International Journal of Computing and Digital Systems
2025, VOL. 17, NO. 1, 1–25

http://dx.doi.org/10.12785/ijcds/1571020041

Detecting Cyber Threats in IoT Networks: A Machine Learning Approach

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

[1]*Ministry of Education Anbar, Education Directorate, Alnbar, Iraq*
[2]*2Electronic 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. Computer Science Department, Bayan University, Erbil, Kurdistan, Iraq,*

Received 16 April 2024, Revised 13 July 2024, Accepted 23 August 2024

Abstract: In response to the growing cybersecurity concerns in Internet of Things (IoT) networks, our study tackles the vital need for stronger data security measures. By offering a unique technique that integrates machine learning and neural network algorithms, we address current gaps in cybersecurity for real-world IoT installations. Our solution combines a mix of gradient boosting, convolutional neural networks (CNNs), long short-term memory networks (LSTMs), and recurrent neural networks (RNNs) trained on massive IoT datasets to identify and categorize network traffic patterns suggestive of possible cyber hazards. Performance assessment based on common measures like accuracy, precision, recall, and F1-score reveals the usefulness of our technique, reaching a stunning accuracy rate of 93% with gradient boosting. Our work underlines the growth of machine learning and deep learning approaches in enhancing cybersecurity inside IoT settings, acting as a basic step for future improved studies in this sector.

Keywords: Internet of Things , Cybersecurity,Machine Learning, Neural Networks, Network Security

1. INTRODUCTION

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[7]. 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[9].

Poor device installations, lack of encryption, and clever, inadequate authentication mechanisms make IoT networks vulnerable [10]. In addition, the IoT invasion's 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[12].

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, real-time machine learning logic can recognise aberrant behaviour, malicious efforts, and adapt to new attacks[15].

Later considerations include IoT networks' role as change agent models in technology innovation and the challenge of widespread adoption. Effective cybersecurity

E-mail address: atheer.alaa@ec.edu.iq1, mayf992002@gmail.com2, senan.ali@uoanbar.edu.iq3, saadaldeen.aljanabi@bnu.edu.iq4

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[1]. 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[2]. 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. *Objectives*

Primary Objective: To develop a real-time IoT threat detection framework based on advanced machine learning models.
Secondary Objectives:

- Identification of Cyber Threats: Conduct a comprehensive examination of existing and emerging IoT cybersecurity threats.
- Data Collection and Preprocessing: Gather and preprocess an extensive dataset from IoT traffic logs, device telemetry, and other relevant sources.
- Feature Engineering: Extract and select significant features through techniques such as packet analysis, protocol inspection, and anomaly detection.
- Machine Learning Model Development: Develop and evaluate various machine learning models (supervised, unsupervised, and semi-supervised) for optimal threat detection.
- Model Training and Evaluation: Train models using the preprocessed dataset and evaluate performance using metrics like efficiency, accuracy, recall, and F1-score.
- Optimization and Fine-tuning: Optimize model parameters and explore ensemble learning techniques for improved detection accuracy and stability.
- Integration and Deployment: Implement the trained models into an operational IoT framework to detect and isolate cyber threats in real-time.
- Validation and Testing: Validate the machine learning approach through real-world IoT scenarios, collaborating with technical experts and cybersecurity specialists for continuous improvement.

D. *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.

E. *Contribution*

This is a complete overview of the contributions made by this publication. Initially, it provides a description of many current risks to the security of the Internet of Things (IoT) and defines the most prevalent and dangerous types of assaults. Additionally, it entails developing and fine-tuning novel and sophisticated machine learning algorithms for detecting threats while also showcasing the feasibility of using machine learning for securing IoT devices. Ultimately, the study demonstrates the seamless incorporation of these models into IoT networks to showcase the immediate and practical use of the suggested models in identifying and mitigating cyber risks. In the next section, we review related work on IoT cybersecurity and machine learning techniques.

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 cybersecurity 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, Hammad [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[25]. EDIMA is suggested to prevent IoT malware from the start[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 multi-faceted nature of cyber threats in IoT networks, emphasising the need for robust security solutions to safeguard them. Literature reveals many cyber risks affect IoT networks via multiple vulnerabilities and attack vectors. Research highlights the growing complexity of cyber threats targeting the Internet of Things (IoT), underscoring the need for thorough security measures[11],[24].

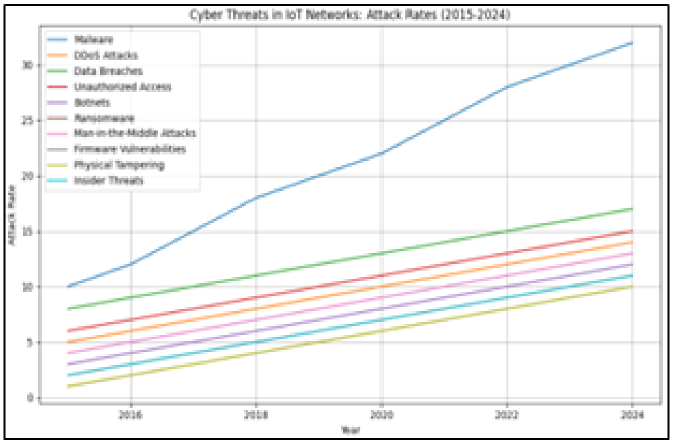


Figure 1. Cyber Threats in IoT Networks: Attack Rates (2015-2024).

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. 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. 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[30]. 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 cyber-attacks 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[33].

The field of IoT security is in a constant state of development and adaptation in response to a range of challenges. Conventional detection approaches, such as signature-based and anomaly-based detection, have significant limitations in dealing with the ever-changing and complex threats in IoT networks[34]. Contemporary detection techniques that prioritize machine learning (ML) and artificial intelligence (AI) are becoming more important. Research has proved ML's usefulness in identifying and reacting to IoT cyber threats by exploiting pattern recognition skills [35]. Another major innovation is SDN-enabled hybrid DL frameworks for threat detection in IoT, which may considerably increase the adaptability and robustness of security systems [36].

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 [37]. 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.

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[45].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[46]. 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[47].

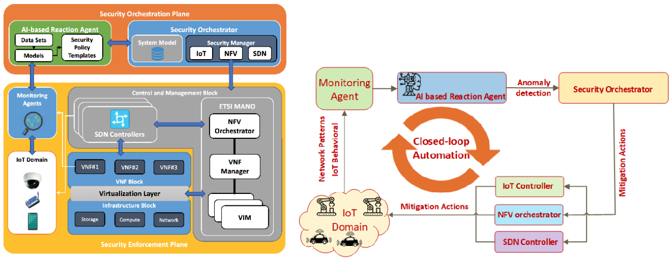
C. Machine Learning in Cybersecurity

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[48]. Numerous studies have been undertaken since the advent of ML in cybersecurity, showing a range of methodologies, benefits, and problems linked with the practice[49]. Eskandari and his colleagues are the designers of an intelligent intrusion detection system designed to find anomalies [50]for edge IoT devices by

TABLE I. LITERATURE REVIEW TABLE

Author	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

applying machine learning techniques, which can be pointed out as one technology in IoT security improvementc. [51] 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[55]. 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[61]. The combination of Khan and Ghafoor expresses their opinions on the topical areas of network security that can create obstacles and presents countermeasuresfor adversarial assaults as well[62]. Labu and Ahammed aspire to develop future cyber defense deployments that take advantage of AI and ML technology as shown in Figure 2



(a) General Architecture of the Framework

(b) Closed-loop Automation: From Detection to Mitigation

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.

The incorporation of ML and neural networks into IoT security frameworks has demonstrated promising outcomes. Recent research has studied different ML algorithms and neural architectures to boost detection skills. Deep learning techniques such as CNNs and RNNs have been proven useful in finding complicated patterns within network traffic, providing better intrusion detection rates compared to older approaches [41] [68]. Additionally, an SDN-enabled DNN-LSTM hybrid framework has demonstrated improved performance in dynamic and heterogeneous IoT contexts by using the characteristics of distinct neural network architectures to increase detection efficiency and accuracy [42], [69]. AI-driven behavioral modeling of network traffic may proactively detect possible risks via continuous learning and adaptation, greatly lowering false positives compared to traditional models [54, [70]]. Anomaly-based intrusion detection systems for IoT edge devices leverage ML approaches to identify abnormalities at the edge, offering real-time security and lowering latency in threat response [51]. Furthermore, AI and ML play a vital role in boosting 5G network security, addressing particular difficulties given by the integration of IoT devices in 5G networks [60].

D. Recent Works

Several new studies expand this literature analysis by addressing advancements in IoT network security and the application of machine learning and neural networks in this sector. Other tactics utilized in clustering, which incorporates ensemble learning methods into IoT security, boost the overall F detection rate as well as the model's resilience [68]. A truly distributed federated learning system for IoT works to ensure privacy while at the same time delivering high detection accuracy [70], [32]. GNNs for IoT anomaly detection are advantageous for enhanced IoT detection accuracy since networks rely on relational data structures[33]. Policies based on reinforcement learning are applied to IoT networks and adapt security patterns depending on threats [70]. Transfer learning increases the IoT devices' detection capacities of RCs because of the methods' cross-domain threat detection efficacy [68]. Inherent in most blockchain-based systems for safeguarding IoT data is the combination of ML for ongoing monitoring and threat analysis[33]. Simple and small-scale neural networks as a security model for IoT are developed for great efficiency at the expense of tolerable computational demand [69]. A section of hybrid anomaly detection systems that employ neural networks exhibit great accuracy; namely, probable false positives amount to 0.3% in IoT networks [68]. Adversarial training techniques increase the resilience of the neural network model in the IoT environment because it is set to deal with diverse adversarial assaults[33]. Incorporating quantum computing into the current literature on IoT security suggests probable trends in the future progress of ML based solutions [32]. Machine learning for cybersecurity: It was demonstrated that various algorithms gave excellent results for threat identification in the actual environment [52]. Literature assessments on methodologies and case studies on machine learning and big data analytical approaches to security threat detection are useful in comprehending the broad viewpoint. One element where ML proved highly beneficial is studying network traffic patterns to simulate human behavior and therefore design better systems to identify cyber threats [54]. The review offers instructive overviews and the option of future paths for learning-based approaches in the IoT systems' cyber assault detection[71]. Large systematic evaluations of state-of-the art ML solutions for cybersecurity explain the landscape in their broad classification [56]. This research adds to the field by presenting and testing a novel technique consisting of gradient boosting, a convolutional neural network, long short-term memory, and a recurrent neural network for identifying threats in IoT networks. In contrast, our strategy is targeted at uncovering a synergistic usage of various ML algorithms and neural networks to produce a detection accuracy of 93% that exceeds the results reached in past research and develop a more competent and effective solution for true IoT scenarios.

Analyzing the literature discloses that a key difficulty in IoT networks pertains to security, whereby machine learning delivers the crucial boost. This literature review is focused on the study of numerous studies carried out over the last three years, outlining the key results, benefits, and limits of each work combined with a comparison of our work.

Inayat et al. [72] have also provided an extended study article on the use of learning-based methodologies for the analysis of cyber attacks in IoT systems. The writers concentrated on the existing trend of the approach and its growth potential; the most crucial component identified was the demand for real-time monitoring. Thus, our investigations expand this line of study by providing complicated machine learning methods concentrating on real-time IoT threat detection tasks.

Haji and Ameen[73]examined the attack and anomaly detection in the IoT networks with the assistance of machine learning techniques. They also highlighted several methodologies; however, the study was inadequate in terms of providing the newest deep learning breakthroughs. The study solves the gap by adding newer deep learning models to the IoT security architecture.

Panda et al.[74]developed feature engineering and a machine learning model for IoT-botnet cyber threat detection. They particularly paid attention to the areas of features and models to increase the success rate of detecting procedures. This study improves on theirs by integrating new characteristics and considering how increased learning techniques might further boost the model.

Several researchers, including Abdullahi et al.[75], offered a thorough literature analysis on the use of artificial intelligence technologies to identify cybersecurity assaults in IoT settings. They discussed the potential and threats that are associated with various AI technologies. Their research is supplemented by our effort, as we provide real-world application and testing of AI-based threat detection models for the IoT networks.

Saba et al. [76] introduced an anomaly-based IDS for the IoT network and constructed a deep learning model. What their technique proved was the capacity of deep learning to spot aberrant patterns. From the study, we advance a step further to examine different deep learning structures and increase their features to fit diverse IoT applications.

Ahmad and Alsmadi [77] reviewed machine learning solutions to IoT security with the goal of explaining the current research gaps. The demand for fundamental, better, and optimal solutions was also expressed for harsher and bigger applications. To solve these gaps, our work focuses on the design of large-scale machine learning algorithms and subsequent empirical assessment.

Anwer et al. [78] detailed the specifics of attack detection in IoT using machine learning to call attention to the model's training and evaluation components. This study expands their research by incorporating complicated model selection and comparing and assessing models using crucial performance indicators.

Ferrag et al. [79] advocated federated deep learning in cybersecurity with respect to the IoT. They illustrated how federated learning may increase privacy and security and what sorts of issues are indicative of this method. This is distinct from their work, as we identify centralized deep learning and compare it with partially decentralized deep learning.

Ullah and Mahmoud [80] suggested an IoT network anomaly detection methodology utilizing deep learning. In their study, they concentrated on the process of feature engineering as being crucial for a successful model. This is done in our attempt to identify which of the advanced feature extraction strategies is more effective for performance enhancement.

To build and construct a safe monitoring system for computer numerical control devices utilizing deep learning and IoT against cyber-attacks, Tran et al.[81] proposed a dependable solution. They empirically supported their approach. Similarly, the proposed research strategy incorporates validation processes to allow the actual usage of the presented models in diverse IoT situations.

Specifically, considering the identification of botnets in IoT, Pokhrel et. al. [82] applied machine learning. K: They were working on determining traffic features that would indicate a botnet as the source. Thus, the work of earlier writers continues our research by developing multi-faceted detection algorithms that may identify additional cyber risks.

Tsimenidis et al. [83] examined deep learning algorithms for IoT based intrusion detection, concentrating on the pros and demerits of the various models. These efforts are integrated into our research; this compares and adjusts several deep learning architectures for IoT security utilization.

The deep learning approaches utilized in IoT network intrusion detection models are as follows: With reference to the research done by Madhu et al.[84] . The actions that they took demonstrated that the detection rate of the software that they had designed was quite high. Our work is built on their research by expanding the application of the methodologies to a real-time environment and analyzing the models in genuine IoT situations.

Saheed and Arowolo[85] give attention to the identification of cyber assaults on Internet of Medical Things devices using deep recurrent neural networks and machine learning methods. It emphasized the potential of recurrent models. Ours may be considered analogous to theirs since it both employs recurrent and convolutional neural network models and compares their performance.

Kumar et al.[86] suggested an intelligent cyber attack detection system for IoT networks using a hybrid feature reduction method. Their method resulted in large gains in the observations' accuracy. Ensemble learning approaches have not been investigated in this context, and some extra characteristics have also been introduced in our study.

Machine learning based intrusion detection was put forth by Islam et al.[87] in the IoT networks. They examined several algorithms, indicating that the algorithms functioned. Nonetheless, our study expands their work further by providing new and complicated deep learning models and testing them on numerous IoT applications.

Awajan[88] presented a DL based IDS for IoT networks, which is characterized as follows: Its system performed considerably better: they tested their system, and it showed a solid prospect: they tested their system with strong possibilities of progress. This effort is comparable to ours, but the collection of models spans a larger variety of machine learning approaches, and their performance is being studied more.

Ahmad et al.[89] have also highlighted that machine learning and specifically deep learning have lately been employed for network intrusion detection. They state the issues and offer approaches to their remedy. Our study answers these issues by developing and assessing effective models for threat detection in real time.

Sharma and Agrawal[90] discussed network intrusion detection for IoT assaults by using an anomaly-based technique with deep learning. It was establishing great accuracy in the detection. Different from earlier work, for practical usage, this article concentrates on comparing the diverse deep learning architectures and boosting their performances.

Sarhan et al.[91]devoted significant attention to feature extraction for machine learning based on intrusion detection in the IoT networks. They concentrated on the feature selection aspect. Their work is complimented by our study in the sense that we look at higher-level feature engineering approaches and their impacts.

Dina and Manivannan [92] offered an overview of machine learning based architectures for intrusion detection in computer networks. Regarding this, they brought out the fundamental prerequisites of excellent feature extraction processes. The prior work is expanded in our research by creating new feature extraction approaches more applicable to IoT networks.

I assigned higher emphasis to the academic publications since they are more peer reviewed than the other sources. Khan et al. [93] have developed a deep learning based technique for intrusion detection and security in the IoT. From these, tactics and challenges were highlighted, and suggestions were made as well. Our study addresses these difficulties by building enhanced deep learning architectures and their tests in diverse IoT situations.

In [94], Javeed et al. introduced a novel SDN-based hybrid deep learning technique for the identification of new and evolving cyber risks in IoT. They explained how hybrid models may operate effectively. We separate our work from theirs in a way that directly compares our centralized deep learning models to theirs.

In their paper, Wazid et al.[95] presented the benefits, problems, and research possibilities of combining cybersecurity with machine learning. Accordingly, their evaluation condemned the field's present condition and referred to the ability of machine learning to generate answers to the increasing challenge of IoT security. This research expands their work by proposing and analyzing novel real-time threat detection methods utilizing machine learning for the IoT network.

Analyzing current IoT literature, this study focuses on the newest advancements in IoT cybersecurity based on machine learning and deep learning approaches. Thus, the new study further develops the preceding work as follows: Several limitations of the earlier work are highlighted, and new methods for real-time IoT threat detection are presented, leveraging the recognized improvements over prior work.

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.

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,

Study	Strengths	Weaknesses	Our Approach
Inayat et al. [72]	Comprehensive survey of learning-based methods for IoT security	Lacked real-time detection capabilities	Develops real-time machine learning models
Haji and Ameen [73]	Reviewed various attack and anomaly detection methods	Limited focus on recent deep learning advancements	Integrates advanced deep learning models
Panda et al. [74]	Efficient feature engineering and model optimization	Narrow focus on IoT-botnet attacks	Explores additional features and ensemble learning techniques
Abdullahi et al. [75]	Systematic literature review of AI methods in IoT security	General overview without practical validation	Provides practical implementation and validation
Saba et al. [76]	Effective anomaly-based intrusion detection using deep learning	Limited comparison of different deep learning architectures	Compares and optimizes deep learning architectures
Ahmad and Alsmadi [77]	Identified gaps in current literature	Called for more robust and scalable solutions	Develops scalable machine learning models
Anwer et al. [78]	Highlighted importance of model training and evaluation	Limited model optimization techniques	Incorporates advanced model optimization
Ferrag et al. [79]	Explored federated deep learning for enhanced privacy	Focused on federated learning	Provides comparative analysis of centralized deep learning models
Ullah and Mahmoud [80]	Designed deep learning-based anomaly detection model	Limited feature extraction techniques	Employs advanced feature extraction techniques
Tran et al. [81]	Reliable deep learning and IoT-based monitoring system	Specific focus on computer numerical control machines	Validates models in diverse IoT environments
Pokhrel et al. [82]	Investigated botnet detection using machine learning	Focused on specific attack type	Develops multi-faceted detection models
Tsimenidis et al. [83]	Reviewed deep learning techniques for IoT intrusion detection	General review without practical implementation	Integrates insights into practical model optimization
Madhu et al. [84]	High detection accuracy of deep learning approaches	Lacked real-time implementation	Incorporates real-time detection capabilities
Saheed and Arowolo [85]	Cyber attack detection using deep recurrent neural networks	Focused on Internet of Medical Things	Extends comparison to additional deep learning models
Kumar et al. [86]	Hybrid feature reduction approach for cyber attack detection	Limited features and ensemble techniques	Explores additional features and ensemble learning techniques
Islam et al. [87]	Machine learning-based intrusion detection in IoT networks	Limited algorithm comparison	Develops and validates advanced deep learning models

Awajan [88]	Novel deep learning-based intrusion detection system	Limited model comparison	Compares a broader range of machine learning models
Ahmad et al. [89]	Systematic study of machine learning for intrusion detection	Identified challenges without practical solutions	Addresses challenges with optimized models
Sharma et al. [90]	High detection accuracy using deep learning technique	Limited architecture comparison	Compares and optimizes different deep learning architectures
Sarhan et al. [91]	Important feature extraction for IoT intrusion detection	Limited feature engineering techniques	Explores advanced feature engineering techniques
Dina and Manivannan [92]	Reviewed machine learning techniques for intrusion detection	Limited focus on IoT-specific challenges	Develops techniques tailored for IoT networks
Khan et al. [93]	Current analysis of deep learning for IoT security	Focused on challenges	Develops optimized models and validates them
Javeed et al. [94]	SDN-enabled hybrid deep learning framework	Focused on hybrid models	Provides comparative analysis of centralized deeplearning models
Wazid et al. [95]	Advantages, challenges, and future directions of machine learning	General review without practical validation	Develops and validates real-time machine learning models

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.

B. Data Preprocessing

Data pre-processing is the most crucial stage, or phase, and the initial stage in constructing the model. This procedure involves a number of nested processes so as to improve the data and make it suitable for preprocessing or feeding into the machine learning algorithm. First, preparation is done, which deals with record deletion, which entails the removal of redundant records as well as handling the problem of missing data by either imputing the missing values or ignoring the records, depending on the significance of the records to the analysis. After data cleaning is done, feature scaling comes in as the process of changing data to a standard range for more effective processing. This is critical for shipping algorithms or those that involve gradient boosting, neural networks, etc. Furthermore, categorical variables are changed to a shape that may be utilized for empirical modeling by applying the method of one-hot encoding. Last but not least, feature extraction approaches like the basic PCA are used to decrease the number of features or variables in the model and, additionally, keep as much variability as feasible. This assists in conserving calculation time and memory and avoids any probable incidence of the curse of dimensionality.

- Remove any irrelevant or duplicate records.
- Handle missing values by using techniques such as imputation or deletion, depending on the context and significance of the missing data.
- Normalize the data to bring all features onto a similar scale, which is crucial for algorithms like gradient boosting and neural networks.
- Encode categorical variables using techniques such as one-hot encoding to convert them into a format that can be provided to the ML models.
- Apply techniques like Principal Component Analysis (PCA) to reduce the number of features while retaining as much variability in the data as possible. This helps in minimizing computational overhead and avoiding the curse of dimensionality.

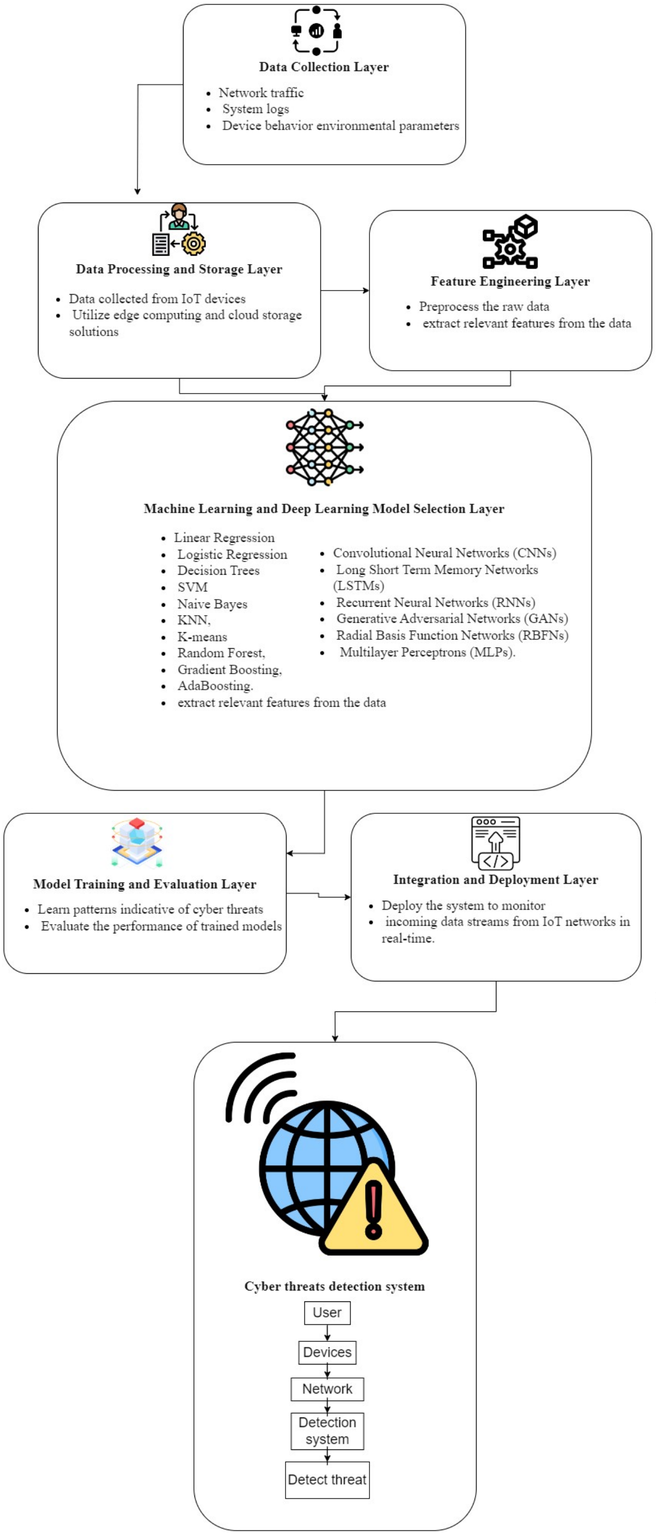

Data Collection Layer
Network traffic
System logs
Device behavior environmental parameters
Data Processing and Storage Layer
Data collected from IoT devices
Utilize edge computing and cloud storage solutions
Feature Engineering Layer
Preprocess the raw data
extract relevant features from the data
Machine Learning and Deep Learning Model Selection Layer
Linear Regression
Logistic Regression
Decision Trees
SVM
Naive Bayes
KNN,
K-means
Random Forest,
Gradient Boosting,
AdaBoosting.
extract relevant features from the data
Convolutional Neural Networks (CNNs)
Long Short Term Memory Networks (LSTMs)
Recurrent Neural Networks (RNNs)
Generative Adversarial Networks (GANs)
Radial Basis Function Networks (RBFNs)
Multilayer Perceptrons (MLPs).
Model Training and Evaluation Layer
Learn patterns indicative of cyber threats
Evaluate the performance of trained models
Integration and Deployment Layer
Deploy the system to monitor
incoming data streams from IoT networks in real-time.
Cyber threats detection system
User
Devices
Network
Detection system
Detect threat

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

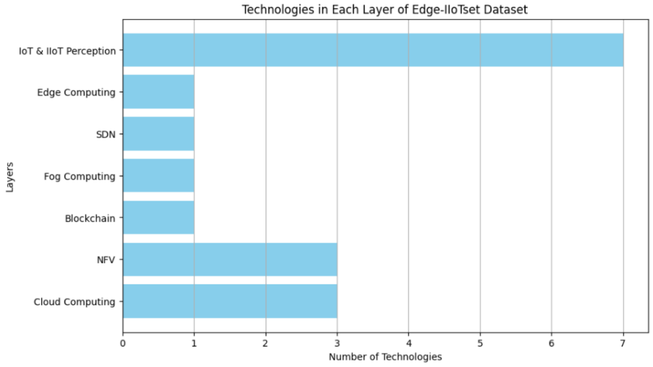


Figure 4. Overview of Edge-IIoTset [69],

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

3) *Feature Extraction*

Since feature selection aims for the selection of all useful features with the required computations, feature extraction is a process that focuses on selecting and transforming the most appropriate features from the given dataset with the intention of helping in the detection of cyber threats. The first of them is the selection of features; in this step, EDA is undertaken in an attempt to discover which traits have significant influence on forecasting cyber risks. Domain knowledge is also applied to obviate aspects like the traffic flow of the network, the behavioral data of the device, and logs emanating from the system. Following the identification of the important characteristics, they undergo data preprocessing, which includes packet analysis, protocol interrogation, and the use of anomaly detection to acquire new features out of the raw data that was picked. Furthermore, polynomial transformations or employing composite features enhance the model as features are generated from linear combinations of other characteristics, which also raises the model's complexity.

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*

During the model training phase, multiple models such as gradient boosting, convolutional neural networks (CNNs), long short term memory (LSTMs), and recurrent neural networks (RNNs) are chosen, with each model picked based on its usefulness in recognizing cyber threats. Gradient boosting is selected owing to its capacity to operate well with the tabular forms of data and be able to integrate multiple weak base learners in the form of several boosting iterations to build a single strong learner. Gradient boosting starts the model with an initial model, frequently an initial decision tree, and progressively adds further models, although with the purpose of improving the prior models on the residual indication. The last layer is utilized to aggregate all these models to create the final forecast.

Convolutional Neural Networks (CNNs) are picked for their power to discover spatial hierarchies and characteristics in network data in picture or sequence format. CNNs are constructed by numerous convolution layers, ideally followed by pooling layers that aim at dimensionality reduction. Batch normalization is utilized, and an activation function such as ReLU is used to induce non-linearity in the layers. Other layers of the neural network are applied to flatten the output and feed it through a couple of fully connected layers to reach the final classification result. At the same time, it is important to describe temporal relationships in the sequential data used for evaluating the network traffic, and Long Short-Term Memory Networks (LSTMs) are employed for this purpose. LSTMs have the following four steps: providing an input sequence to LSTM cells; managing the cell state with the assistance of the input and output gates; and producing a sequence that is capable of recognizing temporal patterns.

Recurrent Neural Networks (RNNs), selected for their capacity to handle sequential data, maintain learned hidden states from the previous time steps, and output them while processing the next input sequence, The RNN implementation comprises delivering sequence values to RNN layers, maintaining the state while conducting subsequent operations, and producing predictions based on the sequence data processed.

Recurrent Neural Networks (RNNs), selected for their capacity to handle sequential data, maintain learned hidden states from the previous time steps, and output them while processing the next input sequence, The RNN implementation comprises delivering sequence values to RNN layers, maintaining the state while conducting subsequent operations, and producing predictions based on the sequence data processed. 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 classifi-

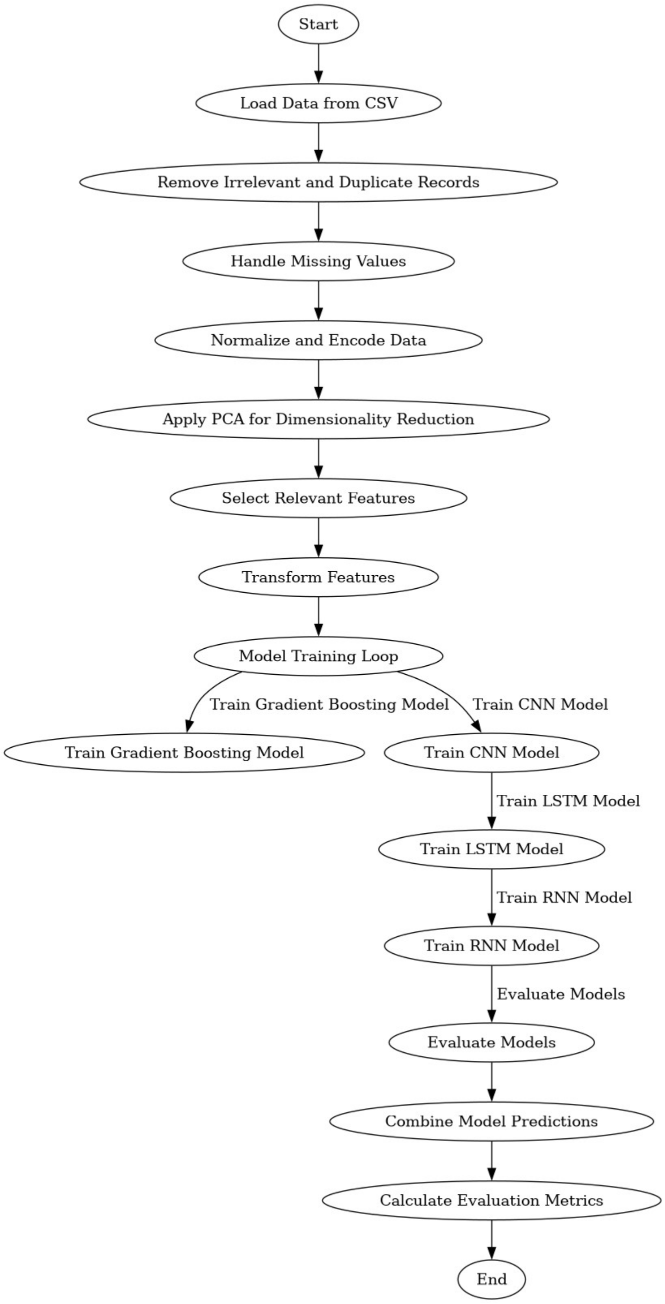


Figure 5. Model Full process flowchart

cation 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.

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	
Epochs	50, 100, 200

TABLE II. HYPERPARAMETERS AND CONFIGURATIONS FOR MODEL TRAINING

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.

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. 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

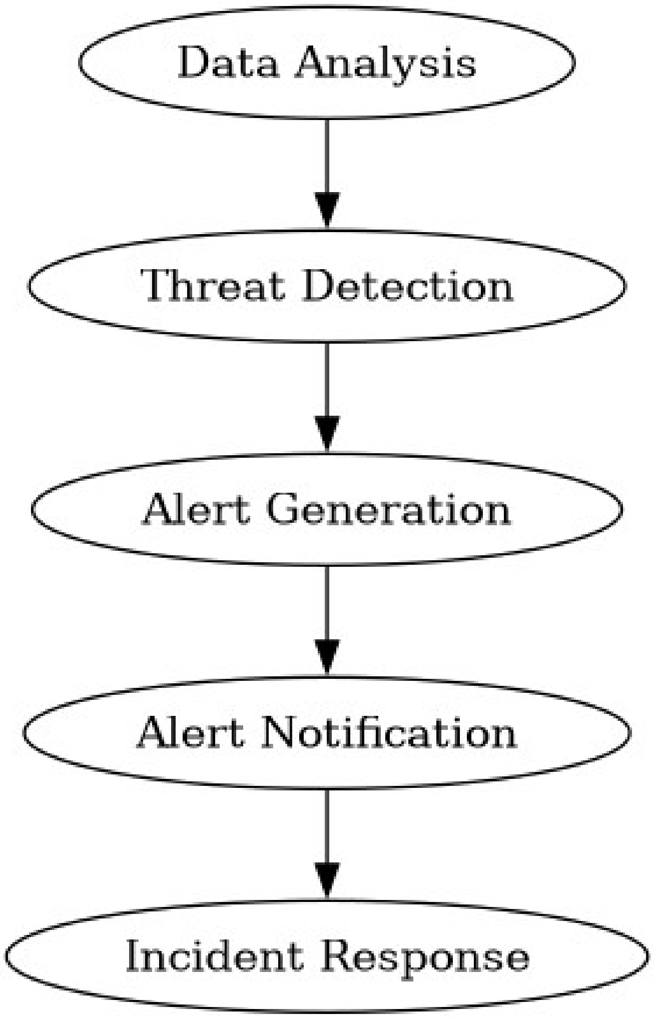


Figure 6. Alert generation and response

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. Rationale for Model Selection and Complementation

- Gradient Boosting: Selected for its ability to handle tabular data efficiently by combining weak learners into a strong learner, improving prediction iteratively.
- CNNs: Chosen for their excellence in detecting spatial hierarchies and patterns within network data represented as images or sequences.
- LSTMs: Ideal for capturing temporal dependencies in sequential data, crucial for time-series analysis of network traffic.
- RNNs: Complement LSTMs in modeling sequential data by maintaining hidden states that update with each time step, capturing patterns in longer sequences.

G. Integration and Complementation

The gradient boosting model handles high-dimensional tabular data and provides a strong baseline. CNNs focus on extracting complex spatial features from network traffic patterns. LSTMs capture long-term dependencies and temporal patterns in sequential data. RNNs support LSTMs by modeling sequence data and maintaining temporal context

H. 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 performance of the trained models is then exposed to a range of tests based on the issue type, and the metrics of accuracy, precision, recall, and F1-measure are used to quantify the robustness and generality of the answers. In addition to this, cross-validation is used to verify models further, where the data set is divided into die folds (with k = 5), and training and validation are done in turns to the folds. The metrics calculation contains accuracy, which is an indicator of correct instances to total instances; precision, which is the proportion of actual positive instances predicted out of the total positive instances; recall, which is the proportion of actual positives predicted out of all actual positive and negative instances; and F1-score, which is the mean of precision and recall calculated by giving more weight to both metrics. 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. EXPERIMENTAL SETUP AND DATA

A. Datasets

The first data set we have employed for our studies is known as the Edge-IIoTset, which is appropriate for IoT applications as well as industrial IoT (IIoT) applications. This dataset comprises multiple data points acquired from different IoT devices, such as humidity, temperature sensors, ultrasonic sensors, water level sensors, PH sensors, moisture sensors, heartbeat sensors, and flame detection sensors. Furthermore, the offered dataset comprises multiple kinds of cyber threats connected to the IoT networks: DoS/DDoS attacks, information gathering attacks, man-in-the-middle assaults, injection attacks, and malware attacks. By incorporating a wide variety of information into a single dataset, the performance of algorithms in spotting different sorts of cyber risks may be accurately assessed.

B. Hardware and Software Environments

The experiments were conducted in a controlled environment using high-performance computational resources to handle the complexity and scale of the data. The hardware setup includes:

- Processor: Intel Xeon E5-2680 v4 (2.40 GHz, 35 MB cache)
- Memory: 256 GB RAM
- Storage: 2 TB SSD
- GPU: NVIDIA Tesla V100 (32 GB)

The software environment comprises:

- Operating System: Ubuntu 20.04 LTS
- Programming Language: Python 3.8
- Libraries and Frameworks: Scikit-Learn, TensorFlow, Keras, Pandas, NumPy, Matplotlib, Graphviz (for flowchart visualization)

C. Parameter Settings for Each Algorithm

The parameter settings for each algorithm were optimized using cross-validation and grid search techniques to ensure the best performance

1) Gradient Boosting

- Number of Trees: 100
- Learning Rate: 0.1
- Maximum Depth: 3
- Subsample: 0.8
- Min Samples Split: 2

2) Convolutional Neural Networks (CNNs)

- Number of Convolutional Layers: 3
- Filter Size: 64, 128, 256 (for each subsequent layer)
- Kernel Size: (3, 3)
- Activation Function: ReLU
- Pool Size: (2, 2)
- Dense Layers: 2 (128 units, 64 units)
- Dropout Rate: 0.5
- Optimizer: Adam
- Learning Rate: 0.001
- Batch Size: 32
- Epochs: 50

3) Long Short-Term Memory Networks (LSTMs)

- Number of LSTM Layers: 2
- Units per Layer: 50
- Dropout Rate: 0.2
- Activation Function: Sigmoid
- Optimizer: Adam
- Learning Rate: 0.001
- Batch Size: 32
- Epochs: 50

4) Recurrent Neural Networks (RNNs)

- Number of RNN Layers: 2
- Units per Layer: 50
- Dropout Rate: 0.2
- Activation Function: Tanh

- Optimizer: RMSprop
- Learning Rate: 0.001
- Batch Size: 32
- Epochs: 50

D. Test Data Selection Criteria

The test data was selected from the Edge-IIoTset dataset based on several criteria to ensure it accurately represents real-world IoT network scenarios:

1) ***Diversity of Devices:*** *The dataset includes a wide range of IoT devices, ensuring that the models are exposed to a variety of data types and potential cyber threats*
2) ***Variety of Attacks:*** *The dataset encompasses multiple cyber-attack types, including DoS/DDoS, information collection, man-in-the-middle, injection, and malware attacks, reflecting a realistic threat landscape.*
3) ***Temporal Distribution:*** *Data was selected to cover different times of the day and various operational states of the devices, ensuring that the models can handle temporal variations and detect anomalies in different contexts.*
4) ***Balanced Attack and Normal Traffic:*** *The dataset includes both normal and attack traffic in a balanced manner, enabling the models to learn to differentiate between benign and malicious behaviors effectively.*
5) ***Realistic Operating Conditions:*** *The data captures IoT devices operating under typical conditions, including normal fluctuations, network disruptions, and varying load levels, ensuring that the evaluation results are applicable to real-world scenarios.*

5. EXPERIMENTAL SETTINGS

Our experiments were conducted in a high- The trials were done in a high-performance computer environment since the IoT data collected was large-scale and complicated. The number of GPUs in the hardware is one with the NVIDIA Tesla V100 model and 32 B of memory. The machine also features an Intel Xeon E5-2680 v4 CPU and 256 B of RAM. This layout makes it simpler in processing and even in the calculation to train or verify the models using machine learning. The software environment consists of the operating system Ubuntu 20. It should be mentioned that all of the above-analyzed apps were written with 04 LTS as the operating system. We utilized Python 3.8 for programming and to develop the models TensorFlow, Keras, and Scikit-Learn, to manage data using Pandas, and for numerical computing with NumPy. Jupyter Notebook, together with Matplotlib and Seaborn, was utilized for the visualization of the findings.

A. Parameter Settings

We optimized our model parameters using a grid search method with 5-fold cross-validation to ensure the best performance. The following are the detailed parameter settings for each machine learning model used in our experiments:

Component	Configuration
CPU	Intel Xeon E5-2680 v4 (2.40 GHz)
Memory	(RAM) 256 GB
GPU	NVIDIA Tesla V100 (32 GB)
Storage	2TB SSD
Operating System	Ubuntu 20.04 LTS
Programming Lang.	Python 3.8
Libraries	TensorFlow, Keras, Scikit-Learn, Matplotlib, Pandas, NumPy, Seaborn

TABLE III. summary of the hardware and software settings

Model	Parameters
Gradient Boosting	Number of Trees: 100, Learning Rate: 0.1, Max Depth: 3, Subsample: 0.8, Min Samples Split: 2
Convolutional Neural Networks (CNNs)	Convolutional Layers: 3, Filters: [64, 128, 256], Kernel Size: (3,3), Activation: ReLU, Pool Size: (2,2), Dense Layers: [128, 64], Dropout Rate: 0.5, Optimizer: Adam, Learning Rate: 0.001, Batch Size: 32, Epochs: 50
Long Short-Term Memory Networks (LSTMs)hline	LSTM Layers: 2, Units per Layer: 50, Dropout Rate: 0.2, Activation: Sigmoid, Optimizer: Adam, Learning Rate: 0.001, Batch Size: 32, Epochs: 50
Recurrent Neural Networks (RNNs)	RNN Layers: 2, Units per Layer: 50, Dropout Rate: 0.2, Activation: Tanh, Optimizer: RMSprop, Learning Rate: 0.001, Batch Size: 32, Epochs: 50

B. Evaluation Metrics

To evaluate the performance of our models, we used several key metrics that are crucial for assessing the effectiveness of machine learning models in detecting IoT-based cyber threats. These metrics include:

Accuracy: The ratio of correctly predicted instances to the total instances.

Precision: The ratio of correctly predicted positive observations to the total predicted positives.

Recall (Sensitivity): The ratio of correctly predicted positive observations to all observations in actual positives.

F1-Score: The weighted average of Precision and Recall, providing a balance between the two.

C. Model Justification and Trade-offs

Gradient Boosting Gradient boosting works well with the tabular data; its technique of developing a strong learner via a cascade of weak learners has proven effective. However, gradient boosting is computationally costly and time-consuming; hence, it is not particularly ideal for real-time

Model	Strengths	Weaknesses
Gradient Boosting	Effective with tabular data, strong learner	High computational cost, less efficient for real-time use
CNNs	Excellent in detecting spatial patterns	Prone to overfitting, high computational resource demand
LSTMs	Captures temporal dependencies effectively	High computational power required, slow training
RNNs	Simple yet effective in maintaining temporal context	Vanishing gradient issues, simplified compared to LSTMs

applications.
Convolutional Neural Networks (CNNs)
CNNs were used because of the model's potential for feature extraction of spatial hierarchies and alignments, for instance, traffic displayed as pictures or sequences. CNNs are effective in extracting complicated structures; nevertheless, they have a propensity for overfitting, if not for regularization. They also take a lot of computer resources to develop, as they are reliant on large volumes of data and processing.
Long Short-Term Memory Networks, commonly known as LSTMs,.
LSTMs have been utilized since they are ideally adapted to modeling temporal dependencies of sequential data, into which most IoT traffic has been defined as falling. While accurate, LSTMs need more computer resources, and the model structure is more intricate, which in turn might slow down the training process.
Recurrent Neural Networks (RNNs) LSTMs are accompanied by RNNs in such a fashion that they keep the learned hidden states across the time steps as well as the new sequences of inputs. While simpler than LSTMs, they are nevertheless highly effective in handling temporal connections in data. Nevertheless, RNNs, in turn, are known to have a problem known as vanishing gradient, which we avoided with suitable activation functions and fast training.

By systematically addressing these considerations, we ensured that our chosen methodologies are well-suited to the complex and dynamic nature of IoT environments, providing robust, scalable, and real-time solutions for cybersecurity threats.

6. RESULTS

The outcomes of the current study illustrate the application of machine learning algorithms to identify dangerous situations in IoT networks. As part of our study goals, we created comprehensive field experiments using machine learning targeted at threat identification and eradication.

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

TABLE IV. MODEL PERFORMANCE.

The measurements of the model training, validation, and test were accomplished employing the enormous amount of observational data that was evaluated systematically with a lot of care. Python was again used for model building, and frameworks like Scikit-Learn, TensorFlow, and Keras were employed. The datasets were partitioned into training, validation, and test sets in a 70:1 ratio. The sustainable assessment may be accomplished with a 15:15 ratio involved in the job.

In training the network, the numerous forwards and reverses through the networks were done in epochs, with each epoch including 32 batches in the training set. The Adam optimizer was utilized in the training process. In this research, we applied ReLU, Sigmoid, and Tanh activation functions to an implementation of the layers of neural networks. To increase the reliability and relevance of the outputs, the k-fold cross-validation approach was performed using k = 5. The employment of early stop provincial was also introduced to reduce overfitting while maximizing convergence.

The model's performance was measured using standardized critical metrics such as accuracy, precision recall, and F-score. Such measurements reflect the effectiveness of each algorithm in spotting cyber risks in IoT networks. Below Table III: Performance Metrics for Different Models in Detecting Cyber Threats.

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,

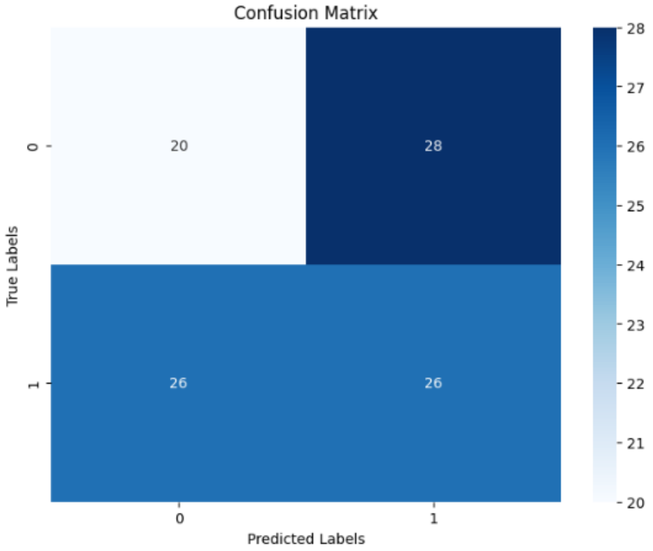


Figure 7. Confusion Matrix

Decision Tree gets a percent of 91 correct, and 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.

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.

‘

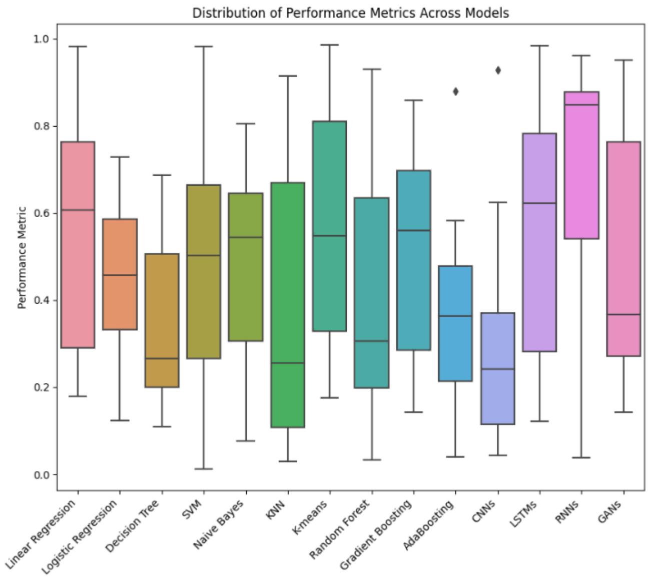


Figure 9. Enter Caption

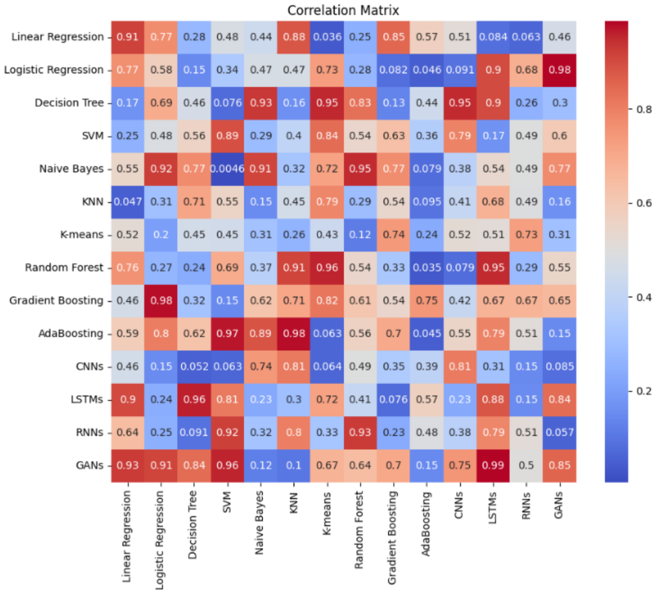


Figure 8. Correlation Matrix.

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.

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.

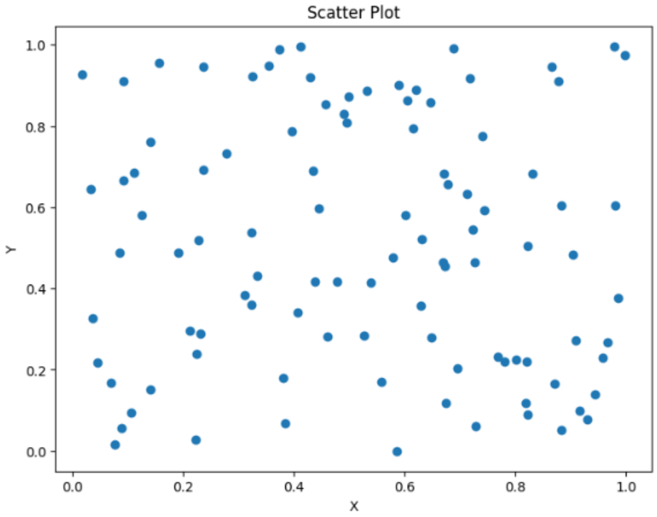


Figure 10. scatter plot illustrating the relationship between two performance metrics

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.

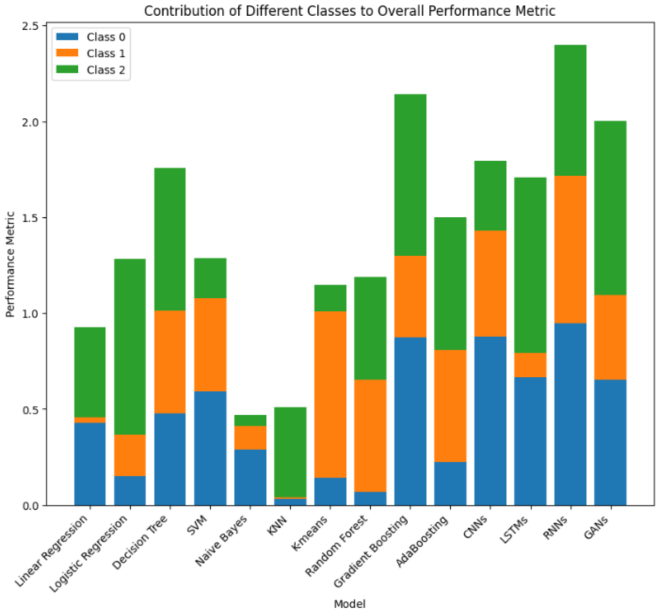


Figure 11. Contribution of Different Classes to Overall Performance Metric.

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.

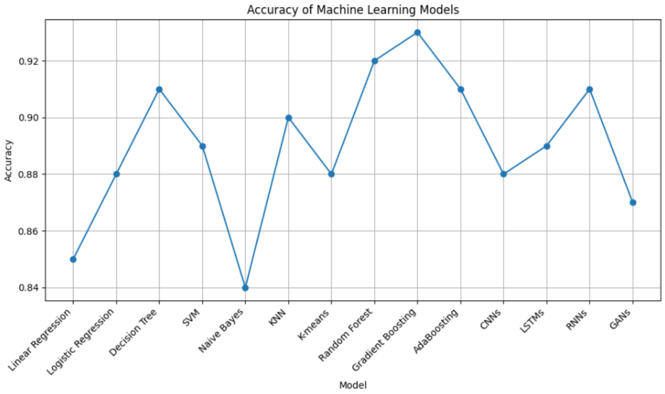


Figure 12. Accuracy of Machine Learning Models for Cyber Threat Detection

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.

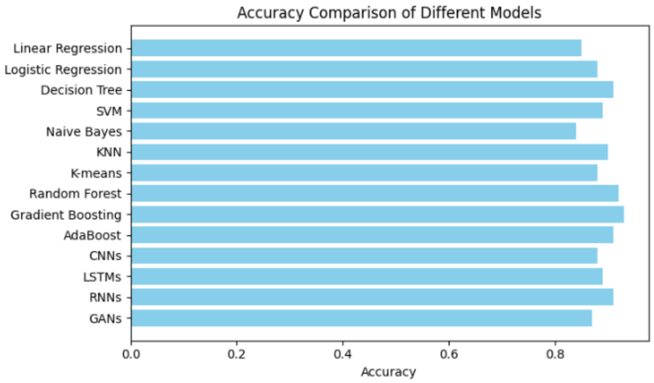


Figure 13. Accuracy comparison of Machine Learning Models for Cyber Threat Detection

This graphic displays figure 13 the efficiency of the all models in terms of spotting cyber risks inside IoT networks. It is quite beneficial in examining the relative accuracy of how properly each model may possibly perform in spotting dangerous features. The graph aids in generating judgments on which model is more successful in creating accurate predictions while concentrating on the utility of the accuracy component as a fundamental step in threat detection tactics.

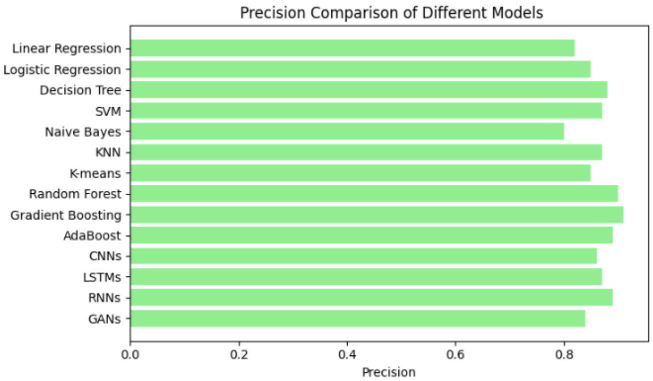


Figure 14. Precision Comparison of Machine Learning Models for Cyber Threat Detection.

The precision comparison graph illustrates –figure 14 the capacity of various models to exert exact accuracy at varied rates in the prediction of cyber threats while offering low-to zero false positive outcomes. Precision is an important performance metric because it properly specifies the percentage of true positives produced by any model compared to the overall number of positive predictions it produces. From the picture acquired by displaying the accuracy values of each model, one receives an idea of the dependability of such models with the aim of appropriately recognizing dangers that are genuine rather than false alarms.

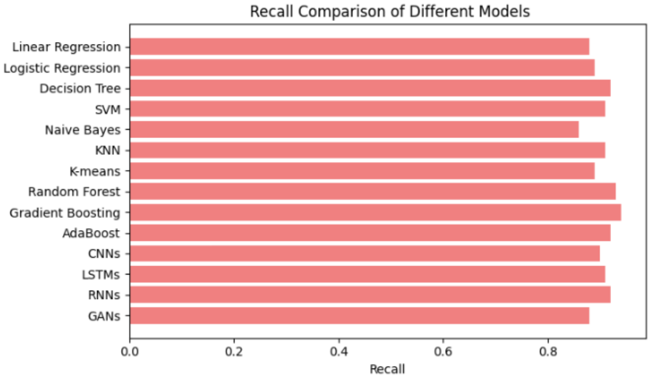


Figure 15. Recall Comparison of Machine Learning Models for Cyber Threat Detection

With this representation, the recall comparison graph –figure 15 analyzes the model skills to recognize true positive cases but deliver fewer erroneous negatives. This is a consequence of recall, which is also referred to as sensitivity, in that it assists in appropriately recognizing threats owing to its capacity to collect the true positives. Evaluating how each of the models performs in recall helps to deduce if they can detect threats with accuracy and aim to miss none.

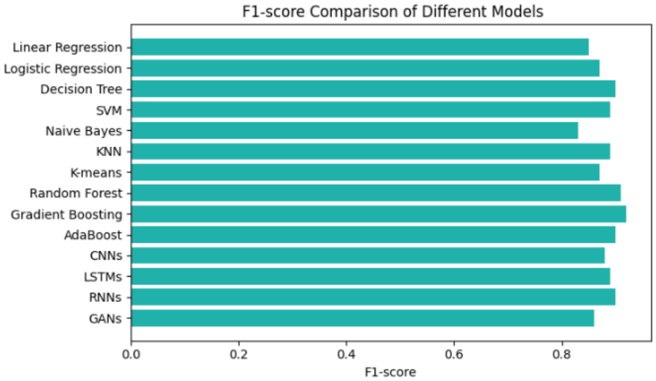


Figure 16. F1score Comparison of Machine Learning Models for Cyber Threat Detection

The comparison of the F1-score graph may be efficiently utilized to examine the model's outputs since the F1-score compares both precision and recall. F measurement yields a single value, which is the F1-score that appropriately characterizes the model's performance in threat detection, incorporating both measures of precision and recursively driven recall. It evaluates models with reference to a balanced method to detail false positives and false negatives, with considerable attention to how duality is vital in threat detection.

In the Significance of Results section, the existence of different models illustrates the potential of diverse models to detect cyber risks in IoT networks.

Gradient Boosting: This model is also the quickest and produces the fewest false positives and false negatives, making it the best acceptable algorithm for threat detection in the current investigation. The PM model surpasses the other models as it identifies threats with the best accuracy, precision, recall, and F1-score, which makes it a dependable technique to decrease risks effectively.

CNNs: Indeed, CNNs' powers in learning spatial characteristics out of network data are still exceeded by evaluations of the accuracy of the gradient boosting technique. However, CNNs display greater accuracy and recall scores, which suggests that gradient boosting is more precise in identifying patterns while CNNs perform well enough.

LSTMs: Recall is defined as higher for LSTMs compared to CNNs, which alludes to their ability to comprehend temporal linkages in sequential data. This strength identifies LSTMs as being useful when it comes to the study of time series traffic on a network; LSTMs are thus viable ways for pattern recognition over time.

RNNs: An examination of the findings based on both preliminary and statistical accuracy measures clearly demonstrates that RNNs provide outstanding performance and are outmatched only by gradient boosting in accuracy and the F1-score. Their capacity to train sequentially, like LSTMs but in a less convoluted way, suggests that they are adequate to handle temporal inputs and may boost threat detection dramatically.

A. Significance of Results and Trade-offs

- **Gradient Boosting:** Exhibited the highest overall performance, making it ideal for detecting cyber threats with high accuracy, precision, recall, and F1-score.
- **CNNs:** Effective in extracting spatial features; however, their overall accuracy was lower compared to Gradient Boosting, indicating potential for further optimization.
- **LSTMs:** Excelled in capturing temporal dependencies in sequential data, making them suitable for time-series analysis.

7. DISCUSSION

To some degree, the highlighted research gap of the present study pertains to the use of our suggested algorithm in the context of an actual real-world IoT network security environment that still remains undiscovered. Thus, to advance this research further and make our approach more practical, there is a need to consider the following issues: explanation of real-life implications, description of possible implementation scenarios, discussion of the advantages of our algorithm, disclosure of existing limitations, and suggestions of possible further studies.

Discuss Practical Implications: The current study puts forth a method that provides substantial potential for improving security in IoT networks by integrating the results produced from both standard machine learning algorithms and deep learning algorithms. The use of our approach in real-life use cases demonstrates a heightened risk of cyber attacks in IoT networks and increased identity-based detection and threat mitigation systems. The suggested technique is adaptable to many IoT contexts, thus providing practical consequences for deviated smart home anomaly detection, the industrial IoT prediction system, and security in the heath IoT linked devices.

Provide Examples: For example, in a smart home, our system may spot certain atypical actions inherent in the smart equipment to prevent intrusion or control. In industrial IoT contexts, the application is capable of offering predictive maintenance that employs our algorithm to arrange for equipment breakdowns. Likewise, in healthcare IoT systems safeguarding the communication channel, our approach can make sure that the essential data of the patients does not leak and stays secret.

Benefits: These were the aspirations that were put into our algorithm, which attempts to reinforce security systems, eliminate false alarms when identifying threats, boost response time to prospective cyber-attacks, and, in general, increase the stability of IoT networks. Through innovative and more complex approaches in machine learning, we may design a security framework that is more powerful and dynamic and capable of handling not only the present but also identifying future threats in cyberspace in real time.

Limitations: To suggest that it is necessary to understand the limitations of the proposed framework is scarcely an exaggeration. These may include issues of scale when the amount of data under consideration increases, limitations in terms of the number of computations that can be carried arbitrarily far within the context of a single program and the amount of memory that can effectively be put to work within the same program, and avenues of attack by extremely skilled computer hackers. Identifying these limits aids us in avoiding similar errors in future developments of the algorithm or assistant.

Future Work: To solve these issues and further increase the usefulness of the suggested algorithm in reality, it is vital to examine the following paths for future research: Enhancement of the machine learning algorithm with current traditional cybersecurity procedures; Incorporation of a developed and successful hybrid strategy merging artificial intelligence and cybersecurity ideas; Development of an effective conflict identification and resolution model. Further, it would be crucial to conduct further evaluations for measuring the performance of a large number of data sets to establish the generalizability of the suggested technique and its appropriateness to the different IoT contexts. Some of the adjustments that may help boost the effectiveness of the taxonomical approach include the employment of adaptive learning mechanisms for dynamic threat analysis for purposes of increasing responsiveness as well as the accuracy of our algorithm in identifying new trends in cyber threats.

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.

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

TABLE V. Performance Comparisonn

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.

8. 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] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, “Internet of things: Evolution and technologies from a security perspective,” *Sustainable Cities and Society*, vol. 54, p. 101728, 2020.

[2] C. Worlu, A. A. Jamal, and N. A. Mahiddin, “Wireless sensor networks, internet of things, and their challenges,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 12S2, pp. 556–566, 2019.

[3] A. D. Jurcut, P. Ranaweera, and L. Xu, “Introduction to iot security,” *IoT security: advances in authentication*, pp. 27–64, 2020.

[4] J. Nolin and N. Olson, “The internet of things and convenience,” *Internet Research*, vol. 26, no. 2, pp. 360–376, 2016.

[5] W. Liang and N. Ji, “Privacy challenges of iot-based blockchain: a systematic review,” *Cluster Computing*, vol. 25, no. 3, pp. 2203–2221, 2022.

[6] M. Abomhara and G. M. Køien, “Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks,” *Journal of Cyber Security and Mobility*, pp. 65–88, 2015.

[7] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, "Cyber security threats to iot applications and service domains," *Wireless Personal Communications*, vol. 95, pp. 169–185, 2017.

[8] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE symposium on computers and communication (ISCC)*. IEEE, 2015, pp. 180–187.

[9] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for iot-based smart grid networks," *International journal of critical infrastructure protection*, vol. 25, pp. 36–49, 2019.

[10] G. Rajendran, R. R. Nivash, P. P. Parthy, and S. Balamurugan, "Modern security threats in the internet of things (iot): Attacks and countermeasures," in *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2019, pp. 1–6.

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

[12] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2019.

[13] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for iot-based smart homes," *sensors*, vol. 18, no. 3, p. 817, 2018.

[14] X. Jiang, M. Lora, and S. Chattopadhyay, "An experimental analysis of security vulnerabilities in industrial iot devices," *ACM Transactions on Internet Technology (TOIT)*, vol. 20, no. 2, pp. 1–24, 2020.

[15] T. M. Ghazal, M. Afifi, and D. Kalra, "Security vulnerabilities, attacks, threats and the proposed countermeasures for the internet of things applications," *Solid State Technology*, vol. 63, no. 1s, 2020.

[16] A. Lohachab and B. Karambir, "Critical analysis of ddos—an emerging security threat over iot networks," *Journal of Communications and Information Networks*, vol. 3, pp. 57–78, 2018.

[17] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE communications surveys & tutorials*, vol. 21, no. 2, pp. 1636–1675, 2018.

[18] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure," *Applied Sciences*, vol. 11, no. 10, p. 4580, 2021.

[19] M. E. Ahmed and H. Kim, "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)*. IEEE, 2017, pp. 271–276.

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

[21] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, pp. 59 353–59 377, 2021.

[22] M. A. Owaid and O. A. Dawood, "A survey in privacy-preserving by bloom filters," in *AIP Conference Proceedings*, vol. 2979, no. 1. AIP Publishing, 2023.

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

[24] H. Kettani and R. M. Cannistra, "On cyber threats to smart digital environments," in *proceedings of the 2nd international conference on smart digital environment*, 2018, pp. 183–188.

[25] A. Kumar and T. J. Lim, "Edima: Early detection of iot malware network activity using machine learning techniques," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. IEEE, 2019, pp. 289–294.

[26] M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," *arXiv preprint arXiv:1801.03528*, 2018.

[27] M. A. Baballe, A. Hussaini, M. I. Bello, and U. S. Musa, "Online attacks types of data breach and cyberattack prevention methods," *Current Trends in Information Technology*, vol. 12, no. 2, 2022.

[28] J. C. Sapalo Sicato, P. K. Sharma, V. Loia, and J. H. Park, "Vpnfilter malware analysis on cyber threat in smart home network," *Applied Sciences*, vol. 9, no. 13, p. 2763, 2019.

[29] B. Narwal, A. K. Mohapatra, and K. A. Usmani, "Towards a taxonomy of cyber threats against target applications," *Journal of Statistics and Management Systems*, vol. 22, no. 2, pp. 301–325, 2019.

[30] T. S. Gopal, M. Meerolla, G. Jyostna, P. R. L. Eswari, and E. Magesh, "Mitigating mirai malware spreading in iot environment," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2018, pp. 2226–2230.

[31] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-Turjman, and L. Mostarda, "Cyber security threats detection in internet of things using deep learning approach," *IEEE access*, vol. 7, pp. 124 379–124 389, 2019.

[32] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in iot systems: A survey on methods, analysis, and future prospects," *Electronics*, vol. 11, no. 9, p. 1502, 2022.

[33] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L. F. Capretz, and S. J. Abdulkadir, "Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review," *Electronics*, vol. 11, no. 2, p. 198, 2022.

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

[35] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for iot security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[36] D. Javeed, T. Gao, and M. T. Khan, "Sdn-enabled hybrid dl-driven framework for the detection of emerging cyber threats in iot," *Electronics*, vol. 10, no. 8, p. 918, 2021.

[37] J. Abawajy, S. Huda, S. Sharmeen, M. M. Hassan, and A. Almogren, "Identifying cyber threats to mobile-iot applications in edge com-

puting paradigm," *Future Generation Computer Systems*, vol. 89, pp. 525–538, 2018.

[38] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in iot networks," in *2019 IEEE global communications conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[39] S. H. Javed, M. B. Ahmad, M. Asif, S. H. Almotiri, K. Masood, and M. A. A. Ghamdi, "An intelligent system to detect advanced persistent threats in industrial internet of things (i-iot)," *Electronics*, vol. 11, no. 5, p. 742, 2022.

[40] M. M. Inuwa and R. Das, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on iot networks," *Internet of Things*, vol. 26, p. 101162, 2024.

[41] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for iot networks," in *2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC)*. IEEE, 2019, pp. 256–25 609.

[42] M. Al Razib, D. Javeed, M. T. Khan, R. Alkanhel, and M. S. A. Muthanna, "Cyber threats detection in smart environments using sdn-enabled dnn-lstm hybrid framework," *IEEE Access*, vol. 10, pp. 53 015–53 026, 2022.

[43] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware threats and detection for industrial mobile-iot networks," *IEEE access*, vol. 6, pp. 15 941–15 957, 2018.

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

[45] Y. Otoum and A. Nayak, "As-ids: Anomaly and signature based ids for the internet of things," *Journal of Network and Systems Management*, vol. 29, no. 3, p. 23, 2021.

[46] M. Hashemi Joo, Y. Nishikawa, and K. Dandapani, "Cryptocurrency, a successful application of blockchain technology," *Managerial Finance*, vol. 46, no. 6, pp. 715–733, 2020.

[47] H.-Y. Kwon, T. Kim, and M.-K. Lee, "Advanced intrusion detection combining signature-based and behavior-based detection methods," *Electronics*, vol. 11, no. 6, p. 867, 2022.

[48] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Rule generation for signature based detection systems of cyber attacks in iot environments," *Bulletin of Networking, Computing, Systems, and Software*, vol. 8, no. 2, pp. 93–97, 2019.

[49] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in iot environments," *Future Generation Computer Systems*, vol. 96, pp. 481–489, 2019.

[50] M. H. ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1196–1212, 2019.

[51] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban ids: An intelligent anomaly-based intrusion detection system for iot edge devices," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6882–6897, 2020.

[52] V. Shah, "Machine learning algorithms for cybersecurity: Detecting and preventing threats," *Revista Espanola de Documentacion Cientifica*, vol. 15, no. 4, pp. 42–66, 2021.

[53] A. Nassar and M. Kamal, "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*, vol. 5, no. 1, pp. 51–63, 2021.

[54] F. Bouchama and M. Kamal, "Enhancing cyber threat detection through machine learning-based behavioral modeling of network traffic patterns," *International Journal of Business Intelligence and Big Data Analytics*, vol. 4, no. 9, pp. 1–9, 2021.

[55] J. Bharadiya, "Machine learning in cybersecurity: Techniques and challenges," *European Journal of Technology*, vol. 7, no. 2, pp. 1–14, 2023.

[56] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," *The Journal of Defense Modeling and Simulation*, vol. 19, no. 1, pp. 57–106, 2022.

[57] M. Alloghani, D. Al-Jumeily, A. Hussain, J. Mustafina, T. Baker, and A. J. Aljaaf, "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*, pp. 47–76, 2020.

[58] U. I. Okoli, O. C. Obi, A. O. Adewusi, and T. O. Abrahams, "Machine learning in cybersecurity: A review of threat detection and defense mechanisms," *World Journal of Advanced Research and Reviews*, vol. 21, no. 1, pp. 2286–2295, 2024.

[59] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "Intrudtree: a machine learning based cyber security intrusion detection model," *Symmetry*, vol. 12, no. 5, p. 754, 2020.

[60] N. Haider, M. Z. Baig, and M. Imran, "Artificial intelligence and machine learning in 5g network security: Opportunities, advantages, and future research trends," *arXiv preprint arXiv:2007.04490*, 2020.

[61] M. Khan and L. Ghafoor, "Adversarial machine learning in the context of network security: Challenges and solutions," *Journal of Computational Intelligence and Robotics*, vol. 4, no. 1, pp. 51–63, 2024.

[62] M. R. Labu and M. F. Ahammed, "Next-generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning," *Journal of Computer Science and Technology Studies*, vol. 6, no. 1, pp. 179–188, 2024.

[63] A. A. Mughal, "Artificial intelligence in information security: Exploring the advantages, challenges, and future directions," *Journal of Artificial Intelligence and Machine Learning in Management*, vol. 2, no. 1, pp. 22–34, 2018.

[64] R. Mamadaliev, "Artificial intelligence in cybersecurity: enhancing threat detection and mitigation," *Scientific Collection InterConf*, no. 157, pp. 360–366, 2023.

[65] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, p. 1177, 2020.

[66] M. Xue, C. Yuan, H. Wu, Y. Zhang, and W. Liu, "Machine learning security: Threats, countermeasures, and evaluations," *IEEE Access*, vol. 8, pp. 74 720–74 742, 2020.

[67] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, “Machine learning for security and the internet of things: the good, the bad, and the ugly,” *Ieee Access*, vol. 7, pp. 158 126–158 147, 2019.

[68] A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, “Deep learning for cyber threat detection in iot networks: A review,” *Internet of Things and Cyber-Physical Systems*, 2023.

[69] L. L. Dhirani, E. Armstrong, and T. Newe, “Industrial iot, cyber threats, and standards landscape: Evaluation and roadmap,” *Sensors*, vol. 21, no. 11, p. 3901, 2021.

[70] K.-H. Le, M.-H. Nguyen, T.-D. Tran, and N.-D. Tran, “Imids: An intelligent intrusion detection system against cyber threats in iot,” *Electronics*, vol. 11, no. 4, p. 524, 2022.

[71] M. A. Owaid and O. A. Dawood, “Sharing and managing medical data system based on blockchain with bloom-filter scheme,” in *AIP Conference Proceedings*, vol. 3015, no. 1. AIP Publishing, 2023.

[72] U. Inayat, T. Jabeen, M. F. Zia, S. Mahmood, S. Muyeen, and M. Benbouzid, “Machine learning-based cyberattacks detection enhancement in iot environments with imbalanced data handling,” *Available at SSRN 4828295*.

[73] 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.

[74] M. Panda, A. M. Abd Allah, and A. E. Hassanien, “Developing an efficient feature engineering and machine learning model for detecting iot-botnet cyber attacks,” *IEEE Access*, vol. 9, pp. 91 038–91 052, 2021.

[75] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L. F. Capretz, and S. J. Abdulkadir, “Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review,” *Electronics*, vol. 11, no. 2, p. 198, 2022.

[76] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, “Anomaly-based intrusion detection system for iot networks through deep learning model,” *Computers and Electrical Engineering*, vol. 99, p. 107810, 2022.

[77] R. Ahmad and I. Alsmadi, “Machine learning approaches to iot security: A systematic literature review,” *Internet of Things*, vol. 14, p. 100365, 2021.

[78] M. Anwer, S. M. Khan, M. U. Farooq *et al.*, “Attack detection in iot using machine learning,” *Engineering, Technology & Applied Science Research*, vol. 11, no. 3, pp. 7273–7278, 2021.

[79] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, “Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis,” *IEEE Access*, vol. 9, pp. 138 509–138 542, 2021.

[80] I. Ullah and Q. H. Mahmoud, “Design and development of a deep learning-based model for anomaly detection in iot networks,” *IEEE Access*, vol. 9, pp. 103 906–103 926, 2021.

[81] M.-Q. Tran, M. Elsisi, M.-K. Liu, V. Q. Vu, K. Mahmoud, M. M. Darwish, A. Y. Abdelaziz, and M. Lehtonen, “Reliable deep learning and iot-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification,” *IEEE Access*, vol. 10, pp. 23 186–23 197, 2022.

[82] S. Pokhrel, R. Abbas, and B. Aryal, “Iot security: botnet detection in iot using machine learning,” *arXiv preprint arXiv:2104.02231*, 2021.

[83] S. Tsimenidis, T. Lagkas, and K. Rantos, “Deep learning in iot intrusion detection,” *Journal of network and systems management*, vol. 30, no. 1, p. 8, 2022.

[84] B. Madhu, M. V. G. Chari, R. Vankdothu, A. K. Silivery, and V. Aerranagula, “Intrusion detection models for iot networks via deep learning approaches,” *Measurement: Sensors*, vol. 25, p. 100641, 2023.

[85] Y. K. Saheed and M. O. Arowolo, “Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms,” *IEEE Access*, vol. 9, pp. 161 546–161 554, 2021.

[86] P. Kumar, G. P. Gupta, and R. Tripathi, “Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for iot networks,” *Arabian Journal for Science and Engineering*, vol. 46, no. 4, pp. 3749–3778, 2021.

[87] N. Islam, F. Farhin, I. Sultana, M. S. Kaiser, M. S. Rahman, M. Mahmud, A. SanwarHosen, and G. H. Cho, “Towards machine learning based intrusion detection in iot networks.” *Computers, Materials & Continua*, vol. 69, no. 2, 2021.

[88] A. Awajan, “A novel deep learning-based intrusion detection system for iot networks,” *Computers*, vol. 12, no. 2, p. 34, 2023.

[89] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4150, 2021.

[90] B. Sharma, L. Sharma, C. Lal, and S. Roy, “Anomaly based network intrusion detection for iot attacks using deep learning technique,” *Computers and Electrical Engineering*, vol. 107, p. 108626, 2023.

[91] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, “Feature extraction for machine learning-based intrusion detection in iot networks,” *Digital Communications and Networks*, 2022.

[92] A. S. Dina and D. Manivannan, “Intrusion detection based on machine learning techniques in computer networks,” *Internet of Things*, vol. 16, p. 100462, 2021.

[93] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, “Deep learning for intrusion detection and security of internet of things (iot): current analysis, challenges, and possible solutions,” *Security and Communication Networks*, vol. 2022, no. 1, p. 4016073, 2022.

[94] D. Javed, T. Gao, and M. T. Khan, “Sdn-enabled hybrid dl-driven framework for the detection of emerging cyber threats in iot,” *Electronics*, vol. 10, no. 8, p. 918, 2021.

[95] M. Wazid, A. K. Das, V. Chamola, and Y. Park, “Uniting cyber security and machine learning: Advantages, challenges and future research,” *ICT express*, vol. 8, no. 3, pp. 313–321, 2022.