers, reservoirs, and canals. By tracking changes in water flow and predicting potential floods or breaches, WSNs provide early warnings to communities and rescue teams. They also allow for the real-time mapping of submerged areas, which is useful for planning rescue routes and identifying accessible paths for evacuation**.**

### 6.4 Victim Tracking and Localization

One of the most challenging aspects of underwater rescue in flooded areas is locating and tracking victims who may be trapped or displaced by the rising waters. WSNs, with their network of sensors, provide an innovative solution to this problem by offering a means to track victims in submerged environments, even under low-visibility conditions.

- **Acoustic Sensors for Victim Detection:** Acoustic sensors embedded in the WSN can detect underwater sounds, such as the voices of trapped victims or distress signals. By analyzing the frequency and intensity of these signals, the system can triangulate the victim's position, even in areas where visibility is near zero.

- **Motion Sensors for Victim Movement Tracking:** Motion sensors, including accelerometers and gyros, can detect the movement of people or objects in the water. These sensors help in tracking the

location and movement of victims, particularly those who may be swept away by currents or displaced to different parts of the flooded area. The system can send real-time alerts to rescuers, guiding them to the exact location of the victim.

- **Enhanced Localization with GPS and Sensor Fusion:** In some cases, a combination of GPS, sonar, and motion sensors can provide highly accurate location data for victims. For example, WSNs equipped with GPS receivers can provide rescuers with precise coordinates, while sonar systems can detect objects or individuals in deeper, murkier waters. Sensor fusion techniques can combine multiple sources of data to pinpoint victim locations with greater accuracy, even in challenging environments.

- **Zero-Visibility Operations:** One of the key advantages of using WSNs for victim tracking is the ability to operate in zero-visibility conditions, which are common in flood situations. Unlike visual-based technologies, acoustic and motion-based sensors can function effectively underwater, allowing rescuers to locate victims even when visibility is severely limited by murky water or debris.

## 7. Communication Challenges in Underwater WSNs

While WSNs hold significant potential for underwater rescue management, their implementation in flooded or submerged environments is fraught with several challenges [41]. These challenges stem from the unique characteristics of underwater communication, which differ significantly from terrestrial environments [42-44]. Below are some of the most critical communication challenges faced by underwater WSNs:

### 7.1 Signal Propagation

One of the most significant challenges in underwater communication is signal propagation. Unlike air or land, water is a highly attenuating medium for most types of wireless signals. Here are some key issues:

- **Attenuation of Radio Waves:** In underwater environments, radio waves (used in traditional wireless communication systems) are absorbed and scattered quickly by water, especially at greater depths. This leads to a sharp decline in signal strength, limiting the range and effectiveness of traditional wireless communication methods like radio frequency (RF) signals.

- **Optical Signal Limitations:** Optical signals (e.g., light) also face substantial attenuation in water, especially as water turbidity and particulates increase. Light-based communication methods, such as visible light communication (VLC), offer high bandwidth but suffer from significant limitations in terms of range and reliability in murky or deeper waters.

- **Acoustic Communication**: To overcome the attenuation problem, acoustic signals are commonly used in underwater WSNs. While acoustic communication is effective over longer distances compared to radio and optical methods, it comes with its own set of challenges:

    - **Noise Interference:** Underwater environments often have significant background noise, including natural sources like waves, marine life, and water currents, as well as artificial sources such as ships and underwater equipment. This noise can interfere with signal transmission, leading to reduced communication quality and data loss.

    - **Limited Bandwidth:** Acoustic communication typically offers lower bandwidth compared to RF or optical signals. This constraint makes it difficult to transmit large volumes of data quickly and can result in delays in real-time communication and monitoring.

Due to these challenges, underwater communication systems must use specialized protocols designed to handle signal degradation, noise, and bandwidth limitations while maximizing reliability.

## 7.2 Network Topology

The dynamic nature of underwater environments poses significant challenges for maintaining a stable network topology:

- **Fluid and Changing Terrain:** Flooded areas are constantly changing due to water currents, rising or falling water levels, and shifting debris. This makes the static placement of sensor nodes or communication devices problematic. For instance, sensor nodes deployed on the seafloor may shift due to strong currents or be buried under sediment, leading to network instability and gaps in coverage.

- **Node Failures:** Underwater networks are also subject to frequent node failures due to physical factors:

    - **Corrosion:** The harsh underwater environment accelerates corrosion in electronic components, especially for nodes left deployed for extended periods.

    - **Damage from Debris:** Floating or submerged debris in floodwaters can physically damage sensor nodes, causing them to fail or become inactive.

    - **Battery Depletion:** The limited lifespan of batteries on sensor nodes poses a significant issue for long-term missions. Once the battery is depleted, the node stops functioning, which may lead to gaps in data collection or loss of critical information.

These dynamic and often unpredictable environmental factors necessitate adaptive network topologies that can reconfigure as needed, ensuring continuous coverage and communication. This could involve the use of mobile sensor nodes, autonomous underwater vehicles (AUVs), or multi-hop communication systems that adapt to changing conditions.

## 7.3 Energy Efficiency

In underwater WSNs, energy efficiency is a crucial concern. Most sensor nodes are battery-powered, and long-term operations in submerged environments exacerbate the challenge of maintaining power. Several factors contribute to the energy efficiency challenge:

- **Limited Battery Life:** The batteries in sensor nodes are typically small, and their capacity is limited. Given the need for continuous monitoring and transmission of data in underwater rescue operations, the energy consumption of these devices must be carefully managed.

- **Continuous Data Transmission:** Sensor nodes in underwater environments must often transmit data continuously to a central processing unit or command center for real-time analysis. However, maintaining a constant data transmission rate significantly drains the battery, especially when using energy-intensive acoustic communication.

To address these challenges, energy-efficient algorithms and power management strategies are essential:

- **Data Compression:** Algorithms that compress data before transmission can help reduce the amount of energy consumed during communication by reducing the data size.

- **Duty Cycling:** By implementing duty cycling, where nodes operate in periodic active and sleep cycles, energy consumption can be reduced. Nodes only transmit or collect data at specific intervals, which extends battery life.

- **Energy Harvesting:** In some cases, the use of energy harvesting techniques, such as converting the movement of water or using solar panels (for surface-based sensors), can help recharge sensor batteries, prolonging network lifetime.

Balancing the trade-off between power consumption and data transmission requirements is critical for maintaining operational efficiency in underwater WSNs.

### 7.4 Real-Time Data Processing

Underwater rescue operations require real-time data processing for effective decision-making. However, several factors hinder the speed and efficiency of data processing in WSNs deployed in underwater environments:

- **Limited Computational Resources on Sensor Nodes:** Sensor nodes in underwater WSNs are typically small, lightweight, and low-cost devices, meaning they often have limited processing power and memory. This limitation restricts their ability to process large volumes of data locally and perform complex computations, such as image processing or machine learning tasks.
- **Communication Delays:** Due to the challenges of underwater communication, including signal attenuation and noise interference, there can be significant delays in transmitting data to a central processing unit (e.g., a command center). This results in latency, which can be detrimental in high-stakes rescue operations where timely responses are critical.
- **Data Fusion and Aggregation:** In many underwater rescue scenarios, multiple sensors (acoustic, pressure, motion, etc.) are deployed to gather data. The challenge here lies in data fusion—the process of combining data from multiple sensors to form a comprehensive picture of the underwater environment. This requires both significant processing power and bandwidth, which may be difficult to achieve under the constraints of underwater WSNs.

To overcome these issues, some strategies can be employed:

- **Edge Computing:** Performing data processing at the sensor node or close to the data source can reduce the amount of raw data that needs to be transmitted, thus reducing communication delays and conserving bandwidth.
- **Collaborative Processing:** Some WSNs use a distributed approach where nodes collaborate and share their processing tasks, allowing for more efficient data aggregation and decision-making without overloading any single node.
- **Efficient Communication Protocols:** Using specialized communication protocols designed to reduce latency and optimize bandwidth usage is essential. Protocols like Delay-Tolerant Networks (DTNs) or low-power wide-area networks (LPWANs) are examples of systems that can handle intermittent connectivity and long-range data transmission more efficiently.

## 8. Technologies and Solutions for Improving WSNs in Underwater Rescue

Underwater WSNs have vast potential in improving the efficiency and effectiveness of rescue operations in flooded or submerged environments [45]. However, to overcome the numerous challenges inherent to underwater conditions, several innovative technologies and solutions can be employed to enhance their performance. Below are key approaches that can improve the capabilities of WSNs for underwater rescue management:

### 8.1 Hybrid Communication Approaches

One of the most significant challenges in underwater WSNs is the limited range and reliability of communication due to the unique properties of water [46]. As discussed earlier, acoustic communication is the most commonly used method, but it suffers from limitations like noise interference, signal attenuation, and low

bandwidth. Combining acoustic communication with other techniques such as optical communication or magnetic induction can help mitigate these issues and improve communication reliability.

- **Acoustic-Optical Hybrid Systems:** Optical communication, though limited in range, offers high bandwidth and can be effective in clear, shallow waters. By integrating optical communication for short-range high-bandwidth data transfer and using acoustic communication for long-range, low-bandwidth transmission, a hybrid system can provide more robust and reliable communication.
- **Magnetic Induction:** Magnetic induction-based communication is another promising alternative, especially for short-range, high-reliability communication in underwater WSNs. It is less affected by water turbidity and can be used in environments where acoustic signals may not be viable.
- **Adaptive Switching:** Hybrid systems can incorporate adaptive switching mechanisms where the communication system dynamically selects the best communication mode based on the environmental conditions (e.g., choosing optical communication when water clarity allows, and switching to acoustic communication in murkier waters).

By integrating multiple communication modalities, WSNs can ensure a more reliable and efficient communication network, enhancing the overall robustness of the system in real-time rescue operations.

## 8.2 Distributed Data Processing

In underwater WSNs, data transmission to a centralized command unit can be delayed due to factors like signal degradation, long transmission distances, and network congestion [47]. To mitigate these issues and enable quicker decision-making, distributed data processing is a promising solution.

- **Edge Computing:** Instead of sending raw data to a central processor, sensor nodes can process data locally through edge computing techniques. By filtering and aggregating data at the node level, only relevant information is transmitted, reducing the amount of data sent over the network and lowering the associated communication overhead.
- **Data Fusion on the Node Level:** Sensor nodes can also use data fusion techniques, where information from multiple sensors is combined at the local node level to create more accurate and meaningful results. This reduces latency and allows for faster local decision-making.
- **Decentralized Decision-Making:** In cases of network failure or if the command center is unreachable due to environmental factors, distributed processing enables sensor nodes to make autonomous decisions based on local data. This is particularly valuable in real-time rescue operations, where quick responses are critical.

By decentralizing data processing, WSNs can operate more efficiently, reducing response times and enhancing the effectiveness of rescue operations, especially in large, dynamic environments like flooded areas.

## 8.3 Energy Harvesting Techniques

One of the major challenges for underwater WSNs is the limited battery life of sensor nodes, which significantly impacts long-term operations [48]. Energy harvesting techniques provide a sustainable solution by utilizing ambient energy sources to power sensor nodes, reducing the reliance on traditional battery replacements.

- **Solar Energy:** For nodes placed near the water's surface or in shallow, clear waters, solar energy harvesting can be effective. Solar-powered sensors can recharge their batteries during the day, reducing the need for frequent manual interventions. However, solar energy is less effective in deep or murky waters.

- **Thermal Energy:** Thermoelectric generators can harvest energy from temperature differences between the water and the surroundings. This can be particularly useful in deep-sea or underwater environments, where there is a consistent thermal gradient between the ocean's cold depths and warmer surface waters.
- **Kinetic Energy:** Piezoelectric or electromagnetic harvesting methods can capture energy from water movement, such as tides, waves, or currents. Sensors can be designed to convert mechanical energy from water motion into electrical power, thus prolonging their operational lifetime.

Energy harvesting can significantly reduce the logistical burden of replacing or recharging batteries in underwater networks, enabling more prolonged and sustainable underwater rescue operations.

### 8.4 Advanced Localization Techniques

Accurately localizing victims and rescuers in submerged environments with low visibility or rapidly changing conditions is one of the most challenging aspects of underwater rescue operations [49]. Advanced localization techniques, combined with machine learning algorithms, can significantly improve the tracking and positioning of both victims and rescue teams.

- **Acoustic Localization:** By using arrays of acoustic sensors, it is possible to triangulate the position of individuals or objects underwater. Advanced signal processing and multi-sensor fusion can improve the accuracy of this method, even in environments with high background noise.
- **Sonar-Based Imaging:** Combining sonar systems with localization algorithms allows rescuers to create real-time maps of the underwater environment. By analyzing sonar data, WSNs can offer detailed, real-time imagery of submerged objects or victims, even in zero-visibility conditions.
- **Machine Learning for Enhanced Localization:** Machine learning (ML) [50] and artificial intelligence (AI) [51] can be employed to enhance localization accuracy. By training models on sensor data from different environmental conditions, ML algorithms can predict the most likely locations of victims or rescuers based on historical data, current conditions, and sensor inputs.

By integrating multiple data sources and advanced computational techniques, WSNs can achieve highly accurate and reliable localization in complex, underwater rescue scenarios.

### 8.5 Robust Sensor Design

Given the harsh and demanding environment in which underwater WSNs operate, the design of the sensors themselves must be tailored to withstand extreme conditions. A robust sensor design ensures long-term operational capability in submerged environments, enhancing the reliability of the entire system.

- **Corrosion-Resistant Materials:** Sensors should be constructed with corrosion-resistant materials such as titanium, ceramics, or specially treated metals. This ensures that sensors can survive prolonged exposure to saltwater and other corrosive substances, reducing the need for frequent maintenance or replacement.
- **Pressure-Resistant Housing:** Sensors must be designed to withstand the high-pressure conditions encountered at significant depths. This requires durable, pressure-sealed casings that protect the internal electronics while maintaining sensor performance.
- **Durability against Debris and Sedimentation:** The harsh underwater environment may contain floating debris or silt that can physically damage or obstruct sensor nodes. By using shock-resistant and debris-resistant designs, sensor nodes can continue to function effectively even in turbulent waters or when submerged in sediment-heavy environments.

- **Self-Diagnostics and Self-Healing:** Advanced sensor designs can incorporate self-diagnostics and self-healing capabilities. For instance, sensors may be able to detect malfunctioning components and automatically recalibrate or reroute data to maintain system functionality.

A robust sensor design ensures that WSNs can operate effectively in the challenging conditions of flooded or submerged environments, increasing the reliability and longevity of the entire system.

## 9. Conclusion

Underwater rescue management in flooded areas presents a significant challenge, but the application of WSNs offers promising solutions. By leveraging real-time data collection, efficient communication, and advanced sensor technologies, WSNs can vastly improve the efficiency, safety, and success of search and rescue operations in such environments. However, challenges related to signal propagation, energy efficiency, and data processing need to be addressed through advanced technologies and strategic deployment. Future research should focus on overcoming these challenges to make WSNs an integral part of disaster response in flood-affected areas. By combining WSNs with other emerging technologies like robotics, AI, and machine learning, the potential for underwater rescue operations will continue to expand, ultimately saving more lives and reducing the impact of floods on affected communities.

## References


1. Alexander, David. *Natural disasters*. Routledge, 2018.
2. Jonkman, Sebastiaan N. "Global perspectives on loss of human life caused by floods." *Natural hazards* 34, no. 2 (2005): 151-175.
3. Hasan, Md Munirul, Md Arafatur Rahman, Arya Sedigh, Ana U. Khasanah, A. Taufiq Asyhari, Hai Tao, and Suraya Abu Bakar. "Search and rescue operation in flooded areas: A survey on emerging sensor networking-enabled IoT-oriented technologies and applications." *Cognitive Systems Research* 67 (2021): 104-123.
4. Aziz, Nor Azlina Ab, and Kamarulzaman Ab Aziz. "Managing disaster with wireless sensor networks." In *13th international conference on advanced communication technology (ICACT2011)*, pp. 202-207. IEEE, 2011.
5. Alexander, Chizhov, and Karakozov Andrey. "Wireless sensor networks for indoor search and rescue operations." *International Journal of Open Information Technologies* 5, no. 2 (2017): 1-4.
6. Wu, Huafeng, Jun Wang, Raghavendra Rao Ananta, Vamsee Reddy Kommareddy, Rui Wang, and Prasant Mohapatra. "Prediction based opportunistic routing for maritime search and rescue wireless sensor network." *Journal of Parallel and Distributed Computing* 111 (2018): 56-64.
7. Goudarzi, Shidrokh, Seyed Ahmad Soleymani, Mohammad Hossein Anisi, Domenico Ciuonzo, Nazri Kama, Salwani Abdullah, Mohammad Abdollahi Azgomi, Zenon Chaczko, and Azri Azmi. "Real-time and intelligent flood forecasting using UAV-assisted wireless sensor network." *Computers, Materials and Continua* 70, no. 1 (2021): 715-738.
8. Lu, Mingxiao, Xiaoguang Zhao, and Yikun Huang. "Fast localization for emergency monitoring and rescue in disaster scenarios based on WSN." In *2016 14th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, pp. 1-6. IEEE, 2016.
9. Pant, Diwaker, Sandeep Verma, and Piyush Dhuliya. "A study on disaster detection and management using WSN in Himalayan region of Uttarakhand." In *2017 3rd International conference on advances in computing, communication & automation (ICACCA)(Fall)*, pp. 1-6. IEEE, 2017.
10. Hasan, Md Munirul, Md Arafatur Rahman, Arya Sedigh, Ana U. Khasanah, A. Taufiq Asyhari, Hai Tao, and Suraya Abu Bakar. "Search and rescue operation in flooded areas: A survey on emerging sensor networking-enabled IoT-oriented technologies and applications." *Cognitive Systems Research* 67 (2021): 104-123.
11. Bhatt, Harshil, G. Pranesh, Samarth Shankar, and Shriyash Haralikar. "Wireless Sensor Networks for Optimisation of Search and Rescue Management in Floods." In *2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pp. 1-6. IEEE, 2021.

12. Jorge, Vitor AM, Roger Granada, Renan G. Maidana, Darlan A. Jurak, Guilherme Heck, Alvaro PF Negreiros, Davi H. Dos Santos, Luiz MG Gonçalves, and Alexandre M. Amory. "A survey on unmanned surface vehicles for disaster robotics: Main challenges and directions." *Sensors* 19, no. 3 (2019): 702.
13. Prasad, Devendra, Afshan Hassan, Deepak Kumar Verma, Pradeepta Sarangi, and Sunny Singh. "Disaster management system using wireless sensor network: A review." In *2021 International Conference on Computational Intelligence and Computing Applications (ICCICA)*, pp. 1-6. IEEE, 2021.
14. Lu, Mingxiao, Xiaoguang Zhao, and Yikun Huang. "Fast localization for emergency monitoring and rescue in disaster scenarios based on WSN." In *2016 14th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, pp. 1-6. IEEE, 2016.
15. Seba, Abderazek, Nadia Nouali-Taboudjemat, Nadjib Badache, and Hamida Seba. "A review on security challenges of wireless communications in disaster emergency response and crisis management situations." *Journal of Network and Computer Applications* 126 (2019): 150-161.
16. Ali, Ahmad, Yu Ming, Sagnik Chakraborty, and Saima Iram. "A comprehensive survey on real-time applications of WSN." *Future internet* 9, no. 4 (2017): 77.
17. Wibisono, Arif, Md Jalil Piran, Hyoung-Kyu Song, and Byung Moo Lee. "A survey on unmanned underwater vehicles: Challenges, enabling technologies, and future research directions." *Sensors* 23, no. 17 (2023): 7321.
18. Larios, Diego Francisco, Julio Barbancho, Gustavo Rodríguez, José Luis Sevillano, Francisco Javier Molina, and Carlos León. "Energy efficient wireless sensor network communications based on computational intelligent data fusion for environmental monitoring." *IET communications* 6, no. 14 (2012): 2189-2197.
19. Li, Wei, Flávia C. Delicato, Paulo F. Pires, Young Choon Lee, Albert Y. Zomaya, Claudio Miceli, and Luci Pirmez. "Efficient allocation of resources in multiple heterogeneous wireless sensor networks." *Journal of Parallel and Distributed Computing* 74, no. 1 (2014): 1775-1788.
20. Balestrieri, Eulalia, Pasquale Daponte, Luca De Vito, and Francesco Lamonaca. "Sensors and measurements for unmanned systems: An overview." *Sensors* 21, no. 4 (2021): 1518.
21. Lim, Cheng Leong, Cindy Goh, and Yun Li. "Long-term routing stability of wireless sensor networks in a real-world environment." *IEEE Access* 7 (2019): 74351-74360.
22. Anuradha, Durairaj, Neelakandan Subramani, Osamah Ibrahim Khalaf, Youseef Alotaibi, Saleh Alghamdi, and Manjula Rajagopal. "Chaotic search-and-rescue-optimization-based multi-hop data transmission protocol for underwater wireless sensor networks." *Sensors* 22, no. 8 (2022): 2867.
23. Chaudhary, Monika, Nitin Goyal, Abderrahim Benslimane, Lalit Kumar Awasthi, Ayed Alwadain, and Aman Singh. "Underwater wireless sensor networks: Enabling technologies for node deployment and data collection challenges." *IEEE Internet of Things Journal* 10, no. 4 (2022): 3500-3524.
24. Murad, Mohsin, Adil A. Sheikh, Muhammad Asif Manzoor, Emad Felemban, and Saad Qaisar. "A survey on current underwater acoustic sensor network applications." *International Journal of Computer Theory and Engineering* 7, no. 1 (2015): 51.
25. Khasawneh, Ahmad, Muhammad Shafie Bin Abd Latiff, Hassan Chizari, MoeenUddin Tariq, and Abdullah Bamatraf. "Pressure based routing protocol for underwater wireless sensor networks: A survey." *KSII Transactions on Internet and Information Systems (TIIS)* 9, no. 2 (2015): 504-527.
26. Barroca, Norberto, Luís M. Borges, Fernando J. Velez, Filipe Monteiro, Marcin Górski, and João Castro-Gomes. "Wireless sensor networks for temperature and humidity monitoring within concrete structures." *Construction and Building materials* 40 (2013): 1156-1166.
27. Song, Byunghun, Haksoo Choi, and Hyung Su Lee. "Surveillance tracking system using passive infrared motion sensors in wireless sensor network." In *2008 International Conference on Information Networking*, pp. 1-5. IEEE, 2008.
28. Zhu, Chunsheng, Hai Wang, Xiulong Liu, Lei Shu, Laurence T. Yang, and Victor CM Leung. "A novel sensory data processing framework to integrate sensor networks with mobile cloud." *IEEE Systems Journal* 10, no. 3 (2014): 1125-1136.
29. Nazir, Mohsin, Aneeqa Sabah, Sana Sarwar, Azeema Yaseen, and Anca Jurcut. "Power and resource allocation in wireless communication network." *Wireless Personal Communications* 119, no. 4 (2021): 3529-3552.
30. Zhang, Jingbin, Zhanxiang Huang, and Xinyu Liu. "Acoustic communication in wireless sensor networks." *CS651, Wireless Sensor Networks* (2005): 1-8.

31. Zungeru, Adamu Murtala, Li-Minn Ang, S. R. S. Prabaharan, and Kah Phooi Seng. "Radio frequency energy harvesting and management for wireless sensor networks." *Green mobile devices and networks: Energy optimization and scavenging techniques* 13 (2012): 341-368.
32. Bogue, Robert. "Underwater robots: a review of technologies and applications." *Industrial Robot: An International Journal* 42, no. 3 (2015): 186-191.
33. Sánchez, Pedro José Bernalte, Mayorkinos Papaelias, and Fausto Pedro García Márquez. "Autonomous underwater vehicles: Instrumentation and measurements." *IEEE Instrumentation & Measurement Magazine* 23, no. 2 (2020): 105-114.
34. Sahoo, Sushil Kumar, Bibhuti Bhusan Choudhury, and Prasant Ranjan Dhal. "Exploring the Role of Robotics in Maritime Technology: Innovations, Challenges, and Future Prospects." *Spectrum of Mechanical Engineering and Operational Research* 1, no. 1 (2024): 159-176.
35. Hyakudome, Tadahiro, Satoshi Tsukioka, Hiroshi Yoshida, Takao Sawa, Shojiro Ishibashi, Akihisa Ishikawa, Junya Ishiwata, Kojiro Watanabe, Masahiko Nakamura, and Taro Aoki. "Autonomous underwater vehicle for surveying deep ocean." In *2009 IEEE International Conference on Industrial Technology*, pp. 1-6. IEEE, 2009.
36. Rodríguez-Molina, Jesús, Sonia Bilbao, Belén Martínez, Mirgita Frasheri, and Baran Cürüklü. "An optimized, data distribution service-based solution for reliable data exchange among autonomous underwater vehicles." *Sensors* 17, no. 8 (2017): 1802.
37. Murphy, A. J., M. J. Landamore, and R. W. Birmingham. "The role of autonomous underwater vehicles for marine search and rescue operations." *Underwater Technology* 27, no. 4 (2008): 195-205.
38. Li, Shen, Andong Zhan, Xiaobing Wu, Panlong Yang, and Guihai Chen. "Efficient Emergency Rescue Navigation with Wireless Sensor Networks." *J. Inf. Sci. Eng.* 27, no. 1 (2011): 51-64.
39. Kondakci, Suleyman, Gökhan Yilmaz, Emre Kocabiyik, Fethican Coskuner, Alper Akçöltekin, and M. Serhat Yüksel. "Ubiquitous monitoring system for critical rescue operations." In *2010 6th International Conference on Wireless and Mobile Communications*, pp. 515-520. IEEE, 2010.
40. Felemban, Emad, Faisal Karim Shaikh, Umair Mujtaba Qureshi, Adil A. Sheikh, and Saad Bin Qaisar. "Underwater sensor network applications: A comprehensive survey." *International Journal of Distributed Sensor Networks* 11, no. 11 (2015): 896832.
41. Awan, Khalid Mahmood, Peer Azmat Shah, Khalid Iqbal, Saira Gillani, Waqas Ahmad, and Yunyoung Nam. "Underwater wireless sensor networks: A review of recent issues and challenges." *Wireless Communications and Mobile Computing* 2019, no. 1 (2019): 6470359.
42. Sandeep, D. N., and Vinay Kumar. "Review on clustering, coverage and connectivity in underwater wireless sensor networks: A communication techniques perspective." *IEEE Access* 5 (2017): 11176-11199.
43. Jindal, Himanshu, Sharad Saxena, and Singara Singh. "Challenges and issues in underwater acoustics sensor networks: A review." In *2014 International Conference on Parallel, Distributed and Grid Computing*, pp. 251-255. IEEE, 2014.
44. Darehshoorzadeh, Amir, and Azzedine Boukerche. "Underwater sensor networks: A new challenge for opportunistic routing protocols." *IEEE Communications Magazine* 53, no. 11 (2015): 98-107.
45. Jouhari, Mohammed, Khalil Ibrahimi, Hamidou Tembine, and Jalel Ben-Othman. "Underwater wireless sensor networks: A survey on enabling technologies, localization protocols, and internet of underwater things." *IEEE Access* 7 (2019): 96879-96899.
46. Gola, Kamal Kumar, and Bhumika Gupta. "Underwater sensor networks:'Comparative analysis on applications, deployment and routing techniques'." *IET Communications* 14, no. 17 (2020): 2859-2870.
47. Wei, Xiaohui, Hao Guo, Xingwang Wang, Xiaonan Wang, and Meikang Qiu. "Reliable data collection techniques in underwater wireless sensor networks: A survey." *IEEE Communications Surveys & Tutorials* 24, no. 1 (2021): 404-431.
48. Alamu, Olumide, Thomas O. Olwal, and Karim Djouani. "Energy harvesting techniques for sustainable underwater wireless communication networks: A review." *e-Prime-Advances in Electrical Engineering, Electronics and Energy* (2023): 100265.
49. Gola, Kamal Kumar, and Shikha Arya. "Underwater acoustic sensor networks: Taxonomy on applications, architectures, localization methods, deployment techniques, routing techniques, and threats: A systematic review." *Concurrency and Computation: Practice and Experience* 35, no. 23 (2023): e7815.
50. Puri, Divyansh, and Bharat Bhushan. "Enhancement of security and energy efficiency in WSNs: Machine Learning to the rescue." In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pp. 120-125. IEEE, 2019.

51. Osamy, Walid, Ahmed M. Khedr, Ahmed Salim, Amal Ibrahim Al Ali, and Ahmed A. El-Sawy. "Coverage, deployment and localization challenges in wireless sensor networks based on artificial intelligence techniques: a review." *IEEE Access* 10 (2022): 30232-30257.

International Journal of Intelligent Communication and Computer Science
Vol. 2, No. 2, 2024, Pages 77-96.

# Leveraging ECG Biometrics for Enhanced Security and Health Monitoring

**Sandeep Tripathi[1] and Rohitashwa Pandey[2]**

[1]Research Scholar, Department of Computer Science and Engineering, Bansal Institute of Engineering and Technology, Lucknow, Affiliated to AKTU, Lucknow
[2]Department of Computer Science and Engineering Bansal Institute of Engineering and Technology, Lucknow,, Affiliated to AKTU, Lucknow

**Review Paper**

Email: sandeeptripathisansoft@gmail.com
Received: 1 Apr 2024, Revised: 11 Sep. 2024 Accepted: 10 Oct 2024

**Abstract:**

Electrocardiogram (ECG) biometrics presents an innovative approach to identity verification and health monitoring, harnessing the unique electrical patterns of individual hearts as a means of authentication. This paper delves into the foundational principles of ECG biometrics, highlighting its distinct advantages over conventional biometric methods such as fingerprints and facial recognition, which can be susceptible to forgery and environmental factors. We provide a comprehensive exploration of the methodology involved in ECG feature extraction, discussing various signal processing techniques that allow for the isolation of key characteristics from ECG waveforms. This includes time-domain analysis, frequency-domain analysis, and advanced techniques such as wavelet transforms, all of which are essential for accurate feature identification. Furthermore, we examine a range of classification algorithms, from traditional machine learning models to cutting-edge deep learning approaches, that are employed to authenticate individuals based on their ECG profiles. The paper also addresses the practical challenges of implementing ECG biometrics in real-world scenarios, including issues related to data privacy, the variability of ECG signals due to factors such as physical condition and electrode placement, and the need for robust security measures to protect sensitive health data. Our findings suggest that ECG biometrics not only significantly enhances security systems by providing a highly reliable and user-friendly authentication method but also contributes to proactive health monitoring by offering insights into cardiovascular health.

**Keywords:** ECG Biometrics, Feature Extraction, Signal Processing, Machine Learning, Classification, Wearable Devices, Health Monitoring, Arrhythmia Detection, Deep Learning, Authentication.

## 1. Introduction

Biometrics has become essential in today's security landscape, offering a reliable and convenient means of identity verification [1]. With traditional methods like passwords and PINs increasingly vulnerable to fraud, biometric technologies such as fingerprints, facial recognition, etc. provide a unique and difficult-to-replicate alternative [2]. These systems enhance security by ensuring only genuine people can access to important and private information while streamlining authentication processes for users [3]. Additionally, biometrics facilitates improved health monitoring, enabling continuous tracking of vital signs and early detection of potential issues [4]. As the digital world

expands, the integration of biometric solutions will play a critical role in enhancing trust and safety across various sectors [5].
As biometric technologies continue to evolve, the requirement of more secure, reliable, and user-friendly identification techniques grows significantly. In an era where data breaches and identity theft are prevalent, organizations and individuals alike seek advanced solutions that not only provide robust security but also enhance the user experience. Traditional biometric modalities have been widely adopted; however, they come with inherent limitations that highlight the need for innovative alternatives [6].

**Limitations of Traditional Biometrics**

1. **Forgibility and Replication**: This is very important and major issue related to the traditional biometric systems [7]. Fingerprint recognition, for example, can be compromised through the use of artificial replicas created from gelatin or silicone. Similarly, anyone can misuse facial recognition systems with photographs or videos, particularly in poorly designed systems that do not incorporate liveness detection measures. This vulnerability raises questions about the reliability of these methods in high-security applications.
2. **Privacy Concerns**: Biometric data is unique to individuals and often considered sensitive information. The collection, storage, and application of such data can result in privacy violations and unauthorized access [8]. Users may be apprehensive about how their biometric information is handled, especially in light of increasing regulatory scrutiny surrounding data privacy. This concern is compounded by the potential for biometric data to be hacked or misused, creating a reluctance to adopt traditional biometric systems.
3. **Environmental Influences**: Environmental factors can significantly impact the performance of traditional biometric systems [9]. For instance, fingerprint readers may struggle to accurately capture prints in dirty or wet conditions, while facial recognition systems can be less effective in low-light scenarios or when the subject is wearing accessories like hats or glasses. Such limitations can hinder the usability and accuracy of these systems in real-world applications.

In this context, ECG biometrics emerges as a promising alternative, leveraging the unique electrical activity of the heart as a means of identification [10]. The heart's electrical signals, captured through an ECG, produce distinct patterns influenced by individual physiological traits. These patterns are not only stable over time but also resistant to external factors, making ECG an attractive option for biometric authentication. Additionally, ECG biometrics offers potential applications in health monitoring, providing insights into an individual's cardiovascular condition while ensuring secure access to sensitive information.
This research article primarily focuses on the methodology of ECG feature extraction, analysing various classification algorithms, and discuss the potential applications and challenges associated with ECG biometrics. This research study aims to present a detailed overview of this innovative field and its implications for future technology in security and healthcare.

## 2. Basic Biometric Systems

Figure 1 shows a basic biometric system. Various stages work together to accurately identify or verify an individual as per their unique physiological or behavioural characteristics [11].
First, the information acquisition step takes place, where a biometric sample (such as a fingerprint, face image, voice recording, or iris scan) is captured using a biometric sensor. This sample can be obtained through various devices such as cameras, fingerprint scanners, or microphones, as per the type of biometric system being used.
After the collection of biometric data, the following step is preprocessing. Preprocessing involves preparing the captured data for feature extraction by enhancing its quality and removing any noise or irrelevant information that may affect the accuracy of the system. This can include steps such as image normalization, noise reduction, and alignment to ensure that the data is in a standard form and is of sufficient quality for analysis.
After preprocessing, the system proceeds with feature extraction. In this stage, distinctive and relevant characteristics or features are identified and extracted from the biometric sample. These features represent the uncommon traits of the person’s biometric data, like the ridges in a fingerprint, the unique patterns in an iris scan, or the frequency patterns in a voice. The goal is of converting the raw biometric data into a compact and informative representation which are then used for comparison and matching.
Next, a biometric template is created. This is a digital reference or signature of the extracted features that serves as a permanent record of the biometric data that is belonged to a particular individual. A secured database is used to store the biometric template, either locally or in a central server, and it serves as the reference point for future identification

or verification tasks. The template is designed to represent the unique characteristics of the individual, making it useful for distinguishing them from others.
In the final step, matching is performed. Here, a matching algorithm is used for comparing the newly captured biometric sample (from the individual attempting to authenticate) with the stored templates. The matching algorithm computes the similarity between the input sample and the stored templates to determine whether they match. In a verification scenario, this step checks if the individual is the real person or not by comparing their input data to a single stored template. In an identification scenario, the system compares the input data to multiple stored templates for correct matching.
If the system finds a match, it confirms the identity of the individual, otherwise, it may reject the sample. The precision and performance of the biometric system highly rely on the quality of the feature extraction, the strength of the matching algorithm, and the precision of the preprocessing steps.

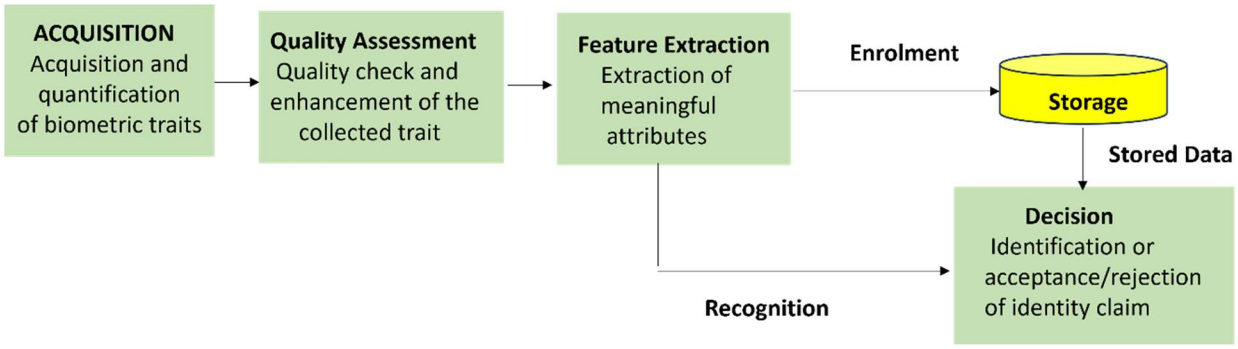


**Figure 1: Block diagram for the Biometric system**

Biometric authentication is classified into two modules which are enrolment and identification module. A sensor is used in the enrolment phase to scan the biometric characteristics for obtaining a digital characteristic. This data is then processed by a feature extractor to optimize the matching process and reduce storage requirements. Then, this processed data is sent a template database. Biometric authentication means verifying a specific person based on unique physiological or behavioural characteristics. As the demand for secure and convenient identification methods grows, various biometric modalities have been developed and deployed across diverse applications.

## 2.1 Behavioural and Physiological Biometrics

Biometrics means the unique physical and behavioural characteristics of a person. These unique features of a person are often used for identification or verification purposes in security systems. Biometrics can be of two main kinds: physiological and behavioural biometrics. Each type relies on different traits and offers distinct advantages and challenges.

### 2.1.1 Physiological Biometrics

Physiological biometrics refers to physical attributes of an individual that are inherent and relatively stable over time. These characteristics are directly linked to the physical body and can often be captured using specialized sensors or imaging technologies.
Most widely used physiological biometrics include:

**a. Fingerprint Recognition**
This is the most commonly used type of recognition system. It has been used in numerous applications for the past many years. It works on the unique patterns of ridges and valleys on the surface of a person's fingers [12]. Each person's fingerprints are distinct, even among identical twins, and they remain stable till person is alive. This type of recognition system records the minutiae (points where ridges end or bifurcate) and use these features to match against stored templates [13]. Fingerprint scanners are very commonly used in mobile devices, law enforcement, and access control systems [14].

**b. Facial Recognition**
This recognition system makes the recognition of a person by using the unique features of an individual's face [15]. Key features analyzed include the gap between eyes, nose shape, jawline, and the overall structure of the face [16]. Modern facial recognition systems use deep learning algorithms to capture and match these features from images or videos [17]. Facial recognition is often used for surveillance, smartphone authentication, and identity verification in airports or public spaces [18].

**c. Iris Recognition**
The coloured part of a person eye is used in this system for recognition. Each person has unique patterns of the iris [19]. It captures high-resolution images of the iris to identify distinctive features such as texture, colour, and patterns [20]. The iris is stable over a person's lifetime and is difficult to alter or forge, making it a reliable method of biometric identification. Iris recognition is commonly used in high-security areas like airports and government buildings [21].

**d. Retina Scan**
A retina scan analyzes the pattern of blood vessels in the retina [22]. This pattern is different in each person, even in twins. Retina scanning is highly accurate and can be used for high-security identification purposes [23]. However, it requires a specialized scanner and may be less convenient than other methods.

**e. Hand Geometry**
Hand geometry recognition captures the shape and size of a person's hand, including finger length, width, and the overall shape of the palm [24]. While hand geometry is not as unique as fingerprints or retina patterns, it offers a relatively easy and non-intrusive method of identification [25]. This method is often used in physical access control systems, such as in secure offices or buildings.

**f. Voice Recognition (Physiological Aspect)**
Voice recognition systems analyse the physical aspects of a person's voice, including pitch, tone, cadence, and the shape of the vocal tract [26]. Although voice recognition is influenced by factors like emotion and health, certain traits remain stable enough to offer reliable identification. Voice-based authentication is often used in mobile devices and call centers [27].

### 2.1.2 Behavioural Biometrics

Behavioural biometrics refer to patterns in the way people act or interact with their environment. Unlike physiological biometrics, which rely on physical traits, behavioural biometrics are dynamic and can change over time depending on context, mood, or physical condition [28]. However, they can provide valuable data for continuous authentication in many applications. Some of the key types of behavioural biometrics include:

**a. Keystroke Dynamics**
In this type of biometric recognition system, the pattern in which a person uses a keyboard for typing is used for recognition [29]. This includes factors such as typing speed, rhythm, pressure on keys, and the time spent between keystrokes (dwell time) [30]. Each individual develops a unique typing pattern, which can be used to authenticate them or detect fraudulent activity. Keystroke dynamics can be integrated into systems as a passive form of authentication, particularly in banking or online security applications [31].

**b. Gait Recognition**
Gait recognition analyzes the way a person walks, including factors like stride length, speed, and the movement of arms and legs [32]. Each person has unique gait and hence it can be used for identification even from a distance or without direct contact. Gait analysis can be captured using video surveillance or specialized sensors and is increasingly used in areas like security monitoring and surveillance [33].

**c. Signature Dynamics**
Signature dynamics focuses on the way a person signs their name. This includes characteristics such as the speed, pressure, and movement patterns during the signature process [34]. Unlike a static image of a signature, dynamic

signature recognition focuses on how the person writes the signature, which remains unique and hard to replicate [35]. This method is often used in banking for check verification and document authentication.

**d. Speech Recognition**
While speech recognition also has a physiological component (voice), it has a significant behavioural aspect, as it involves how a person speaks rather than just what they say [36]. Speech patterns, including cadence, accent, pitch, and even the rhythm of speech, can be unique to an individual. Continuous speech recognition systems can be used for identifying or verifying individuals in phone systems, voice-controlled assistants, and security applications [37].

**e. Mouse Dynamics**
This recognition system uses the way a user interacts with a mouse or touchpad for recognition purpose [38]. This includes speed, movement patterns, pressure, and click habits. Similar to keystroke dynamics, mouse dynamics can serve as a behavioural biometric to authenticate users or track unusual behaviour patterns in applications like online banking, e-commerce, and user verification systems [39].

**f. Eye-Tracking**
Eye-tracking technology analyzes how an individual looks at objects or moves their eyes during a task [40]. It can capture the pattern of eye movements (such as saccades and fixations) and the way a person shifts their gaze. Eye-tracking is often used with various other forms of biometrics for continuous authentication, especially in mobile devices and online systems where users engage in repetitive tasks [41].
A detailed overview of Physiological and Behavioural Biometrics is given in below table.

**Table 1: Comparison of Physiological and Behavioural Biometrics**

| Feature | Physiological Biometrics | Behavioural Biometrics |
|---|---|---|
| **Stability** | Highly stable over time (e.g., fingerprints, iris patterns) | Can change over time or in different conditions (e.g., gait, typing speed) |
| **Uniqueness** | Generally, more unique (e.g., DNA, fingerprint) | Unique but may be influenced by temporary factors (e.g., mood, stress) |
| **User Acceptance** | May require intrusive scanning (e.g., retina scan, fingerprint) | Often less intrusive (e.g., keystroke dynamics, gait recognition) |
| **Use Case** | Identification and verification in high-security environments | Continuous authentication, fraud detection, and behaviour analysis |
| **Security** | High accuracy, difficult to fake | Can be spoofed or imitated under certain circumstances (e.g., imitating signature or voice) |

## 3. Introduction to ECG: Understanding the Basics

Electrocardiography (ECG) is used for assessing the electrical activity of the heart. By capturing the electrical impulses that trigger heartbeats, ECG provides crucial insights into heart function and health [42]. This section will explain how ECG works, outline its key components—the P wave, QRS complex, and T wave—and discuss how these components reflect individual physiological differences.

### 3.1 How ECG Works

An ECG measures the heart's electrical activity with the help of electrodes positioned on the body surface of the person. These electrodes capture the electrical signals produced by the heart as it contracts and relaxes. When the heart beats, it creates an electrical impulse that propagates through the heart muscle, leading to contractions that pump blood throughout the body【43】.
The ECG machine records this electrical activity as a series of waves on a graph, typically over a duration of 10 seconds or longer. The resulting waveform represents the heart’s electrical activity, which can be analysed for abnormalities that may indicate various cardiovascular conditions.

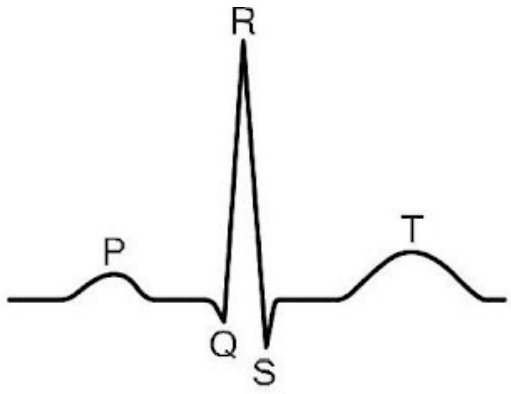


**Figure 2: ECG peaks representation**

### 3.2 Important Components of ECG

The ECG waveform consists of numerous distinct components (Figure 2), each representing different phases of the cardiac cycle [44]:

**P Wave**: The P wave represents the depolarization of the atria, the two upper chambers of the heart. It is the first wave in the ECG cycle and is typically small and rounded. The P wave indicates the electrical impulse originating from the sinoatrial (SA) node, the heart's natural pacemaker. The size and shape of the P wave can provide insights into atrial enlargement or other abnormalities.

**QRS Complex**: The QRS complex follows the P wave and represents the depolarization of the ventricles, the heart's lower chambers. This complex is typically sharp and tall, reflecting the rapid electrical activity that causes ventricular contraction. The QRS complex is critical for assessing ventricular function. Its duration and morphology can indicate various conditions, such as bundle branch blocks, ventricular hypertrophy, or myocardial infarction. A prolonged QRS duration, for example, may suggest conduction delays within the ventricles.

**T Wave**: It represents the repolarization of the ventricles, indicating the recovery phase after contraction. The T wave is generally broader and more rounded than the P wave. The T wave's shape and height can provide insights into electrolyte imbalances, ischemia, or other cardiac issues. Abnormalities in the T wave, such as inversion or flattening, can signal underlying conditions that require further investigation.

### 3.3 Reflection of Individual Physiological Differences

The components of an ECG not only provide information about heart activity but also reflect individual physiological differences. Several factors can influence the shape and duration of the ECG waves, including:

**Age**: Normal ECG patterns can vary significantly with age. For instance, older adults may show changes in wave morphology due to age-related cardiac remodelling.

**Sex**: There are inherent differences in ECG readings between males and females, often attributed to physiological variations in heart size and hormonal influences. For example, the QT interval tends to be longer in females.

**Physical Condition**: Athletes may exhibit specific ECG patterns indicative of enhanced cardiac efficiency, such as a lower heart rate or increased voltage in certain waveforms. Conversely, individuals with cardiovascular diseases may present with abnormal waveforms that signal underlying pathologies.

**Genetic Factors**: Genetic predispositions can influence heart structure and function, impacting ECG readings. For example, certain inherited conditions may lead to prolonged QT intervals or predispose individuals to arrhythmias, reflected in their ECG patterns.

## 4. ECG Signal Processing Techniques

ECG signals are crucial in order to monitor the electrical activity of the heart. However, noise and artifacts cause contamination in these signals, which can distort the accurate representation of heart activity. Some common sources of noise in ECG signals include electrical interference, motion artifacts (e.g., from patient movement), and baseline wander (e.g., due to respiration or improper electrode placement).

### 4.1 Filtering Process

Filtering is an essential pre-processing step to enhance the signal quality and improve the accuracy of feature extraction, which in turn enhances the performance of ECG-based diagnostic systems. To remove these unwanted noise components, several types of filters are used. Each filter type targets specific frequencies that correspond to particular types of noise or artifacts.

#### a. Low-Pass Filters

Low-pass filters are developed to filter out the signals above a set cutoff frequency [45]. These filters remove high-frequency noise, such as muscle artifacts or electrical interference from other devices. Muscle artifacts, often seen in the form of high-frequency oscillations, can obscure the true rhythm of the ECG signal. By applying a low-pass filter, this high-frequency noise can be suppressed, allowing for clearer identification of heartbeats and other important features in the ECG waveform. For instance, low-pass filters are typically set with a cutoff frequency of around 30–50 Hz, as per the specific features of the ECG data.

#### b. High-Pass Filters

In contrast to low-pass filters, high-pass filters are used to eliminate low-frequency noise, particularly baseline wander, which occurs due to movements in the patient, respiration, or improper electrode contact [46]. Baseline wander can cause slow shifts in the signal's baseline, making it challenging to detect the rapid, high-frequency changes associated with the heart's electrical activity. These filters are developed to permit high-frequency components—specifically the rapid fluctuations corresponding to the heart's electrical impulses to pass while attenuating slower, low-frequency signals. These filters typically have a cutoff frequency around 0.5–1 Hz, which is effective for removing unwanted baseline shifts without distorting the main components of the ECG signal.

#### c. Band-Pass Filters

Band-pass filters combine the functionality of both low-pass and high-pass filters. These filters allow only signals within a specified frequency range to pass, while attenuating frequencies outside this range [47]. For ECG signals, the frequency range of interest typically lies between 0.5 Hz and 100 Hz, as this range contains the primary characteristics of the heart's electrical activity. By using a band-pass filter, both high-frequency noise (like muscle artifacts) and low-frequency disturbances (such as baseline wander) can be effectively filtered out. The result is a cleaner ECG signal that retains the key information needed for accurate feature extraction and analysis. Band-pass filters are particularly valuable for isolating the relevant heart rate frequencies and ensuring that noise from surrounding environments is minimized.

### 4.2 Normalization

Normalization is an essential step in pre-processing ECG signals to standardize their amplitude and scale. Raw ECG signals can vary significantly across different individuals, devices, and recording conditions [48]. These variations can make it difficult to compare and analyze features across datasets or subjects. By applying normalization techniques, the amplitude and scale of the ECG signals are standardized, allowing for more consistent and accurate feature extraction, and ultimately improving the performance of downstream analysis or machine learning models. Two common methods of normalization used in ECG signal processing are Min-Max Normalization and Z-score Normalization.

**a. Min-Max Normalization**

Min-Max normalization rescales the values of the ECG signal to fit within a predefined range, typically between 0 and 1. This is done by transforming each signal value according to the following equation:

$$X_{norm} = \left( \frac{X - X_{\min}}{X_{\max} - X_{\min}} \right) \quad (1)$$

Where, X is the original signal value, $X_{\min}$ and $X_{\max}$ are the minimum and maximum values in the ECG signal, $X_{norm}$ is the normalized value.

This method ensures that the relative characteristics of the ECG signal are maintained, but the entire signal is scaled to a consistent range. Min-Max normalization is particularly useful for preparing ECG signals for machine learning models that require input features to be within a fixed range, such as neural networks. By scaling the signals to a [0, 1] range, the model can more easily process and learn from the data, as it prevents one feature from dominating due to larger numerical values.

### b. Z-score Normalization

Z-score normalization, also known as standardization, transforms the ECG signal so that it has a mean of 0 and a standard deviation of 1. This is done by subtracting the mean of the signal from each value and then dividing by the standard deviation:

$$X_{norm} = \left( \frac{X - \mu}{\sigma} \right) \quad (2)$$

where, X is the original signal value, μ is the mean of the signal, σ is the standard deviation of the signal.

This method is particularly effective when dealing with ECG signals that exhibit varying amplitude or when it is important to detect unusual patterns or outliers in the data. By centering the signal around zero and scaling it by the standard deviation, Z-score normalization standardizes the signal across different datasets, making it easier to compare data points regardless of their original scale. This method is commonly used when the goal is to perform statistical analysis, anomaly detection, or to feed the normalized data into machine learning algorithms that rely on standardized inputs.

## 4.3 Segmentation

It is a very important step in ECG signal processing that involves dividing the continuous ECG waveform into discrete intervals or segments, typically corresponding to individual heartbeats or cardiac cycles [49]. The heartbeats in an ECG signal are not static in time, and their durations and characteristics can vary between individuals or even across different cardiac conditions. By segmenting the ECG signal into manageable and meaningful parts, the signal can be analysed more effectively, enabling focused analysis of specific phases within the cardiac cycle. This is particularly important for tasks such as heart rate variability analysis, arrhythmia detection, and feature extraction for classification. The segmentation process generally involves identifying key markers within the ECG signal, such as the R peak, and extracting surrounding segments of the signal that represent individual heartbeats. These segments are then processed and analysed individually, providing more accurate results and insights into the heart's electrical activity.

### a. R-Peak Detection

In ECG signals, the most prominent and easily identifiable feature is the QRS complex, which represents the depolarization of the ventricles. Within the QRS complex, the R wave stands out as the highest peak, making it the most critical marker for detecting the beginning of each cardiac cycle. Accurate R-peak detection is foundational for segmentation, as it marks the start of one heartbeat and provides a reliable reference point for extracting the rest of the cycle [50]. Several algorithms are used to identify R peaks within an ECG signal. Traditional approaches, like the Pan-Tompkins algorithm, employ a combination of filtering, differentiation, squaring, and moving window integration

to detect the R peaks with high accuracy. More modern approaches, such as those based on machine learning, can provide even more precise detection by learning the characteristics of R peaks and adjusting to various signal qualities, such as noise and artifacts. Once R peaks are detected, the corresponding intervals surrounding each peak can be extracted to form individual heartbeats, providing a precise representation of each cardiac cycle. This step is crucial because the analysis of a single heartbeat or segment allows for more accurate feature extraction and classification in various diagnostic tasks.

**b. Windowing Techniques**

Once the R peaks are detected, windowing techniques are employed to extract the ECG signal segments corresponding to individual heartbeats. A "window" is defined around each R peak, typically including a specified number of samples before and after the peak [51]. The length of the window is chosen based on the duration of a typical heartbeat, which generally lasts between 600 ms and 1000 ms, but may vary depending on the heart rate or health conditions of the individual.

The windowed segment typically encompasses the P wave, QRS complex, and T wave, capturing the complete cycle of ventricular depolarization and repolarization. This ensures that all relevant features of the ECG, such as heart rate, rhythm, and abnormalities like arrhythmias, are retained within each segment. The number of samples before and after the R peak can be adjusted as per the requirement of the analysis. For instance, in some cases, a longer window may be required to capture more details, such as the full duration of the T wave, while a shorter window may suffice for basic heart rate analysis.

Once the segments are extracted, they can be processed individually, and relevant features can be extracted from each window. This segmented approach allows for more targeted analysis of the heart's electrical activity, and it is particularly useful for detecting abnormalities in specific phases of the cardiac cycle, such as premature ventricular contractions, atrial fibrillation, or other arrhythmic events.

## 5. ECG Feature Extraction

ECG feature extraction is a critical step in analyzing electrocardiographic (ECG) signals, particularly for applications such as biometric authentication, health monitoring, and diagnosing cardiovascular conditions [52]. The basic aim of feature extraction is to identify unique and meaningful characteristics from the raw ECG data that can be used to classify, recognize, or predict various heart-related conditions. This process typically involves a range of signal processing techniques designed to upgrade the quality of the ECG signal and extract relevant features for further analysis.

Below, we discuss the main methods used in ECG feature extraction:

### 5.1 Time-Domain Analysis

Time-domain analysis focuses on evaluating the ECG signal based on its characteristics in the time domain, such as the shape, duration, and amplitude of the waveform. It is one of the most straightforward and widely used methods in ECG analysis [53].

**Key Features**

- **PR Interval**: The PR interval is measured from the beginning of the P wave to the beginning of the QRS complex. This interval is important in assessing the electrical conduction from the atria to the ventricles and can be indicative of conditions like heart block.

- **QRS Duration**: This represents the duration of the QRS complex, which reflects the time it takes for the ventricles to depolarize. Prolonged QRS duration may be a sign of ventricular conduction delays or other heart abnormalities.

- **QT Interval**: The QT interval spans from the start of the Q wave to the end of the T wave. It represents the time taken for the ventricles to contract and relax. A prolonged QT interval can be associated with an increased risk of arrhythmias and other cardiac conditions.

**Amplitudes**

- The amplitude of the P wave, QRS complex, and T wave can be measured directly. These amplitudes provide valuable information about the atrial and ventricular function. For instance, an abnormally large or small QRS amplitude could indicate a condition like hypertrophy or ischemia, while changes in T wave amplitude could point to issues such as electrolyte imbalances.

## 5.2 Frequency-Domain Analysis

While time-domain analysis offers insights into the shape and timing of the ECG waveform, frequency-domain analysis provides a different perspective by transforming the ECG signal into the frequency domain [54]. This is typically achieved using techniques such as the Fast Fourier Transform (FFT), which decomposes the signal into its constituent frequency components.
Frequency-domain analysis can reveal important spectral features, including:

- **Dominant Frequencies**: The ECG signal contains several dominant frequencies that correspond to different phases of the cardiac cycle. For example, the frequency components related to the QRS complex are typically higher than those related to the P and T waves.

- **Spectral Characteristics**: These characteristics help identify abnormalities in the signal's frequency content, which may be indicative of conditions such as atrial fibrillation, heart failure, or other arrhythmias.

Frequency-domain features can be particularly useful for detecting subtle anomalies that might not be as evident in the time domain, offering a complementary layer of analysis that enhances the overall diagnostic capability.

## 5.3 Wavelet Transform

In addition to traditional time-domain and frequency-domain methods, wavelet transform is quite useful for ECG feature extraction. Unlike the Fourier transform, which only provides information about the frequencies present in a signal, wavelet transform gives both time and frequency information, making it highly effective for analyzing non-stationary signals like ECG [55].
Wavelet transforms break the signal into different frequency components at various scales, allowing for a more detailed analysis of transient events and rapid changes in the ECG. This can be particularly beneficial for detecting arrhythmias and other sudden heart conditions.

## 5.4 Nonlinear Dynamics

ECG signals, especially those associated with certain types of arrhythmias, often exhibit nonlinear dynamics. Methods like entropy-based features are used to quantify the irregularity or complexity of the signal [56]. High entropy values may indicate chaotic heart rhythms, while low entropy may reflect a more regular pattern, such as normal sinus rhythm. These nonlinear features are useful for detecting abnormal heart rhythms, where traditional linear methods might struggle.

### a. Power Spectral Density (PSD)

PSD measures the power (or energy) distribution of the signal across different frequencies. By analyzing the PSD of an ECG signal, we can determine which frequency components contribute most to the signal's overall power [57]. This is particularly useful for identifying abnormalities related to heart rhythms and detecting potential issues like arrhythmias or ischemic events.
PSD can also be used to assess the overall health of the heart by identifying deviations from typical frequency patterns that are associated with certain heart conditions. For instance, changes in the low-frequency and high-frequency bands in the PSD may signal issues related to autonomic nervous system activity, heart rate variability, or myocardial ischemia.

### b. Dominant Frequencies

Identifying dominant frequencies in the ECG signal helps reveal the most prominent components of the heart's electrical activity [58]. Each phase of the cardiac cycle—such as atrial depolarization, ventricular depolarization, and repolarization—has associated frequencies that are fundamental to understanding the heart's functioning. Abnormalities in these dominant frequencies may indicate arrhythmias, tachycardia, or bradycardia.

- Tachycardia (high heart rate) may cause higher frequency components in the ECG signal, while bradycardia (low heart rate) could result in a shift toward lower frequency ranges.
- Detecting shifts in these dominant frequencies can be crucial in diagnosing arrhythmias or irregular heartbeats.

### c. Time-Frequency Analysis

Time-frequency analysis is a powerful technique that combines both time-domain and frequency-domain methods, making it particularly suitable for analyzing non-stationary signals such as ECG [59]. ECG signals are inherently dynamic, with the frequency characteristics changing over time due to various factors like heart rate variability, changes in rhythm, or the presence of arrhythmias.

Unlike traditional frequency-domain methods, which assume that the signal is stationary (i.e., its frequency content does not change over time), time-frequency analysis allows for capturing how the frequency components evolve as the signal progresses. This technique is valuable for detecting transient features and non-stationary phenomena in the ECG that may be missed by other methods. For instance, arrhythmic events like premature ventricular contractions (PVCs) or atrial fibrillation can be better identified with time-frequency methods**.**

### d. Wavelet Transform

The Wavelet Transform is another sophisticated method used in ECG signal analysis. Unlike the Fourier transform, which only provides frequency information, the wavelet transform decomposes the signal into different frequency components while preserving time information [60]. This makes wavelet transforms particularly useful for detecting transient features or sudden changes in the ECG signal, which may not be evident in traditional frequency-domain analysis.

The wavelet transform allows for a multiresolution analysis, meaning it can capture both high-frequency and low-frequency components at different scales. This is useful for detecting both short-term events (e.g., PVCs or ectopic beats) and long-term patterns (e.g., changes in heart rate or rhythm) that might indicate broader cardiac issues [61].

In practice, wavelet transforms provide a more flexible and detailed analysis of the ECG signal, especially when dealing with complex patterns or transient events that occur over short periods.

### e. Short-Time Fourier Transform (STFT)

The STFT is a technique that segments the ECG signal into smaller time windows and applies the Fourier Transform to each window separately [62]. The result is a two-dimensional representation of the signal, where one axis represents time, the other represents frequency, and the intensity (or magnitude) of the signal is indicated by colour or amplitude. STFT is particularly useful for observing how the frequency components of the ECG signal evolve over time. This is important for detecting time-varying features, such as changes in heart rhythm, the onset of arrhythmias, or the effect of different physiological conditions on the heart [63]. By visualizing the signal in the time-frequency domain, STFT provides a more detailed view of the ECG signal, highlighting variations that might otherwise be overlooked in a purely time-domain or frequency-domain analysis.

## 6. Classification Algorithms for ECG Biometrics

The ECG signals classification plays a pivotal role in leveraging their distinct characteristics for numerous applications, such as biometric authentication, health monitoring, and cardiac disease diagnosis [64]. The ECG signals contain vital information about the electrical activity of the heart, and by accurately classifying them, we can detect abnormalities, identify specific cardiac conditions, and even use them for personal identification. Generally, the decision-making stage for most of the ECG biometric algorithms use the classifiers. For these classifiers, original templates stored by the biometric system at the time of enrollment of subjects are necessary to let the algorithm to pay

attention to the separation between the subjects. The classifier is intended to have its function to assist in the identification or verification function of the system when needed. In identification tasks, classifiers are used more frequently than features and some of the models are SVM's, Nearest Neighbour classifiers and ANNs. All of these methods help to enhance the reliability of the described biometric system.

## 6.1 Machine Learning (ML) Approaches

These techniques are used for classifying ECG signals after extracting meaningful features [65]. These approaches can be of two types: supervised learning or unsupervised learning methods. Both are very useful in improving the accuracy and efficiency of ECG classification.

### 6.1.1 Supervised Learning Methods

In this type of method, the model is trained on labeled data, meaning each input is paired with a corresponding output label [66]. The model learns to map input features to the correct labels during training. In the context of ECG classification, the features extracted from the ECG signals are used as inputs, while the output could represent different cardiac conditions, such as normal sinus rhythm, arrhythmia, or other specific heart diseases.

#### a. Support Vector Machines (SVM)

SVM are one of the most powerful supervised learning algorithms used for classification tasks. SVM constructs an optimal hyperplane that best separates different classes in a high-dimensional feature space [67]. One of the key strengths of SVM is its ability to handle non-linearly separable data by using kernel functions, which map the input data into higher-dimensional spaces where a linear hyperplane can be used to separate the classes.
In ECG classification, SVM can be employed to classify various heart conditions or to identify specific patterns in the ECG signal for biometric authentication. The technique performs well even with small to medium-sized datasets and is capable of managing high-dimensional features extracted from ECG signals.

#### b. Neural Networks

These are ML models which are developed on the basis of the human brain's structure and functioning. These networks consist of layers of interconnected nodes (or neurons) that process and transform input data [68]. Neural networks are highly effective at modeling complex, non-linear relationships, making them suitable for tasks such as ECG classification.
Feedforward Neural Networks (FNN) [69], a basic type of neural network, can be used for ECG classification tasks by learning the relationship between extracted features and the output labels. More advanced neural network architectures, such as Recurrent Neural Networks (RNNs) [70], are particularly well-suited for time-series data like ECG signals. RNNs can capture temporal dependencies in the sequential nature of ECG data, which is essential for detecting abnormal heart rhythms and other dynamic cardiac events.

#### c. Decision Trees and Random Forests

These are supervised learning models that partition the input feature space into decision regions based on splitting rules, typically involving binary decisions at each node [71]. Each branch represents a decision outcome, and the leaf nodes contain the predicted class label. While decision trees can be prone to overfitting, they offer a transparent and interpretable approach to classification.
Random Forests, an ensemble method, improve upon decision trees by combining various decision trees to develop a robust classification model [72]. The ensemble approach helps reduce overfitting and enhances accuracy by averaging the results of many trees, each trained on a random subset of the data. In ECG classification, decision trees and random forests can classify different heart conditions based on the extracted features, while providing intuitive results that are easy to interpret.

### 6.1.2 Unsupervised Learning Methods

In unsupervised learning, the algorithm works with unlabelled data and aims to figure out the concealed patterns or groupings within the data [73]. These methods are useful for exploratory analysis, identifying inherent structures in ECG data, and preprocessing data for supervised learning.

#### a. Clustering Algorithms

Clustering is a key unsupervised learning method that groups similar data points together based on their feature similarities. Popular clustering algorithms, such as k-means and hierarchical clustering, can be used to identify natural groupings within ECG data, revealing patterns that may represent different physiological states or cardiac conditions [74]. For example, clustering may identify groups of ECG signals that correspond to normal heartbeats or those indicative of arrhythmic episodes.
Clustering helps uncover relationships in data, facilitating the discovery of previously unknown conditions or anomalies, which can then be further analyzed using supervised methods. It is often applied as a preprocessing step in ECG classification systems to organize the data and guide subsequent classification efforts.

### b. Principal Component Analysis (PCA)

PCA is a dimensionality reduction technique that transforms the data into a new coordinate system, where the first few dimensions (principal components) capture the most variance in the data [75]. This technique is particularly useful for reducing the complexity of ECG data by eliminating redundant features while retaining the most important information.PCA can be used as a preprocessing step before applying classification algorithms. On decreasing the number of features in the ECG data, PCA enhances the computational efficiency of the classifier and helps improve its performance. It can also mitigate issues such as multicollinearity, which may arise when features are highly correlated. In ECG classification, PCA is helpful for simplifying the data, making it easier for machine learning models to learn from the features and perform accurate classifications.

### 6.2 Deep Learning Models

These models have gained prominence in recent years. This is due to the fact that these models can automatically extract features from raw data without the need for extensive preprocessing.

### 6.2.1 Convolutional Neural Networks (CNNs)

CNNs are specialized neural networks that excel in processing structured grid data, such as images and sequential data like electrocardiogram (ECG) signals. Unlike traditional neural networks, which treat inputs as flat vectors, CNNs are designed to capture the spatial relationships inherent in grid-like data [76]. At the core of CNNs are convolutional layers, which apply convolutional operations to the input data. These layers automatically learn to detect various features at different levels of abstraction. This hierarchical learning process allows CNNs to identify simple features in the initial layers, like edges or corners, and gradually build up to more complex structures, such as shapes or objects, in deeper layers [77]. The use of shared weights and local receptive fields in convolutional layers significantly reduces the number of parameters, making CNNs more efficient and effective at learning from large datasets. Additionally, pooling layers are often incorporated to down-sample the feature maps, further emphasizing the most relevant information while reducing computational load. CNNs are particularly effective in applications such as image recognition, where they can classify images, detect objects, and segment regions.In the case of sequential data like ECG signals, CNNs can learn temporal patterns and variations, aiding in the detection of anomalies or predicting health conditions. CNNs can be applied to classify ECG signals directly from raw waveform data or spectrograms generated through time-frequency analysis, achieving high accuracy in recognizing patterns associated with different cardiac conditions.

### 6.2.2 Long Short-Term Memory Networks (LSTMs)

LSTM networks are a kind of recurrent neural network (RNN) which are specially designed to effectively learn from sequences of data by retaining information over extended periods [78]. This capability is essential for processing time-

dependent signals, such as electrocardiogram (ECG) readings, where understanding the temporal context is crucial for accurate interpretation.

LSTMs address the common challenges faced by traditional RNNs, particularly the issues of vanishing and exploding gradients. They achieve this through a unique architecture that includes memory cells and gates. The memory cells store information, while the gates—specifically the input, output, and forget gates—regulate the flow of information into, out of, and within the cell. This allows LSTMs to maintain relevant information over long sequences while discarding less important data [79].

In ECG signals, LSTMs can effectively model the temporal dynamics of the heart's electrical activity. They are capable of capturing complex patterns and anomalies that may occur over time, making them highly useful for tasks such as arrhythmia detection and predicting cardiovascular events. By leveraging their ability to learn from historical data, LSTMs enhance the performance of predictive models in healthcare applications.

Overall, LSTMs represent a significant advancement in the field of sequence modelling, enabling more accurate analysis and predictions for a wide range of time-dependent data.

LSTMs are effective for tasks such as arrhythmia detection or biometric authentication, as they can capture temporal dependencies and patterns within the ECG signal.

## 7. Evaluation Metrics

These metrices are used to evaluate the performance of ECG classification systems [80]:

**Accuracy:** Accuracy measures the proportion of correctly classified instances among the total instances. It is calculated as:

$$A = \frac{T^+ + T^-}{T^+ + F^+ + T^- + F^-} \tag{3}$$

While accuracy is a useful measure, it can be misleading in cases of class imbalance, where one class significantly outnumbers the others.

**Precision:** Precision indicates the proportion of true positive predictions among all positive predictions.

$$P = \frac{T^+}{T^+ + F^+} \tag{4}$$

Precision is particularly important in contexts where false positives carry significant consequences, such as in medical diagnoses.

**Recall:** Recall measures the proportion of true positives among all actual positive instances. It is calculated as**:**

$$R = \frac{T^+}{T^+ + F^-} \tag{5}$$

High recall is critical in medical applications where failing to identify a condition can have serious implications.

**F1-Score:** The F1-score is the harmonic mean of precision and recall, providing a balance between the two. It is calculated as:

$$F = \frac{2PR}{P + R} \tag{6}$$

The F1-score is particularly useful in situations with class imbalance, offering a single metric that considers both false positives and false negatives.

## 8. Applications of ECG Biometrics

ECG biometrics plays a significant role across numerous domains including security systems and health monitoring. By leveraging the unique electrical patterns of the heart, ECG can enhance security protocols and improve health outcomes. This section explores two primary applications: security systems and health monitoring.

### 8.1 Security Systems

ECG biometrics offer a promising approach to enhancing security systems. This is done by with the inclusion of an additional layer of authentication based on an individual's unique heart rhythm. One significant application is in secure access control. By integrating ECG biometrics, access systems can authenticate users on the basis of their heart signals, which are unique to each person, thereby improving security beyond traditional methods such as passwords and fingerprints [81]. This approach has several benefits, including increased security since ECG patterns are intrinsically tied to the individual's physiology, making them much harder to spoof compared to fingerprints or facial recognition. Moreover, it enhances user convenience, as ECG biometrics allow for quick, non-intrusive authentication, typically through devices like smartwatches or other wearable technology, making the process seamless.

In the context of financial transactions, ECG biometrics can further strengthen security by adding an extra verification layer during digital payments. This added protection can help prevent fraud by confirming a user's identity through their unique heart signals, significantly reducing the risk of unauthorized access. The integration of ECG in financial transactions also bolsters user trust, as individuals feel more secure knowing that their sensitive financial data is being protected by advanced biometric verification, encouraging broader adoption of digital payment platforms [82].

User authentication is another area where ECG biometrics can provide robust security. As an authentication method, ECG can serve as a multifactor authentication system, complementing traditional methods like passwords or PINs, thus enhancing overall security without compromising user experience. Additionally, it enables remote access for users, allowing them to authenticate their identity through wearable devices. This method provides secure access to sensitive systems and information without the need for physical tokens or passwords, making it especially convenient for those on the go.

### 8.2 Health Monitoring

In the realm of health monitoring, ECG biometrics can be seamlessly integrated into wearable devices such as smartwatches and fitness trackers to offer continuous, real-time health insights [83]. These devices enable users to monitor their heart activity regularly, which can lead to early detection of abnormalities and ultimately improve cardiovascular health. Furthermore, they can provide personalized health insights, analyzing ECG data to generate recommendations for exercise, stress management, and lifestyle adjustments, tailored to the individual's needs.

ECG biometrics are also crucial in anomaly detection, where they can identify irregular heart rhythms such as arrhythmias [84]. This capability is beneficial for timely intervention, as abnormal heart rhythms can be detected early, allowing for prompt medical action to prevent serious cardiovascular events. Additionally, ECG-based remote monitoring makes it possible for the specialist to monitor the patients' heart health from a distance, facilitating proactive care management and reducing the need for frequent in-person visits.

Finally, real-time alerts for cardiovascular events are another significant advantage of ECG biometrics [85]. Advanced algorithms can analyse ECG data in real time to detect critical conditions like atrial fibrillation or even heart attacks. Such alerts can trigger immediate notification to users or their caregivers, ensuring emergency response is prompt, which is critical in life-threatening situations. These systems also foster enhanced patient engagement.

## 9. Challenges and Future Directions in ECG Biometrics

ECG biometrics holds great potential for revolutionizing both security systems and health monitoring applications, but several challenges remain that hinder its widespread adoption and effectiveness. One of the primary challenges is signal quality and noise contamination. ECG signals are inherently prone to various types of noise and interference, such as motion artifacts, electrical noise, and baseline wander. These distortions can significantly degrade the accuracy of feature extraction and classification, leading to incorrect or inconsistent biometric results. In real-world applications, where individuals may be on the move or in noisy environments, ensuring high-quality, noise-free ECG data is a significant hurdle. Advances in signal processing techniques, such as adaptive filtering and noise reduction algorithms, are necessary to overcome this challenge and improve the robustness of ECG biometrics.

### 9.1 Inter-individual Variability in ECG Signals

Another significant challenge is inter-individual variability. Although ECG signals are unique to each individual, the features derived from these signals can vary considerably across different people, even for the same person under different conditions. Components like age, gender, health conditions, and environmental influences can all lead to

variations in heart rhythms. This variability makes it difficult to develop generalized models that perform consistently across diverse populations. In addition, the complexity of the ECG signal itself, with its various waves, intervals, and morphologies, requires highly sophisticated feature extraction and classification techniques to capture the subtle differences that distinguish one individual from another. To address these issues, researchers are focusing on improving personalized models that adapt to individual differences, as well as multi-modal biometrics, which combine ECG with other biometric traits to increase accuracy and reliability.

## 9.2 Real-Time Processing Challenges

Real-time processing is another critical challenge in ECG biometrics, especially in health monitoring applications. The need for continuous, real-time analysis of ECG data, particularly in wearable devices like smartwatches and fitness trackers, requires efficient and fast algorithms that can process large amounts of data with minimal latency. This places high demands on both the computational resources and the energy efficiency of the devices used. As ECG-based systems become more integrated into daily life, the ability to monitor heart health and perform biometric authentication on the go will depend on the development of lightweight, energy-efficient algorithms that can deliver real-time results without draining battery life or overloading the device's processing capacity.

## 9.3 Integration with Existing Security and Healthcare Systems

Furthermore, the integration of ECG biometrics with existing security and healthcare infrastructures remains a challenge. While many organizations and healthcare providers are keen to adopt ECG biometrics, the integration of these systems with existing databases, networks, and authentication protocols can be complex. The development of standardized, interoperable systems that allow for seamless integration of ECG-based authentication with other forms of identity verification (like passwords, fingerprint scanners, or facial recognition) is essential for broader adoption. Additionally, healthcare providers must assure that ECG data is securely stored, shared, and transmitted, adhering to standard privacy regulations.

## 9.4 Future Directions in ECG Biometrics

In terms of future directions, researchers are exploring the potential of deep learning techniques for ECG biometric analysis. Conventional ML techniques often rely on manual feature extraction, but deep learning models, particularly CNNs and RNNs, have the potential to automatically learn relevant features from raw ECG signals. These models could help improve accuracy and reduce the reliance on handcrafted features, making ECG biometrics more scalable and adaptable to a wider range of users and use cases. Furthermore, advances in edge computing could allow for real-time ECG analysis to be performed directly on wearable devices, minimizing latency and mitigating the requirement of transmitting sensitive biometric data to central servers.

### a. Multi-modal Biometric Systems

The integration of ECG biometrics with multi-modal systems is another promising future direction. By combining ECG with other biometric modalities systems can achieve higher levels of accuracy and security. Multi-modal systems could leverage the complementary strengths of different biometrics to mitigate the limitations of individual modalities, such as the variability of ECG signals or the susceptibility of face recognition to lighting conditions.

## b. Personalized and Context-Aware Systems

Finally, as more data is collected through wearable devices and other personal health technologies, there is an opportunity to develop personalized, context-aware ECG biometric systems. These systems could account for factors such as an individual's health status, physical activity level, or emotional state, tailoring the biometric authentication process to be more accurate and adaptable. For example, ECG patterns might change during exercise, stress, or illness, and incorporating such context into biometric models could improve their robustness in dynamic, real-world environments.

## 10. Conclusion

This research article presented a comprehensive exploration of ECG-based biometric systems, focusing on their potential for secure authentication and health monitoring. By leveraging advanced signal processing techniques such as filtering, normalization, and segmentation, along with feature extraction methods like time-domain, frequency-domain, and wavelet analysis, we demonstrated how ECG signals can be effectively utilized for both individual identification and health condition monitoring. The integration of ML algorithms, particularly deep learning models like Bi-LSTM, further enhances the accuracy and robustness of ECG classification systems. The research highlights the growing potential of ECG biometrics in practical applications, including secure access control, financial transactions, and continuous health monitoring through wearable devices. Despite the promising results, challenges such as signal noise, inter-individual variability, and the need for real-time processing remain. It is quite important to deal with these issues to have a broad adoption of ECG-based biometrics in diverse real-world applications. Future research should explore further optimization techniques, multi-modal systems, and the development of context-aware algorithms to enhance the efficiency and versatility of ECG biometrics. With continued advancements, ECG biometrics holds the potential to redefine personal security and health management, offering a reliable and non-intrusive solution for both authentication and health monitoring.

## References


1. Jain, Anil K., Karthik Nandakumar, and Arun Ross. "50 years of biometric research: Accomplishments, challenges, and opportunities." *Pattern recognition letters* 79 (2016): 80-105.
2. Maltoni, Davide, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of fingerprint recognition*. Vol. 2. London: springer, 2009.
3. Bodepudi, Anusha, and Manjunath Reddy. "Cloud-Based Biometric Authentication Techniques for Secure Financial Transactions: A Review." *International Journal of Information and Cybersecurity* 4, no. 1 (2020): 1-18.
4. Millett, Lynette I., and Joseph N. Pato, eds. "Biometric recognition: Challenges and opportunities." (2010).
5. Rao, P. Muralidhara, and Bakkiam David Deebak. "Security and privacy issues in smart cities/industries: technologies, applications, and challenges." *Journal of Ambient Intelligence and Humanized Computing* 14, no. 8 (2023): 10517-10553.
6. de Luis-García, Rodrigo, Carlos Alberola-Lopez, Otman Aghzout, and Juan Ruiz-Alzola. "Biometric identification systems." *Signal processing* 83, no. 12 (2003): 2539-2557.
7. Sarkar, Arpita, and Binod K. Singh. "A review on performance, security and various biometric template protection schemes for biometric authentication systems." *Multimedia Tools and Applications* 79, no. 37 (2020): 27721-27776.
8. Kindt, Els J. "Privacy and data protection issues of biometric applications." In *A Comparative Legal Analysis*, vol. 12. Springer, 2013.
9. Bolme, David S., Ryan A. Tokola, Chris B. Boehnen, Tiffany B. Saul, Kelly A. Sauerwein, and Dawnie Wolfe Steadman. "Impact of environmental factors on biometric matching during human decomposition." In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1-8. IEEE, 2016.
10. Uwaechia, Anthony Ngozichukwuka, and Dzati Athiar Ramli. "A comprehensive survey on ECG signals as new biometric modality for human authentication: Recent advances and future challenges." *IEEE Access* 9 (2021): 97760-97802.
11. Palma, David, and Pier Luca Montessoro. "Biometric-based human recognition systems: an overview." *Recent Advances in Biometrics* 27 (2022): 1-21.
12. Dargan, Shaveta, and Munish Kumar. "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities." *Expert Systems with Applications* 143 (2020): 113114.
13. Socheat, Sek, and Tianjiang Wang. "Fingerprint enhancement, minutiae extraction and matching techniques." *Journal of Computer and Communications* 8, no. 05 (2020): 55.
14. Shebaro, Bilal, Oyindamola Oluwatimi, and Elisa Bertino. "Context-based access control systems for mobile devices." *IEEE Transactions on Dependable and Secure Computing* 12, no. 2 (2014): 150-163.
15. Bruce, Vicki, and Andy Young. "Understanding face recognition." *British journal of psychology* 77, no. 3 (1986): 305-327.
16. Gates, Kelly A. *Our biometric future: Facial recognition technology and the culture of surveillance*. Vol. 2. NYU Press, 2011.

17. Kortli, Yassin, Maher Jridi, Ayman Al Falou, and Mohamed Atri. "Face recognition systems: A survey." *Sensors* 20, no. 2 (2020): 342.
18. Gates, Kelly A. *Our biometric future: Facial recognition technology and the culture of surveillance*. Vol. 2. NYU Press, 2011.
19. Bowyer, Kevin W., and Mark J. Burge, eds. *Handbook of iris recognition*. Springer London, 2016.
20. Lee, Young Won, and Kang Ryoung Park. "Recent iris and ocular recognition methods in high-and low-resolution images: A survey." *Mathematics* 10, no. 12 (2022): 2063.
21. Bharathi, B., and P. Bindhu Shamily. "A review on iris recognition system for person identification." *International Journal of Computational Biology and Drug Design* 13, no. 3 (2020): 316-331.
22. Abràmoff, Michael D., Mona K. Garvin, and Milan Sonka. "Retinal imaging and image analysis." *IEEE reviews in biomedical engineering* 3 (2010): 169-208.
23. Hill, Robert "Buzz. "Retina identification." *Biometrics: Personal identification in networked society* (1996): 123-141.
24. Ahmad, Irfan, and Manzoor Khan. *Hand recognition using palm and hand geometry features*. LAP LAMBERT Academic Publishing, 2017.
25. Jaswal, Gaurav, Amit Kaul, and Ravinder Nath. "Multimodal biometric authentication system using hand shape, palm print, and hand geometry." In *Computational Intelligence: Theories, Applications and Future Directions-Volume II: ICCI-2017*, pp. 557-570. Singapore: Springer Singapore, 2018.
26. Li, Xiaochang, and Mara Mills. "Vocal features: from voice identification to speech recognition by machine." *Technology and culture* 60, no. 2 (2019): S129-S160.
27. Wang, Chen, Yan Wang, Yingying Chen, Hongbo Liu, and Jian Liu. "User authentication on mobile devices: Approaches, threats and trends." *Computer Networks* 170 (2020): 107118.
28. Fairhurst, Michael, Cheng Li, and Márjory Da Costa-Abreu. "Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data." *IET Biometrics* 6, no. 6 (2017): 369-378.
29. Crawford, Heather. "Keystroke dynamics: Characteristics and opportunities." In *2010 Eighth International Conference on Privacy, Security and Trust*, pp. 205-212. IEEE, 2010.
30. Bergadano, Francesco, Daniele Gunetti, and Claudia Picardi. "User authentication through keystroke dynamics." *ACM Transactions on Information and System Security (TISSEC)* 5, no. 4 (2002): 367-397.
31. Porwik, Piotr, Rafal Doroz, and Tomasz Emanuel Wesolowski. "Dynamic keystroke pattern analysis and classifiers with competence for user recognition." *Applied Soft Computing* 99 (2021): 106902.
32. Wan, Changsheng, Li Wang, and Vir V. Phoha, eds. "A survey on gait recognition." *ACM Computing Surveys (CSUR)* 51, no. 5 (2018): 1-35.
33. Tao, Weijun, Tao Liu, Rencheng Zheng, and Hutian Feng. "Gait analysis using wearable sensors." *Sensors* 12, no. 2 (2012): 2255-2283.
34. Linden, Jacques, Raymond Marquis, Silvia Bozza, and Franco Taroni. "Dynamic signatures: A review of dynamic feature variation and forensic methodology." *Forensic science international* 291 (2018): 216-229.
35. Fischer, Andreas, and Réjean Plamondon. "Signature verification based on the kinematic theory of rapid human movements." *IEEE Transactions on Human-Machine Systems* 47, no. 2 (2016): 169-180.
36. Gaikwad, Santosh K., Bharti W. Gawali, and Pravin Yannawar. "A review on speech recognition technique." *International Journal of Computer Applications* 10, no. 3 (2010): 16-24.
37. Isyanto, Haris, Ajib Setyo Arifin, and Muhammad Suryanegara. "Performance of smart personal assistant applications based on speech recognition technology using IoT-based voice commands." In *2020 International conference on information and communication technology convergence (ICTC)*, pp. 640-645. IEEE, 2020.
38. Shen, Chao, Zhongmin Cai, Xiaohong Guan, Youtian Du, and Roy A. Maxion. "User authentication through mouse dynamics." *IEEE Transactions on Information Forensics and Security* 8, no. 1 (2012): 16-30.
39. Khan, Simon, Charles Devlen, Michael Manno, and Daqing Hou. "Mouse dynamics behavioral biometrics: A survey." *ACM Computing Surveys* 56, no. 6 (2024): 1-33.
40. Zagermann, Johannes, Ulrike Pfeil, and Harald Reiterer. "Measuring cognitive load using eye tracking technology in visual computing." In *Proceedings of the sixth workshop on beyond time and errors on novel evaluation methods for visualization*, pp. 78-85. 2016.
41. Punde, Pramodini A., Mukti E. Jadhav, and Ramesh R. Manza. "A study of eye tracking technology and its applications." In *2017 1st International Conference on Intelligent Systems and Information Management (ICISIM)*, pp. 86-90. IEEE, 2017.

42. Gacek, Adam. "An introduction to ECG signal processing and analysis." In *ECG Signal Processing, Classification and Interpretation: A Comprehensive Framework of Computational Intelligence*, pp. 21-46. London: Springer London, 2011.
43. Gacek, Adam, and Witold Pedrycz, eds. *ECG signal processing, classification and interpretation: a comprehensive framework of computational intelligence*. Springer Science & Business Media, 2011.
44. Halhuber, Max J., Robert Günther, and Max Ciresa. *ECG: An introductory course a practical introduction to clinical electrocardiography*. Springer Science & Business Media, 2012.
45. Christov, Ivaylo, Tatyana Neycheva, and Ramun Schmid. "Fine tuning of the dynamic low-pass filter for electromyographic noise suppression in electrocardiograms." In *2017 Computing in Cardiology (CinC)*, pp. 1-4. IEEE, 2017.
46. Censi, Federica, Giovanni Calcagnini, Michele Triventi, Eugenio Mattei, Pietro Bartolini, Ivan Corazza, and Giuseppe Boriani. "Effect of high-pass filtering on ECG signal on the analysis of patients prone to atrial fibrillation." *Annali dell'Istituto superiore di sanita* 45 (2009): 427-431.
47. Nobunaga, T., H. Tanaka, I. Tanahashi, T. Watanabe, and Y. Hattori. "Optimised band-pass filter to ensure accurate ECG-based identification of exercising human subjects." *Electronics Letters* 53, no. 4 (2017): 222-224.
48. Sun, P., Q. H. Wu, A. M. Weindling, A. Finkelstein, and K. Ibrahim. "An improved morphological approach to background normalization of ECG signals." *IEEE Transactions on biomedical engineering* 50, no. 1 (2003): 117-121.
49. Beraza, Idoia, and Iñaki Romero. "Comparative study of algorithms for ECG segmentation." *Biomedical Signal Processing and Control* 34 (2017): 166-173.
50. Qin, Qin, Jianqing Li, Yinggao Yue, and Chengyu Liu. "An Adaptive and Time-Efficient ECG R-Peak Detection Algorithm." *Journal of healthcare engineering* 2017, no. 1 (2017): 5980541.
51. Kumar, K. Sravan, Babak Yazdanpanah, and G. S. N. Raju. "Performance comparison of windowing techniques for ECG signal enhancement." *International Journal of Engineering Research* 3, no. 12 (2014): 753-756.
52. Karpagachelvi, S., Muthusamy Arthanari, and M. Sivakumar. "ECG feature extraction techniques-a survey approach." *arXiv preprint arXiv:1005.0957* (2010).
53. Khan, Tasnova Tanzil, Nadia Sultana, Rezwana Binte Reza, and Raqibul Mostafa. "ECG feature extraction in temporal domain and detection of various heart conditions." In *2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, pp. 1-6. IEEE, 2015.
54. Lin, Chia-Hung. "Frequency-domain features for ECG beat discrimination using grey relational analysis-based classifier." *Computers & Mathematics with Applications* 55, no. 4 (2008): 680-690.
55. Seena, V., and Jerrin Yomas. "A review on feature extraction and denoising of ECG signal using wavelet transform." In *2014 2nd international conference on devices, circuits and systems (ICDCS)*, pp. 1-6. IEEE, 2014.
56. Udhayakumar, Radhagayathri Krishnavilas. "Analysing Irregularity and Complexity in Short-length Heart Rate Variability Signals." PhD diss., The University of Melbourne, 2019.
57. Khazaee, Ali, and Ataollah Ebrahimzadeh. "Classification of electrocardiogram signals with support vector machines and genetic algorithms using power spectral features." *Biomedical Signal Processing and Control* 5, no. 4 (2010): 252-263.
58. Singh, Anupreet Kaur, and Sridhar Krishnan. "ECG signal feature extraction trends in methods and applications." *BioMedical Engineering OnLine* 22, no. 1 (2023): 22.
59. Al-Fahoum, Amjed S., and Ausilah A. Al-Fraihat. "Methods of EEG Signal Features Extraction Using Linear Analysis in Frequency and Time-Frequency Domains." *International Scholarly Research Notices* 2014, no. 1 (2014): 730218.
60. Bajaj, Nikesh. "Wavelets for EEG analysis." *Wavelet theory* (2020): 1-16.
61. Islam, Md Rabiul, and Mohiuddin Ahmad. "Wavelet analysis based classification of emotion from EEG signal." In *2019 international conference on electrical, computer and communication engineering (ECCE)*, pp. 1-6. IEEE, 2019.
62. Huang, Jingshan, Binqiang Chen, Bin Yao, and Wangpeng He. "ECG arrhythmia classification using STFT-based spectrogram and convolutional neural network." *IEEE access* 7 (2019): 92871-92880.
63. Cao, Minh, Tianqi Zhao, Yanxun Li, Wenhao Zhang, Peyman Benharash, and Ramin Ramezani. "ECG Heartbeat classification using deep transfer learning with Convolutional Neural Network and STFT technique." In *Journal of Physics: Conference Series*, vol. 2547, no. 1, p. 012031. IOP Publishing, 2023.

64. Houssein, Essam H., Moataz Kilany, and Aboul Ella Hassanien. "ECG signals classification: a review." *International Journal of Intelligent Engineering Informatics* 5, no. 4 (2017): 376-396.
65. Sahoo, S., M. Dash, S. Behera, and S. Sabut. "Machine learning approach to detect cardiac arrhythmias in ECG signals: A survey." *Irbm* 41, no. 4 (2020): 185-194.
66. Sarkar, Pritam, and Ali Etemad. "Self-supervised learning for ecg-based emotion recognition." In *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3217-3221. IEEE, 2020.
67. Karpagachelvi, S., M. Arthanari, and M. Sivakumar. "Classification of electrocardiogram signals with support vector machines and extreme learning machine." *Neural Computing and Applications* 21 (2012): 1331-1339.
68. Sánchez, FA Rivera, and JA González Cervera. "ECG classification using artificial neural networks." In *Journal of Physics: Conference Series*, vol. 1221, no. 1, p. 012062. IOP Publishing, 2019.
69. Hosseini, H. Gholam, Dehan Luo, and Karen Jane Reynolds. "The comparison of different feed forward neural network architectures for ECG signal diagnosis." *Medical engineering & physics* 28, no. 4 (2006): 372-378.
70. Salloum, Ronald, and C-C. Jay Kuo. "ECG-based biometrics using recurrent neural networks." In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2062-2066. IEEE, 2017.
71. Mert, Ahmet, Niyazi Kilic, and Aydın Akan. "ECG signal classification using ensemble decision tree." *J Trends Dev Mach Assoc Technol* 16, no. 1 (2012): 179-182.
72. Li, Taiyong, and Min Zhou. "ECG classification using wavelet packet entropy and random forests." *Entropy* 18, no. 8 (2016): 285.
73. Nezamabadi, Kasra, Neda Sardaripour, Benyamin Haghi, and Mohamad Forouzanfar. "Unsupervised ECG analysis: A review." *IEEE Reviews in Biomedical Engineering* 16 (2022): 208-224.
74. Lin, Zetao, Yaozheng Ge, and Guoliang Tao. "Algorithm for clustering analysis of ECG data." In *2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, pp. 3857-3860. IEEE, 2006.
75. Sharma, L. N., Samarendra Dandapat, and Anil Mahanta. "Multichannel ECG data compression based on multiscale principal component analysis." *IEEE Transactions on Information technology in Biomedicine* 16, no. 4 (2012): 730-736.
76. Labati, Ruggero Donida, Enrique Muñoz, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti. "Deep-ECG: Convolutional neural networks for ECG biometric recognition." *Pattern Recognition Letters* 126 (2019): 78-85.
77. Kiranyaz, Serkan, Turker Ince, and Moncef Gabbouj. "Real-time patient-specific ECG classification by 1-D convolutional neural networks." *IEEE transactions on biomedical engineering* 63, no. 3 (2015): 664-675.
78. Chauhan, Sucheta, and Lovekesh Vig. "Anomaly detection in ECG time signals via deep long short-term memory networks." In *2015 IEEE international conference on data science and advanced analytics (DSAA)*, pp. 1-7. IEEE, 2015.
79. Lu, Peng, Saidi Guo, Yingying Wang, Lianxin Qi, Xinzhe Han, and Yuchen Wang. "Ecg classification based on long short-term memory networks." In *Proceedings of the 2nd International Conference on Healthcare Science and Engineering 2nd*, pp. 129-140. Springer Singapore, 2019.
80. Rathakrishnan, Kalaivani, Seung-Nam Min, and Se Jin Park. "Evaluation of ECG features for the classification of post-stroke survivors with a diagnostic approach." *Applied Sciences* 11, no. 1 (2020): 192.
81. Wu, Shun-Chi, Pei-Lun Hung, and A. Lee Swindlehurst. "ECG biometric recognition: unlinkability, irreversibility, and security." *IEEE Internet of Things Journal* 8, no. 1 (2020): 487-500.
82. Khaldi, Amine, Med Redouane Kafi, and Billel Meghni. "Electrocardiogram signal security by digital watermarking." *Journal of Ambient Intelligence and Humanized Computing* 14, no. 10 (2023): 13901-13913.
83. Arquilla, Katya, Andrea K. Webb, and Allison P. Anderson. "Textile electrocardiogram (ECG) electrodes for wearable health monitoring." *Sensors* 20, no. 4 (2020): 1013.
84. Serhani, Mohamed Adel, Hadeel T. El Kassabi, Heba Ismail, and Alramzana Nujum Navaz. "ECG monitoring systems: Review, architecture, processes, and key challenges." *Sensors* 20, no. 6 (2020): 1796.
85. Wang, Peng, Zihuai Lin, Xucun Yan, Zijiao Chen, Ming Ding, Yang Song, and Lu Meng. "A wearable ECG monitor for deep learning based real-time cardiovascular disease detection." *arXiv preprint arXiv:2201.10083* (2022).