ISSN: 2182-2069 / E-ISSN: 2182-2077

Analysis of Internet of Things to Enhance Security Using Artificial Intelligence based Algorithm

Noha Mostafa Mohamed Said[1*], Sabna Machinchery Ali[2], Naseema Shaik[3],
Khan Mohamed Jarina Begum[4], Dr. Anwaar Ahmed Abd elLatif Shaban[5], and
Dr. Betty Elezebeth Samuel[6]

[1*]Department of Computer Science, College of Engineering & Computer Science, Jazan University, Jazan, Saudi Arabia. nsaid@jazanu.edu.sa, https://orcid.org/0009-0004-9315-1138

[2]Department of Computer Science, College of Engineering & Computer Science, Jazan University, Jazan, Saudi Arabia. saAli2@jazanu.edu.sa, https://orcid.org/0009-0001-4581-525X

[3]Computer Science Department, College of Science and Arts, King Khalid University, Abha, Saudi Arabia. nshibrahim@kku.edu.sa, https://orcid.org/0009-0002-2270-5792

[4]Department of Computer Science, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia. jkhanmohamed@jazanu.edu.sa, https://orcid.org/0000-0002-7197-190X

[5]Center for E-Learning, Jazan University, Jazan, Saudi Arabia. aabdellatef@jazanu.edu.sa, https://orcid.org/0009-0000-9130-4699

[6]Department of Computer Science, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia. bsamuel@jazanu.edu.sa, https://orcid.org/0000-0002-3141-7277

Received: July 27, 2024; Revised: September 7, 2024; Accepted: October 7, 2024; Published: November 30, 2024

Abstract

Exploring creative methods to secure IoT networks is vital due to the enormous security concerns created by the rapid proliferation of the Internet of Things (IoT). To increase the security of the IoT, this study examines the use of artificial intelligence (AI), specifically deep learning (DL) as well as machine learning (ML) techniques. Three state-of-the-art DL algorithms—Long Short-Term Memory (LSTM), Deep Belief Networks (DBN), Convolutional Neural Networks (CNN)—along with three ML methods—CatBoost, LightGBM, and XGBoost—are examined. These algorithms are renowned for their capability to handle big, as well as unbalanced datasets. This work test how well each algorithm can identify anomalies, categorize attacks, and forecast vulnerabilities using an IoT security dataset, such as CICIDS 2017 as well as IoT-23. The research evaluates algorithms by comparing their accuracy and training time. Classification tasks are where CatBoost and LightGBM really good, but when it comes to sequential data and complicated attack patterns, DL algorithms like CNN and LSTM are good. To provide the groundwork for creating AI-driven security solutions optimised for IoT systems, this research sheds light on the benefits and drawbacks of each method.

Keywords: IoT Security, Deep Learning, Internet of Things, Anomaly Detection, Cybersecurity, Machine Learning.

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 4 (November), pp. 590-604.
DOI: *10.58346/JISIS.2024.I4.037*

*Corresponding author: Department of Computer Science, College of Engineering & Computer Science, Jazan University, Jazan, Saudi Arabia.

1 Introduction

A concept known as the IoT describes embedded computer objects that are uniquely and recognizable linked within the current internet infrastructure, allowing them to gather as well as share data without the need for human involvement. Through the use of sensors and software, this technology expands the capabilities of the internet beyond conventional computer devices to include a vast array of physical things that can interact and communicate with their surroundings (Rupanetti & Kaabouch, 2024). A work categorizes the challenges of maintaining IoT security, examining the application of AI in IoT security, providing security frameworks along with tactics, underscoring ethical as well as privacy issues, and providing insights from real-world case studies (Humayun et al., 2024). An article provides a thorough assessment of research obstacles, unresolved problems, and necessary future research (Saied et al., 2024).

A study, based on comprehensive IP IOT fusion technology, proposes an AI network security management optimization method. Because of this, managing network security will be more precise and practical. Based on findings from studying the all-IP IoT's integration technology, this study has created a model for managing the network's security in an IoT setting (Fei, 2024). Another study has focused on modern cybersecurity solutions that use AI to make them better and to solve privacy and security issues (Messinis et al., 2024). In order to increase customer loyalty, this study looks at how cutting-edge technologies like AI, the IoT, along with big data may improve consumer engagement, happiness, relationships, and experiences. This provide a comprehensive examination of potential integrations between these technologies, emphasizing their potential to enhance various facets of customer loyalty (Rane, 2023).

Another paper provides a comprehensive analysis of smart tourism destinations (STDs) in light of IoT as well as AI integration, including their current state, problems, and possible future trajectory (Lukita et al., 2023). It explores various AI methods and data collection systems enabled by the IoT that have the potential to improve destination management and the traveler experience. However, addressing issues such as data security and privacy is imperative (Salman & Alomari, 2023). This article delves into the applications, difficulties, as well as potential profits of combining AI with IoT-based sensors. With the use of AI, smart sensors can track things like energy consumption, weather, and the state of buildings and infrastructure in real time (Rane et al., 2023).

Securing IoT networks is dominant to prevent malicious activities such as unauthorized access, data theft, as well as denial-of-service (DoS) attacks. Traditional security mechanisms are often inadequate for the scale and complexity of IoT networks. As such, the integration of AI, particularly ML and DL, holds promise in improving IoT security. The following contributions constitute the main points of this paper.

- Using two well-known IoT security datasets, CICIDS 2017 and IoT-23, this study compares and contrasts three state-of-the-art ML algorithms (CatBoost, XGBoost, as well as LightGBM) with three state-of-the-art DL algorithms (CNN, LSTM, along with DBN) as they pertain to IoT security.
- This research looks at the models' accuracy, precision, recall, and F1 scores to see how they identify and categorize different types of IoT security threats, including DoS, Distributed DoS (DDoS), and botnet attacks.
- This work also looks at the algorithms' strengths and shortcomings.

Here is a structure of the work organization: Section 2 reviews relevant research on various algorithms that analyze the IoT with the goal of improving security. Section 3 discusses the proposed technique. Section 4 includes details on the research findings, along with some limitations of the current study. Section 5 concludes the work, and the next section contains the references.

2 Literature Review

Fuentes-Peñailillo et al., (2024) explored the smart crop management through the integration of technologies like digital agriculture. This approach considers modern agricultural tools like the IoT, remote sensing, and AI. Given that different climates impact the resources available for agriculture, this is crucial. The IoT and sensor network integration allow farmers to monitor crop health in real-time, providing information on soil conditions, insect presence, environmental variables as well as plant water status. Optimal fertilization, irrigation, and pest management may result from data-driven decisions. Unmanned aerial vehicles (UAVs) and drones, among other technologies, may improve monitoring capabilities via precise crop growth tracking and thorough field surveys.

Aruchamy et al., (2023) outlined a study that proposes an approach to energy-aware intrusion detection as well as safe routing, based on AI. Developers may use this model to create an IoT-enabled WSN. This approach begins by activating the intrusion detection system, which will then classify different sorts of attacks. Then integrate a judgment process based on game strategy with the intrusion detection model to determine the need for security. Finally, an energy-conscious ad hoc on-demand distance vector method provides safe routing between several nodes. Many applications have combined the IoT along with wireless sensor networks (WSNs) to facilitate reliable communication systems. In order to transmit the detected data to the cloud, the IoT nodes use WSN.

Mazhar et al., (2023) discussed that by automating chores, boosting productivity, as well as lowering anxiety, IoT has the possibility to improve life in a number of settings, including schools and smart cities. Cyberattacks and threats significantly impact intelligent IoT applications. Due to new threats and weaknesses, many of the old techniques for securing the IoT are now useless (Alizadeh et al., 2020). For the security protocols of future IoT systems, AI-efficient ML and DL will be necessary (Pragadeswaran et al., 2024). Using the capabilities of AI, particularly ML and DL solutions, is essential for the next-generation IoT system to have a continually growing as well as current security system (Kotenko et al., 2017). This study examines IoT security intelligence from all possible perspectives.

Padmanaban et al., (2023) introduced the notion of Internet objects and then describes the domains and applications that this technology impacts. This study also examines the role of Internet objects as a technology infrastructure and building management system, enabling intelligent control, entertainment control, and temperature control in smart homes. Internet objects show a crucial part in enhancing the quality of life in societies, particularly in smart homes. Because the smart house has AI and can do certain tasks autonomously, it may provide a report on its environmental conditions and the landlord's instructions. In reality, it can enhance the security of a smart home by utilizing Internet technology, web-based objects, and applications that leverage this technology to monitor and control the house's devices more effectively.

Srinadi et al., (2023) discussed that financial systems and cryptocurrencies have gained popularity. In order to reduce investment risk as well as portfolio construction, fraud, predict price along with trend, AI is required. The study highlights contemporary AI research on Bitcoin, the most well-known cryptocurrency. This examines IoT as well as AI strategies in relation to Bitcoin and cryptocurrencies. This work also identified a number of possible research avenues and areas to enhance the efficacy of the results. In recent years, cybersecurity and AI have expanded quickly. Finance, institutions, markets, and the law have all profited immensely from its adoption. AI mimics intelligent devices that resemble humans. Money AI is changing how people communicate about money. For the financial industry, it optimizes economic risk management, quantitative research, marketing, and credit decisions.

Ghazal, (2021) gave details about how to handle patient records and monitor patients precisely, since healthcare institutions have been embracing technological innovations in recent years. Despite the complexity of the health care information and communication technology network, security remains a significant concern. Conventional algorithms may find it challenging to organize and protect unstructured data, such as electronic papers and reports, that are not part of organized databases. The current clustering approach suffers from efficiency issues with data transmission. This article recommends the IoT with AI System (IoT-AIS) for enhancing health care security. IoT technology creates wireless sensor networks. IoT networks connect the digital and physical worlds. This use IoT-AIS to encrypt and monitor patient data.

Kuzlu et al., (2021) discussed concerns about cybersecurity that have grown in tandem with the IoT explosive growth in recent years. The development of intricate algorithms to safeguard networks and systems, particularly IoT systems, is at the forefront of cyber security. Cybercriminals have found methods to exploit AI, and they have even begun deploying hostile AI in their efforts to launch cybersecurity attacks. This article compiles information from several surveys and research articles on AI, the IoT, and attacks with and against AI in order to provide a comprehensive presentation and summary of relevant literature in these areas. Additionally, it delves into the interconnections among these three domains.

Subeesh & Mehta, (2021) highlighted that agriculture automation has emerged as the sole viable choice and a need in the majority of nations where crop development is just not feasible. AI and the IOT have already begun to make inroads into every sector, including agriculture. Advances in digital technology have enabled smart systems to monitor, operate, and visualize a variety of agricultural activities in real-time, with intelligence similar to that of human specialists, leading to revolutionary transformations in agriculture. The study discusses the uses of IoT as well as AI in the development of smart farm equipment, fertilizer application, irrigation systems, weed, drones for plant protection, insect control, crop health monitoring, smart machine structures, greenhouse culture, etc.

Khan et al., (2023) defined collaborative approaches that integrate blockchain, the IoT as well as AI with ML. The IoT permissionless network architecture enables a blockchain that provides solutions for cross-chain platforms, known as "B-SMEs." This research tackles these difficulties as well as proposes a secure framework with a standardized process hierarchy/lifecycle for distributed small and medium-sized firms (SMEs). Another area that B-SMEs tackle in this setting is lightweight stakeholder authentication. To do this, B-SMEs employ one of three unique chain codes. It supervises the registration of participating SMEs, manages daily information, facilitates communication between nodes, and scrutinizes transaction data pertaining to partnership exchanges before permanently integrating into the blockchain. Table 1 lists the pros and limitations of the existing work.

Table 1: Existing Work Review

Papers and Authors	**Method**	**Advantages**	**Limitations**
(Kotenko et al., 2017)	IOT	Works with threats and vulnerabilities.	-
(Ghazal, (2021	IoT-AIS	The security of the health care network.	Does not use any real-time mobile application.
(Kuzlu et al., 2021)	IOT	Works well cybersecurity attacks.	This work does not consider current risks and its vulnerabilities.
(Khan et al., 2023)	SMEs	Work with SMEs' transparency, provenance, integrity, availability, trustworthiness as well as dependability across two different enterprises.	-

3 Proposed Methodology

Analyzing the efficacy of these models for identifying and categorizing IoT attacks, this research investigates the potential use of DL as well as ML algorithms to increase IoT security. The approach makes use of the CICIDS 2017 and IoT-23 datasets, two of the most well-known in the IoT security space. This work initially preprocesses the datasets to deal with missing values, normalise features, and identify key properties. Then this work test three ML algorithms such as XGBoost, LightGBM, and CatBoost with three DL algorithms such as CNN, LSTM, and DBN. Each model is trained and assessed using classification measures such as F1-score, AUC-ROC, precision, accuracy, as well as recall. Thus the models' ability is tested to identify different types of attacks such as botnets, DDoS attacks, along with DoS. Figure 1 displays the proposed flow diagram.

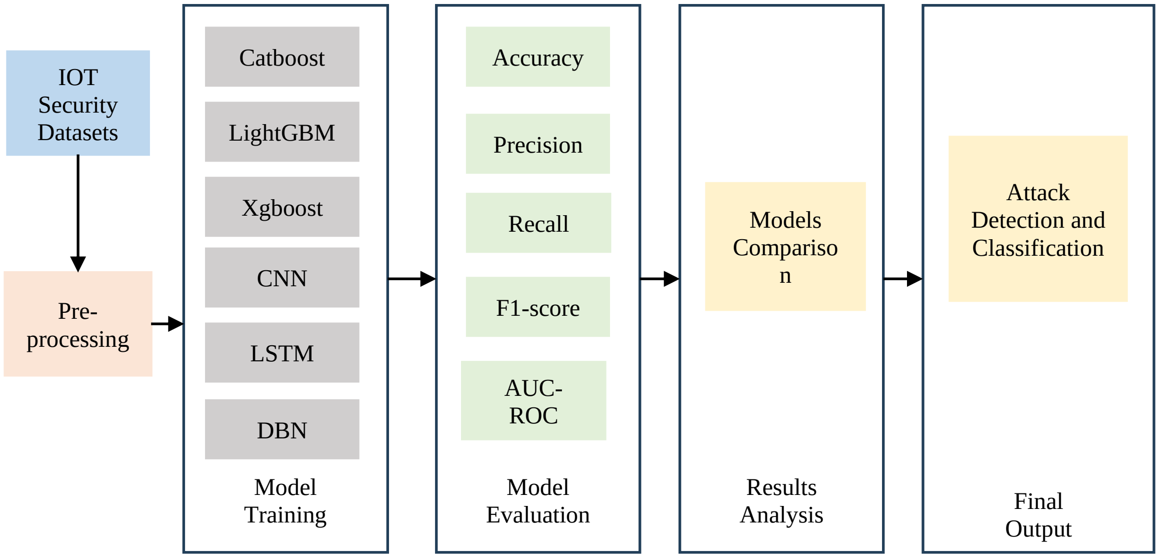

Figure 1: Proposed Flow

3.1. Dataset Description

The proposed models are assessed using two well-known IoT security datasets, CICIDS 2017 and IoT-23. The Canadian Institute for Cybersecurity gathered the CICIDS 2017 dataset, which includes IoT device traffic data under both normal and attack situations. Attacks such as DoS, botnet attacks as well as DDoS pertain to this category. Connectivity time, packet count, and byte count are some of the characteristics that reflect network traffic in the dataset. The IoT-23 dataset includes labeled traffic from IoT devices with both benign and IoT attacks, such as port scanning, DoS, and DDoS. This dataset is relatively new. In both datasets, more than twenty characteristics per record represent details of network traffic.

3.2. Dataset Preprocessing

Normalization, feature selection, and data cleaning are all parts of dataset preprocessing. Data cleaning involves removing superfluous characteristics, duplicates, and missing information from datasets. One key component of feature selection is prioritizing pertinent features according to their impact on IoT security. The process of data normalisation ensures that features are on the same scale, which is crucial for ML and DL models.

3.2.1. Data Cleaning

Data cleaning can identify and eliminate errors and inconsistencies in data. Due to the prevalence of noise, missing values, and irrelevant information in sensor data and network traffic logs, data cleaning is of the utmost importance when it comes to IoT security datasets. This, in turn, might impact the effectiveness of ML models. Addressing missing numbers and detecting and removing outliers are part of data cleaning. Outliers are extreme numbers that significantly deviate from the rest of the data. Outliers may distort the model's performance. The Z-score method is used in this research to find outliers (Larriva-Novo et al., 2021). To find out how far off from the mean certain data points are, the Z-score method uses a specific amount of standard deviations. The Z-score formula is mentioned in equation (1) represents X. In this context, μ stands for the data mean and σ for the standard deviation.

$$Z = \frac{X-\mu}{\sigma} \qquad (1)$$

3.2.2. Feature Selection

Feature selection improves the model's performance during training by picking out the most important features (variables) and removing the ones that aren't useful, redundant, or noisy. Big datasets with plenty of features that don't necessarily help the current job (attack categorization or anomaly detection) are common in IoT security applications. The feature selection process incorporates a filter mechanism to evaluate the significance of each feature, independent of the ML algorithm. A popular statistical test that assesses the feature's independence from the target variable is the Chi-square test (Ahakonye et al., 2023) is used in this research and is equated in equation (2).

$$X^2 = \sum \frac{(O_i - E_i)^2}{E_i} \qquad (2)$$

Where O_i is the observed frequency and E_i is the expected frequency.

3.2.3. Data Normalization

The goal of data normalization, also known as scaling, is to standardize the scale of features. This is crucial since many ML algorithms are sensitive to the scale of the data, and features with high values could end up dominating the learning process and producing subpar results. IoT security uses normalisation to normalise features like packet count and byte size, which may have widely varying ranges (Gupta et al., 2022). Min-max scaling is a technique for data normalization; it scales the data to a predetermined range, usually between 0 and 1, to ensure consistency. The Min-Max scaling formula is in equation (3):

$$x_{normalized} = \frac{x - min(x)}{max(x) - min(x)} \quad (3)$$

Where x is the original value and $max(x)$ and $min(x)$ are the maximum as well as minimum values of the feature.

3.3. Model Evaluation and Metrics

The three ML algorithms (Lucas et al., 2023) and three DL methods used in this research are detailed in the below sub-sections.

3.3.1. Machine Learning Algorithms

3.3.1.1. CatBoost

CatBoost eliminates the need for tedious preprocessing by automatically handling category features using a gradient boosting technique. It particularly excels in handling skewed datasets, a problem that plagues many IoT security applications. Equation (4) a general description of gradient boosting.

$$f(x) = \sum_{i=1}^{M} \alpha_i h_i(x) \quad (4)$$

Where $f(x)$ is the predicted output, α_i are the coefficients for each tree and $h_i(x)$ are the individual decision trees. By effectively managing categorical variables, CatBoost optimizes the α_i coefficients and decreases overfitting.

3.3.1.2. LightGBM

Compared to conventional boosting techniques, LightGBM's usage of a leaf-wise tree growth algorithm makes it a faster and more memory-efficient gradient boosting framework. Large datasets with high-dimensional features are no problem for LightGBM. For LightGBM, equation (5) holds significant importance.

$$L = \sum_{i=1}^{N} log(p_i) \quad (5)$$

Where L is the loss function (log-loss in classification) and p_i is the predicted probability of class i.

3.3.1.3. XGBoost

For classification problems, another excellent gradient boosting method is XGBoost. To prevent overfitting, it employs a pruning strategy in addition to regularization. Here is the XGBoost objective function in equation (6):

$$L(\theta) = \sum_{i=1}^{N} L(\hat{y}_i y_i) + \sum_{j=1}^{M} \Omega\left(f_j\right) \quad (6)$$

Where L is the loss function and $\Omega\left(f_j\right)$ is the regularization term for the j-th tree.

3.3.2. Deep Learning Algorithms

3.3.2.1. Convolutional Neural Networks

Images, videos, and time-series data are examples of data with a grid-like topology, and CNNs, a family of DL algorithms, are ideal for processing these types of data. Through a series of layers that concentrate on distinct components of the input, CNNs efficiently extract geographical features from data. Typical raw input data (pictures, network packets, etc.) makes up the input layer. The data input layer is a matrix containing the data values. Input layers for data on IoT security may include time-series or sensor data. A CNN's core component is the convolutional layer. This layer captures spatial features by passing the input data through a sequence of filters, also called kernels. Every filter goes through the data in its own unique way, highlighting key patterns like edges or shapes in the feature maps it computes. Mathematically, this process looks as in equation (7):

$$f(x,y) = \sum_{i=1}^{k} \sum_{j=1}^{k} w_{ij}.x_{ij} \qquad (7)$$

Where w_{ij} is the weights of the filter and x_{ij} represents input pixel at position (i,y). Equation (8) subjects the output to a non-linear activation function known as a relu (rectified linear unit).

$$f(x) = \max(0,x) \qquad (8)$$

This function enhances the expressive ability of CNNs and helps them learn more complicated patterns. The spatial dimensions of the feature maps are decreased using pooling layers (often max pooling), which lowers computational strain while preserving important features. In a feature map subregion, max pooling finds the highest possible value. The pooling as well as convolution layers flatten the feature maps into a one-dimensional vector before passing them on to the fully connected, and dense layers. These layers use the features retrieved by the layers below to generate the final predictions. IoT security tasks, such as anomaly detection along with intrusion detection, greatly benefit CNNs due to their ability to automatically learn patterns in network traffic or sensor data and identify deviations that may signal malicious behavior (Konatham, 2023; Alghamdi, 2022).

3.3.2.2. Long Short-Term Memory

One kind of RNN, known as LSTM, models data sequences as well as records long-term dependencies. LSTMs are especially helpful for time-series data or data with temporal correlations, such as sensor logs or network traffic logs in IoT contexts, where previous events may have an impact on future occurrences. Each time-series input is a vector describing the features at a particular time step; they make up the input layer. The LSTM processes the data stream using an evolving internal state. The building blocks of an LSTM unit are several essential parts. The first gate is the forget Gate, which decides which bits of data to remove from the cell's state. It returns a value between 0 and 1 that represents the desired level of memory retention in equation (9).

$$f_t = \sigma\left(W_f.[h_{t-1}, x_t] + b_f\right) \qquad (9)$$

The input gate then chooses the extra data to store in the cell state in equation (10).

$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i) \qquad (10)$$

This study uses the input gate as well as the prior cell state to update the new cell state in equation (11).

$$C_t = f_t.C_{t-1} + i_t.\tilde{C}_t \qquad (11)$$

The output gate then determines which portion of the cell state to output depending on the updated cell state in equation (12).

$$o_t = \sigma(W_o.[h_{t-1}, x_t] + b_o) \qquad (12)$$

To create predictions, use the hidden state h_t and to keep track of long-term dependencies, use the cell state C_t. To generate predictions for attack detection or classification in IoT security systems, a dense layer receives the results from the previous time step after processing the sequence. When it comes to IoT security, LSTMs are perfect for analyzing time-series data because they can spot anomalies or patterns in sequential events, including unexpected spikes in network traffic that might be a sign of a DDoS attack or strange behavior from IoT devices (Konatham, 2023; Alghamdi, 2022).

3.3.2.3. Deep Belief Networks

Multiple layers of latent, stochastic variables make up DBNs, which is a sort of generative DL model. They enable the model to learn hierarchical features as well as illustrations of the input data via the use of several stacked restricted Boltzmann machines (RBMs). The raw data, often normalised and preprocessed, makes up the input layer. This data might be anything from sensor readings from IoT devices to network traffic. There are both visible and hidden layers in an RBM, making it a kind of probabilistic graphical model. The visible layer displays the observed data. The hidden layer represents the learned features. Every unit in the visible layer links to every unit in the hidden layer, with weights dictating the intensity of the connection. This calculate the activation function of each hidden unit using the sigmoid function in equation (13).

$$P(h_i = 1|v) = \sigma\left(b_i + \sum_j v_j w_{ij}\right) \qquad (13)$$

w_{ij} represents the weight between the visible unit v_j, the hidden unit h_i, and itself. Learning rules include modifying weights so that the discrepancy between observed and network-reconstructed data is as little as possible. A DBN uses the hidden layer of one RBM as the input to the next RBM. This stacking enables the network to learn more abstract features. After pretraining the stacked RBMS, fine-tune the DBN using a supervised learning approach, such as backpropagation, to optimise the weights and produce predictions. DBNs can find attacks or strange patterns in data that haven't been seen before that are related to the security of the IoT because they are good at modelling complex patterns in data and can learn features without being told what to do (Alghaithi et al., 2024).

4 Results

This section gives the results of the chosen ML and DL algorithms for improving IoT security. The performance measures for attack classification and anomaly detection tasks include accuracy, F1-score, training time, precision as well as recall.

4.1. Evaluation Metrics

The metrics offer a comprehensive assessment of the model's performance in IoT security applications, where accuracy is crucial but may not fully reveal the situation due to class imbalances or severe false positives/negatives. Combine these metrics to gain a clearer idea of the models' real-world usefulness in detecting and classifying IoT security attacks and anomalies. Accuracy is the proportion of correct predictions (both true positives along with true negatives) out of all predictions. Across all classes, it provides a broad sense of the model's performance in equation (14).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (14)$$

Where TP denotes True Positives (correctly predicted positive class), TN represents True Negatives (correctly predicted negative class), FP signifies False Positives (incorrectly predicted as positive) and FN mentions False Negatives (incorrectly predicted as negative). Precision measures the accuracy of the positive predictions in equation (15).

$$Precision = \frac{TP}{TP+FP} \qquad (15)$$

The model's capacity to identify positive cases is measured by recall in equation (16).

$$Recall = \frac{TP}{TP+FN} \qquad (16)$$

To get the F1-score, take the harmonic mean of the recall as well as precision scores. In cases where the class distribution is not uniform or if both false positives along with false negatives are significant, its ability to strike a compromise between recall and precision makes it a valuable tool in equation (17).

$$F1 - score = 2.\frac{Precision.Recall}{Precision+Recall} \qquad (17)$$

Plotting the genuine positive rate (recall) against the false positive rate at various threshold levels creates the Receiver Operating Characteristic (ROC) curve. One metric to assess a classifier's performance is the area under the ROC curve (AUC). A higher AUC value indicates a better model in equation (18). Table 2 shows model performance on CICIDS 2017 dataset.

$$AUC - ROC = \int_0^1 True\ Positive\ Rate(TPR) d(False\ Positice\ Rate(FPR)) \ (18)$$

Table 2: Model Performance on CICIDS 2017 Dataset

Algorithm	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**AUC-ROC (%)**	**Training Time (seconds)**
CatBoost	94.2	93.5	94.0	93.7	98.1	245
LightGBM	93.7	92.8	93.5	93.1	97.8	210
XGBoost	92.5	91.8	92.2	92.0	97.5	280
CNN	96.5	95.2	96.0	95.6	99.0	540
LSTM	95.1	94.0	94.8	94.4	98.7	500
DBN	94.0	93.3	93.9	93.6	98.4	460

With an AUC-ROC of 99% and an accuracy of 96.5% on the CICIDS 2017 dataset, CNN is clearly the best model in terms of performance. Outperforming competing algorithms, it detects normal and attack traffic with a recall of 96.0% and a precision of 95.2%. Not only does CNN perform better than CatBoost and LightGBM in terms of accuracy and precision, but they lag behind CNN in terms of F1-score as well as AUC-ROC as well. With a mere 210 seconds, LightGBM provides the fastest model during training, closely followed by CatBoost. However, CNN is a perfect fit for security applications that require high accuracy and detection performance, as its superior detection capabilities more than compensate for its slightly longer training period of 540 seconds. Table 3 shows the attack type classification performance on CICIDS 2017 dataset.

Table 3: Attack Type Classification Performance on CICIDS 2017 Dataset

Attack Type	**Catboost (%)**	**LightGBM (%)**	**XGBoost (%)**	**CNN (%)**	**LSTM (%)**	**DBN (%)**
DoS	94.5	93.8	92.1	97.2	96.3	95.1
DDoS	93.7	93.0	91.9	96.8	95.0	94.4
Botnet	92.4	91.5	90.8	95.6	94.2	93.6
Port Scan	95.3	94.6	93.5	98.1	96.7	95.9

On the CICIDS 2017 dataset, CNN regularly outperforms other methods for attack type classification. It achieves accuracy rates over 96% for DoS, DDoS, and Port Scan attacks in particular. Similar to LightGBM, CatBoost produces excellent results; however, CatBoost is particularly effective at identifying Denial of Service and Port Scan attacks. The XGBoost model has worse recall rates when it comes to identifying DDoS and botnet attacks, even though it's competitive when it comes to accuracy. In terms of reliability in detecting different sorts of attacks, CNN is the clear winner when it comes to multi-class classification jobs in IoT security contexts. Table 4 shows model performance on IoT-23 dataset.

Table 4: Model Performance on IoT-23 Dataset

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC (%)	Training Time (seconds)
CatBoost	92.8	91.9	92.4	92.1	97.6	230
LightGBM	92.1	91.0	92.0	91.5	97.1	205
XGBoost	91.2	90.5	91.0	90.7	96.9	270
CNN	95.0	94.5	94.2	94.3	98.6	530
LSTM	94.3	93.4	93.9	93.6	98.2	480
DBN	93.6	92.8	93.2	93.0	97.9	440

Again, CNN excels on the IoT-23 dataset, this time with the best accuracy (95.0%), precision (94.5%), and AUC-ROC (98.6%), demonstrating its competence in handling IoT security data. It is the best all-around option for identifying attacks and typical behaviors; it surpasses LSTM and DBN in recall and F1-score. While LightGBM and CatBoost are comparable in terms of precision, CNN outperforms them in terms of AUC-ROC and recall. Although CNN requires more training time (530 seconds), it is the best model for detecting attacks on the IoT because of its better generalization and anomaly detection capabilities. Table 5 shows the attack type classification performance on IoT-23 dataset.

Table 5: Attack Type Classification Performance on IoT-23 Dataset

Attack Type	Catboost(%)	LightGBM(%)	XGBoost(%)	CNN(%)	LSTM(%)	DBN(%)
DoS	92.7	92.0	91.1	95.0	94.3	93.5
DDoS	92.1	91.3	90.5	94.5	93.8	93.0
Botnet	91.5	90.7	89.9	94.0	93.4	92.7
Port Scan	94.2	93.5	92.4	96.0	95.1	94.3

On the IoT-23 dataset, CNN has superior performance compared to other algorithms when it comes to attack type classification. This is particularly true when it comes to identifying DoS and Port Scan attacks, as CNN obtains accuracy rates over 95%. When it comes to detecting port scans and DDoS attacks, CNN and LSTM are superior, while CatBoost and LightGBM do well with DoS and botnet attacks. While CNN handles other sorts of attacks more quickly, LSTM demonstrates good performance when it comes to identifying botnet attacks. When it comes to attack classification on the IoT-23 dataset, CNN is the clear winner. This makes it the go-to model for critical IoT security jobs that need rapid and precise detection of various attack scenarios.

4.2. Discussions

The findings show the advantages and disadvantages of each method in terms of IoT security when applied to the CICIDS 2017 and IoT-23 datasets using the ML and DL algorithms, respectively. Across all datasets, CNN achieves the best results compared to other models in terms of accuracy, AUC-ROC, precision as well as recall. It is the best option for IoT security duties because of its capacity to learn intricate patterns from sequential data and its resilience to various attack types. One potential drawback of CNN is its longer training period, which might hinder its use in real-time scenarios where processing speed is paramount. While CNN outperforms LSTM and DBN in terms of overall accuracy, they do a better job of managing sequential attack patterns and time-series data. However, CatBoost, LightGBM, and XGBoost outperform CNN for simpler attack scenarios and have quicker training durations overall. They also do well on classification tasks, especially when it comes to detecting denial-of-service and port scans.

The training time and resource consumption of DL models may be a major issue in resource-constrained IoT contexts, even if these models are excellent at handling complicated data patterns. When speed and scalability are paramount, however, ML models such as LightGBM and CatBoost provide a better balance between performance as well as computational economy. A more versatile and scalable security system might be the result of future research into hybrid models that merge ML and DL techniques. Unsupervised learning methods could be another way to study how to make anomaly detection better in dynamic IoT environments, especially when dealing with new and unexpected attack vectors.

5 Conclusion

This study of different ML and DL methods for making IoT safer uses datasets from both CICIDS 2017 and IoT-23. It finds that CNN models are often better than the others in terms of accuracy, AUC-ROC, precision as well as recall. A potential drawback for real-time applications is the substantial training time and processing resources needed by CNN, despite its excellent performance in attack classification and its ability to identify complicated attack patterns. On the other hand, ML models such as CatBoost, LightGBM, and XGBoost are well-suited to computationally efficient IoT settings because of their quick training periods and ability to handle skewed datasets well. To strike a better balance between speed and accuracy, researchers might look at hybrid models in the future that use ML and DL techniques together. It may be possible to spot new and changing attack patterns in ever-changing IoT systems by combining unsupervised learning methods for anomaly detection. To make these models even more scalable and useful in real time, this need to look at transfer learning and edge computing. Lastly, looking into the possibility of combining context-aware and adaptive security frameworks with testing on bigger and more varied IoT security datasets could help in tailoring solutions for specific IoT applications, providing strong protection against new threats.

References

[1] Ahakonye, L. A. C., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2023). SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection. *Internet of Things*, *21*, 100676. https://doi.org/10.1016/j.iot.2022.100676

[2] Alghaithi, H. R. O., Alshehhi, M. M. A. M., & Murugan, T. (2024, June). IoT Network Anomaly Detection Using Machine Learning and Deep Learning Techniques-Research Study. In *2024 IEEE Students Conference on Engineering and Systems (SCES)* (pp. 1-6). IEEE. https://doi.org/10.1109/SCES61914.2024.10652305

[3] Alghamdi, R. (2022). *Intrusion Detection System for Internet of Things with Deep Learning* (Doctoral dissertation, Ecole Polytechnique, Montreal (Canada)).

[4] Alizadeh, M., Andersson, K., & Schelen, O. (2020). A survey of secure internet of things in relation to blockchain. *Journal of Internet Services and Information Security (JISIS), 10*(3), 47-75. https://doi.org/10.22667/JISIS.2020.08.31.047

[5] Aruchamy, P., Gnanaselvi, S., Sowndarya, D., & Naveenkumar, P. (2023). An artificial intelligence approach for energy-aware intrusion detection and secure routing in internet of things-enabled wireless sensor networks. *Concurrency and Computation: Practice and Experience*, *35*(23), e7818. https://doi.org/10.1002/cpe.7818

[6] Fei, W. (2024). Research on optimization algorithms for artificial intelligence network security management based on All IP Internet of Things fusion technology. *Computers and Electrical Engineering, 115*, 109105. https://doi.org/10.1016/j.compeleceng.2024.109105

[7] Fuentes-Peñailillo, F., Gutter, K., Vega, R., & Silva, G. C. (2024). Transformative technologies in digital agriculture: Leveraging Internet of Things, remote sensing, and artificial intelligence for smart crop management. *Journal of Sensor and Actuator Networks*, *13*(4), 39. https://doi.org/10.3390/jsan13040039

[8] Ghazal, T. M. (2021). Internet of things with artificial intelligence for health care security. *Arabian Journal for Science and Engineering*, 48, 5689 (2023). https://doi.org/10.1007/s13369-021-06083-8

[9] Gupta, K., Sharma, D. K., Gupta, K. D., & Kumar, A. (2022). A tree classifier based network intrusion detection model for Internet of Medical Things. *Computers and Electrical Engineering*, *102*, 108158. https://doi.org/10.1016/j.compeleceng.2022.108158

[10] Humayun, M., Tariq, N., Alfayad, M., Zakwan, M., Alwakid, G., & Assiri, M. (2024). Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey. *IEEE Access*, *12*, 25469–25490. https://doi.org/10.1109/ACCESS.2024.3365634

[11] Khan, A. A., Laghari, A. A., Li, P., Dootio, M. A., & Karim, S. (2023). The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises. *Scientific Reports*, *13*(1), 1656. https://doi.org/10.1038/s41598-023-28707-9

[12] Konatham, B. R. (2023). *A secure and efficient IIoT anomaly detection approach using a hybrid deep learning* technique. Theses.

[13] Kotenko, I. V., Saenko, I., & Kushnerevich, A. (2017). Parallel big data processing system for security monitoring in Internet of Things networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *8*(4), 60-74. https://doi.org/10.22667/JOWUA.2017.12.31.060

[14] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things*, *1*(1), 7. https://doi.org/10.1007/s43926-020-00001-4

[15] Larriva-Novo, X., Villagrá, V. A., Vega-Barbas, M., Rivera, D., & Sanz Rodrigo, M. (2021). An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. *Sensors*, *21*(2), 656. https://doi.org/10.3390/s21020656

[16] Lucas, T. J., De Figueiredo, I. S., Tojeiro, C. A. C., De Almeida, A. M. G., Scherer, R., Brega, J. R. F., ... & Da Costa, K. A. P. (2023). A Comprehensive Survey on Ensemble Learning-Based Intrusion Detection Approaches in Computer Networks. *IEEE Access*, *11*, 122638–122676. https://doi.org/10.1109/ACCESS.2023.3328535

[17] Lukita, C., Pangilinan, G. A., Chakim, M. H. R., & Saputra, D. B. (2023). Examining the impact of artificial intelligence and internet of things on smart tourism destinations: A comprehensive study. *Aptisi Transactions on Technopreneurship (ATT)*, *5*(2sp), 135-145. https://doi.org/10.34306/att.v5i2sp.332

[18] Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y. Y., Haq, I., Ullah, I., ... & Hamam, H. (2023). Analysis of IoT security challenges and its solutions using artificial intelligence. *Brain Sciences*, *13*(4), 683. https://doi.org/10.3390/brainsci13040683

[19] Messinis, S., Temenos, N., Protonotarios, N. E., Rallis, I., Kalogeras, D., & Doulamis, N. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. *Computers in Biology and Medicine*, 108036. https://doi.org/10.1016/j.compbiomed.2024.108036

[20] Padmanaban, S., Nasab, M. A., Shiri, M. E., Javadi, H. H. S., Nasab, M. A., Zand, M., & Samavat, T. (2023). The role of internet of things in smart homes. *Artificial Intelligence-based Smart Power Systems*, 259-271. https://doi.org/10.1002/9781119893998.ch13

[21] Pragadeswaran, S., Subha, N., Varunika, S., Moulishwar, P., Sanjay, R., Karthikeyan, P., Aakash, R., & Vaasavathathaii, E. (2024). Energy Efficient Routing Protocol for Security Analysis Scheme Using Homomorphic Encryption. *Archives for Technical Sciences*, *2*(31), 148–158. https://doi.org/10.70102/afts.2024.1631.148

[22] Rane, N. (2023). Enhancing customer loyalty through Artificial Intelligence (AI), Internet of Things (IoT), and Big Data technologies: improving customer satisfaction, engagement, relationship, and experience. *Internet of Things (IoT), and Big Data Technologies: Improving Customer Satisfaction, Engagement, Relationship, and Experience*. http://dx.doi.org/10.2139/ssrn.4616051

[23] Rane, N., Choudhary, S., & Rane, J. (2023). Artificial Intelligence (AI) and Internet of Things (IoT)-based sensors for monitoring and controlling in architecture, engineering, and construction: applications, challenges, and opportunities. http://dx.doi.org/10.2139/ssrn.4642197

[24] Rupanetti, D., & Kaabouch, N. (2024). Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. *Applied Sciences*, *14*(16), 7104. https://doi.org/10.3390/app14167104

[25] Saied, M., Guirguis, S., & Madbouly, M. (2024). Review of artificial intelligence for enhancing intrusion detection in the internet of things. *Engineering Applications of Artificial Intelligence*, *127*, 107231. https://doi.org/10.1016/j.engappai.2023.107231

[26] Salman, R. H., & Alomari, E. S. (2023). Survey: Homomorphic Encryption-based Deep Learning that Preserves Privacy. *International Academic Journal of Science and Engineering*, *10*(2), 153–163. https://doi.org/10.9756/IAJSE/V10I2/IAJSE1019

[27] Srinadi, N. L. P., Hermawan, D., & Jaya, A. A. N. A. (2023). Advancement of banking and financial services employing artificial intelligence and the internet of things. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *14*(1), 106-117. https://doi.org/10.58346/JOWUA.2023.I1.009

[28] Subeesh, A., & Mehta, C. R. (2021). Automation and digitization of agriculture using artificial intelligence and internet of things. *Artificial Intelligence in Agriculture*, *5*, 278-291. https://doi.org/10.1016/j.aiia.2021.11.004

Authors Biography

Noha Mostafa Mohamed Said, working as an assistant professor in the department of Computer Science, college of Engineering and Computer Science at Jazan University in Kingdom of Saudi Arabia. She graduated in Bachelor of Instructional Technology (1996 – 2000) Assiut University – Faculty of Education, Instructional Technology Department General Evaluation: very good with Honor Degree. She graduated in Special Diploma in Education (2001 – 2003) Assiut University – Faculty of Education, Instructional Technology, She secured Master of Instructional Technology (2006 – 2009) Helwan University – Faculty of Education, Instructional Technology Department. Research: “A distance training program to acquire implementation skills of virtual classrooms in Instructional Situations of secondary stage”. She secured P.hD in Instructional Technology (2011 – 2014) Cairo University – Instructional Technology Department , Research: “Developing a Training Program Based on Blended Learning to Develop Secondary Stage Teachers' Abilities on Using the Technological Techniques”. She is in teaching profession for more than 12 years. Her research findings have been published in SCOPUS/Google-indexed international journals. She has presented 5 papers in National and International Journals, Conference and Symposiums. Her main area of interest includes E-Learning, Cloud Computing, Artificial Intelligence, and cyber security.

Sabna Machinchery Ali, is a young and dynamic individual with a strong academic background in Cyber security and Information Technology. She is currently a Lecturer in the Department of IT and Security, Jazan University, Kingdom of Saudi Arabia. She has teaching experience of more than 20 years in the areas of IT Security and computer Science. She was the Head of Department for the Department of IT and Security, University college Abu Arish under Jazan university. She worked as the coordinator for Centre for computer Science and Information Technology (CCSIT), Vatakara Campus ,University of Calicut, Kerala , India. She is passionate about research, believes in learning, striving for enhancing skills. Currently her Research area is Information Security and Cryptography. She published many papers in this area.

Naseema Shaik, I am a networking and artificial intelligence expert with over 13 years of experience in teaching and research. Currently, I am working as an assistant professor of computer science at King Khalid University in Saudi Arabia. My research interests include computer networks, machine learning, deep learning, and artificial intelligence. Throughout my career, I have focused my research on developing innovative applications of AI and machine learning to solve real-world problems. I enjoy teaching students and helping them develop skills and knowledge that they can apply in their future careers. In my spare time, I like reading books on new technologies, playing sports, and spending time with my family. I believe in the power of education to transform people's lives, and I aim to inspire my students to pursue their dreams and make a positive impact on the world.

Khan Mohamed Jarina Begum, is a lecturer at Jazan University in Saudi Arabia. She holds an MCA, MPhil, and is currently working closer to a PhD. She has over 19 years of university-level teaching experience in Libya and Saudi Arabia, as well as 4 years of industry experience in Dubai. She has also published articles in highly indexed journals and conferences.

Dr. Anwaar Ahmed Abd elLatif Shaban, is a lecturer at the Center for E-Learning, Jazan University, Saudi Arabia, with extensive experience in designing, developing, and evaluating e-learning programs. She holds a Ph.D. in Educational Technology from Cairo University, a Master's in Educational Technology from Cairo University, and a Bachelor's in Educational Technology and Teaching from Zagazig University. Her research interests include e-learning program design and development, e-learning management systems, and educational game production. Dr. Anwar has published several articles and has participated in numerous conferences on educational technology.

Dr. Betty Elezebeth Samuel, is currently working as a Lecturer in the Department of Computer Science and Information Technology & Security at Jazan University in Jazan, Kingdom of Saudi Arabia. She received her Ph.D. from St. Peters Institute of Higher Education and Research in Chennai, India in 2017, her Master’s Degree in Computer Science and Engineering from Anna University in Chennai, India in 2008, and her Master’s Degree in Computer Application from Anna University in Chennai, India in 2005. Her areas of specialization include Artificial Intelligence, Cloud Computing, Ethical Hacking, and Networking. She is a highly motivated individual with outstanding presentation, research, and communication skills, and she is an expert in teaching.