International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-14 Issue-1, May 2025

Machine Learning-Based Detection of Wormhole Attacks in IoT Networks Using Classification Models

Manar Almalki, Samah Alajmani

Abstract: ***The widespread adoption of Internet of Things (IoT) networks has introduced new cybersecurity challenges, particularly wormhole attacks. These attacks pose a significant threat to IoT environments by manipulating network routing without altering packet contents, making them difficult to detect using traditional intrusion detection systems (IDS). This study examines the application of machine learning (ML) techniques for detecting wormhole attacks in Internet of Things (IoT) networks. The research compares five machine learning classifiers: Sparse Representation Classifier (SRC), Multi-Layer Perceptron (MLP), Linear Discriminant Analysis (LDA), Quadratic Discriminant Analysis (QDA), and XGBoost, based on metrics such as accuracy, precision, recall, F1-score, and computational efficiency. Data preprocessing techniques were applied to a publicly available IoT dataset to improve the performance of these models. Among the classifiers tested, XGBoost demonstrated superior performance with a detection accuracy of 99.97%, outpacing both traditional and deep learning models. The results highlight the potential of ensemble learning approaches in enhancing IoT security, especially for real-time applications in resource-constrained environments. The study emphasises the importance of striking a balance between detection accuracy and computational efficiency when selecting models for dynamic Internet of Things (IoT) networks. Future work will explore federated learning and hybrid deep learning models to further improve the detection capabilities of wormhole attacks in IoT settings.***

Keywords: ***Anomaly Detection, Cybersecurity, Intrusion Detection, IoT Security, Machine Learning, Wormhole Attacks, XGBoost.***

Abbreviations:
AODV: Ad hoc On-demand Distance Vector
ML: Machine Learning
KNN: K-Nearest Neighbours
GBM: Gradient Boosting Machine
DLBMs: Deep Learning-Based Models
CNM: Conventional Network Monitoring
IQR: Interquartile Range
DT: Decision Trees
DL: Deep Learning
RTT: Round-Trip Time
NB: Naïve Bayes
IDS: Intrusion Detection Systems
SVMs: Support Vector Machines
SGD: Stochastic Gradient Descent
WNCS: Wireless Network Coding Systems
ICMP: Internet Control Message Protocol
MLP: Multi-Layer Perceptron
QDA: Quadratic Discriminant Analysis
SRC: Sparse Representation Classifier
LDA: Linear Discriminant Analysis
MLP: Multilayer Perceptron
FPR: False Positive Rate
MLP: Multi-Layer Perceptron
PR: Precision-Recall

Manuscript Received on 21 March 2025 | First Revised Manuscript Received on 27 March 2025 | Second Revised Manuscript Received on 22 April 2025 | Manuscript Accepted on 15 May 2025 | Manuscript published on 30 May 2025.
*Correspondence Author(s)
Manar Mishal Almalki*, Department of Cybersecurity, Taif University, Taif, Saudi Arabia. Email ID: S44680292@students.tu.edu.sa, ORCID ID: 0009-0002-0678-5083
Samah Hazzaa Alajmani, Assistant Professor, Department of Information Technology, Taif University, Taif, Saudi Arabia. Email ID: s.ajmani@tu.edu.sa, ORCID ID: 0009-0000-7152-9559

I. INTRODUCTION

The growing penetration of the Internet of Things (IoT) in major industries such as health, industrial automation, and smart cities has accompanied remarkable progress in real-time data processing, automation, and decision-making [1]. These advantages are, nonetheless, accompanied by significant security threats, since IoT networks are subject to several cyber vulnerabilities, primarily as a result of their distributed nature, limited processing power, and absence of built-in security measures [2]. Wormhole attacks pose a serious threat by compromising network integrity through the manipulation of routing paths, thereby misleading legitimate nodes into choosing malicious routes. This can result in serious disruptions, such as data interception, packet loss, and unauthorized access, which present serious risks to mission-critical applications like medical monitoring systems, smart grids, and industrial control networks [3].

A wormhole attack occurs when multiple compromised nodes establish a low-latency direct link, or tunnel, between distant points in the network, thereby tricking routing systems into selecting these compromised routes. Unlike conventional cyberattacks, wormhole attacks do not modify packet payloads; instead, they manipulate network topology, making them extremely hard to detect [4]. Traditional intrusion detection systems (IDS) are based on signature detection and encryption methods; however, these approaches usually prove ineffective against wormhole attacks due to their covert and protocol-independent nature. Therefore, improved detection mechanisms must be developed to protect IoT networks from such advanced attacks.

In recent years, machine learning (ML) solutions have emerged as viable alternatives to IoT security, demonstrating their ability to identify sophisticated attack patterns, classify network abnormalities, and adapt to evolving cyber threats [5].

Several works have explored machine learning-based solutions for detecting wormhole attacks, demonstrating their superiority over rule-based and heuristic solutions. Deep learning models and ensemble learning architectures have been particularly effective in modelling nonlinear attack behaviour and enhancing detection accuracy. Nevertheless, challenges remain in identifying the most suitable model that achieves a trade-off among high detection accuracy, low computational cost, and real-time applicability in resource-limited IoT environments [6].

This study aims to develop and compare machine learning-based detection models for wormhole attacks in Internet of Things (IoT) networks. We compare five machine learning classifiers —Sparse Representation Classifier (SRC), Multi-Layer Perceptron (MLP), Linear Discriminant Analysis (LDA), Quadratic Discriminant Analysis (QDA), and XGBoost —to determine the optimal model for detecting wormhole attacks. The models are evaluated based on accuracy, precision, recall, F1-score, and computational complexity to check their suitability for deployment in low-power IoT networks. The research contributes to the literature by providing a detailed comparison of machine learning-based security mechanisms, highlighting the superiority of ensemble learning and deep learning models in addressing sophisticated cyberattacks.

The remainder of this paper is organized as follows: Section 2 reviews the literature, explaining what has already been done regarding wormhole attack detection and pointing out existing research gaps. Section 3 describes the proposed methodology for detecting wormhole attacks. Section 4 presents the results and discusses the efficiency and effectiveness of the proposed method, while Section 5 summarises the paper and provides recommendations on areas for further study.

II. LITERATURE REVIEW

The detection and prevention of wormhole attacks against IoT and ad-hoc networks have been a prominent area of research, resulting in various proposed techniques, including traditional network monitoring methods, machine learning (ML), and deep learning (DL) models. Traditional techniques primarily include topology-based, cryptographic, or signal-strength-based solutions. AI-based models enhance detection effectiveness through automated anomaly detection and greater scalability within dynamic networks. This section offers a structured overview of the earlier literature, identifies methodological variations, and provides a comparative assessment of the current studies.

A review of related studies was conducted to develop an optimal detection framework for identifying wormhole attacks in IoT and ad-hoc networks. Comparative research results in Table I are relevant to this study, highlighting key technologies, contributions, and limitations. The study begins with conventional network monitoring methods, shifts towards machine learning and deep learning-based detection models, and culminates with hybrid approaches utilising AI-based intrusion detection systems.

A. Traditional Wormhole Attack Detection Approaches

Early studies on detecting wormhole attacks focused on conventional security mechanisms, including round-trip time (RTT) analysis, topology-based approaches, and cryptographic authentication techniques. These methods aimed to detect routing anomalies created by hostile tunnels in the network.

Zaw Tun and Aung Htein Maw (2008) suggested an algorithm for wormhole tunnel detection based on round-trip time (RTT) and neighbourhood counts, the goal being the detection of wormhole tunnels based on observation of anomalous delay and abnormal connectivity between nodes in Ad hoc On-Demand Distance Vector (AODV) networks [7]. The simulation results indicated that RTT-based detection of wormhole tunnels is accurate, requiring no special hardware or encryption keys. However, the scheme could not detect multi-hop wormhole attacks and was highly dependent on network topology stability, hence reducing its scalability for use in dynamic IoT networks.

Ji (2015) examined wormhole attacks on Wireless Network Coding Systems (WNCS) using measurement of change in the Expected Transmission Count (ETX) metric as a key vulnerability [8]. The paper proposes two novel detection models: a centralised one with trusted control nodes for anomaly detection and a peer-to-peer model (DAWN) based on anomalous packet traffic changes for decentralised detection. DAWN detected 89.43% of the time; however, the study identified some disadvantages related to collusion resistance, as victim nodes could misrepresent routing parameters to evade detection.

Traditional detection mechanisms offer theoretical security enhancements; however, their practical implementation in massive-scale IoT systems is hampered by high false positives, network topology dependence, and computational inefficiencies. Researchers have investigated machine learning-based detection models that dynamically learn attacks, thereby providing enhanced scalability and accuracy.

B. Machine Learning-Based Approaches

The application of machine learning models to detect wormhole attacks has increased tremendously, as they can recognise attack patterns in network traffic data and enhance the effectiveness of real-time detection.

Gupta, Singh, and Tiwari (2022) carried out a systematic review of machine learning techniques in wormhole detection and established that Support Vector Machines (SVMs) and Decision Trees (DTs) are the top-performing classification algorithms [9]. The research found that hybrid approaches, which combine traditional network monitoring techniques with machine learning-based anomaly detection, yield better detection rates with fewer false positives than standalone cryptographic or topological approaches. The study identified significant limitations, including high energy consumption, lengthy processing times, and difficulty in adapting to dynamic network topologies.

Prasad, Tripathi, and Dahal (2019) Analysed machine learning models for detecting wormhole attacks, comparing the performance of Naïve Bayes (NB) and Stochastic Gradient Descent (SGD) classifiers [10]. The paper presented a dataset of 20 features, including hop count, packet size, and message type measurements. It demonstrated that SGD outperformed traditional DelPHI-based detection

methods, achieving a detection rate of 93.12%. However, their approach required massive labelled datasets, which were problematic for deployment on real-time IoT networks where data labelling is impossible.

A study on the performance of various machine learning classifiers like K-Nearest Neighbours (KNN), Decision Trees (DT), Convolutional Neural Networks (CNN), and Linear Discriminant Analysis (LDA) [11] was carried out by Abdan and Seno (2022). The outcome revealed that Decision Trees performed optimally with 98.9% accuracy, surpassing CNN with 96.4% and SVM with 98.2%. In contrast, KNN and LDA were less effective in classification. Despite these enhancements, the study identified real-time adaptability and computational complexity as vital concerns of ML-based wormhole detection systems.

Although ML-based models improve detection rates, their implementation in real-time, resource-constrained IoT networks is made more difficult by their customary requirement for substantial processing resources and large labelled datasets. Researchers have turned to deep learning techniques to solve these obstacles, which provide improved accuracy and flexibility.

C. Deep Learning Approaches for Wormhole Attack Detection

Recent developments in deep learning techniques have made it easier to create precise and flexible intrusion detection systems for preventing wormhole attacks.

To detect wormhole attacks in IoT networks, Abdullah, Albaihani, Osman, and Omar (2024) developed an LSTM-based Intrusion Detection System (IDS) with a 99% accuracy rate, outperforming Decision Trees at 94% and Naïve Bayes at 93% [12]. Their research highlighted the importance of temporal pattern recognition in network anomaly detection, noting that LSTM models are particularly effective in identifying evolving attack patterns. The study noted that LSTM models require greater computational resources, which complicates their real-time deployment in IoT systems. In their AI-based study of wormhole attack detection techniques, Hanif et al. (2022) evaluated deep learning architectures (DLAs) such as hybrid machine learning models (HMLMs), Long Short-Term Memory networks (LSTMs), and Convolutional Neural Networks (CNNs) [13]. The review revealed significant issues with DL-based wormhole identification, including high false-positive rates and computational inefficiencies. It suggested the adoption of lightweight neural network architectures and federated learning techniques to improve real-time detection efficiency.

Deep learning-based models (DLBMs) offer better detection accuracy; however, significant challenges remain, including high computational requirements and the need for large amounts of labelled datasets, which limit widespread deployment. Hybrid detection approaches (HDAs) incorporate machine learning (ML), deep learning (DL), and conventional network monitoring (CNM) techniques as a proposed solution.

D. Hybrid Detection Approaches

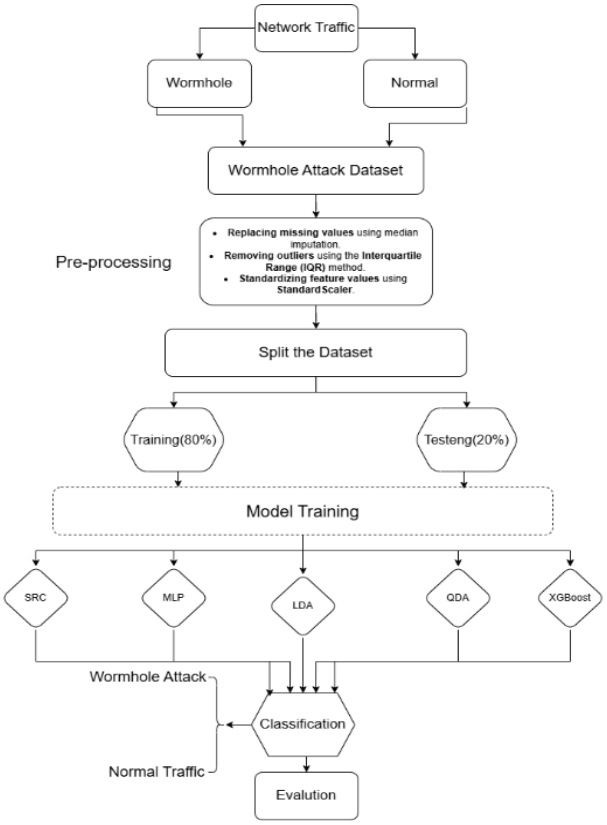
Hybrid detection systems integrate multiple security features to enhance the detection rate while minimising computational overhead. For wormhole and ranking attacks detection in RPL-based IoT networks, Zahra et al. (2022) suggested a hybrid model that employs Gradient Boosting Machine (GBM) for high classification accuracy at low computing costs [14]. The study identified challenges in managing dynamic network topologies, indicating a requirement for enhancements in real-time adaptability, despite its efficiency.

Table-I: Existing Works with Key Technologies and Drawbacks

Authors	Detection Method	Key Contributions	Limitations
Zaw Tun & Aung Htein Maw (2008) [7]	RTT-Based Detection	Identified wormhole tunnels via delay-based anomaly detection	High false positives, ineffective for multi-hop networks
Ji (2015) [8]	ETX-Based Detection	Developed DAWN model (89.43% accuracy) for distorted network coding metrics	Vulnerable to collaborative attacks, limited scalability
Gupta, Singh, and Tiwari (2022) [9]	ML-Based Detection	Identified SVM and Decision Trees as effective classifiers	High energy consumption, dataset dependency
Prasad, Tripathi, and Dahal (2019) [10]	Naïve Bayes, SGD	SGD classifier achieved a 93.12% detection rate	Requires large labelled datasets, limits real-time use
Abdan & Seno (2022) [11]	Decision Trees, CNN	DT achieved 98.9% accuracy, outperforming other ML models	High computational complexity
Abdullah, Albaihani, Osman, and Omar (2024) [12]	LSTM-Based IDS	Achieved 99% detection rate, highest precision	High computational cost, limited IoT scalability
Hanif et al. (2022) [13]	CNN, Hybrid ML Models	CNN-based IDS improved classification accuracy	Requires extensive labelled datasets, real-time limitations
Zahra et al. (2022) [14]	GBM-Based Hybrid IDS	Achieved high classification accuracy with low computational cost	Limited adaptability in dynamic networks

III. METHODOLOGY

The model under consideration aims to identify wormhole attacks in IoT networks by analysing network traffic patterns with the aid of machine learning. The detection process is systematic, beginning from dataset preparation, where inconsistencies and missing values are addressed. Subsequently, data pre-processing enhances data quality by removing outliers and normalising features. Feature analysis is done in the feature analysis step, where the dataset's feature correlations are analysed to optimise the detection process. Then, different machine learning models are built to identify network traffic as usual or malicious. Model testing is done using standard performance measures to measure accuracy and effectiveness. Figure 1 represents the end-to-end process of the proposed detection framework.



[Fig.1: Proposed Model's Flowchart]

A. Wormhole Attack Dataset

This study utilises an openly accessible IoT-based intrusion detection dataset, specifically designed to evaluate the performance of machine learning algorithms in detecting various types of network intrusions, including wormhole attacks. The dataset contains 637,462 samples, out of which 485,334 are labelled as regular traffic and 152,128 as malicious instances, related explicitly to wormhole attacks. Table II provides a concise description of the primary features of the dataset along with their descriptions.

Table-II: Dataset Features and Descriptions

Feature Name	Description	Data Type
duration	Total duration of the packet	float64
Plength	Packet length	int64
Mlength	Maximum length of the packet	int64
HoP	Hop count (number of nodes traversed)	int64
Sno	Sequence number of the packet	int64
Sindex	Source index of the packet	int64
land	Whether the packet has landed	int64
Tmode	Transmission mode	int64
Neighbours	Number of neighbours detected	int64
Hflow	Flow rate of the hops	int64
AvgFlow	Average flow rate across the network	float64
Lflow	Low flow rate	int64
AvgHopCount	Average number of hops per transmission	float64
failedConnection	Number of failed connection attempts	int64
Failed Rate	Rate of failed connections	float64
AODV	Presence of the AODV protocol	float64
ICMP	Presence of ICMP protocol	float64
UDP	Presence of the UDP protocol	float64
Unknown MsgType	Unknown message type ratio	float64
Route Error	Route error frequency	float64
Route Reply	Route reply frequency	float64
Route Reply Acknowledgement	Route reply acknowledgement presence	float64
Route Request	Route request frequency	float64

B. Data Preprocessing

The dataset underwent pre-processing procedures to maintain data quality and enhance model performance. The techniques described address missing values, outliers, and feature scaling to improve consistency and accuracy in machine learning-based wormhole attack detection.

i. Addressing Missing Values

The dataset's missing values were identified and imputed using the median method. This approach reduces bias brought on by mean imputation or arbitrary value swaps while preserving the dataset's statistical distribution. The dataset is kept balanced and reliable for model training by filling in missing values with the median of each feature.

ii. Detection and Removal of Outliers

Outliers were identified and eliminated by applying the Interquartile Range (IQR) method. This technique identifies outliers that may adversely affect classification performance by examining the first (Q1) and third quartiles (Q3) of each feature's distribution [15]. Any value falling outside the range defined by:

$$IQR=Q3-Q \quad \ldots \quad (1)$$

$$\text{Lower Bound}=Q1-1.5\times IQR \quad \ldots \quad (2)$$

$$\text{Upper Bound}=Q3+1.5\times IQR \quad \ldots \quad (3)$$

It was identified as an outlier and excluded from the dataset. This prevents models from being influenced by anomalous data points that do not accurately reflect standard network traffic behaviour.

iii. Feature Normalization

The dataset was standardised by scaling numerical features using StandardScaler, which adjusts each feature to have a mean of zero and a standard deviation of one. This normalization guarantees that all features contribute equally to model training, thereby preventing attributes with larger numerical ranges from overshadowing the learning process [16]. The transformation is expressed as follows:

$$X\_scaled= (X-\mu)/\sigma \quad \ldots \quad (4)$$

X is the original feature value, μ is the mean, and σ is the standard deviation.

iv. Dataset Splitting Strategy

The features were standardised by scaling numerical features with StandardScaler, which transforms each feature to have a mean of zero and a standard deviation of one. The normalisation helps all features contribute equally to model training, thereby preventing attributes with larger numerical ranges from dominating the model's learning. The transformation is given as:

The dataset was divided into training and testing sets for assessing model generalisation. An 80-20 split was used, where 80% of the dataset was allocated for training and 20% for testing. This ensures a sufficient number of samples for both training and

evaluation.

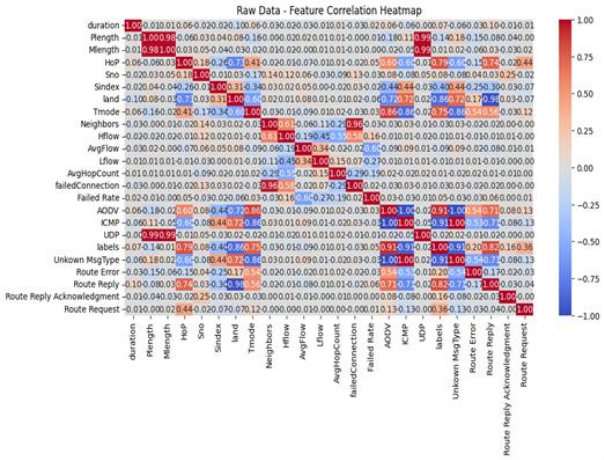
These preprocessing methods ensured that models learn from clean, balanced, and standardized input data, preparing the dataset for efficient machine learning-based lassification.

C. Feature Analysis

Feature analysis plays a vital role in determining the importance of various attributes in identifying wormhole attacks in IoT networks. This study departs from standard feature selection by retaining all the features. Instead of removing less significant or redundant attributes, it conducts correlation analysis to comprehend relationships among various attributes. A correlation heatmap was created to observe the relationship between features and verify the correlation among them. Although high-correlation-value features (above 0.8) were found, direct feature removal did not occur, as each feature was determined to help learn complex patterns of network traffic classification.

By preserving all the dataset's features, the models were given a deep pool of features, allowing them to understand complex interrelations between various network parameters. This helped avoid the loss of vital information and ensured that the models could utilise all the provided data to enhance their predictive performance in differentiating regular traffic from wormhole attack traffic.

Figure 2 illustrates the Correlation Heatmap of Dataset Features. The correlation heatmap visually shows the relationships between the various features in the dataset. Features with higher correlation values indicate stronger relationships, while features with lower correlation values suggest weaker connections. This analysis ensures that all pertinent data points are used efficiently by illuminating how various features contribute to the identification of wormhole attacks.



[Fig.2: Correlation Heatmap of Dataset Features]

D. Machine Learning Models Used

By retaining all the properties of the dataset, the models were provided with a rich feature set, enabling them to learn complex relationships between different network parameters. By conserving essential data, the models were able to utilise all available data to enhance their prediction accuracy and distinguish legitimate traffic from that of wormhole attacks.

Multiple machine learning models were selected to detect wormhole attacks in IoT networks based on their performance in anomaly detection and network traffic classification. Each model varies in strengths compared with pattern detection, feature extraction, and computationally efficient analysis. Below are detailed descriptions of the chosen models.

i. Sparse Representation Classifier

SRC is a classification technique that represents data using a sparse linear combination of basis vectors. This approach identifies patterns that are less reliant on large datasets, making it particularly useful for anomaly detection and other applications. SRC can discern between attack and regular traffic with accuracy because of sparse coding techniques [17].

ii. Multi-Layer Perceptron

A feedforward neural network with several layers using nonlinear activation functions is called a multilayer perceptron (MLP). This technique is frequently used in intrusion detection and is capable of learning complex decision boundaries [18]. The model is organized in the following manner:

- Input layer: Accepts feature vectors that represent network traffic.
- Hidden layers perform weighted transformations and apply non-linear activations.
- The output layer produces classification probabilities for both normal and attack traffic.

iii. Linear Discriminant Analysis

LDA is a supervised learning technique that enhances class separability and reduces data dimensionality. By projecting input features to an optimal subspace, LDA optimizes classification performance, particularly when the dataset feature set has linear relations [19].

iv. Quadratic Discriminant Analysis

Quadratic Discriminant Analysis (QDA) improves Linear Discriminant Analysis (LDA) by using quadratic decision boundaries to depict class distributions. QDA allows different covariance matrices for each class, which makes it more suitable for datasets with non-linear feature distributions than LDA, which assumes a standard covariance structure among classes [20].

v. Extreme Gradient Boosting (XGBoost)

XGBoost is a decision tree-based gradient boosting method designed for high-performance classification applications. By integrating weak classifiers into a robust ensemble model, the learning process is streamlined, improving computing efficiency and accuracy [21]. Notable benefits consist of:

- Utilizing integrated imputation techniques to address missing values.
- Regularization strategies to reduce overfitting.
- Parallelization of execution improves scalability for large datasets.

E. Model Training and Evaluation

A systematic training and assessment procedure was implemented to determine how well the selected machine learning models (MLMs) detected wormhole assaults. The preprocessed dataset was used

to train the models, and their classification performance was then evaluated using unseen data.

i. Training Process

The dataset was split into 80% for training and 20% for testing to obtain adequate data for learning and evaluation purposes. Every model was trained using the training set, and its performance was assessed using the test set. The following steps made up the training process:

- Feature Scaling: Input features were standardized with StandardScaler to ensure numerical consistency.
- Model Fitting: Each model was trained on the labelled training data with optimised hyperparameters.
- The trained models classified test samples into regular and wormhole attack traffic.
- Performance Evaluation: The model outputs were compared with actual labels to calculate evaluation metrics.

ii. Evaluation Metrics

A comprehensive assessment was conducted using multiple evaluation metrics to ensure a balanced analysis of model performance. The metrics chosen are outlined below, accompanied by their corresponding equations [22].

iii. Accuracy

Accuracy measures the proportion of correctly classified instances out of the total dataset. It is given by:

$$\text{Accuracy} = (TP+TN)/(TP+TN+FP+FN) \quad \ldots \quad (5)$$

Where:

TP = True Positives (correctly classified attacks).

TN = True Negatives (correctly classified regular traffic).

FP = False Positives (regular traffic misclassified as attacks).

FN = False Negatives (attacks misclassified as regular traffic).

- *Precision*

Precision indicates the proportion of correctly identified attack instances among all predicted attacks. It is defined as:

$$\text{Precision} = TP/(TP+FP) \quad \ldots \quad (6)$$

- *Recall*

Recall (or Sensitivity) measures the model's ability to detect actual attacks correctly. It is given by:

$$\text{Recall} = TP/(TP+FN) \quad \ldots \quad (7)$$

- *F1-Score*

The F1-score is the harmonic mean of precision and recall, providing a balanced evaluation when dealing with imbalanced datasets. It is calculated as:

$$F1 = (2\times\text{Precision}\times\text{Recall})/(\text{Precision}\times\text{Recall}) \quad \ldots \quad (8)$$

- *AUC-ROC Curve*

The Area Under the Receiver Operating Characteristic (AUC-ROC) curve evaluates the trade-off between the actual positive rate (recall) and the false positive rate (FPR) across different classification thresholds. A higher AUC score indicates better discrimination between attack and normal traffic instances.

- *Computational Time*

To measure the efficiency of each model, computational time was recorded during both the training and inference phases. This helps assess the trade-off between model accuracy and processing speed, which is crucial for real-time IoT security applications.

IV. RESULTS AND DISCUSSION

This section explains a detailed comparison of the models for detecting wormhole attacks in IoT networks. The performance of the models was compared using various evaluation metrics, including accuracy, precision, recall, F1-score, AUC-ROC, and computational time. The outcomes were also compared with another research that utilized the same dataset to determine the efficiency of the proposed scheme.

A. Performance Analysis of the Models

Five classifiers were evaluated based on their ability to distinguish between normal and malicious traffic to identify the most effective model for detecting wormhole attacks. Table III provides an overview of their performance.

Among the models, XGBoost significantly outperformed the others, achieving the highest accuracy (99.97%) while maintaining a strong balance between precision (99.92%) and recall (99.95%). MLP also demonstrated strong performance but required considerably longer computational time, making it less suitable for real-time applications. In contrast, models like LDA and QDA achieved reasonable accuracy but suffered higher false favourable rates, reducing their reliability in real-world scenarios.

Figure 3 presents the confusion matrices for the evaluated models: (a) Confusion matrix for the Sparse Representation Classifier (SRC), illustrating its classification performance and false positive rate; (b) Confusion matrix for the Multi-Layer Perceptron (MLP), highlighting its strong classification accuracy and minimal misclassification errors; (c) Confusion matrix for Linear Discriminant Analysis (LDA), demonstrating its ability to distinguish between normal and malicious traffic, albeit with a higher false positive rate; (d) Confusion matrix for Quadratic Discriminant Analysis (QDA), showcasing its improved recall but lower precision; (e) Confusion matrix for XGBoost, confirming its superior classification accuracy with minimal false positives and false negatives.

We created ROC curves to get a clearer picture of our models' performance. These graphs show the balance between the actual positive and false favourable rates. After checking the AUC to pinpoint the best models for classification, we discovered that XGBoost and MLP stood out as the most successful.

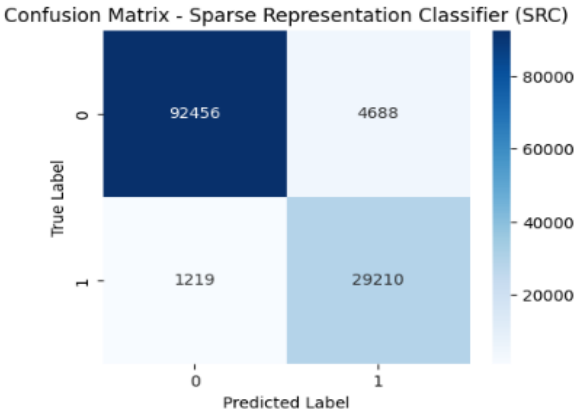
The Precision-Recall (PR) curve serves as another crucial tool to evaluate performance. It shows how precision and recall balance each other. XGBoost and MLP showed the most steady balance between precision and recall,

proving they work well to spot wormhole attacks. Refer to Figure 4, which highlights the performance of our models. In part (a), you'll find ROC curves, which give us a clear picture of the balance each model strikes between the actual positive rate (TPR) and the false positive rate (FPR). XGBoost and MLP are the real stars here, with their top-notch AUC scores showing they're the most skilled at classification.

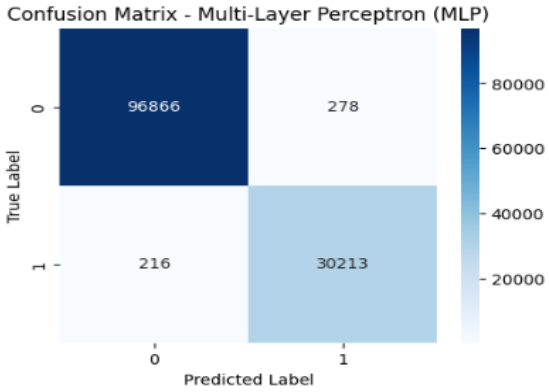
In part (b), we have the Precision-Recall (PR) curves, which help us understand how precision and recall vary among the models. Just like before, XGBoost and MLP come out on top, proving they are exceptional at identifying wormhole attacks.

Table-III: Model Performance Summary

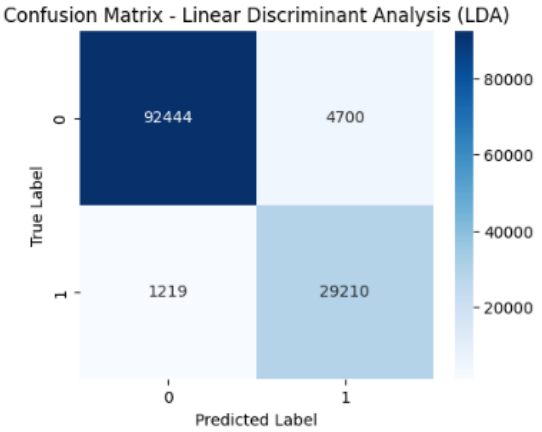
Model	Training Accuracy	Validation Accuracy	Accuracy	Precision	Recall	F1-score	AUC-ROC
SRC	95.36%	95.37%	95.37%	86.17%	95.99%	90.81%	50.00%
MLP	99.51%	99.52%	99.52%	98.91%	99.08%	98.99%	99.98%
LDA	95.35%	95.36%	95.36%	86.14%	95.99%	90.80%	98.99%
QDA	95.57%	95.54%	95.54%	84.50%	99.54%	91.41%	99.43%
XGBoost	99.97%	99.97%	99.97%	99.92%	99.95%	99.93%	99.99%



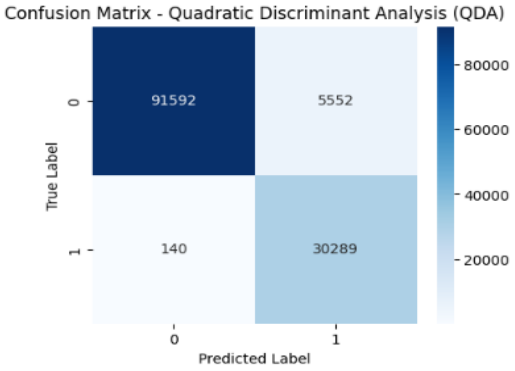
[Fig.3: (a) Confusion Matrix for SRC]



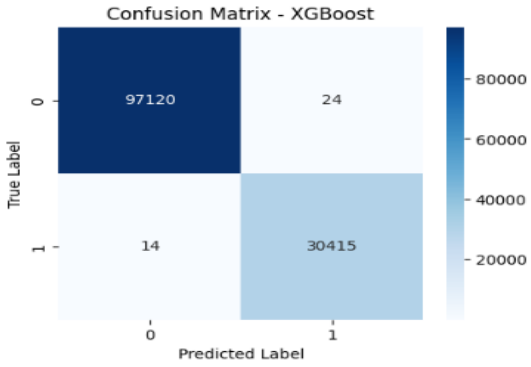
[Fig.3: (b) Confusion Matrix for MLP]



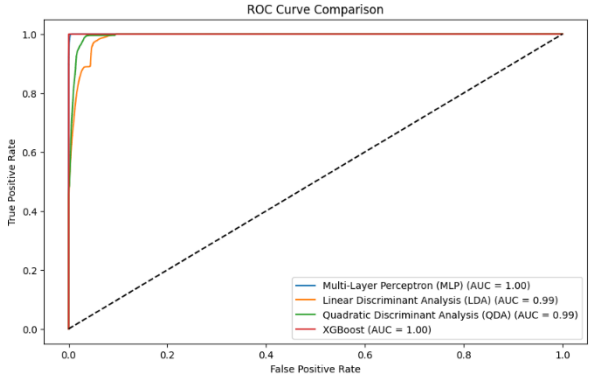
[Fig.3: (c) Confusion Matrix for LDA]



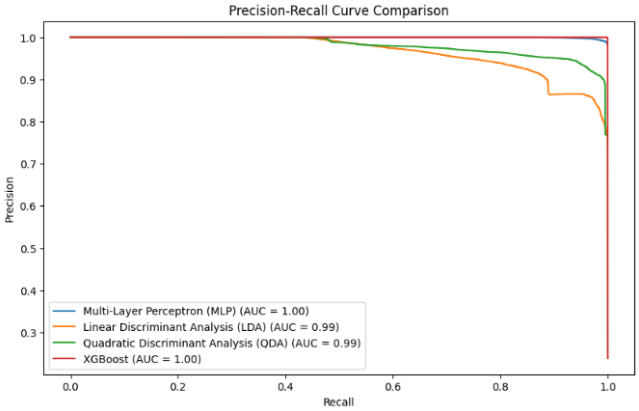
[Fig.3: (d) Confusion Matrix for QDA]



[Fig.3: (e) Confusion Matrix for XGBoost]



[Fig.4: (a) ROC Curve Comparison of All Models]



[Fig.4: (b) Precision-Recall Curve Comparison]

Table-IV: Comparison with Other State-of-the-Art Methods

Author	Method-Algorithm	Result				
		Accuracy	Precision	Recall	F1-score	AUC-ROC
Abdullah, Albaihani, Osman, and Omar (2024) [12]	LSTM	99.00%	98.70%	98.40%	98.50%	-
	Decision Tree	94.00%	94.00%	93.80%	93.90%	-
	Naïve Bayes	93.00%	90.50%	91.00%	90.70%	-
Our Proposed Models	SRC	95.37%	86.17%	95.99%	90.81%	50.00%
	MLP	99.52%	98.91%	99.08%	98.99%	99.98%
	LDA	95.36%	86.14%	95.99%	90.80%	98.99%
	QDA	95.54%	84.50%	99.54%	91.41%	99.43%
	XGBoost	99.97%	99.92%	99.95%	99.93%	99.99%

B. Comparison with a Related Study Utilizing the Same Dataset

To further support the effectiveness of the proposed strategy, the results obtained were regularly compared with those of a previous study that utilised the same dataset but employed different machine learning approaches. Table IV presents this comparison and provides an overall evaluation of the performance of other models on all significant classification criteria, offering some insight into the comparative strengths and limitations of different strategies.

The results indicate that XGBoost outperformed all models from the other study, particularly in terms of accuracy and computational efficiency. While LSTM in the previous survey showed strong performance, XGBoost achieved higher accuracy with lower computational requirements, making it a more practical choice for real-time IoT security.

C. Discussion

The findings conclude that XGBoost is the highest-performing model in wormhole attack detection, surpassing traditional models and deep learning models in terms of both accuracy and computational cost. Compared to other methods that used the same dataset, XGBoost achieved superior classification performance with a very low false positive and false negative rate, making it highly suitable for practical applications.

Additionally, the SRC and QDA models were characterised by low precision but high recall, leading to a higher incidence of false alarms. It would imply model choice such that precision and recall are proportionate, ensuring that there are no excessive alarms, while maintaining accuracy.

The ability of XGBoost in this study reflects the effectiveness of ensemble learning approaches to securing IoT networks. Being a computationally efficient and highly predictable algorithm, XGBoost provides a stable process for identifying wormhole attacks in adaptive networks.

V. CONCLUSION AND FUTURE WORK

In short, this study successfully developed a machine learning-based detection of wormhole attacks and tested five models to compare their performance in securing IoT networks.

The result indicates that XGBoost outperforms all other models with the best accuracy of 99.97% and, therefore, the most reliable model to detect wormhole attacks. XGBoost was also observed to achieve improved classification performance with lower computational overhead compared to baseline and deep learning-based models, making it very suitable for real-time intrusion detection in resource-constrained IoT networks. The findings of this study are beneficial in enhancing IoT security by providing a scalable and efficient detection approach that can effectively identify wormhole attacks with negligible false positives. Comparison with the advanced method used in the reference paper also confirms the efficacy of the proposed method, as it establishes relevance with real-world network security systems. Various potential enhancements can be considered to increase detection efficiency and address future cyberattacks.

Integrating deep learning methods, such as CNNs, RNNs, and XGBoost, will enhance feature extraction and classification, providing accurate detection.

Coupling real-time anomaly detection with NIDS would enable the model to observe live traffic, making it an even more effective means of detecting current attacks. Yet another potential avenue of research is implementing federated learning platforms to enable models to learn across different IoT devices, while ensuring data privacy and reducing reliance on centralised processing. Based on these solutions, future research can be optimally tuned and adjusted to make wormhole attack detection systems more adaptive, less prone to false positives, and better immune to sophisticated cyberattacks in dynamic IoT environments.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it was conducted without any external influence.
- **Ethical Approval and Consent to Participate:** The data provided in this article is

exempt from the requirement for ethical approval or participant consent.

- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Thamilarasu, G., & Chawla, S. (2019). Towards Deep-Learning-Driven intrusion detection for the internet of things. Sensors, 19(9), 1977. DOI: https://doi.org/10.3390/s19091977
2. Alghamdi, R., & Bellaiche, M. (2022c). A cascaded federated deep learning based framework for detecting wormhole attacks in IoT networks. Computers & Security, 125, 103014. DOI: https://doi.org/10.1016/j.cose.2022.103014
3. Reddy, R. C. S., Mallikarjuna, A. G., Rathaiah, M., Reddy, B. S., Raghava, E. V., Srinivas, T. A. S., Sarabu, A., Ramasekhar, G., & Suneetha, S. (2024b). Wormhole detection scheme with adaptive deep neural network and hybrid Multi-Objective mitigation for the Internet of Things. African Journal of Biomedical Research. DOI: https://doi.org/10.53555/ajbr.v27i3.5445
4. Tatar, E. E., & Dener, M. (2021b). Wormhole attacks in IoT-based networks. 2021 6th International Conference on Computer Science and Engineering (UBMK), 68, 478–482. DOI: https://doi.org/10.1109/ubmk52708.2021.9558996
5. Thamilarasu, G., & Chawla, S. (2019b). Towards Deep-Learning-Driven intrusion detection for the internet of things. Sensors, 19(9), 1977. DOI: https://doi.org/10.3390/s19091977
6. Alshehri, A. H. (2024b). Wormhole attack detection and mitigation model for Internet of Things and WSN using machine learning. PeerJ Computer Science, 10, e2257. DOI: https://doi.org/10.7717/peerj-cs.2257
7. Tun, Z., & Maw, A. H. (2008). Wormhole attack detection in wireless sensor networks. World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 2(10), 2184–2189. https://www.ucsy.edu.mm/ucsy/publications/wireless/WASET2008.pdf
8. Prasad, M., Tripathi, S., & Dahal, K. (2019c). Wormhole attack detection in ad hoc networks using machine learning techniques. 2022 13th International Conference on Computing, Communication, and Networking Technologies (ICCCNT). DOI: https://doi.org/10.1109/icccnt45670.2019.8944634
9. Gupta, C., Singh, L., & Tiwari, R. (2022b). Wormhole attack detection techniques in ad-hoc networks: A systematic review. Open Computer Science, 12(1), 260–288. DOI: https://doi.org/10.1515/comp-2022-0245
10. Prasad, M., Tripathi, S., & Dahal, K. (2019d). Wormhole attack detection in ad hoc network using machine learning technique. 2022 13th International Conference on Computing, Communication, and Networking Technologies (ICCCNT). DOI: https://doi.org/10.1109/icccnt45670.2019.8944634
11. Abdan, M., & Seno, S. A. H. (2022b). Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad hoc Network (MANET). Wireless Communications and Mobile Computing, 2022, 1–12. DOI: https://doi.org/10.1155/2022/2375702
12. Abdullah, A., Albaihani, A. N. A., Osman, B., & Omar, Y. (2024b). Detecting Wormhole Attack in Environmental Monitoring System for Agriculture using Deep Learning. Journal of Advanced Research in Applied Sciences and Engineering Technology, 51(2), 153–176. DOI: https://doi.org/10.37934/araset.51.2.153176
13. Hanif, M., Ashraf, H., Jalil, Z., Jhanjhi, N. Z., Humayun, M., Saeed, S., & Almuhaideb, A. M. (2022b). AI-Based wormhole attack detection techniques in wireless sensor networks. Electronics, 11(15), 2324. DOI: https://doi.org/10.3390/electronics11152324
14. Zahra, F., Jhanjhi, N., Brohi, S. N., Khan, N. A., Masud, M., & AlZain, M. A. (2022b). Rank and wormhole attack detection model for RPL-based Internet of Things using Machine learning. Sensors, 22(18), 6765. DOI: https://doi.org/10.3390/s22186765
15. Khan, M. S., Nath, T. D., Hossain, M. M., Mukherjee, A., Hasnath, H. B., Meem, T. M., & Khan, U. (2023b). Comparison of multiclass classification techniques using the dry bean dataset. International Journal of Cognitive Computing in Engineering, 4, 6–20. DOI: https://doi.org/10.1016/j.ijcce.2023.01.002
16. Thakker, Z. L., & Buch, S. H. (2024b). Effect of feature scaling pre-processing techniques on machine learning algorithms to predict particulate matter concentration for Gandhinagar, Gujarat, India. International Journal of Scientific Research in Science and Technology, 410–419. DOI: https://doi.org/10.32628/ijsrst52411150
17. Hajigholam, M., Raie, A., & Faez, K. (2020b). Using sparse representation Classifier (SRC) to calculate dynamic coefficients for multitask joint spatial pyramid matching. Iranian Journal of Science and Technology Transactions of Electrical Engineering, 45(1), 295–307. DOI: https://doi.org/10.1007/s40998-020-00351-3
18. Elghamrawy, S. M., Lotfy, M. O., & Elawady, Y. H. (2022b). An intrusion detection model based on deep learning and multi-layer perceptron in the Internet of Things (IoT) network. In Lecture notes on data engineering and communications technologies (pp. 34–46). DOI: https://doi.org/10.1007/978-3-031-03918-8_4
19. Gatea, M. J., & Hameed, S. M. (2022b). An Internet of Things botnet detection model using regression analysis and linear discrimination analysis. Iraqi Journal of Science, 4534–4546. DOI: https://doi.org/10.24996/ijs.2022.63.10.36
20. Hasan, M. K., Ghazal, T. M., Alkhalifah, A., Bakar, K. a. A., Omidvar, A., Nafi, N. S., & Agbinya, J. I. (2021b). Fischer Linear Discrimination and Quadratic Discrimination Analysis–Based Data Mining Technique for Internet of Things Framework for Healthcare. Frontiers in Public Health, 9. DOI: https://doi.org/10.3389/fpubh.2021.737149
21. Wang, X., & Lu, X. (2020b). A Host-Based anomaly detection framework using XGBoost and LSTM for IoT devices. Wireless Communications and Mobile Computing, 2020, 1–13. DOI: https://doi.org/10.1155/2020/8838571
22. Ntayagabiri, J. P., Bentaleb, Y., Ndikumagenge, J., & Makhtoum, H. E. (2025). A comparative analysis of supervised Machine learning algorithms for IoT attack detection and Classification. Journal of Computing Theories and Applications, 2(3), 395–409.

DOI: https://doi.org/10.62411/jcta.11901

AUTHOR'S PROFILE

Manar Mishal Almalki holds a bachelor's degree in computer engineering from the College of Computers and Information Technology at Taif University, Taif, Saudi Arabia. I am pursuing a master's degree in cybersecurity. My professional expertise includes understanding security vulnerabilities and exploring methods to enhance system protection. I thrive in diverse and challenging settings, adapting to new technologies and problem-solving in dynamic environments. Committed to Through continuous learning, I stay up-to-date with advancements in cybersecurity, developing my skills and expanding my knowledge in the field.

Samah Hazzaa Alajmani received the B.Sc. degree in 2004 and Ph.D. in 2019 from King Abdulaziz University, Jeddah, Saudi Arabia, both in Computer Science. She earned an M.Sc. in Information Technology from the Queensland University of Technology, Brisbane, Australia. She is an Assistant Professor at Taif University, Taif, Saudi Arabia. Her research interests include Cybersecurity, AI, IoT, Deep Learning, and Machine learning.