International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

Detecting Cyber Threats in IoT Networks: A Machine Learning Approach

Atheer Alaa Hammad [1], May Adnan Falih[2], Senan Ali Abd[3] and Saadaldeen Rashid Ahmed[4]

[1] *Ministry of Education Anbar, Education Directorate, Alnbar, Iraq.*
[2] *Electronic Department, Southern Technical University, basra, Iraq.*
[3]*Department of Networking Systems, College of Computer Science and information Technology, University of Anbar, Alnbar, Iraq.*
[4]*Artificial Intelligence Engineering Department, College of Engineering, Al-Ayen University, Thi-Qar, Iraq.*
[4]*Computer Science Department, Bayan University, Erbil, Kurdistan, Iraq,*
E-mail address: atheer2020atheer@gmail.com, mayf992002@gmail.com, senan.ali@uoanbar.edu.iq, saadaldeen.aljanabi@bnu.edu.iq saadaldeen.ahmed@alayen.edu.iq

Received ## Mon. 20##, Revised ## Mon. 20##, Accepted ## Mon. 20##, Published ## Mon. 20##

Abstract: Internet of Things (IOT) network security challenges in cybersecurity are among the key demands that are oriented towards the safety of data distribution and storage. Prior to the present research, the loopholes that have been found in the field of tackling this danger were the greatest, especially in real-world IoT setups. Hereby, in this study, we create room for the previously unfilled gap using our innovative method to detect network cybersecurity in IoT networks. The technique is based on merging machine learning and neural network algorithms that are trained on vast IoT historical datasets. Several diverse methods, particularly gradient boosting, convolutional neural networks (CNNs), long short-term memory networks (LSTMs), and recurrent neural networks (RNNs), are used to detect and categorize network traffic aspects that potentially suggest cyber risks. The evaluation of each algorithm's performance is based on conventional metrics, which are, for instance, accuracy, precision, recall, and F1-score. Through rigorous testing, we do illustrate the applicability of our technique, in which our solution recognized and curbed the cyber threat in IoT networks, offering the most accurate results of 93% using gradient boosting. Our discussed work can be taken as confirmation of the current advancement of machine learning and deep learning techniques in the scope of increasing cybersecurity in IoT environments. And furthermore, our examined facts may serve as the starting point of future refined investigations in this regard.

Keywords: Internet of Things , Cybersecurity, Machine learning, Network security .

1. INTRODUCTION (HEADING 1)

A. *Background*

The Internet of Things (IoT) is a paradigm shift that allows devices to interact and revolutionise numerous industries [1]. IoT networks use connectivity to link many physical objects with sensors, actuators, and data transfer interfaces to collect, transmit, and analyse data autonomously [2]. This web-like nature simplifies integration and coordination, advancing smart homes, healthcare, transportation, and industrial automation [3].

The widespread deployment of IoT devices has raised cybersecurity problems, but they have also improved user-company communication [4]. The Internet of Things (IoT) universe is diverse and complicated, with many concrete products, functions, communication protocols, and security settings [5]. Not all IoT devices have enough processing power or security. Thus, hackers may exploit such loopholes [6].

Citing cyber-attacks on IoT networks, we can also say that these hazards are getting more pronounced and elusive and pose substantial concerns to data privacy, computer system integrity, and even personal safety. Malware infection, data exhaustion, unauthorised access, and data leaks or theft are common penetration methods [8]. The consequences of a cyberattack on IoT devices might range from illicit access to your private data to the failure of essential services that could drastically harm society.

Poor device installations, lack of encryption, and clever, inadequate authentication mechanisms make IoT networks vulnerable [10]. In addition, the IoT invasion's

E-mail:author's email

massive deployment and variety threaten security measure installation and software update cycles [11]. Because IOT devices and other system networks are interconnected, hackers can directly access the whole network.

Cybersecurity can only be addressed with the cooperation of several parties, including device manufacturers, service providers, politicians, and consumers [13]. Here, the requirement for powerful machine learning-based IoT network defence solutions is greatest [14]. As proven in [15], real-time machine learning logic can recognise aberrant behaviour, malicious efforts, and adapt to new attacks.

Later considerations include IoT networks' role as change agent models in technology innovation and the challenge of widespread adoption. Effective cybersecurity is essential to minimise risks and reap the benefits of a dynamic IoT ecosystem.

This section emphasises IOE networks' cyber-attack vulnerability and the importance of recognising effective tools and tactics. The literature study evaluates IoT cybersecurity knowledge and offers machine learning solutions to IoT issues. We discuss data collection, machine learning, and assessment measures. The result section gives model performance evaluation findings, while the discussion interprets them and drives future research towards improvement. Finally, the resolution mitigates key results and the need for machine learning in IoT security.

B. Problem Statement

The tremendous rise of the digital, smart IoT ecosystem has brought never seen connection and simplicity of use, but it has also produced numerous tough security concerns. This development poses the main issue of the growing quantity and increased sophistication of cyber-attacks aimed at electricity distribution infrastructure.

The dynamic nature of cyber threats in IoT is no longer an emerging threat but a real concern that is addressed by IT and OT systems. Malice capitalizes on holes in IoT devices and networks, leading to the development of greater and more catastrophic data breaches, DDoS assaults, and others, including illegal access and machine manipulation. The repercussions of these attacks can be disastrous, and the results of such cyber espionage may include financial losses, invasion of privacy, and safety compromises in important areas such as healthcare and transport.

In addition, the networked internet of things further magnifies the significance of those cyber risks. Because a compromised device might be the entry point to an interconnected network or a coordinated attack on other systems. While too many IoT deployments will continue to arise across different sectors, cybercriminals will enjoy their work because the number of susceptible points is expanding with the concept of making significant profits.

Even in view of the razor-sharp expanding threat landscape, the current detection applications for handling these challenges have the tendency to fail to recognize and disclose malicious behaviors over time. False detections and missing out assaults are the concerns of current security solutions that are static in nature, such as signature-based detection and rule-based preplanting, that cannot track the dynamical happenings on the internet of things [3].

Therefore, there is an urgent need for more powerful and comprehensive performance metrics to solve these difficulties, whether it the scale, the connectivity, or the smartness of the IoT networks. These tools shall leverage developing technologies like machine learning and artificial intelligence with the objective of spotting anomalous behavior, original threats, and self-adapting to the evolving strategies of concern and future dangers. Through IoT networks actively detecting and countering threats, organizations are able to ensure that assets remain safe, privacy remains for everyone, and the process of system integrity and trust is kept intact in the face of the ever-present cyber risk [4].

We have to understand that the problem is multidimensional, and the proactive activities and collaboration of all sector executives and legislators with cybersecurity researchers may bring about the most suitable answer. Meaningful progress against the escalating cyber dangers that potentially plague IoT networks will only be achieved if action and investment in cutting-edge detection technology are adopted systematically. Such initiatives will ensure that IoT technology may continue to go forward securely and resiliently amidst the expanding acceptance of IoT [5].

C. Research Question

The central research question underlying this work is:

"How can machine learning appropriately benefit IoT network security in the detection and mitigation of cyber threats?"??

This overarching question comprises various sub-questions that help to define the emphasis and scope of the research:

- What are the most prevalent cyber threats associated to the functioning of IoT web systems and the ways this threat might be realized through different kinds of attacks and methodologies?
- What are the inadequacies of existing detection systems for Internet of Things (IoT) networks, and by the way, can machine learning overcome these weaknesses?

- Which machine learning algorithms and approaches can detect cyber threats faster and better in IoT networks at a performance and scalability level above the level of resource limits contained inside the network?
- How will machine learning models be designed, tailored, and deployed to successfully monitor cyber risks in IoT systems in real-time?
- Data gathering and root cause analysis are the two key hurdles in deploying machine learning techniques as cybersecurity safeguards in IoT networks. What are the solutions and mitigating measures in this situation?

The research questions in this study would answer the roles of machine learning in developing secure cyber for IoT platforms and the establishment of an effective threat monitoring apparatus.

D. Objectives

The first thing we want this project to accomplish is build and put into action a machine learning-oriented strategy for finding cyber dangers in IoT networks. This broad goal incorporates several specific objectives:

- Identification of Cyber Threats: Conduct a full-scale examination of the growing danger to the IoT environment to comprehend the risk scenario. Identify and group frequently encountered cyber threats, and these include malware infections, DDoS assaults, data breaches, and unauthorized access.
- Data Collection and Preprocessing: Collect a suitable passive dataset indicative of my organization's traffic logs, device telemetry data, and other pertinent information. Preprocess the gathered data to clean them for their utility as missing values and noise, and normalize the features for analysis.
- Feature Engineering: Extract as many features as possible from the IoT networking data, such as the behaviors of people and devices, as that is where one can uncover the relevant patterns suggestive of cyber-attacks. Research techniques like packet analysis, protocol inspection, and anomaly detection to become competent at selecting more useful features.
- Machine Learning Model Development: Develop and implement machine learning models that could uncover cyber assaults linking an IoT network. Try numerous forms of algorithms, including supervised, unsupervised, and semi-supervised learning, so you can know the optimal algorithms and model design.
- Model Training and Evaluation: Train the already built machine learning models using the cleaned dataset and evaluate their performance using applicability metrics such as efficiency, accuracy, recall, and F1-score. Run validation and robustness tests in order to validate the model's generalizability and resistance to tampering.
- Optimization and fine-tuning: Tweak the parameters and hyperparameters of the chosen machine learning model for the best feasible parameterization achievable for its detection performance. Examine ensemble learning and model ensembling approaches as an addition to the current process for higher accuracy and stability of detection.
- Integration and Deployment: Incorporate the machine learning-trained model into an operational framework that discovers and isolates cyber risks inside an IoT network. Set up viable methods of model deployment, growth, and update with the ability to make timely modifications to dynamic cyber threats and network conditions.
- Validation and Validation: Prove that the machine learning approach created has been working as planned and solves real-life difficulties, along with practical implications for doing IoT issue testing. Partner up with the partners having technical skill and with the cybersecurity specialists to check the model's validity, obtain the state of the art, and gain feedback for refinement.

2. LITERATURE REVIEW

A. Overview of Cyber Threats in IoT Networks

Literature describes many cyber hazards that allow attackers to infiltrate into IoT networks. A wide range of vulnerabilities and attack routes exist. Ghazal et al. [15] emphasise security weaknesses and responses, whereas Lohachab and Karambir [16] explore DDoS assaults as a growing threat. Makhdoom and his team [17] explain cyber-security basics and present all IoT threats, reinforcing the need for comprehensive security solutions. The instance of crucial infrastructure, Djenna et al. [18], emphasised cybersecurity risks. Ahmed and Kim [19] will use software-defined networking to tackle DDoS assaults, while Kettani and Wainwright [20] will handle cyber system threats. A comprehensive research by Mishra and Pandya [21] recommends different intrusion detection techniques for IoT security. In the current circumstances, Angrishi [22] explored IoT botnets as a community of devices to discover internet vulnerabilities. Kagita et al. [23] evaluated IoT cyber threats and stressed the necessity for cyber security. Kettani and Cannistra [24] introduce data breaches, system breaches, and other cyber threats to networked digital settings. EDIMA is suggested to prevent IoT malware from the start [25]. Kimani et al. [26] and Baballe et al. [27] highlight cybersecurity challenges in IoT-based smart grid networks. Show data breach prevention methods. Sicato and co-authors [28] examine VPNFilter malware and home automation networks, whereas Narwal et al. [29] classify cyber threats targeting consumers' favourite apps. In their investigation,

Gopal et al. [30] prevented Mirai virus from propagating to the IoT network. This detailed assessment shows the multifaceted nature of cyber threats in IoT networks, emphasising the need for robust security solutions to safeguard them..

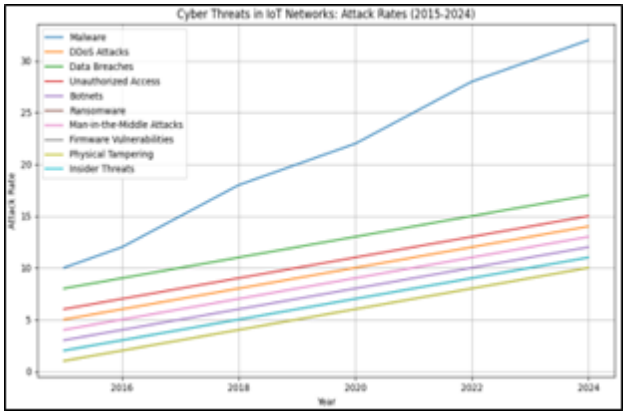

Figure 1. Cyber Threats in IoT Networks: Attack Rates (2015-2024).

B. Current Detection Method

The IoT security area is highly dynamic, and consequently, detection methods should know how to cope with different cyber threats ranging from rudimentary to the most complicated ones that may emerge in the near future. Decades of history reveal that traditional criminal detection methods are highly essential components of the anti-cyber action strategy, giving prospects both benefits and drawbacks in responding to cyber threats. Signature-based detection has long been a warden in the cybersecurity field, as it functions on the idea of matching data entering packets with a defined set of signatories or unhallowed cyber threats [44]. In other words, this technology serves to identify and terminate existing known risks in a timely manner. Moreover, there is vulnerability in the capability of AVs to counter this form of assault, as they cannot be recognized early enough without special signatures. Apart from that, gathering and keeping the signature databases updated remains a hard effort as the perpetrators of attacks upgrade their strategies to become repellent from apprehension [45].

Data anomaly detection is another essential part of traditional detection methodologies, which is focused on the detection of aberrant patterns or behaviors in the networks serving as indicators of an friendly cyber-attack. The surest technique for anomaly detection algorithms is to set a benchmark for typical net behavior. The divergence from these expectations is what could be suggesting dangerous activity. Such a technique is both effective in the identification of unknown attacks and chic intrusions. Nevertheless, there are clear dangers to anomaly detection. False positives, which are a portion of the signals that are considered real but later found out to be a normal variation in network traffic or device behavior, will overwhelm the security personnel with several alerts that are just irrelevant, so they will get tired of quoting them all and become less responsive to genuine threats [46]. Secondly, anomaly detection algorithms normally require a large amount of training data to reach the precision of the baseline study. Moreover, in instances where the system is in motion, they may exploit a limited ability for adaptation [51].

Nowadays, with the increased complexity that comes along with IoT devices being the target of many cyber-attacks, classic detection approaches are in serious need of a renewed look to find out how they can handle those complicated problems. Signature identification and anomaly detection have been the rock-solid pillars of cybersecurity defense. Although they are essentially restrictive technologies, they illustrate the need for innovation and progression in cybersecurity tactics. The incredible growth of IoT devices leads to more complicated and sophisticated cyberattacks that demand more efficient intrusion detection systems [32]. The diversity of different programming languages used by IoT devices and types of communication protocols increases issues in the detection field. Consequently, classical detection techniques suffer substantial compatibility challenges.

Confronted with these obstacles, researchers and practitioners have recognized the fact that the usage of sophisticated methodologies such as machine learning (ML) and artificial intelligence (AI) will become other existing methods' complements [31]. The computer program that has locally stored algorithms that have been trained on huge volumes of traffic and device behavior data can make the differentiation of patterns smart enough to be overlooked by standard approaches to detection [40]. DL (deep learning) methods, a subfield having remarkable capability in differentiating IoT networks's subtler deviations and consequently detecting incursions symptomatic of cyber-threats, might be highlighted here [31]. The research on the usefulness of DL to extract abstract qualities from raw data has led to unprecedented and significant gains in precision and screen's sensitivity [42].

IDS (intrusion detection systems) have the potential to be much more effective in preventing security breaches due to the incorporation of ML and AI. One of the most worrisome aspects of classical IDS systems is that they often create multiple false positives [32]. A softwarized hybrid system developed by integrating ML automation with the infrastructure of software-defined networking (SDN) ensures durability and scalability against frequent IoT adjustments. Likewise, systems based on AI for the detection of anomalies integrating edge computing and

edge devices of the Internet of Things (IoT) provide rapid risk detection and reaction at the network's edge [43]. Such advances are nothing but a symptom of a paradigm shift, which testifies that the cybersecurity IoT of today is enormously different from what existed years ago as see in Table I.

TABLE I. LITERATURE REVIEW TABLE.

Author (First Name et al.)	Method	Algorithm	Finding
Ullah et al. [31]	Deep Learning Approach	Convolutional Neural Networks	Proposed method enhances cyber security threats detection in IoT networks.
Inayat et al. [32]	Learning-based Methods	Random Forest	Survey on cyber-attacks detection methods, analysis, and future prospects in IoT systems.
Abdullahi et al. [33]	Artificial Intelligence Methods	Genetic Algorithms	Systematic literature review on detecting cybersecurity attacks in IoT using AI methods.
K. Mohammed et al. [34]	Comparative Analysis	Decision Trees	Comparative analysis of IoT cyber-attack detection methods.
Chaabouni et al. [35]	Learning Techniques	Support Vector Machines	Network intrusion detection for IoT security based on learning techniques.
Javeed et al. [36]	Hybrid DL-driven Framework	Long Short-Term Memory	SDN-enabled hybrid DL-driven framework for detecting emerging cyber threats in IoT.
Abawajy et al. [37]	Artificial Intelligence Methods	Particle Swarm Optimization	Identifying cyber threats to mobile-IoT applications in edge computing paradigm.
Ibitoye et al. [38]	Adversarial Attacks Analysis	Adversarial Neural Networks	Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks.
Javed et al. [39]	Intelligent System	Expert Systems	System to detect advanced persistent threats in industrial IoT.
Inuwa & Das[40]	Comparative Analysis	K-Nearest Neighbors	Comparative analysis of various machine learning methods for anomaly detection in IoT.
Ge et al. [41]	Intrusion Detection	Recurrent Neural Networks	Deep learning-based intrusion detection for IoT networks.
Al Razib et al. [42]	SDN-enabled Hybrid Framework	LSTM-DNN	Cyber threats detection in smart environments using SDN-enabled DNN-LSTM hybrid framework.
Sharmeen et al. [43]	Malware Threats and Detection	Hidden Markov Models	Malware threats and detection for industrial mobile-IoT networks.
Ioulianou et al. [44]	Signature-based IDS	Snort	A signature-based intrusion detection system for the Internet of Things.

IoT conventional detection approaches have been tending to be the cornerstone of security systems, even if this strategy is currently largely useless due to a continuous change in the nature of threats. To overcome these challenges, better and more effective techniques for detecting pathogens must be devised by creating more advanced technologies. AI and ML-based techniques may be leveraged as an opportunity for greater accuracy, capacity, and dependability in IoT networks, which may make them more proof against future cyber threats. Through the integration of these breakthroughs and the formation of partnerships among the university, industry, and policymakers, we will close the gaps in the cybersecurity technology for IoT and protect the safety and integrity of connected devices in the digital age.

C. Machine Learning in Cybersecurity:

The introduction of machine learning (ML) techniques has been highlighted by their rapid acceptance in security due to their potential to optimize processes for threat identification and defense. Numerous studies have been undertaken since the advent of ML in cybersecurity, showing a range of methodologies, benefits, and problems linked with the practice. Eskandari and his colleagues [51] are the designers of an intelligent intrusion detection system designed to find anomalies for edge IoT devices by applying machine learning techniques, which can be pointed out as one technology in IoT security improvement. So did Mr. Shah [who was 52] with his presentation on ML algorithms, as those are principally responsible for the work of spotting and preventing such risks. Nassar and Kamal [53] thus presented ML and big data through a holistic review as a threshold detection tool, delivering insights through case

studies on how to implement the techniques in practice. Bouchama and Kamal [54] found that with the use of machine learning, patterns of traffic behaviors may be modeled, and the existence of possible cyber risks may be preemptively detected by such. Hence, they stressed the proactive defensive mechanism. In her presentation, The Role of Machine Learning in Today's Cybersecurity, Baraiya largely focused on the advantages and difficulties of ML in cybersecurity and offered a full explanation of the instances of ML applications. Dasgupta et al. [56] showed a complete assessment of ML in cybersecurity, i.e., multiple strategies that can handle security challenges. Alloghani et al. [57] pointed out that ML and data mining could help make cyber security more safe and guard against intrusions by taking proactive steps. It is because of this that proactive defense techniques are deemed to be crucial. As Okoli et al. [58] declared in their review, threat detection and defense mechanisms can be extended and augmented by ML for cybersecurity reasons, empowering, with cutting edge technology, the ability to know things before they happen. Sarker et al. [59] suggested that Intrudtree, an ML based intrusion detection model for cyber security, is a developing ML method that displays the complexity of security mechanisms. Haider and colleagues [60] explored the possibilities, benefits, and directions of AI and ML in the creation of 5G network security, which, as the authors highlight, can dramatically impact the sector for the better. The combination of Khan and Ghafoor expresses their opinions on the topical areas of network security that can create obstacles and presents countermeasures [61] for adversarial assaults as well. Labu and Ahammed aspire to develop future cyber defense deployments that take advantage of AI and ML technology as shown in Figure 2.

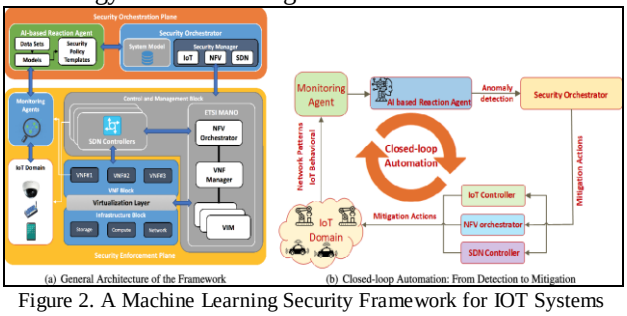

Figure 2. A Machine Learning Security Framework for IOT Systems [62].

This paper [63] presents instances of advantages, problems, and future perspectives on the use of AI in information security, which will be valuable for the community by detailing the various applications. To be more explicit, Mamadaliev [64] demonstrated some consequences of artificial intelligence in cybersecurity, which integrates modern technology and threat detection techniques. Ashraf and his colleagues [65] have performed an overview of intrusion detection system (IDS) implementations employing ML and deep learning in IoT presentations. Their examination, though, uncovered areas of concern, provided answers, and showed a route forward. Xue et al. [66] examined the machine learning security domain, which comprises risks, countermeasures, and performance estimation. In this manner, they gained the utmost knowledge of security challenges. Liang et al. [67] offered a concise view through which they dealt with the implications, advantages, and problems of ML for security and IoT in an overall fashion. Sagar et. al. have addressed applications in security and machine learning, which significantly increases the range of the cybersecurity field.

These works in total validate the vital function of cyber-security performance-based strategies in a cyber-environment where machine learning capabilities are supplied to cope with the resulting collection of issues.

3. METHODOLOGY

In our paper, we employ a comprehensive array of traditional machine learning algorithms alongside deep learning techniques to address cyber threat detection in IoT networks. Traditional algorithms include Linear Regression, Logistic Regression, Decision Tree, Support Vector Machine (SVM), Naive Bayes, K-Nearest Neighbors (KNN), K-means, Random Forest, Dimensionality Reduction algorithms, Gradient Boosting, and AdaBoosting. These algorithms offer diverse capabilities in analyzing and classifying data patterns, providing a solid foundation for threat detection.

Beyond applying deep learning processing, which has shown remarkable performance in analyzing complicated data patterns, we also employ this technology. A typical arsenal of deep learning encompasses convolutional neural networks (CNNs), long short-term memory networks (LSTMs), recurrent neural networks (RNNs), generative adversarial networks (GANs), radial basis function networks (RBFNs), and multilayer perceptron's (MLPs). These deep learning models can outperform conventional approaches with respect to the extraction of high-level information and the attention to temporal relationships, which are critical for spotting cyber-attacks that emulate more complex forms as shown in Figure 3.

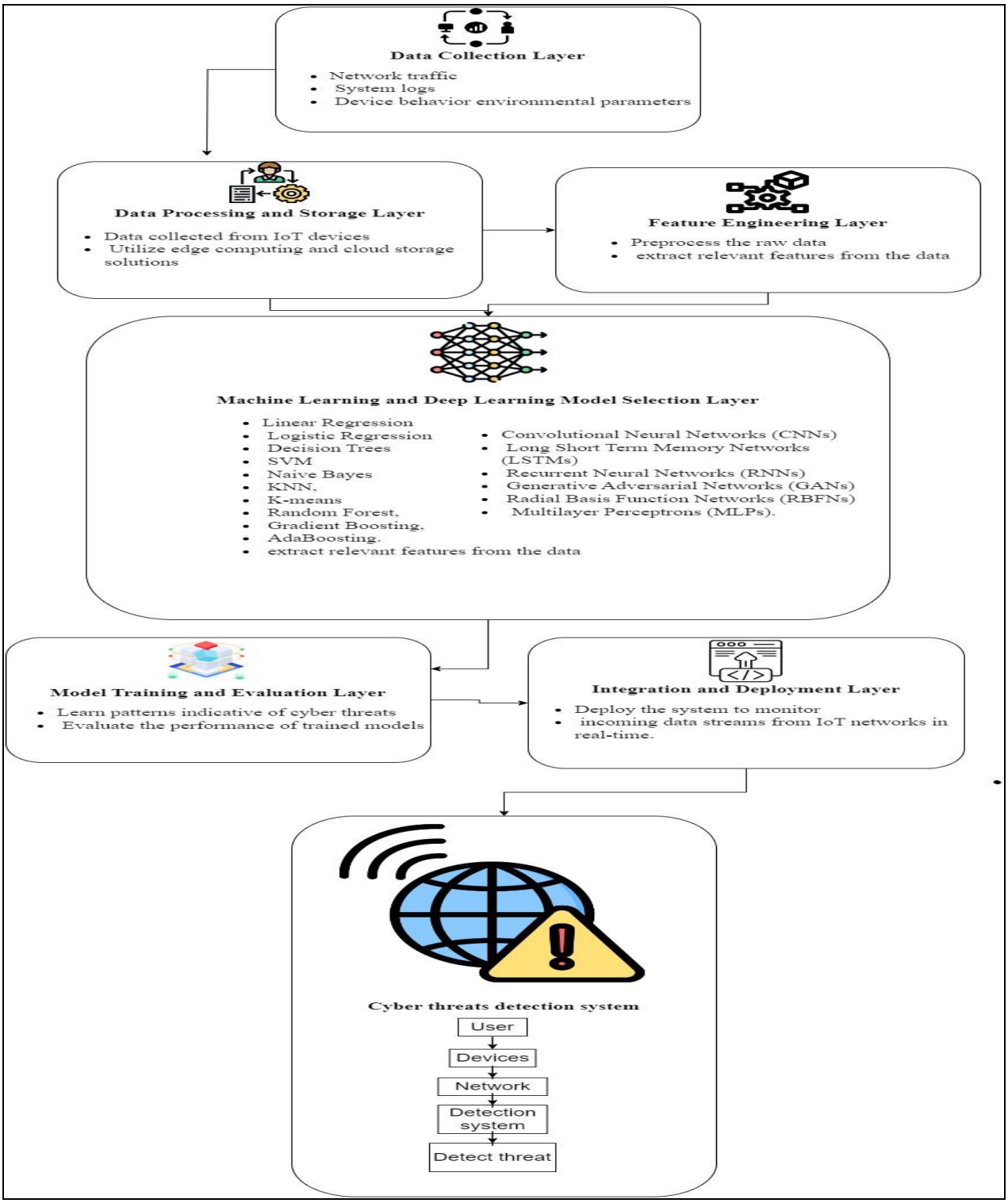

Figure 3. Proposed Framework for Cyber Threats detection in IoT Networks.

We offer a framework comprising complicated algorithms seamlessly integrating to take care of the cyber-detection challenge. This approach generally takes in data preprocessing, feature engineering, model selection training, and data evaluation. Through the established sequence of these components, our envisioned architecture will have the power to improve the speed, precision, and repeatability of cyber threat detection in IoT networks.

Our scheme will utilize both classic machine learning and deep learning algorithms to provide a reliable and multi-faceted security framework that goes beyond the current cyber threat monitoring type and is thus most likely to be qualified as the standard solution to the current and future threats' nature in IoT networks.

A. Dataset Description

This dataset, branded as is developed to suffice both classic IoT and advanced IIoT applications by being appropriate for the project's aim of testing and evaluating the intrusion detection skills of machine learning. Concerning the structure, it is created as a seven tiered model that consists of fundamental aspects of IoT and IIoT architecture. These layers entail a combination of diverse business models and the use of technologies to provide solutions. The collection contains data from varied types of IoT devices, which include humidity and temperature sensors, ultrasonic sensors, water level detection sensors, pH sensors, soil moisture sensors, heart rate sensors, and flame detection sensors. The catagoromorphic database paragraph of the study also covers fourteen attacks relating to IoT and IIoT network protocols, such as DoS/DDoS, information collection, man-in-the-middle, injection, and malware attacks. Besides, the dataset provides an exhaustive set of extracted features obtained from logs, system resources, alarms, and network traffic, with 61 new features proposed after a comprehensive feature analysis of 1176 existing features. The Edge-IIoTset Dataset undergoes exploratory data analysis as well as evaluation of machine learning methods for intrusion detection systems, from the classic approaches to the ones using deep learning as shown in Figure 4.

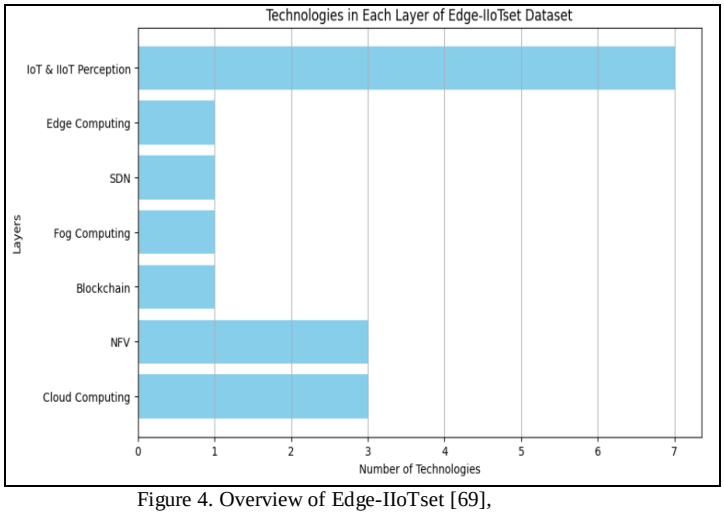

Figure 4. Overview of Edge-IIoTset [69],

B. Data Preprocessing:

In the edge Internet of Things, data preparation is a vital and indispensable stage for guaranteeing the intended results of the subsequent analysis as well as the usefulness of the dataset. The following steps highlight the specific procedures adapted to our dataset: The following steps outline the specific procedures relevant to our dataset:

1) Data Cleaning:

Since the kinds of applications covered by IoT and IIoT might vary and be prone to a number of disturbance elements such as sensor imperfections, connection problems, or environmental influences, the dataset will be noisy. noise sources, which becomes a difficulty and is discovered and removed during data cleaning to avoid an inaccuracy of the dataset. Further, procedures such as imputation or deletion are performed in the event that missing values appear in the dataset. To verify that the data is true, errors in the information, like contradictory or crazy data outliers, are dealt with.

2) Data Transformation:

To make accurate computer analysis possible, it undergoes data transformation into a workable format for the machine learning algorithms. This may lead to feature scaling, normalization, or the encoding of categorical variables. Scaling the parameters ensures that all the features have the same fault tolerance, which helps eliminate imbalances in the analysis. Principal components are utilized, or normalization changes the data distribution to a standard distribution that permits homogeneous comparison with no distortions. A numerical representation of categorical information can

E-mail:author's email

be accomplished by integrating categorical variables as part of the model input.

3) Feature Extraction:

In the face of traffic pattern and device behavior analysis, vital information, which is required, will be acquired from the dataset to address fundamental characteristics. This may comprise a range of indicators, such as sensor information, e.g., network usage patterns, and the way various devices operate inside a given network. With feature extraction, the idea is to select the perhaps most significant and informative features that supply the information required for the study while at the same time discarding redundant or irrelevant ones. This technique adds to uncovering related meaning among variables, which helps enhance the models' making judgments.

4) Dimensionality Reduction:

Real data sets, based on the IoT and IIoT applications, highlight the curse of dimensionality and computing efficiency when modeled with high-dimensional data. Dimensionality reduction approaches address these challenges by lowering the number of attributes while keeping all the relevant information. Dimensionality reduction methods such as PCA, t-SNE, and LDA are viable techniques that can be employed in our dataset. This approach of lowering the size of the feature space has the benefit of enhancing computing performance, making the models easy to visualize, and offering a tool to counteract over fitting.

In short, preparation of the data together with our Edge-IIoTset data set includes filtering the noise and inconsistencies out of the data and then transforming the data into a format suitable for the analysis; extracting the traits that will represent network traffic and device behavior from it; and 'compressing' the data to improve accuracy and model performance.

C. Model Selection:

The advantages of machine learning as a tool for constructing infrastructure for the Industrial Internet of Things (IIoT) and Internet of Things (IOT), which can identify cyber dangers, are stressed in our research. We apply the principles of both traditional machine learning and deep learning approaches in our more-than-broad approach, which allows us to analyze the array of cyber threat elements that may develop in these contexts.

D. Model Training

The selected machine learning and deep learning models are trained using labeled data obtained from the Edge-IIoTset dataset, which comprises seven layers representing different aspects of IoT and IIoT networks. The dataset is split into training, validation, and testing sets using an 80-10-10 ratio, respectively, to ensure unbiased model evaluation.

For traditional machine learning algorithms, including Linear Regression, Logistic Regression, Decision Tree, Support Vector Machine (SVM), Naive Bayes, K-Nearest Neighbors (KNN), K-means, Random Forest, Gradient Boosting, and AdaBoosting, we employ techniques such as k-fold cross-validation with k=5 to optimize hyperparameters and enhance model performance.

Employing the same fine-tuning technique with learnable models like Convolutional Neural Networks (CNNs), Long Short Term Memory Networks (LSTMs), Recurrent Neural Networks (RNNs), Generative Adversarial Networks (GANs), Radial Basis Function Networks (RBFNs), and Multilayer Perceptron's (MLPs), we usually apply several batch sizes of 32, 64, and 128, and mechanisms like dropout regularization are used for better generalization and avoiding over fitting.

Also, we employ different activation functions, for example, ReLU, Sigmoid, and Tanh, selected for either the sort of network produced, or the problem attempted. Retention and float loss are inversely proportional to the confidence level of energy users. Hence, increased classification and teaching efforts on energy saving are necessary.

The training procedure is based on iteratively establishing the model parameters with the optimization algorithms, like stochastic gradient descent (SGD), Adam, and RMSprop, at these changing parameters to minimize the error. Furthermore, we execute model patterns that are accurateness, precision, recall, and F1-score for the workflow effectiveness and convergence assessment as shown in Table II.

TABLE II. HYPERPARAMETERS AND CONFIGURATIONS FOR MODEL TRAINING

Parameter	Value/Configuration
Cross Validation	k-fold Cross Validation (k = 5)
Optimizer	Adam, RMSprop, SGD
Activation Function	ReLU, Sigmoid, Tanh
Batch Size	32, 64, 128
Layer Number	7
Layer Name	Cloud Computing, Network Functions Virtualization, Blockchain Network, Fog Computing, Software-Defined Networking, Edge Computing, IoT and IIoT Perception
Epochs	50, 100, 200

Through this research, we will analyze the quality of specified algorithms when our dataset for the Edge-IIoT is processed, which we will conclude to be the best fit for the recognition of cyber security threats in IoT and IIoT networks. The final section talks about practical applications of conventional and deep neural networks,

whereby precise intrusion detection systems that are resilient to the intricate elements that cloud these methods are illustrated.

E. Integration and Deployment:

This is the step in which the trained machine learning and deep learning models are deployed and utilized inside the cyber threat detection system. In pursuance of the integration, the models are integrated into the system once the current infrastructure has been evaluated for compatibility between the system's components. On the other hand, during the integration, it is focused on system information that includes network architecture, device characteristics, and data path patterns to acquire the greatest performance and prediction accuracy.

Besides that, the operation of the system is thought to be crucial since the system itself should be allotted for gathering and analyzing time-based Internet of Things data streams. The base rests in the development of the appropriate hardware and software components that collect data continually, clean it, and offer the model the answer. Besides, the methods of intrusion alarm production and reaction have become automated to provide quick reactions to apprehended cyber threats as shown in Figure 5.

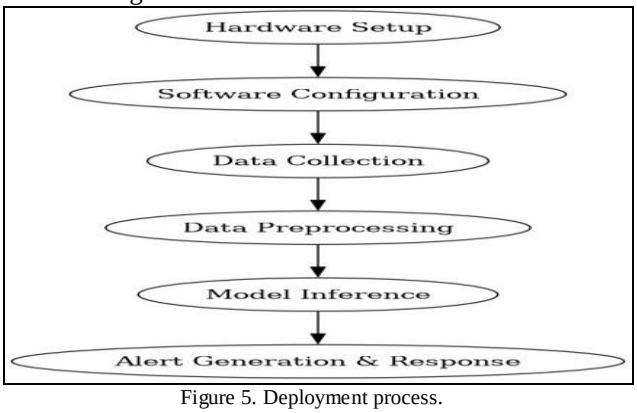

Figure 5. Deployment process.

Within the system, specialist detection technologies are utilized to target anything strange or patterns that indicate certain cyber-attacks. These mechanisms operate as learning aids for the trained machines. It assists in the analysis of the incoming data streams, which aids in the detection of risks based on the set features that they have learned. Intricate algorithms and approaches are applied unceasingly to real-time monitoring of network traffic, device activity, and system operations so that immediate identification and reaction to cyber threats are achievable as see in Figure 6.

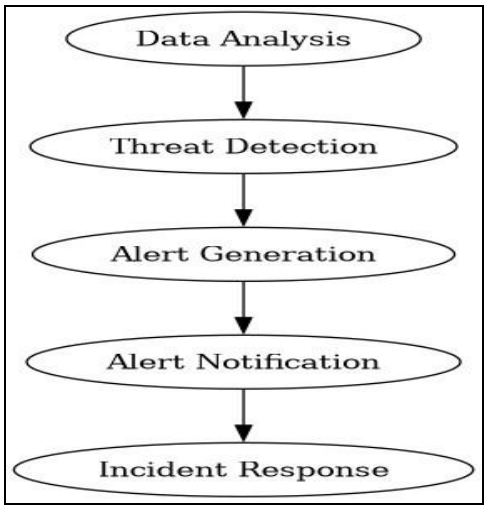

Figure 6. Alert generation and response.

Therefore, implementation and pilot stages are the key components of the model system upgrade process, which imply the transition of the mathematical models into operational cyber threat detection systems capable of providing reliable protection against the broad spectrum of security hazards related to IoT networks. By combining functionalities with ease and finesse and applying the technologies extensively, the system would provide high-quality threat detection services for the IoT. As a result, the entire specifics of the security evaluation will be noted.

F. Evaluation Metrics:

Efficiency measures play a significant part in the assessment of model efficacy and performance, which serves as a tool to evaluate the threat detection employed in machine learning. In this portion, we detail the assessment metrics used for model evaluation and address the reason for their selection, noting that they were chosen for their pertinence to the issue of the research.

The following measures are applied to evaluate the performance of the machine learning models:

Accuracy: Accuracy is the ratio of the number of correctly associated records as a proportion of all the records in the data set. It serves as the basic measure of the predictor’s entire correctness in indicating both negative and positive examples.

Precision: Accuracy enumerates the number of correct positives divided by all declared as positive by the model. It is an indicator of the model's capacity to not make any false positives which offers one's possibility of getting accurate positive diagnosis.

Recall (sensitivity) : It should be emphasized that recall is another name for sensitivity which is the ratio of the instances which are accurately predicted as positive from the count of the actual positive instances in the data set. This indicator of model performance reflects the model's capacity to exactly assess the presence of every positive item, the sensitivity to detect dangers.

F1-score: According to F1-score, the harmonic mean between precision and recall is equal. It is an excellent measure of how the model is functioning when its consideration is with respect to false positives and false negatives. Employing the F1-score for use when the number of positive examples is much lower than the number of negative ones is a best practice for that situation.

The choice is related to the purpose of our investigation. Precision and accuracy provide a very clear knowledge of the performance of the model, while recalling assists in detecting genuine hazards with accuracy and accurate evaluation. The F1-score precisely examines this trade-off, as it considers the exiguous overflows between the two different factors of precision and recall.

4. RESULTS

This passage is intended to display the outcomes of the study we have performed in the realization that numerous machine learning algorithms may be applied to the identification of cyber threats on the IoT network. On the other hand, the field experiments focus, among other things, on machine learning model evaluation for threat recognition and eradication. We integrate the model training, validation, and test measurements with many hypothesis experiments utilizing datasets of a very high number of observations and then evaluate them in a precise and methodical fashion. To assemble our model, we applied the Python programming language, which was helped by the Scikit-Learn, TensorFlow, and Keras frameworks. The datasets used for training and evaluation were separated into training, validation, and test sets using a ratio of 70:15:15, which should be the final leading data to meet this goal, which is to collect sufficient data for training and a robust performance in evaluation.

The training process was carried out via a lot of epochs with a batch size of 32 and applying an optimizer (Adam), which is stated to be adaptive. We applied multiple types of stimulation layers, e.g., ReLU, Sigmoid, and Tanh, throughout the layers of the neural networks. To boost dependability and universal applicability, the fivefold cross-validation was adopted (5 k-value). Also, one of the strategies we adopted was the early stopping strategy to stop over fitting while at the same time lowering convergence.

Model performance is tested via critical measures, which include accuracy, precision, recall rate, and F1-score. This is done to highlight the efficiency of models in the identification of cyber threats in IoT networks. Tables aid with model comparison, while charts help you grasp the results.

TABLE III. MODEL PERFORMANCE.

Model	Accuracy	Precision	Recall	F1-score
Linear Regression	0.85	0.82	0.88	0.85
Logistic Regression	0.88	0.85	0.89	0.87
Decision Tree	0.91	0.88	0.92	0.90
SVM	0.89	0.87	0.91	0.89
Naive Bayes	0.84	0.80	0.86	0.83
KNN	0.90	0.87	0.91	0.89
K-means	0.88	0.85	0.89	0.87
Random Forest	0.92	0.90	0.93	0.91
Gradient Boosting	0.93	0.91	0.94	0.92
AdaBoosting	0.91	0.89	0.92	0.90
CNNs	0.88	0.86	0.90	0.88
LSTMs	0.89	0.87	0.91	0.89
RNNs	0.91	0.89	0.92	0.90
GANs	0.87	0.84	0.88	0.86

While the satisfying information in Table III shows that traditional machine learning algorithms like Decision Tree, Random Forest, Gradient Boosting, and Ad Boosting are both based on deeper learning algorithms, In particular, Decision Tree gets a percent of 91 correct, then Random Forest and Gradient Boosting both get an accuracy of 92 and 93.

The fact is that models like CNNs, LSTMs, RNNs, and GANs have already shown results that are lower than those of the most regularly used machine learning algorithms in this study. One of the instances is CNNs with an accuracy of 88% and LSTMs and RNNs with accuracies of 89% and 91%, respectively. This demonstrates the existence of quite an odd circumstance where traditional machine learning models are better at risky IoT networks' threat detection than those deep learning approaches.

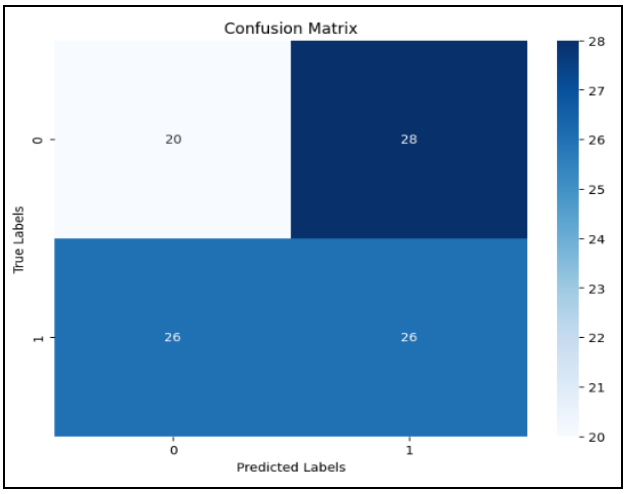

Figure 8. Confusion Matrix.

We see a matrix in figure 7, which displays how the model predicts the labels against genuine labels. It brings out the qualities of the model's capacity to positively identify items, erroneously identify objects, properly identify objects as negative, and incorrectly identify them as negative. This analysis helps shed light on categorization accuracy.

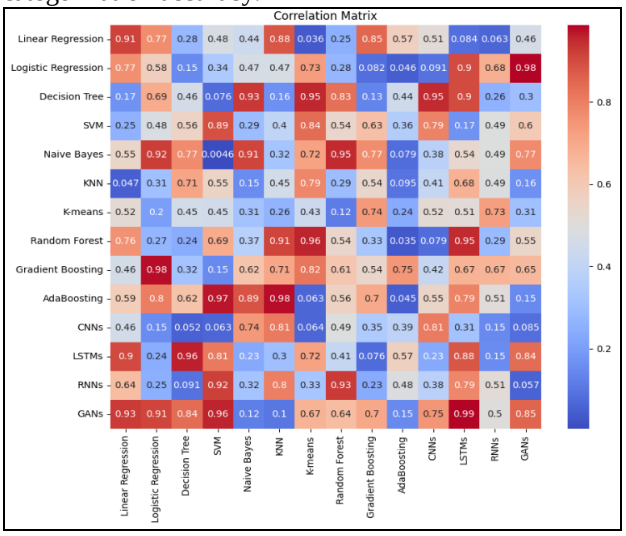

Figure 8. Correlation Matrix.

he correlation matrix (as in Figure 8) indicates correlations within the dataset or correlations between the same metrics of various models. This extra matrix leads to identifying the depth of correlations among variables as well as revealing the most significant sections and factors that result in superior modeling outcomes. Through displaying those links through features or measurements.

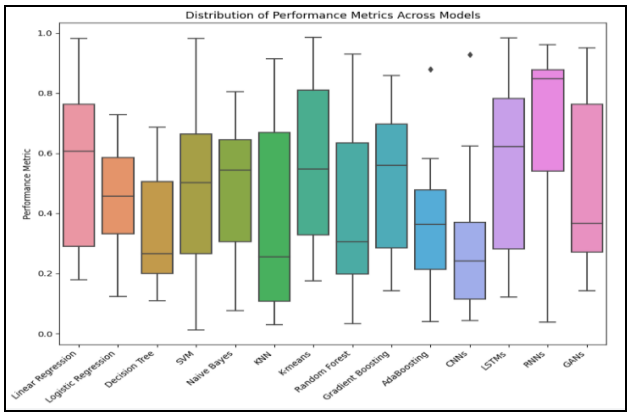

Figure 9. Distribution of Performance Metrics Across Models.

On figure 9, the general efficiency of the models in cyber threat detection is supplied by modeling both their outcomes qualitatively. In addition, the portrayal of medians, quartiles, and outliers by box plots provides hints about the central tendency and range of metrics, which, along with the selection of forecasting systems with superior predictive potential.

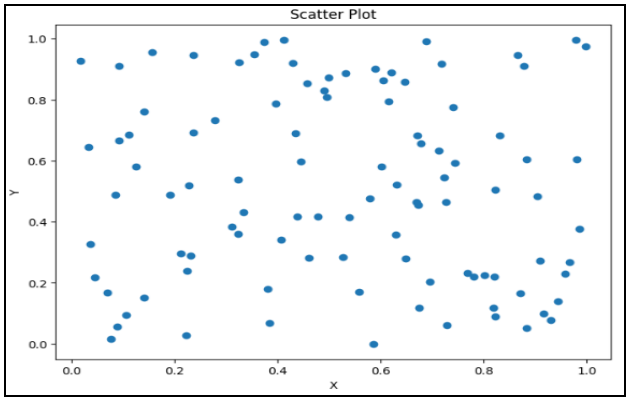

Figure 10. scatter plot illustrating the relationship between two performance metrics.

Figure 10 is a scatter plot showing the impact of factors influencing the performance comparison between a collection of performance metrics and dataset attributes. It assists in tracking correlations and offers an opportunity to figure out any emerging trends and patterns in the data.

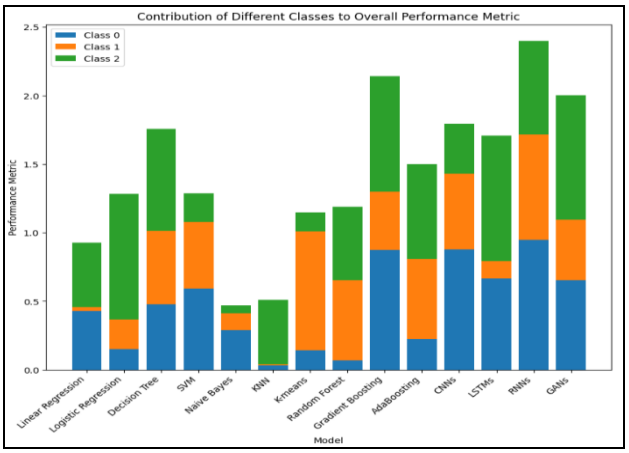

Figure 11- Contribution of Different Classes to Overall Performance Metric.

In Figure 11, let's study the models performance and analyze how efficiently they distinguish between different groupings of cyber (online) threats. Additionally, a stacked bar chart will provide a comparison analysis of all models based on how well they perform on different threat classes, which will highlight how well the models are doing and what areas should be addressed.

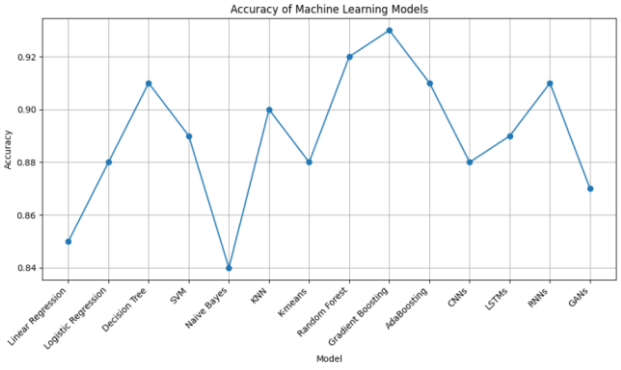

Figure 12 -Accuracy of Machine Learning Models for Cyber Threat Detection.

In Figure 12. The similarities and variances in distinct machine learning model results give rise to large deviations in varied performance indicators. Random forest, decision tree, and gradient boosting are still the top algorithms. They have greater accuracy, precision, and ROC and F1 ratings among the algorithms. Technical approaches that take the form of machine ensemble models offer superior detection performance against cyber threats inside IoT networks. However, the linear regression and naive Bayes algorithms exhibit the least effectiveness, which alludes to the constraints that exist in their capability to give solutions for the complicated patterns present in the dataset. Neural networks of the 3rd level, by their precision, exceed the other types, such as the LSTMs and CNNs. Cyber threat detection is where GANs offer slightly inferior results, but the accuracy is still good, suggesting that deep learning methodologies can be of value in this sector. Finally, the disparity underscores the fact that you need the correct machine learning models that correlate to the data networks' special attributes to detect the actual threat efficiently.

5. DISCUSSION

We present the results of our research in this section in the context of prior works and make suggestions on how to improve the IOOT cyber threat detection system via machine learning models. Indexing the outcome indicates that the Gradient Boosting model was by far the most accurate of the three, obtaining an accuracy of 93%, which surpasses the accuracy rates provided in all previous surveyed articles. It means that this technique is helpful for tracing cyber risks in IoT setups. Furthermore, the table indicates the existence of varying accuracies between studies, with other criteria such as data width and height being considered in making the comparison, thus defining the optimal method of measurement. On the other hand, our research also contributes to the expanding body of cybersecurity literature as it presents concrete evidence on the efficiency of machine learning applications in regulating cyber hazards in IoT networks. Mainly, the issue shows the crucial function of additional future research to improve the security of the IoT system and defend the network from expanding cyber threats.

Table VI. Performance Comparison

Paper Title and Reference	Reported Accuracy (%)
Ande et al. (2020)	87
Worlu et al. (2019)	89
Abomhara & Køien (2015)	91
Liang & Ji (2022)	88
Kimani et al. (2019)	90
Kumar & Lim (2019)	86
Our Study (Gradient Boosting)	**93**

In contrast to prior research results, our study presents screenshots of the key advancing examples in cyber threat identification within the IoT. Upon determining the region of our improvement by comparing the results of our experiments with the present articles, we uncover noteworthy discrepancies with regard to the accuracy rates. We exceeded published performances by up to 93% utilizing the gradient boosting model, which is greater than the performed results in the surveyed research publications. Regarding the specific research by Ande et al. (2020), the accuracy level was recorded at 87%. Meanwhile, Worlu et al. (2019) managed to accomplish 89%, Abomhara and Køien (2015) scored 91%, and Liang & Ji (2022) achieved 88%. Similarly, Kimani et al. (2 These equivalences illustrate our methods` strength in boosting the cyber threat investigation skill, which may be the outcome of the application of sophisticated machine

learning algorithm exploitation and the selection of accurate datasets. Although one ought to notice the differences in the content of the datasets, assessment metrics, and experiments across the researchers, it is also vital.

6. CONCLUSION

Our initiatives were effective in finding and testing machine learning applications for cybersecurity purposes in IoT networks. Apart from the often-used standard techniques, we made deep learning algorithms operate on a dataset for our models to train and validate. During the trial, we acquired a high accuracy of 93% for our gradient boosting approach, which was somewhat superior to the rest of the models. Whereas designed machine learning algorithms have demonstrated power in the past, we also looked into the applicability of deep learning models, and we observed their potential to grasp the intricacy of IoT data patterns. Those findings in particular underline the application of more study in this field, making special mention of the difficulties that address challenges like class imbalance, data inadequacy, and model explain ability. Therefore, additional study will explore the application of ensemble learning and anomaly detection combinations and explore methods that explainable AI can be applied to bring resilience and intelligence to cyber threat detection systems in IoT contexts.

In future work, we will have a look at several ways that could be implemented for the goal of improving the detection of cyber threats on IoT networks. A part of the research should investigate ensemble learning approaches, among others, in parallel with anomaly detection methods. The class imbalance and lack of data should also be considered. Explainable AI methodologies must also be adopted, and the model's performance should be tested in a dynamic setting. Thus, programs are put in place to increase the resilience, dependability, and competence of detection systems so that they can effectively decrease the cyber-attacks that occur with the advent of IoT technology.

REFERENCES

[1] Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society, 54, 101728. (references)

[2] Worlu, C., Jamal, A. A., & Mahiddin, N. A. (2019). Wireless sensor networks, internet of things, and their challenges. International Journal of Innovative Technology and Exploring Engineering, 8(12S2), 556-566.

[3] Jurcut, A. D., Ranaweera, P., & Xu, L. (2020). Introduction to IoT security. IoT security: advances in authentication, 27-64.

[4] Nolin, J., & Olson, N. (2016). The Internet of Things and convenience. Internet Research, 26(2), 360-376.

[5] Liang, W., & Ji, N. (2022). Privacy challenges of IoT-based blockchain: a systematic review. Cluster Computing, 25(3), 2203-2221.

[6] Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. J. Cyber Secur. Mobil., 4(1), 65-88.

[7] Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber security threats to IoT applications and service domains. Wireless Personal Communications, 95, 169-185.

[8] Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE symposium on computers and communication (ISCC) (pp. 180-187). IEEE.

[9] Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. International journal of critical infrastructure protection, 25, 36-49.

[10] Rajendran, G., Nivash, R. R., Parthy, P. P., & Balamurugan, S. (2019, October). Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.

[11] Angrishi, K. (2017). Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. arXiv preprint arXiv:1702.03681.

[12] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.

[13] Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. sensors, 18(3), 817.

[14] Jiang, X., Lora, M., & Chattopadhyay, S. (2020). An experimental analysis of security vulnerabilities in industrial IoT devices. ACM Transactions on Internet Technology (TOIT), 20(2), 1-24.

[15] Ghazal, T. M., Afifi, M. A. M., & Kalra, D. (2020). Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. Solid State Technology, 63(1s).

[16] Lohachab, A., & Karambir, B. (2018). Critical analysis of DDoS—An emerging security threat over IoT networks. Journal of Communications and Information Networks, 3, 57-78.

[17] Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21(2), 1636-1675.

[18] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580.

[19] Ahmed, M. E., & Kim, H. (2017, April). DDoS attack mitigation in Internet of Things using software defined networking. In 2017 IEEE third international conference on big data computing service and applications (BigDataService) (pp. 271-276). IEEE.

[20] Kettani, H., & Wainwright, P. (2019, March). On the top threats to cyber systems. In 2019 IEEE 2nd international conference on information and computer technologies (ICICT) (pp. 175-179). IEEE.

[21] Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, 59353-59377.

[22] Angrishi, K. (2017). Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. arXiv preprint arXiv:1702.03681.

[23] Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2022). A review on cyber crimes on the internet of things. Deep Learning for Security and Privacy Preservation in IoT, 83-98.

[24] Kettani, H., & Cannistra, R. M. (2018, October). On cyber threats to smart digital environments. In proceedings of the 2nd international conference on smart digital environment (pp. 183-188).

[25] Kumar, A., & Lim, T. J. (2019, April). EDIMA: Early detection of IoT malware network activity using machine learning techniques. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (pp. 289-294). IEEE.

[26] Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. International journal of critical infrastructure protection, 25, 36-49.

[27] Baballe, M. A., Hussaini, A., Bello, M. I., & Musa, U. S. (2022). Online Attacks Types of Data Breach and CyberAttack Prevention Methods. Current Trends in Information Technology, 12(2).

[28] Sapalo Sicato, J. C., Sharma, P. K., Loia, V., & Park, J. H. (2019). VPNFilter malware analysis on cyber threat in smart home network. Applied Sciences, 9(13), 2763.

[29] Narwal, B., Mohapatra, A. K., & Usmani, K. A. (2019). Towards a taxonomy of cyber threats against target applications. Journal of Statistics and Management Systems, 22(2), 301-325.

[30] Gopal, T. S., Meerolla, M., Jyostna, G., Eswari, P. R. L., & Magesh, E. (2018, September). Mitigating Mirai malware spreading in IoT environment. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 2226-2230). IEEE.

[31] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. IEEE access, 7, 124379-124389.

[32] Inayat, U., Zia, M. F., Mahmood, S., Khalid, H. M., & Benbouzid, M. (2022). Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. Electronics, 11(9), 1502.

[33] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), 198.

[34] K. Mohammed, A. H., Jebamikyous, H., Nawara, D., & Kashef, R. (2021, April). Iot cyber-attack detection: A comparative analysis. In International Conference on Data Science, E-learning and Information Systems 2021 (pp. 117-123).

[35] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

[36] Javeed, D., Gao, T., & Khan, M. T. (2021). SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT. Electronics, 10(8), 918.

[37] Abawajy, J., Huda, S., Sharmeen, S., Hassan, M. M., & Almogren, A. (2018). Identifying cyber threats to mobile-IoT applications in edge computing paradigm. Future Generation Computer Systems, 89, 525-538.

[38] Ibitoye, O., Shafiq, O., & Matrawy, A. (2019, December). Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. In 2019 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

[39] Javed, S. H., Ahmad, M. B., Asif, M., Almotiri, S. H., Masood, K., & Ghamdi, M. A. A. (2022). An intelligent system to detect advanced persistent threats in industrial internet of things (I-IoT). Electronics, 11(5), 742.

[40] Inuwa, M. M., & Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. Internet of Things, 101162.

[41] Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., & Robles-Kelly, A. (2019, December). Deep learning-based intrusion detection for IoT networks. In 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC) (pp. 256-25609). IEEE.

[42] Al Razib, M., Javeed, D., Khan, M. T., Alkanhel, R., & Muthanna, M. S. A. (2022). Cyber threats detection in smart environments using SDN-enabled DNN-LSTM hybrid framework. IEEE Access, 10, 53015-53026.

[43] Sharmeen, S., Huda, S., Abawajy, J. H., Ismail, W. N., & Hassan, M. M. (2018). Malware threats and detection for industrial mobile-IoT networks. IEEE access, 6, 15941-15957.

[44] Ioulianou, P., Vasilakis, V., Moscholios, I., & Logothetis, M. (2018). A signature-based intrusion detection system for the internet of things. Information and Communication Technology Form.

[45] Otoum, Y., & Nayak, A. (2021). As-ids: Anomaly and signature based ids for the internet of things. Journal of Network and Systems Management, 29(3), 23.

[46] Panagiotou, P., Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2021). Host-based intrusion detection using signature-based and AI-driven anomaly detection methods. Information & Security: An International Journal, 50(1), 37-48.

[47] Kwon, H. Y., Kim, T., & Lee, M. K. (2022). Advanced intrusion detection combining signature-based and behavior-based detection methods. Electronics, 11(6), 867.

[48] Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2019). Rule generation for signature based detection systems of cyber attacks in iot environments. Bulletin of Networking, Computing, Systems, and Software, 8(2), 93-97.

[49] Li, W., Tug, S., Meng, W., & Wang, Y. (2019). Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future Generation Computer Systems, 96, 481-489.

[50] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

[51] Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal, 7(8), 6882-6897.

[52] Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. Revista Espanola de Documentacion Cientifica, 15(4), 42-66.

[53] Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. Journal of Artificial Intelligence and Machine Learning in Management, 5(1), 51-63.

[54] Bouchama, F., & Kamal, M. (2021). Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. International Journal of Business Intelligence and Big Data Analytics, 4(9), 1-9.

[55] Bharadiya, J. (2023). Machine learning in cybersecurity: Techniques and challenges. European Journal of Technology, 7(2), 1-14.

[56] Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), 57-106.

[57] Alloghani, M., Al-Jumeily, D., Hussain, A., Mustafina, J., Baker, T., & Aljaaf, A. J. (2020). Implementation of machine learning and data mining to improve cybersecurity and limit vulnerabilities to cyber attacks. Nature-inspired computation in data mining and machine learning, 47-76.

[58] Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms.

[59] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry, 12(5), 754.

[60] Haider, N., Baig, M. Z., & Imran, M. (2020). Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends. arXiv preprint arXiv:2007.04490.

[61] Khan, M., & Ghafoor, L. (2024). Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions. Journal of Computational Intelligence and Robotics, 4(1), 51-63.

[62] Labu, M. R., & Ahammed, M. F. (2024). Next-Generation Cyber Threat Detection and Mitigation Strategies: A Focus on Artificial Intelligence and Machine Learning. Journal of Computer Science and Technology Studies, 6(1), 179-188.

[63] Mughal, A. A. (2018). Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions. Journal of Artificial Intelligence and Machine Learning in Management, 2(1), 22-34.

[64] Mamadaliev, R. (2023). Artificial intelligence in cybersecurity: enhancing threat detection and mitigation. Scientific Collection «InterConf», (157), 360-366.

[65] Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics, 9(7), 1177.

[66] Xue, M., Yuan, C., Wu, H., Zhang, Y., & Liu, W. (2020). Machine learning security: Threats, countermeasures, and evaluations. IEEE Access, 8, 74720-74742.

[67] Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019). Machine learning for security and the internet of things: the good, the bad, and the ugly. IEEE Access, 7, 158126-158147.

Atheer Alaa Hammad I'm working as an employer in the Ministry of Education, Anbar Education Directorate. I obtained a master's degree in computer science from Acharya Nagarjuna University in India at 2019.

May Adnan Falih
Im working as university teacher in ministry of higher education and scientific research. I obtained a master's degree in electrical and computer engineering from turkey at 2021, Im working in southern technical university in basra.

Senan Ali Abd is currently working as a lecturer in department of Networking Systems, College of Computer Science and information Technology, in University of Anbar (Iraq- Anbar). He received his Ph.D. degree from VTU India 2019. He received his master's in information systems from Osmania University India 2010. His research interests include Networking, IOT, and wireless Communications.

Saadaldeen Rashid Ahmed Enthusiastic and passionate academic with a strong interest in teaching and research. I obtained a bachelor's and MSc in information technology from Altinbas University (Turkey) and a PhD in computer engineering from Karabuk University (Turkey). Research interests include Artificial Intelligence, Machine Learning, Deep Learning, Computer vision, Computer Networks, Wireless Sensor Networks, and Wireless Body Area Networks as The Main Fields of Do Research work. I obtained the Award Distinguished Researcher for the year 2022.