Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.054836 Published Online: 11 October 2024

ARTICLE

A Novel Hybrid Architecture for Superior IoT Threat Detection through Real IoT Environments

Bassam Mohammad Elzaghmouri[1], Yosef Hasan Fayez Jbara[2], Said Elaiwat[3], Nisreen Innab[4,*], Ahmed Abdelgader Fadol Osman[5], Mohammed Awad Mohammed Ataelfadiel[5], Farah H. Zawaideh[6], Mouiad Fadeil Alawneh[7], Asef Al-Khateeb[8] and Marwan Abu-Zanona[8]

[1]Department of Computer Science, Faculty of Computer Science and Information Technology, Jerash University, Jerash, 26150, Jordan

[2]Computer Engineering Department, College of Engineering & Information Technology Buraydah Colleges, Buraydah, 51418, Saudi Arabia

[3]Faculty of Architecture and Design, Al-Zaytoonah University of Jordan, Amman, 11733, Jordan

[4]Department of Computer Science and Information Systems, College of Applied Sciences, AlMaarefa University, Diriyah, Riyadh, 13713, Saudi Arabia

[5]Applied College, King Faisal University, Al-Ahsa, 31982, Saudi Arabia

[6]Department of Business Intelligence and Data Analysis, Faculty of Financial Sciences and Business, Irbid National University, Irbid, 21110, Jordan

[7]Faculty of Information Technology, Ajloun National University, Ajlun, 26810, Jordan

[8]Department of Management Information Systems, College of Business Administration, King Faisal University, Al-Ahsa, 31982, Saudi Arabia

*Corresponding Author: Nisreen Innab. Email: ninnab@um.edu.sa

Received: 08 June 2024 Accepted: 22 August 2024

ABSTRACT

As the Internet of Things (IoT) continues to expand, incorporating a vast array of devices into a digital ecosystem also increases the risk of cyber threats, necessitating robust defense mechanisms. This paper presents an innovative hybrid deep learning architecture that excels at detecting IoT threats in real-world settings. Our proposed model combines Convolutional Neural Networks (CNN), Bidirectional Long Short-Term Memory (BLSTM), Gated Recurrent Units (GRU), and Attention mechanisms into a cohesive framework. This integrated structure aims to enhance the detection and classification of complex cyber threats while accommodating the operational constraints of diverse IoT systems. We evaluated our model using the RT-IoT2022 dataset, which includes various devices, standard operations, and simulated attacks. Our research's significance lies in the comprehensive evaluation metrics, including Cohen Kappa and Matthews Correlation Coefficient (MCC), which underscore the model's reliability and predictive quality. Our model surpassed traditional machine learning algorithms and the state-of-the-art, achieving over 99.6% precision, recall, F1-score, False Positive Rate (FPR), Detection Time, and accuracy, effectively identifying specific threats such as Message Queuing Telemetry Transport (MQTT) Publish, Denial of Service Synchronize network packet crafting tool (DOS SYN Hping), and Network Mapper Operating System Detection (NMAP OS DETECTION). The experimental analysis reveals a significant improvement over existing detection systems, significantly enhancing IoT security paradigms. Through our experimental analysis, we have demonstrated a remarkable enhancement in comparison to existing detection systems, which significantly strengthens the security standards of IoT. Our model effectively addresses the need for advanced, dependable, and adaptable

security solutions, serving as a symbol of the power of deep learning in strengthening IoT ecosystems amidst the constantly evolving cyber threat landscape. This achievement marks a significant stride towards protecting the integrity of IoT infrastructure, ensuring operational resilience, and building privacy in this groundbreaking technology.

KEYWORDS

A hybrid deep learning model; IoT threat detection; real IoT environments; cybersecurity; attention mechanism

1 Introduction

The IoT has brought about a new phase in the digital revolution, turning ordinary objects into interconnected, intelligent systems that can exchange data without human intervention [1]. The technological advancement has resulted in groundbreaking applications across different fields, such as improving urban infrastructure, industrial automation, healthcare, and home automation [2]. However, the rapid expansion of IoT networks has also increased the range and complexity of cyber-attacks, which pose significant challenges to the security and integrity of these systems [3]. Due to the importance of IoT applications in areas such as healthcare monitoring and smart cities, the impact of security vulnerabilities can be significant [4]. It is crucial to ensure that IoT ecosystems are resilient against cyber threats not only as a technological requirement but also as a fundamental necessity for protecting data privacy, system reliability, and public trust [5]. IoT security challenges are pivotal in the landscape where the proliferation of interconnected devices escalates the complexity and scale of potential cyber threats [6]. It tackles the diverse nature of attacks, ranging from high-volume DOS attacks that cripple device functionalities to sophisticated exploits targeting inherent vulnerabilities in IoT protocols and applications [7]. By integrating advanced detection and defense mechanisms, the model is designed to counteract the prevalent network layer intrusions like Address Resolution Protocol (ARP) poisoning and to mitigate intricate application-layer threats such as unauthorized MQTT publish attempts [8].

Fig. 1 shows a comprehensive architecture underlying cyber-attacks targeting IoT devices. The importance of this study lies in its timely response to the urgent need for advanced security measures within the IoT ecosystem. Traditional methods heavily rely on domain knowledge to identify anomalous traffic patterns, which may need to be revised with the ever-evolving Internet traffic. Although traditional threat detection models are effective, they should address IoT environments' unique complexities and dynamic nature. These models often struggle with the high variability of IoT device capabilities, the vast scale of IoT networks, and the ever-evolving landscape of cyber threats [9]. Additionally, relying solely on signature-based or anomaly-based detection methods has revealed inherent limitations, particularly regarding adaptability and resource efficiency [10]. Deep Learning effectively detects network intrusions as it can handle intricate nonlinear relationships [11]. As a result, there is a growing demand for innovative approaches that enhance the detection and reliability of threat prevention while aligning with the operational constraints of IoT systems.

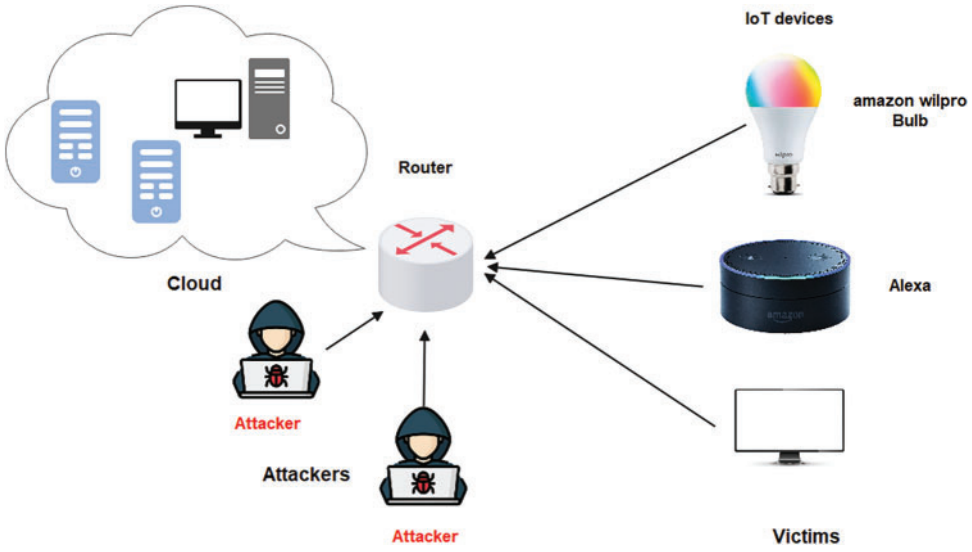

Figure 1: General architecture cyber-attacks of IoT devices

The research paper introduces a novel hybrid model that integrates Convolutional Neural Networks (CNN) [12], Bidirectional Long Short-Term Memory (BLSTM) [13], Gated Recurrent Units (GRU) [14], and Attention mechanisms [15] to fortify IoT security. It leverages the strengths of each approach to create a synergistic framework capable of detecting and classifying a comprehensive collection of cyber threats with high precision and minimal false positives. The proposed model is designed to be scalable, ensuring its applicability across diverse IoT settings, from resource-constrained sensors to more capable devices. Our model proves superior performance in detecting and classifying an array of IoT-specific threats, supported by comprehensive evaluation metrics such as Cohen Kappa and MCC. Benchmarking against current state-of-the-art methods shows our model's superior accuracy, precision, and adaptability, particularly in handling real-time, varied IoT environments. It significantly progresses IoT security, producing a scalable and valuable solution to the complex landscape of cyber threats.

The study contributes significantly to the field of IoT security in various key aspects:

- Presents a unique combination of CNN, BLSTM, GRU, and Attention mechanisms that are designed for enhanced IoT threat detection. It addresses the disadvantages of existing frameworks by increasing the detection accuracy and adaptability to complex IoT environments.
- Propose a scalable and adaptable model to various IoT network sizes and types, ensuring it can effectively address evolving cyber threats.
- Rigorously evaluate the proposed model using diverse real-time IoT data, employing metrics such as Cohen Kappa, MCC, precision, recall, and F1-score. Our results prove notable improvements over traditional and state-of-the-art methods, particularly precision and recall.

The remainder of this paper is as follows:

Section 2 contextualizes the research within the existing body of knowledge, highlighting how this study diverges from previous research. Section 3 provides a comprehensive view of the research design and analytical procedures, presented systematically through subdivisions covering data handling, the model's architecture, and the performance metrics. In Section 4, the empirical setup and findings are described and interpreted, providing a thorough understanding of the research's empirical core.

Finally, Section 5 discusses the implications of the research outcomes, establishing its contribution and proposing future directions for the following work and impact within the field.

2 Related Work

IoT has transformed various sectors, but it has also brought in security threats. Integrating artificial intelligence in the IoT domain has opened up exciting new possibilities for device identification and attack traffic detection. Studies demonstrate that leveraging AI can enable us to be more proactive in detecting and preventing possible security breaches. Advanced deep learning holds great potential to identify and overcome cyber threats by analyzing complex and multi-dimensional data in IoT settings. This section reviews IoT network traffic security and analyzes threat detection models applied for edge devices.

The authors in [16] proposed a threat detection model that uses Machine Learning (ML) algorithms. It achieved a malicious traffic detection rate from 0.935 to 0.97 accuracy. It highlights the potential of ML in improving detection rates but also indicates the need for improvement in accuracy and adaptability to evolving threats. In [17], a proposed model was developed to address security threats from bots using different ML algorithms. The model was trained and tested using and without feature engineering and Synthetic Minority Over-sampling Technique (SMOTE) algorithm. It highlights the importance of feature selection and data balancing in improving ML model accuracy. A recent paper [18] analyzed ML algorithms for attack and anomaly detection in IoT security. It also introduces potential ML-based IoT protection technologies after reviewing relevant literature. Anwer et al. [19] proposed a framework to classify attacks from network traffic using ML algorithms. Their finding showed that the Random Forest algorithm achieved the best performance rate of 0.853. This promising result highlights the necessity for more robust methods to address the increasing complexity of IoT threats. While the authors in [20] proposed a lightweight botnet attack model that adopts efficient ML algorithms and a feature selection approach that achieves around 99% accuracy. Meanwhile, Reference [21] introduced a system that uses a deep learning network to identify malicious traffic that could attack connected IoT devices. It is communication protocol-independent, reducing deployment complexities. The IDS showed reliable performance in experimental analysis, with an average accuracy of 93.74%. The federated learning-based approach in [22] demonstrated the effectiveness of distributed learning models in IoT security, achieving 98% accuracy by training on multiple views of MQTT protocol datasets. Another innovative approach in [23] combined signature-based and anomaly-based detection techniques using ensemble learning, achieving a 96% accuracy rate, and highlighting the effectiveness of hybrid methods in enhancing detection capabilities.

Further advancements in deep learning for IoT security include a CNN network to extract essential features from raw data, significantly improving attack detection accuracy to 98.04% according to [24]. Also, Reference [25] achieved a commendable 0.993 Area Under the Receiver Operating Characteristic Curve (AUC-ROC) demonstrating the potential of CNNs in identifying IoT devices and addressing vulnerabilities. Additionally, CNNs can be utilized to identify IoT devices within datasets, providing a proactive approach to identifying and addressing potential vulnerabilities in these devices [26]. Hybrid deep learning frameworks, including CNN, BLSTM, and GRU have effectively incorporated BLSTM models to elevate multiclass malware family identification for detecting IoT-based botnet attacks [27]. Findings from this approach outperformed other single network techniques in identifying attacks within IoT networks, achieving 99.46% accuracy [28]. The proposed research is driven by the persistent requirement for resilient, adaptable, and effective IoT security solutions capable of tackling the complex and growing landscape of cyber threats.

3 Methodology

The methodology section provides a thorough explanation of the procedures and analytical techniques utilized to explore IoT network traffic data dynamics, with a particular focus on threat detection:

- We examine the composition and preprocessing of the dataset with an in-depth discussion of the RT-IoT2022 dataset.
- We present a comprehensive overview of our innovative hybrid model's architecture design, which offers a solid basis for interpreting intricate data structures.
- We demonstrate the performance metrics that validate the model's efficacy.

3.1 Data Description and Preprocessing

This study utilizes the RT-IoT2022 dataset [29], a varied compilation of real-time IoT network traffic data containing various devices and network behaviors, including benign and malicious activities. The proposed dataset, with data sourced from various devices such as ThingSpeak-LED and Wipro-Bulb and employing MQTT protocol for temperature sensing (MQTT-Temp) alongside simulated network attacks, provides a comprehensive basis for developing advanced IDS. The RT-IoT2022 dataset's generation involved an intricate setup simulating an IoT environment with 'victim' and 'attacker' devices, facilitating the collection of authentic network traffic data. The setup enabled the capture and analysis of nuanced traffic patterns and attack vectors, crucial for the dataset's relevance in training sophisticated IDS solutions. Data from various IoT devices and attack simulations were systematically recorded, labeled, and integrated into the dataset, providing a rich, multidimensional resource for developing and validating the proposed IDS framework. The RT-IoT2022 dataset is meticulously curated from an operational IoT infrastructure, encapsulating the multifaceted nature of IoT network traffic. It includes normal operational data from various IoT devices and data simulating sophisticated cyber-attack scenarios such as Brute-Force SSH attacks and DDoS attacks. The dataset's bidirectional network traffic data is captured, leveraging the Zeek network monitoring tool integrated with the Flowmeter plugin, thereby ensuring a granular analysis of network interactions and anomalies.

Data preprocessing is a crucial step before deploying a model. The dataset underwent several preprocessing steps to enhance the model's interpretability and effectiveness [30]. The proposed steps include normalization, one-hot encoding, feature scaling, and outlier management. Normalization was applied to numerical data to ensure consistency in data scale across various features [31]. We transformed normalized feature values to a standard range, essential for preventing model bias due to scale discrepancies. One-hot encoding was implemented for categorical data such as protocol or attack type [32]. We transform categorical variables into a binary matrix, enabling the model to process and learn from these non-numerical data points efficiently [33]. Feature scaling was executed to ensure each feature contributed equitably to the model's performance. Then, adjusted numerical data to a standard scale without distorting differences in the ranges of values. Outlier management was performed by employing robust statistical methods. We identified outliers and appropriately managed them to prevent their undue influence on the model's training and predictive accuracy.

3.2 Model Architecture Overview

Our proposed hybrid model features a refined architecture to maintain IoT threat detection. It is achieved by integrating several advanced neural network architectures to create a comprehensive analytical framework. The model's design addresses the complex characteristics of IoT data and integrates several specialized networks, including CNN, BLSTM, Gated GRUs, and Attention mechanisms.

This section provides detailed information about the system framework, including data preprocessing, sampling strategies, and the integration of model components. The proposed hybrid model aims to prevent cyber-attacks originating from IoT devices, as outlined in Fig. 2. To ensure high-quality input data, we've developed a comprehensive preprocessing pipeline that includes several key steps. First, we use one-hot encoding to transform categorical data into a binary matrix format that neural networks can effectively process. Next, we employed outlier management techniques to identify and address anomalous data points that could skew the training process. It helps ensure a more stable and accurate model. We then normalized the data to bring all features onto a similar scale, which is essential for optimizing the neural network's performance. Following normalization, we extracted relevant characteristics from the raw data to enhance the model's ability to detect patterns.

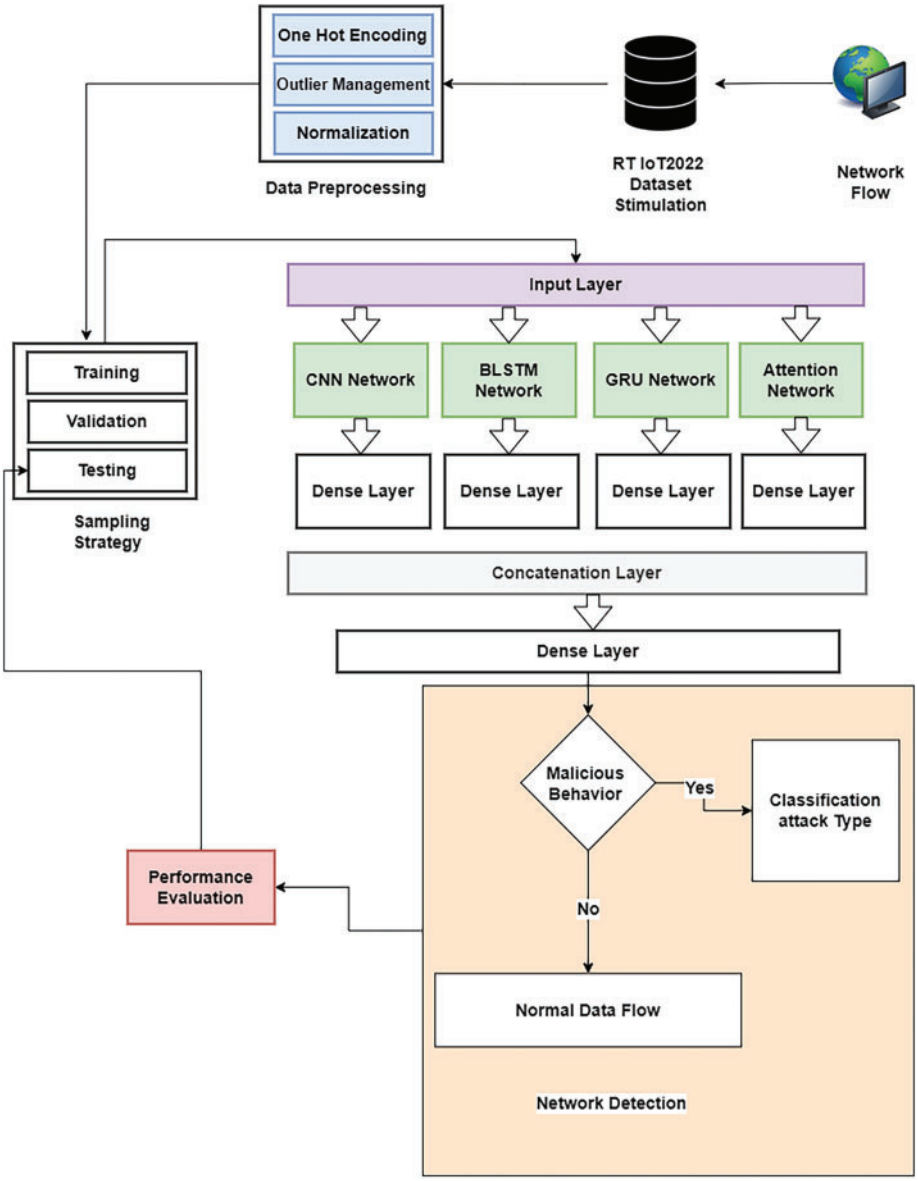

Figure 2: Proposed hybrid model architecture for preventing cyber-attacks from IoT devices

Next, we converted the processed data into temporal sequences, essential for capturing time-dependent patterns inherent in IoT network traffic. It enables the model to understand and predict behaviors over time, a critical aspect of threat detection. To maintain the model's robustness and ensure that the training and test datasets represent the diverse threat types present in the data, we applied stratified sampling. This technique involves dividing the data into strata based on threat types and then sampling proportionally from each stratum. It guarantees that all threat categories are adequately represented in the training and testing phases, enhancing the model's generalizability and reliability across different scenarios. The architecture uses multiple neural network frameworks to detect and classify potential threats in IoT environments. The model utilizes CNNs to process input data, benefiting from their ability to identify spatial hierarchies and patterns. BLSTMs are employed to comprehend temporal dependencies, providing a deeper understanding of the sequential data characteristic of network flows. GRUs are also utilized, improving the model's ability to manage information over time with a more efficient parameterization than traditional LSTMs. An Attention Network is incorporated to prioritize critical data segments, enhancing the model's focus and interpretability regarding the most relevant features for the detection task. These networks converge at a Concatenation Layer, combining the diverse feature maps into a unified representation, followed by Dense Layers, which consolidate the learned features for final classification [34].

CNNs are essential networks for extracting hierarchical features from spatial data [35]. The key operation at the core of CNNs involves applying convolutional filters to the input data, resulting in feature maps that capture patterns within the input domain. The CNN component is vital in extracting spatial features from the dataset. Our model utilizes a 128-filter CNN layer, with each filter having a kernel size of 3. A ReLU activation function is applied to introduce non-linearity and facilitate feature extraction. Following convolution, we apply a MaxPooling layer with a pool size of 2 to reduce dimensionality and then a Flatten layer to convert the pooled feature map into a 1D array. Finally, a Dense layer with 64 units is introduced to serve as a fully connected layer to interpret the CNN features. Mathematically, it involves using an input (X) and a filter (W) to perform a convolution operation at a specific spatial location (i, j), expressed as follows:

$$F(i, j) = \sum_{m} \sum_{n} X(i+m, j+n)\, W(m, n), \tag{1}$$

where $F(i, j)$ represents the feature map generated by applying a convolutional filter W to the input X. Following this, sequential layers are applied to add non-linearity and reduce dimensions. These layers include Rectified Linear Unit (ReLU) and pooling layers.

The BLSTM layer is a type of LSTM architecture designed to analyze data in both forward and reverse directions, improving the network's ability to capture dependencies across temporal sequences. The following set of equations can describe the main structure of the LSTM unit:

– Forget gate:

$$f_t = \sigma\left(W_f \cdot [h_t - 1, x_t] + b_f\right), \tag{2}$$

– Input gate:

$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t] + b_i\right), \tag{3}$$

– Cell state update:

$$C_t = \tanh\left(W_c \cdot [h_{t-1}, x_t] + b_c\right), \tag{4}$$

– final cell state:

$$C_t = f_t * C_{t-1} + i_t * C_t, \tag{5}$$

– Output gate:

$$o_t = \sigma\left(W_o \cdot [h_{t-1},\ x_t] + b_o\right), \tag{6}$$

– Hidden state:

$$h_t = o_t * \tanh\left(C_t\right), \tag{7}$$

where σ represents the sigmoid activation function, $*$ represents element-wise multiplication, and W and b are the weights and biases for each gate. Our model incorporates advanced BLSTM Networks and GRUs to capture temporal dependencies in IoT network data effectively. The BLSTM layers are designed to understand sequential patterns by processing data forward and backward. In contrast, the GRU layer simplifies the recurrent architecture while preserving its ability to capture long-term dependencies. Our BLSTM layer has 64 units in each direction, and another BLSTM layer with 32 units follows this to refine temporal feature extraction further. A Dense layer with 64 units is subsequently applied to interpret the BLSTM outputs. GRUs are a type of neural network architecture that simplifies the LSTM architecture. The GRU architecture combines the functionality of the forget and input gates into a single update gate. The simplification results in a more efficient and streamlined neural network. The procedures of GRUs can be outlined as follows:

– Update gate:

$$u_t = \sigma\ \left(W_u \cdot [h_{t-1},\ \ x_t] + b_i\right), \tag{8}$$

– Reset gate:

$$v_t = \sigma\ \left(W_v \cdot [h_{t-1},\ x_t] + b_v\right), \tag{9}$$

– Candidate activation:

$$\tilde{h}_t = \tanh\left(W_{\cdot}[v_t \cdot h_{t-1},\ x_t] + b\right), \tag{10}$$

– Final output:

$$h_t = (1 - u_t) * h_{t-1} + u_t * \tilde{h}_t. \tag{11}$$

In comparison, the GRU layer with 64 units and a Dense layer with 64 units efficiently process time-series data for identifying evolving threat patterns in real-time IoT environments.

The Attention network in the model is essential for enhancing focus on significant portions of the data. It computes context-aware representations by assigning weights to various input parts, allowing the model to prioritize relevant information. The mechanism is integrated after the embedding layer, with subsequent flattening and a Dense layer with 64 units to synthesize the attentive signals. During the prediction phase, attention mechanisms allow the model to focus on relevant parts of the input data. To calculate the attention score for a given input x_i and context e, the following formula:

$$a_i = \frac{\exp\left(score\left(x_i,\ e\right)\right)}{\sum_j \exp\left(score\left(x_j,\ e\right)\right)}, \tag{12}$$

The "score" refers to a mechanism that evaluates how well inputs align with the surrounding context. The attention layer's output is a sum of inputs, weighted based on their respective attention scores.

The processed features from the CNN, BLSTM, GRU, and Attention components are integrated at a Concatenation Layer. This layer combines the different feature maps into one cohesive representation, capturing spatial, temporal, and context-aware information. The concatenated features then go through Dense layers, refining the feature representation and preparing the data for classification. The fusion of these layers serves as the basis of the hybrid model, culminating in a final Dense layer that utilizes softmax activation to classify various types of IoT threats accurately. Each layer is designed to efficiently detect intricate patterns and anomalies in IoT network data, creating a strong framework for reliable threat detection and classification. It allows the model to classify various IoT threats effectively and offer a probabilistic measure of the presence of each threat type. The proposed hybrid model adeptly captures spatial and temporal dependencies inherent in IoT threat data by combining these frameworks. This detailed architecture design showcases a sophisticated approach to IoT security, tackling the unique strengths of each neural network component to provide a comprehensive, multi-dimensional analysis of potential threats. Our model represents a significant advancement in the field, giving an effective and adaptable solution for detecting and mitigating cyber threats in IoT environments. The proposed model architecture's intricate and comprehensive design showcases a deep understanding of the complexities of IoT data, exemplifying a sophisticated approach to improving cybersecurity measures in IoT networks. By capitalizing on the unique strengths of each neural network component, the model provides a sophisticated, multi-dimensional analysis of potential threats, representing a significant stride forward in IoT security research.

3.3 Performance Metrics

The effectiveness of the deep learning model's ability to detect IoT threats is determined by analyzing key performance metrics that provide insight into different aspects of the model's performance. The comprehensive evaluation includes traditional metrics such as accuracy, precision, recall, and F1-score, FPR, Detection Time, as well as more nuanced measures such as the Cohen Kappa Score, MCC, Zero-One Loss, and Hamming Loss [36]. By considering this range of metrics, a thorough understanding of the model's strengths and weaknesses can be obtained, enabling a meaningful comparison to existing methodologies in the field. Where the True Positive (TP) and True Negative (TN) refer to the accurately predicted results. Meanwhile, false positives (FP) and false negatives (FN) refer to false predicted results. These metrics hold standard significance in the evaluation of the proposed model and are defined as follows:

Accuracy (ACC) is the primary indicator of a model's overall performance. It aggregates all true results divided by all tested data as calculated in:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN}. \tag{13}$$

Precision (P) measures the reliability of the model's positive classifications:

$$P = \frac{TP}{TP + FP}. \tag{14}$$

The Recall ensures that all relevant instances are identified, which is crucial to scenarios where missing out on a threat could have detrimental consequences.

$$\text{Recall} = \frac{TP}{TP + FN}. \tag{15}$$

F1-score provides a harmonic mean of precision and Recall, offering a single metric to gauge the balance between the model's precision and Recall:

$$F1 - score = \frac{2 \times Recall \times precision}{Recall + precision}. \tag{16}$$

Cohen Kappa Score measures agreement between two raters who classify N items into C categories. The Kappa score is useful in assessing classification reliability and correcting for chance agreement, defined as:

$$\kappa = \frac{p_o - p_e}{1 - p_e}, \tag{17}$$

where p_o represents the observed proportion of agreement, and p_e denotes the theoretical probability of agreement by chance.

Matthews Correlation Coefficient (MCC) offers a balanced measure even when the classes are of very different sizes, defined as:

$$\text{MCC} = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}. \tag{18}$$

Zero-One Loss counts the number of misclassifications, providing a straightforward indicator of the errors made by the model:

$$\text{Zero} - \text{One Loss} = \sum_{i=1}^{n} I(y_i \neq \widehat{y_i}) \tag{19}$$

Hamming Loss quantifies the ratio of incorrectly predicted labels to the total count of labels, serving as a crucial metric in multi-label classification tasks, defined as:

$$\text{Hamming Loss} = \frac{1}{N} \sum_{i=1}^{n} \frac{xor(y_i, \widehat{y_i})}{L}. \tag{20}$$

4 Environmental Settings and Results

This section provides detailed information about the research conditions and the findings that were obtained. At first, the environmental settings list the hardware and software specifications, including processor details, memory capacity, operating systems, and key software libraries. Then, the results section presents the outcomes of the experiment in a precise and meticulous manner. It explains the standard quantitative metrics and uses advanced statistical measures to assess the reliability and significance of the findings. It validates the experimental design and methodology and evaluates the research's impact critically. It offers a comprehensive understanding of the study's implications and potential applications.

4.1 Environmental Settings

The Environmental Settings section is crucial as it provides the contextual framework for the research, validates the findings, and extends the work under similar conditions. The environmental settings delineate the hardware setup, detailing the computational resources utilized in the study. The experiments were conducted using a system equipped with an Intel Xeon Processor E5-2640 v4,

2.40 GHz, 32 GB RAM, and an NVIDIA Tesla K80 GPU, which provides an overview of the hardware environment.

Moreover, the software environment includes the operating system version, the development environments, and any relevant libraries or frameworks employed during the research. Table 1 details the settings of the proposed model, and specific configurations, such as optimizer choice, which are crucial for reproducibility and transparency.

Table 1: Hybrid deep learning model configuration settings

Parameter	Value/Setting
Processor	Intel Xeon processor E5-2640 v4, 2.40 GHz
RAM	32 GB
GPU	NVIDIA Tesla K80
Operating system	Ubuntu 18.04 LTS
Environment	Python 3.10
Optimizer	Adam
Learning rate	Configurable
Epochs	50
Batch size	128

4.2 Results and Analysis

In this section, we comprehensively assess the hybrid model's performance on the RT-IoT2022 dataset and present a detailed analysis of its results. The model's high efficacy was demonstrated through a 5-fold cross-validation process, ensuring its applicability across different subsets of the dataset. The performance metrics precisely show exceptional results. Accuracy, Precision, Recall, and F1-score are all reported to be just above 99%, indicating the model's outstanding ability to classify and predict accurately across the dataset. The hybrid model performs exceptionally well detecting attacks such as 'MQTT Publish,' 'DOS SYN Hping,' 'NMAP OS DETECTION,' and 'NMAP XMAS TREE SCAN.' All standard metrics got a peak at 1.0. It indicates that the hybrid model accurately identifies these attacks with no false positives (precision = 1) and captures every instance of the actual attacks with no false negatives (recall = 1). As a result, the model achieves a perfect F1-score, a strong indicator of its balance between precision and recall. Meanwhile, a five-fold cross-validation accuracy rate of 99.57% indicates the hybrid model's ability to accurately identify the most positive and negative instances in the dataset. Precision, at 99.068%, reflects the model's reliability in its positive predictions, while the Recall value of 99.57% denotes its effectiveness in identifying all relevant instances. The F1-score, at 99.568, provides a balanced measure between precision and recall, highlighting the model's consistent performance across both metrics. Further, the Cohen Kappa Score of 0.99 and the MCC of 0.99 are specifically significant. The Cohen Kappa Score adjusts for any random agreement between predictions and actual values, with the model achieving a near-perfect score, which suggests a high degree of reliability in its predictive accuracy. Similarly, the MCC, a more refined measure of the quality of binary classifications, indicates an excellent predictive performance, confirming the model's effectiveness in distinguishing between classes in a balanced manner. The Zero-One Loss and Hamming Loss metrics further boost our understanding of the model's performance. The Zero-One Loss, at 0.0038, reflects the balance of misclassifications made by the model. At the

same time, the Hamming Loss, mirroring this value at 0.0038, provides an additional outlook on the model's error rate, specifically in the context of label predictions.

The comprehensive analysis demonstrates the robustness and high accuracy of the hybrid model on the RT-IoT2022 dataset. It provides a view of its performance across various metrics, strengthening the model's applicability and effectiveness in real-world IoT security contexts. The detailed description of each metric, supported by practical data, offers a solid basis for the model's validation, ensuring the reliability and significance of the proposed findings.

4.3 Discussion

The analysis of experimental results in the discussion section carries significant weight, especially when examining the proposed hybrid deep learning model against traditional machine learning algorithms, as indicated in Table 2. This section delves into the implications of the findings, offering an in-depth understanding that contextualizes the hybrid model's exceptional performance in the broader landscape of machine learning and cybersecurity applications.

Table 2: Comparison between a proposed hybrid model and traditional machine learning algorithms

Techniques	5-folds ACC (%)	Precision	Recall	F1-score	FPR	Detection time
SVM	81.5	73.96	81.5	74.71	0.06	50.68
Logistic regression	82.79	88.32	82.79	82.79	0.0198	0.011
K-nearest neighbors	97.62	97.60	97.62	97.60	0.002	11.68
Random forest	98.2	98.2	98.3	98.02	0.0003	0.128
Extra trees	95.4	93.14	95.12	93.65	0.005	0.17
Proposed model	99.62	99.61	99.62	99.61	0.00084	6.5

Table 2 compares the proposed hybrid deep learning model and various machine learning techniques, including Support Vector Machines (SVM) [37], Logistic Regression [38], K-nearest neighbors [39], Random Forest [40], and Extra Trees [41]. The table briefly demonstrates that the proposed model outperforms its counterparts, with a 99.62% 5-fold cross-validation accuracy rate, highlighting its superior predictive abilities in IoT security. This comparison demonstrates the hybrid model's effectiveness and positions its performance within a comparative framework to evaluate its relative strengths.

Table 2 comprehensively compares the proposed hybrid model and traditional machine learning algorithms based on various performance metrics, including 5-fold accuracy (ACC), precision, recall, F1-score, FPR, and detection time. The SVM algorithm achieves a 5-fold accuracy of 81.5%, with a precision of 73.96%, recall of 81.5%, and an F1-score of 74.71%, but it has a relatively high detection time of 50.68 s and an FPR of 0.06. Logistic Regression improves slightly in accuracy at 82.79%, exhibiting a high precision of 88.32% and balanced recall and F1-scores at 82.79%. Its detection time is significantly lower at 0.011 s and maintains a low FPR of 0.0198. The KNN algorithm demonstrates superior performance with an accuracy of 97.62%, precision and recall at 97.60%, and an F1-score of 97.60%, combined with a minimal FPR of 0.002 and a detection time of 11.68 s. Random Forest and Extra Trees classifiers perform comparably, with Random Forest achieving an accuracy of 98.2%, precision of 98.2%, recall of 98.3%, and an F1-score of 98.02%, alongside an extremely low FPR of

0.0003 and a detection time of 0.128 s. Extra Trees, while slightly lower in accuracy at 95.4%, offers robust precision at 93.14%, recall at 95.12%, and an F1-score of 93.65%, with an FPR of 0.005 and a detection time of 0.17 s. The proposed hybrid model, however, outperforms all traditional algorithms, achieving an outstanding accuracy of 99.62%, precision of 99.61%, recall of 99.62%, and an F1-score of 99.61%, with a notably low FPR of 0.00084 and a detection time of 6.5 s. This analysis demonstrates the efficacy and superiority of the proposed hybrid model in terms of accuracy and balanced performance metrics, making it a highly effective solution for intrusion detection.

In Fig. 3, we compare the proposed model's performance with a notable model by Sharmila et al. [29], who used a Quantized autoencoder (QAE) algorithm. The bar chart highlights the outstanding performance of our model, which outperforms the other model of all metrics, demonstrating its superior ability to balance false positives and false negatives effectively.

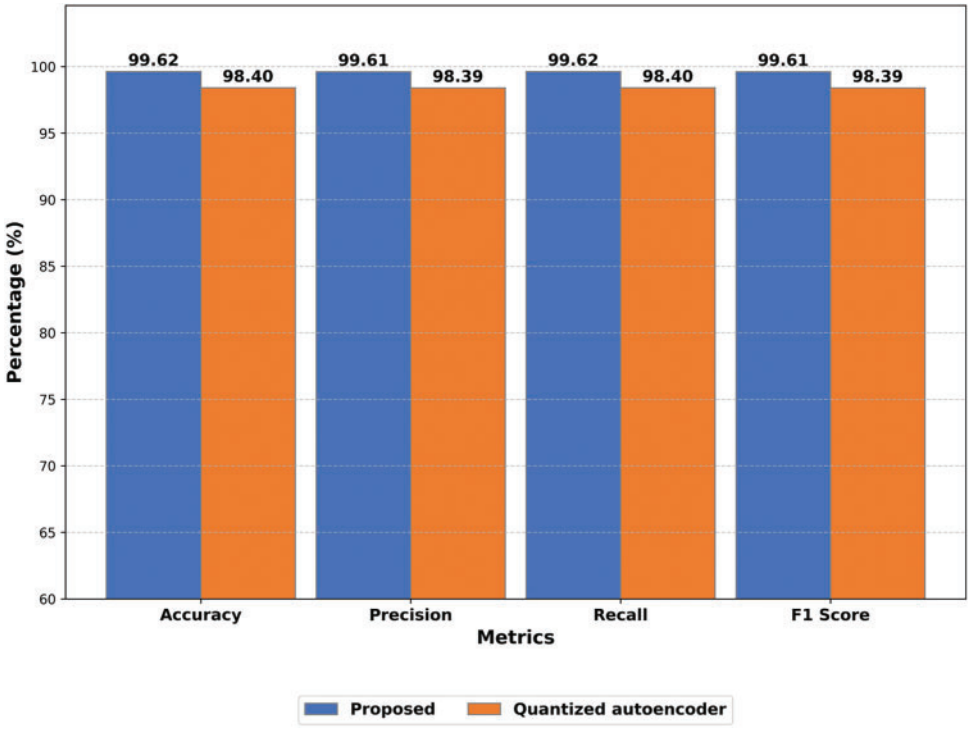

Figure 3: Comparative analysis of the proposed model *vs*. Sharmila et al. [29] on the RT-IoT2022 dataset of detecting cyber-attacks on IoT devices

To provide a more in-depth analysis of the results, we suggest discussing statistical significance and advanced metrics like the Cohen Kappa Score and MCC, as presented in the results section. These measures offer valuable insights into the model's predictive reliability and quality. For instance, the near-perfect Cohen Kappa Score indicates that the model's accuracy goes beyond what would be expected by chance alone, which speaks volumes about its robustness. Similarly, the high MCC value attests to the model's ability to make balanced binary classifications, which is crucial in high-stakes fields like cybersecurity, where the cost of false positives or false negatives can be significant. The hybrid model's exceptional performance could be attributed to its capacity to harness the strengths of various learning methods, indicating a hopeful path for future machine learning architecture research. Furthermore, one could reflect on the practical significance of these findings for IoT security

applications in the real world, underscoring how utilizing these advanced models could enhance defenses against ever-evolving cyber threats.

Table 3 compares several IDSs designed for Internet of Things (IoT) networks, emphasizing their performance indicators regarding accuracy percentages, datasets, and techniques. The table methodically illustrates how various IDS strategies have changed and become more effective in recent years. Reference [42], for example, used autoencoders with the NSL-KDD dataset and achieves 95.79% accuracy. While findings in [43] achieved a greater accuracy of 97.1% by using LSTM networks with the SDNIoT dataset. Additionally, Reference's [44] application of CNN to the CSE-CICIDS2018 dataset showed a noteworthy improvement with an accuracy of 98.15%. Using the IoT-based botnet and RT-IoT2022 datasets, References [29] and [45] demonstrate advanced methodology and achieve accuracies of 98.34% and 98.4%, respectively, by utilizing Quantized Autoencoder and Bidirectional Long Short-Term Memory with Gated Recurrent Unit (BLSTM-GRU) techniques. To comprehensively assess scalability and robustness with the same RT-IoT2022 dataset, various techniques such as artificial neural networks with swarm analysis [46], Particle Swarm Optimization with Deep Learning [47], and others can provide a more thorough evaluation. Notably, a study [48] applied a Multi-Layer Perceptron achieved 99%, while our proposed hybrid model achieved the highest accuracy of 99.62%, demonstrating its advanced threat detection capabilities. Using a Hybrid Architecture on the RT-IoT2022 dataset, the suggested model notably exceeds the other approaches, achieving an outstanding accuracy of 99.62%. This comparative study highlights the steady improvement in IDS efficiency, which is supported by novel machine learning architectures and the use of a variety of recent datasets. However, despite its strengths, potential limitations include the need for further optimization to enhance scalability across various and large-scale IoT environments, ensuring consistent performance and efficiency as network size and complexity increase.

Table 3: Comparative analysis of various existing IDSs based on the IoT networks

Reference	Dataset	Methods	Results in %
[42]	NSL-KDD	Autoencoders	95.79
[43]	SDNIoT	LSTM	97.1
[44]	CSE-CICIDS2018	CNN	98.15
[45]	IoT-based botnet	BLSTM-GRU	98.34
[46]	RT-IoT2022	Artificial neural networks and swarm analysis techniques	91
[47]	RT-IoT2022	Particle swarm optimization and deep learning	92
[48]	RT-IoT2022	Multi-layer perceptron	99
[29]	RT-IoT2022	Quantized autoencoder	98.4
Proposed model	RT-IoT2022	Hybrid architecture	99.62

5 Conclusion and Future Works

This study represents significant findings in IoT security by introducing a cutting-edge hybrid deep learning model that combines CNNs, BLSTMs, GRUs, and attention mechanisms to enhance the detection and classification of cyber threats in IoT environments. The model's outstanding capacity

to accurately identify a wide range of cyber threats has been confirmed through rigorous testing on the RT-IoT2022 dataset, showcasing its superior performance across accuracy, precision, recall, and F1-scores. This model's effectiveness is proof of the potential of integrating diverse neural network architectures, setting a new standard in the field of IoT security by addressing the nuanced challenges of real-world IoT systems.

Future research efforts will focus on refining these models for greater scalability and adaptability, exploring their application in different IoT settings, and expanding their capabilities to anticipate and counter emerging cyber threats, further enhancing the resilience of IoT ecosystems against sophisticated attacks.

Acknowledgement: Nisreen Innab would like to express sincere gratitude to AlMaarefa University, Riyadh, Saudi Arabia, for supporting this research. Ahmed, Asef, Mohamed and Marwan extend sincere thanks and appreciation to the administration of King Faisal University in the Kingdom of Saudi Arabia for providing all forms of support to the university's faculty members, especially in the field of scientific research.

Funding Statement: This article is funding from Deanship of Scientific Research in King Faisal University with Grant Number KFU241648.

Author Contributions: Conceptualization: Ahmed Abdelgader Fadol Osman and Asef Alkateeb; methodology: Bassam Mohammad Elzaghmouri and Marwan Abu-Zanona; formal analysis: Nisreen Innab Mohammed Awad Mohammed Ataelfadiel and Marwan Abu-Zanona; original draft preparation: Farah H. Zawaideh, Mouiad Fadeil Alawneh; review and editing: Bassam Mohammad Elzaghmouri; visualization: Said Elaiwat and Mouiad Fadeil Alawneh and Asef Al-Khateeb and Yosef Hasan Fayez Jbara; project administration: Nisreen Innab and Farah Zawaidah. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data openly access available in a public repository in [49].

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Sahai, R. Goel, and G. Singh, "Building the world of internet of things," in *Advanced Soft Computing Techniques in Data Science, IoT and Cloud Computing*, S. Dash, S. K. Pani, A. Abraham, Y. Liang, eds., Cham: Springer International Publishing, 2021, vol. 89, pp. 101–119. doi: 10.1007/978-3-030-75657-4_5.

[2] M. A. Khan *et al.*, "Smart android based home automation system using internet of things (IoT)'," *Sustainability*, vol. 14, no. 17, 2022, Art. no. 10717. doi: 10.3390/su141710717.

[3] R. Sharma and R. Arya, "Security threats and measures in the Internet of Things for smart city infrastructure: A state of art," *Trans. Emerg. Telecomm. Technol.*, vol. 34, no. 11. 2023, Art. no. e4571. doi: 10.1002/ett.4571.

[4] Z. N. Aghdam, A. M. Rahmani, and M. Hosseinzadeh, "The role of the Internet of Things in healthcare: Future trends and challenges," *Comput. Methods Programs Biomed.*, vol. 199, 2021, Art. no. 105903. doi: 10.1016/j.cmpb.2020.105903.

[5] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1256–1270, 2020. doi: 10.1109/TEM.2020.2978014.

[6] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh and W. -C. Hong, "Internet of things: Evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, 2021, Art. no. 1809. doi: 10.3390/s21051809.

[7] M. Aziz Al Kabir, W. Elmedany, and M. S. Sharif, "Securing IoT devices against emerging security threats: Challenges and mitigation techniques," *J. Cyber Secur. Tech.*, vol. 7, no. 4, pp. 199–223, 2023. doi: 10.1080/23742917.2023.2228053.

[8] S. Lakshminarayana, A. Praseed, and P. S. Thilagam, "Securing the IoT application layer from an MQTT protocol perspective: Challenges and research prospects," *IEEE Commun. Surv. Tutorials*, 2024. doi: 10.1109/COMST.2024.3372630.

[9] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions," *IEEE Commun. Surv. Tutorials*, vol. 25, pp. 1775–1807, 2023. doi: 10.1109/COMST.2023.3280465.

[10] I. Martins, J. S. Resende, P. R. Sousa, S. Silva, L. Antunes and J. Gama, "Host-based IDS: A review and open issues of an anomaly detection system in IoT," *Future Gener. Comput. Syst.*, vol. 133, pp. 95–113, 2022. doi: 10.1016/j.future.2022.03.001.

[11] R. Qaddoura, A. M. Al-Zoubi, H. Faris, and I. Almomani, "A multi-layer classification approach for intrusion detection in IoT networks based on deep learning," *Sensors*, vol. 21, no. 9, 2021, Art. no. 2987. doi: 10.3390/s21092987.

[12] H. Asgharzadeh, A. Ghaffari, M. Masdari, and F. S. Gharehchopogh, "Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced Capuchin search algorithm," *J. Parallel Distr. Comput.*, vol. 175, pp. 1–21, 2023. doi: 10.1016/j.jpdc.2022.12.009.

[13] N. E. Oueslati, H. Mrabet, and A. Jemai, "A survey on intrusion detection systems for IoT networks based on long short-term memory," in *Int. Conf. Model Data Eng.*, Sousse, Tunisia, Springer, 2023, pp. 237–250.

[14] G. Zhao, C. Ren, J. Wang, Y. Huang, and H. Chen, "IoT intrusion detection model based on gated recurrent unit and residual network," *Peer Peer Netw. Appl.*, vol. 16, no. 4, pp. 1887–1899, 2023. doi: 10.1007/s12083-023-01510-z.

[15] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "IDS-attention: An efficient algorithm for intrusion detection systems using attention mechanism," *J. Big Data*, vol. 8, no. 1, p. 149, Dec. 2021. doi: 10.1186/s40537-021-00544-5.

[16] O. Salman, I. H. Elhajj, A. Chehab, and A. Kayssi, "A machine learning based framework for IoT device identification and abnormal traffic detection," *Trans. Emerg. Tel. Tech.*, vol. 33, no. 3, Mar. 2022, Art. no. e3743. doi: 10.1002/ett.3743.

[17] S. Pokhrel, R. Abbas, and B. Aryal, "IoT security: Botnet detection in IoT using machine learning," 2021, *arxiv:2104.02231*.

[18] S. H. Haji and S. Y. Ameen, "Attack and anomaly detection in IoT networks using machine learning techniques: A review," *Asian J. Res. Comput. Sci.*, vol. 9, no. 2, pp. 30–46, 2021. doi: 10.9734/ajrcos/2021/v9i230218.

[19] M. Anwer, S. M. Khan, and M. U. Farooq, "Attack detection in IoT using machine learning," *Eng., Technol. Appl. Sci. Res.*, vol. 11, no. 3, pp. 7273–7278, 2021. doi: 10.48084/etasr.4202.

[20] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based IoT-botnet attack detection with sequential architecture," *Sensors*, vol. 20, no. 16, 2020, Art. no. 4372. doi: 10.3390/s20164372.

[21] A. Awajan, "A novel deep learning-based intrusion detection system for IoT networks," *Computers*, vol. 12, Feb. 2023, Art. no. 2. doi: 10.3390/computers12020034.

[22] D. C. Attota, V. Mothukuri, R. M. Parizi, and S. Pouriyeh, "An ensemble multi-view federated learning intrusion detection for IoT," *IEEE Access*, vol. 9, pp. 117734–117745, 2021. doi: 10.1109/ACCESS.2021.3107337.

[23] N. Jeffrey, Q. Tan, and J. R. Villar, "Using ensemble learning for anomaly detection in cyber-physical systems," *Electronics*, vol. 13, no. 7, 2024, Art. no. 1391. doi: 10.3390/electronics13071391.
[24] B. A. Alabsi, M. Anbar, and S. D. A. Rihan, "CNN-CNN: Dual convolutional neural network approach for feature selection and attack detection on internet of things networks," *Sensors*, vol. 23, no. 14, 2023, Art. no. 6507. doi: 10.3390/s23146507.
[25] A. Kumar and I. Sharma, "CNN-based approach for IoT intrusion attack detection," in *2023 Int. Conf. Sustainable Comput. Data Commun. Syst. (ICSCDS)*, Erode, Tamil Nadu, India, IEEE. 2023, pp. 492–496. Accessed: Apr. 03, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10104967/
[26] K. Kostas, "CNN based IoT device identification," Apr. 26, 2023, *arXiv:2304.13894*.
[27] V. Gaur and R. Kumar, "DDoSLSTM: Detection of distributed denial of service attacks on IoT devices using LSTM model," in *2022 Int. Conf. Commun., Comput. Internet Things (IC3IoT)*, Chennai, India, IEEE, 2022, pp. 1–7.
[28] H. Alkahtani and T. H. Aldhyani, "Botnet attack detection by using CNN-LSTM model for Internet of Things applications," *Secur. Commun. Netw.*, vol. 2021, pp. 1–23, 2021. doi: 10.1155/2021/3806459.
[29] B. S. Sharmila and R. Nagapadma, "Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset," *Cybersecurity*, vol. 6, no. 1, Sep. 2023, Art. no. 41. doi: 10.1186/s42400-023-00178-5.
[30] A. M. Eid, B. Soudan, A. B. Nassif, and M. Injadat, "Comparative study of ML models for IIoT intrusion detection: Impact of data preprocessing and balancing," *Neural Comput. Appl.*, vol. 36, no. 13, pp. 6955–6972, May 2024. doi: 10.1007/s00521-023-09183-2.
[31] X. Yu, Y. Huang, Y. Zhang, M. Song, and Z. Jia, "Network intrusion traffic detection based on feature extraction," *Comput. Mater. Contin.*, vol. 78, no. 1, pp. 473–492, 2024. doi: 10.32604/cmc.2023.044999.
[32] A. Sezgin and A. Boyacı, "AID4I: An intrusion detection framework for industrial internet of things using automated machine learning," *Comput. Mater. Contin.*, vol. 76, no. 2, pp. 2121–2143, 2023. doi: 10.32604/cmc.2023.040287.
[33] S. Aktar and A. Y. Nur, "Towards DDoS attack detection using deep learning approach," *Comput. Secur.*, vol. 129, 2023, Art. no. 103251. doi: 10.1016/j.cose.2023.103251.
[34] A. Thakkar and R. Lohiya, "Attack classification of imbalanced intrusion data for IoT network using ensemble-learning-based deep neural network," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11888–11895, 2023. doi: 10.1109/JIOT.2023.3244810.
[35] K. Ren, S. Yuan, C. Zhang, Y. Shi, and Z. Huang, "CANET: A hierarchical cnn-attention model for network intrusion detection," *Comput. Commun.*, vol. 205, pp. 170–181, 2023. doi: 10.1016/j.comcom.2023.04.018.
[36] L. Dhanya, R. Chitra, and A. A. Bamini, "Performance evaluation of various ensemble classifiers for malware detection," *Mat. Today: Proc.*, vol. 62, pp. 4973–4979, 2022.
[37] C. Ioannou and V. Vassiliou, "Network attack classification in IoT using support vector machines," *J. Sens. Actuator Netw.*, vol. 10, no. 3, 2021, Art. no. 58. doi: 10.3390/jsan10030058.
[38] D. F. Doghramachi and S. Y. Ameen, "Internet of Things (IoT) security enhancement using XGboost machine learning techniques," *Comput. Mater. Contin.*, vol. 77, no. 1, pp. 717–732, 2023. doi: 10.32604/cmc.2023.041186.
[39] H. Babbar, S. Rani, D. K. Sah, S. A. AlQahtani, and A. K. Bashir, "Detection of Android malware in the Internet of Things through the K-nearest neighbor algorithm," *Sensors*, vol. 23, no. 16, 2023, Art. no. 7256. doi: 10.3390/s23167256.
[40] R. R. Chowdhury, A. C. Idris, and P. E. Abas, "Identifying SH-IoT devices from network traffic characteristics using random forest classifier," *Wirel. Netw.*, vol. 30, no. 1, pp. 405–419, 2024. doi: 10.1007/s11276-023-03478-3.
[41] A. Sarwar *et al.*, "IoT networks attacks detection using multi-novel features and extra tree random-voting ensemble classifier (ER-VEC)," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 12, pp. 16637–16651, 2023. doi: 10.1007/s12652-023-04666-x.

[42] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, "Attack classification of an intrusion detection system using deep learning and hyperparameter optimization," *J. Inf. Secur. Appl.*, vol. 58, 2021, Art. no. 102804. doi: 10.1016/j.jisa.2021.102804.

[43] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," *Information*, vol. 14, no. 1, Jan. 2023. doi: 10.3390/info14010041.

[44] A. A. Hagar and B. W. Gawali, "Deep learning for improving attack detection system using CSE-CICIDS2018," *NeuroQuantology*, vol. 20, no. 6, 2022, Art. no. 3064.

[45] A. K. Kumar, K. Vadivukkarasi, and R. Dayana, "A novel hybrid deep learning model for botnet attacks detection in a secure IoMT Environment," in *2023 Int. Conf. Intell. Syst. Commun., IoT Secur. (ICISCoIS)*, Coimbatore, India, IEEE, 2023, pp. 44–49.

[46] S. Leoshchenkoa, A. Oliinyka, S. Subbotina, and T. Kolpakovaa, "Implementation of swarm intelligence methods for preprocessing in neuroevolution synthesis," 2023. Accessed: Jul. 29, 2024. [Online]. Available: https://ceur-ws.org/Vol-3702/paper36.pdf

[47] G. R. Kumar, N. S. Govekar, A. Karthik, G. Nijhawan, A. H. Alawadi and V. Asha, "Real-time monitoring and anomaly detection in hospital IoT networks using machine learning," in *2023 Int. Conf. Artif. Intell. Innov. Healthcare Ind. (ICAIIHI)*, Raipur, India, IEEE. 2023, pp. 1–8. Accessed: Jul. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10489821/

[48] G. Airlangga, "Comparative analysis of machine learning models for intrusion detection in internet of things networks using the RT-IoT2022 dataset," *MALCOM: Indonesian J. Mach. Learn. Comput. Sci.*, vol. 4, no. 2, pp. 656–662, 2024. doi: 10.57152/malcom.v4i2.1304.

[49] RT-IoT2022, *UCI Machine Learning Repository*. Irvine, CA, USA: University of California, 2023. doi: 10.24432/C5P338.