Systematic Analysis of threats, Machine Learning solutions and Challenges for Securing IoT environment

Bharti Yadav[1], Deepak Dasaratha Rao[2], Yasaswini Mandiga[3], Nasib Singh Gill[1], Preeti Gulia[1], Piyush Kumar Pareek[4,*]

[1]Department of Computer Science & Applications, Maharshi Dayanand University,
Rohtak, Haryana, India
[2]Department of Computer Science, Indian Institute of Technology, Patna, Orchid- 0000-0001-5959-3136, India
[3]Asst. Professor, Dept. of IT, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, TN, India
[4]Professor and Head Department of AIML and IPR Cell Nitte Meenakshi Institute of Technology Bengaluru, India
Emails: bharti.yadav0801@gmail.com; deepakrao@ieee.org; mandigayasaswini@velhightech.com; nasib.gill@mdurohtak.ac.in; preeti@mdurohtak.ac.in; eepakrao@ieee.org; piyush.kumar@nmit.ac.in

Abstract

The Internet of Things (IoT) has revolutionized our daily lives, affecting everything from healthcare to transportation and even home automation and industrial control systems. However, as the number of connected devices continues to rise, so do the security risks. In this review, we explore the different types of attacks that target various layers of IoT infrastructure. To counter these threats, researchers have proposed using machine learning (ML) and deep learning (DL) techniques for detecting different types of attacks. However, our examination of existing literature reveals that the effectiveness of these techniques can vary greatly depending on factors like the dataset used, the features considered, and the evaluation methods employed. Finally, we delve into the current challenges facing Intrusion Detection Systems (IDS) in their mission to protect IoT environments from evolving threats.

Keywords: IoT; Machine Learning; Security; Threats

1. Introduction

The Internet of Things is referred to as IoT. It characterizes a network comprised of real objects, or "things," that are fitted with software, sensors, and other technology so they can communicate and share information online. These objects can be everyday devices, machines, vehicles, appliances, or even people and animals, which possess the capacity to gather and transfer data without the need for direct human-computer interaction.[1] By 2025, 7.544 billion IoT devices are expected, and 73.1 ZB of data generated by IoT devices is predicted. The proliferation of IoT technology has significant implications for various industries, including healthcare, agriculture, transportation, manufacturing, and urban planning. However, it also raises important considerations regarding privacy, security, and data management, as the vast amount of data generated by IoT devices must be handled responsibly to protect user information and ensure the integrity of the system. This study examines alternative risk-reduction strategies and offers a thorough examination of the security issues with IoT devices.

2. Threats and Security approaches in IoT Devices

The IoT device category emerged from numerous large-scale applications and positively affected everyday life in a way that minimized effort. [2] WSN technology is the foundation of the majority of IoT devices because it offers a suitable platform for communication [3]. The three main threats to WSN security are node destruction, node duplication, and denial of service (DoS). IoT presents distinct security challenges that extend from the physical layer to the application layer due to its interconnected layers. There are several threats that target these levels, including as application-level attacks, network eavesdropping, and physical manipulation. As a result, security

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

strategies that include anomaly detection, access control, and encryption must be customized for every layer. In order to strengthen the resilience of IoT ecosystems against increasing cyber threats, it is imperative to comprehend these risks and security techniques across many layers. Each layer in the Internet of Things [4] architecture is vulnerable to distinct attacks and has its own vulnerabilities [50].

A. Security Attacks on Perception Layer

The perception layer [24] is made up of several items that have sensors attached to them, such as cameras, robots, and smart meters. It is the responsibility of this layer to identify and collect particular sensor data, such as acceleration, sound waves temperatures direction, moisture, and chemicals in the atmosphere. Following collection, after reaching the network layer, the information processing system receives these data.

- Node Capture Attacks: Node capture attacks are a type of security threat where an attacker gains unauthorized access to a node within a network, such as a computer, server, or IoT device. Once compromised, the attacker can manipulate or intercept data traffic, steal sensitive information, or launch further attacks within the network. These attacks often involve exploiting vulnerabilities in software or hardware, such as weak passwords, unpatched software, or insecure network configurations. Usually, the objective of node capture attacks is to jeopardize the availability, confidentiality, or integrity of the targeted system or network.

- Malicious Code Injection Attack: Malicious code injection involves attackers inserting harmful code into the perception layer, which encompasses sensors, actuators, and the interfaces connecting them. These attacks aim to manipulate the data sensed or transmitted by the IoT device, leading to various consequences such as false readings, unauthorized access, or disruption of device functionality. For instance, attackers might inject code into a sensor to manipulate environmental data, leading to false readings and incorrect decisions by the device's control systems. The integrity and dependability of IoT applications may be jeopardized by this manipulation, posing a risk to public safety or compromising security. Defending against such attacks requires implementing strong authentication, encryption, and intrusion detection methods to guarantee the reliability of information gathered and sent by Internet of Things devices at the perception layer.

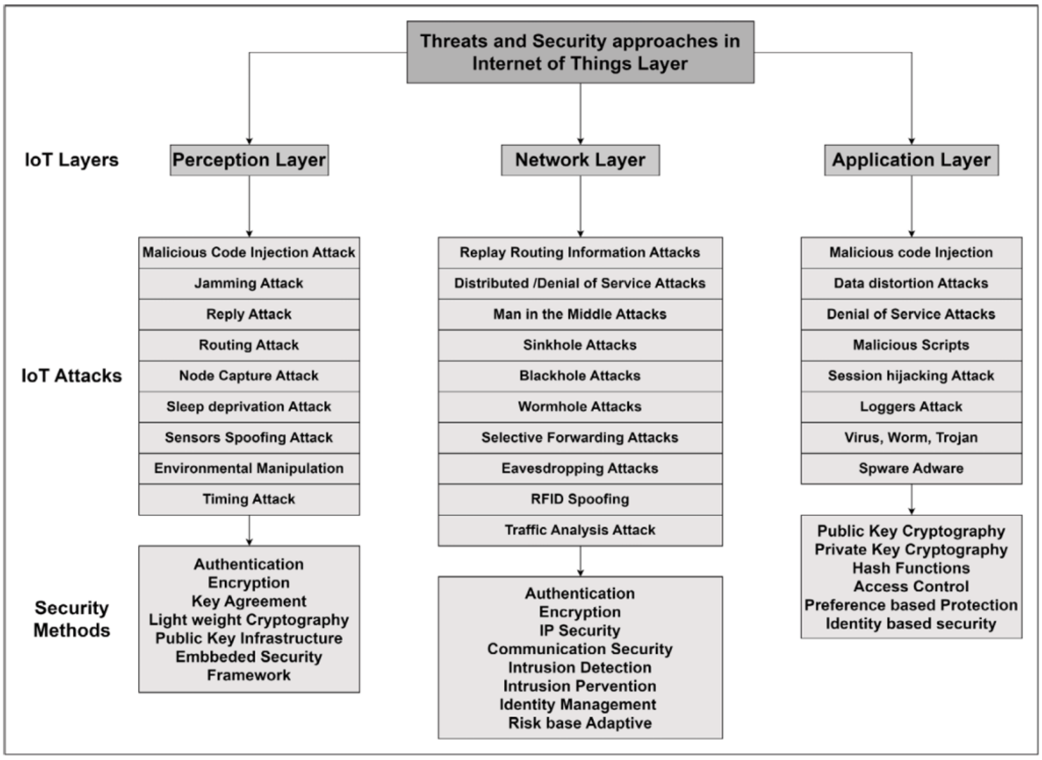

Figure 1. IoT architecture with its attacks and security solution [23]

- Sleep Deprivation Attack: Sleep deprivation attacks deplete an edge device's battery; methods to guarantee the reliability of information gathered and sent by Internet of Things devices at the perception layers are similar to denial-of-service attacks, even though edge devices are often designed to operate at minimal power. Making changes to the hardware or adding codes that loop endlessly into the memory increases consumption.

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

- Jamming attack: Attacks referred to as "jamming”, disrupt or modify signals by interfering with the tag reader's air interface. This type of attack can be accomplished passively, for example, by shielding, which can be successful because of the sensitivity of the interface, or by using a powerful, long-range transmitter. When radio noise matched to the frequency of the RFID system occurs, the system can be jammed.

- Replay attack: Replay attack occurs when an approved person uses the same authentication code again. This can be done by copying the authorized tag or by listening in on signals transmitted by a device that has the proper card and antenna. Certain information is required for replay assaults, and the tag provides it through communications.

- Timing attack: A timing attack is a type of security breach where an attacker measures how long a system takes to respond to different inputs. By analyzing these response times, the attacker can infer information about the system's inner workings, such as cryptographic keys or sensitive data. This technique can be used to exploit vulnerabilities in security protocols, leading to unauthorized access or data leaks. Defending against timing attacks involves implementing consistent response times or adding random delays to make it harder for attackers to extract meaningful information

B. Security Attacks on Network Layer

Across heterogeneous networks, the network layer is in charge of transmitting and receiving data between various objects or applications via a variety of communication technologies, protocols, interfaces, and gateways. The network layer [24] determines how to distribute the data to hubs, gateways, and IoT devices via integrated networks once the perception layer has processed it [51].

- Sybil and Clone ID Attacks: Using sybil attacks, one way to get access to a greater portion of a network or defeat vote manipulation strategies is to move the identity of a legitimate node to another node.. By utilizing many logical entities, sybil attacks eliminate the requirement for additional nodes and let a single physical node control a substantial area of a network.
- Wormhole Attack: Typically, these assaults focus on network typologies and traffic patterns. Two attackers who build a tunnel that permits traffic to be sent along this path only execute a wormhole attack.
- Denial of Service (DoS): DoS assaults seek to interrupt a specific network or computing source, which may result in a decrease in the network's capacity. IoTs are susceptible to both simple and distributed DoS assaults. A simple attack needs a tool to send packets in order to crash or restart a system or network; however a DDoS attack can use one attacker with less force than a proxy. These attacks have the potential to interrupt and block access to networks [58].
- Man-in-the-Middle attack: Attacks known as "man-in-the-middle" employ a number of strategies to intercept and alter connections between nodes. The attackers can view the data once the node-node communication is broken and the data is updated in real time.
- Sinkhole Attack: Attacks known as "sinkholes" occur when a network's nodes are compromised. They then utilize these compromised nodes to provide misleading routing information to neighbouring nodes, posing as the fastest path to the base and subsequently deleting or changing packets that are routed through them.
- Black hole Attack: A cyberattack known as a "blackhole attack" occurs when a malevolent node in a network intercepts data packets and, instead of transmitting them as intended, drops or discards them. This attack creates a "black hole" where data seemingly disappears without reaching its destination. The attacker may use this tactic to disrupt communication, deny service, or launch further attacks within the network. It's particularly problematic in scenarios such as routing protocols where nodes rely on each other to forward data.
- Spoofed, Alter, Replay Routing Information: Spoofing, modifying, and replaying routing with the intention of affecting routing data in node-to-node exchanges are examples of mutual direct attacks. Spoofing attacks take use of vulnerabilities in a system's ability to identify an IoT device, such as the creation of a routing loop or a phony error message.
- Eavesdropping attack: Unauthorized communication between two parties is known as eavesdropping, and it enables an attacker to listen in on confidential information being conveyed. This type of attack can compromise confidentiality and privacy, as the attacker can capture data such as passwords, financial information, or personal conversations. Eavesdropping attacks often exploit weaknesses in network security, encryption protocols, or physical security measures to intercept data covertly.

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

C. Security Attacks on Application Layer

In IoT architecture, the application layer [24] manages the interaction between end-users and IoT devices. It facilitates tasks such as data processing, analysis, and presentation of information collected from IoT devices to users through various interfaces like web applications or mobile apps. Additionally, it coordinates device management functionalities, including software updates, security configurations, and remote control of devices. The application layer plays a crucial role in enabling users to interact with and derive value from IoT systems [53].

- Malicious scripts: these pertain to Internet of Things (IoT) devices that are online. Malicious codes, sometimes known as x-scripts, are executed to carry out the attack. These scripts appear authentic and require user access, allowing for data theft and system failure.
- Data distortion attacks: It employ software code to cause harm to systems or have other unintended effects while evading detection by antivirus programs. The code may initiate automatically or upon the user's execution of a designated action.
- Malware attack: Malware, often known as malicious software, is a broad category of destructive programs intended to interfere with, harm, or obtain unauthorized access to computer systems. These malicious entities include viruses, worms, Trojans, ransomware, and spyware, posing significant threats to cybersecurity. Malware can propagate through a variety of channels, taking advantage of flaws in software and user behavior, including email attachments, compromised websites, and portable devices. For this author [5] introduced an innovative model SB-BR-STM, In the realm of IoT ensemble learning classifiers, a unique split, transform, and merge (STM) block and squeezed-boosted channel (S.B.) are applied for feature space analysis as well as for effective and efficient malware detection. Through empirical evaluation, the unique hybrid framework that has been suggested performs exceptionally well, showing 97.12% F1-score, 95.77% accuracy, and 98.50% precision. Recall, and 98.42% precision. Furthermore, the deep CNN's STM block for the proposed classification architecture makes use of the concepts of region-heterogeneity and homogeneity also.

3. Intrusion Detection System in IoT

An IoT incursion [12] is an unlawful action or activity that harms the Internet of Things ecosystem. Viewed alternatively, any attack that compromises the availability, confidentiality, or integrity of information is seen to constitute an intrusion [52]. For example, an attack that stops authorized users from accessing computer systems is called an incursion. A hardware or software system that maintains system security by identifying hostile behavior on computer systems is known as an intrusion detection system (IDS). Detecting hostile network traffic and unauthorized computer activity is the main objective of intrusion detection systems (IDS), as these things cannot be detected by traditional firewalls. Consequently, computer systems are today quite resilient against hostile operations that can compromise their confidentiality, availability, or integrity. The two main subcategories of intrusion detection systems are Signature-based Intrusion Detection System (SIDS) and Anomaly-based Intrusion Detection System (AIDS).

A. Signature-based intrusion detection systems (SIDS)

Sometimes referred to as knowledge-based detection. Pattern matching techniques are used by SIDS to locate known attacks. Matching algorithms are employed in SIDS to locate a prior intrusion. Stated differently when the signature of an intrusion coincides with the signature of an earlier incursion that has already been recorded in the signature database, an alert is set off. To identify malware, the host's logs are examined for commands or actions that have been identified as such in the past. The terms Knowledge-Based Detection and Misuse Detection have also been applied to SIDS in the literature. The main idea is to compile a database of intrusion signatures, compare the set of activities being taken with the signatures that are already in place, and raise an alarm if a match is found. A rule that looks like this, for instance, might be written as follows: "if (source IP address=destination IP address) then label as an attack." SIDS usually offer very good detection accuracy for known incursions. However, SIDS is unable to detect zero-day attacks until the signature of the new assault is obtained and stored, as there isn't a matching signature in the database. Many popular tools employ SIDS, such as Netstat.

Conventional SIDS methods find it difficult to identify attacks that involve several packets since they examine network packets and compare them to a signature database. Given the complex nature of today's malware, it could be necessary to extract signature data from several packets. IDS must also bring the contents of previous packets with it. In general, a number of approaches the main idea is to compile a database of intrusion signatures, compare the set of activities being taken with the signatures that are already in place, and raise an alarm if a match is found. been developed for producing SIDS signatures, including state machine signatures, formal language string patterns, and semantic requirements. Due to the lack of a signature for zero-day attacks, SIDS methods have grown less and less effective as their frequency has increased. The other elements that compromise the suitability of this

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

conventional framework include the increasing frequency of targeted attacks and polymorphic malware types. One potential solution to this problem is to use AIDS techniques. AIDS functions by identifying suitable and inappropriate conduct, as illustrated in the ensuing section, rather than by profiling deviant behavior.

B. Anomaly-based intrusion detection system (AIDS)

Many scholars have noted that AIDS [12] can overcome the restrictions of SIDS. AIDS uses statistical, knowledge-based, or machine learning techniques to construct a normal model of a computer system's behaviour. Any discernible deviation from the model's predicted behaviour is regarded as an anomaly and could be interpreted as an incursion. This kind of strategy depends on the ability to distinguish between malicious and typical user behaviour. Unusual user activity that deviates from the norm is what defines an intrusion. A new line of inquiry known as "Unknown detection" has been put up to find unknown intrusions in order to remedy this problem.[6]
The training phase and the testing phase are the two stages of the development of AIDS. In the training phase, a model of usual behaviour is learned using the typical traffic profile. In the testing stage, a new set of data is used to improve the system's capacity to adjust to unknown incursions. The primary benefit of AIDS is its capacity to detect zero-day threats. Because it doesn't need a signature database to identify odd user behaviour. When the action under examination diverges from typical behavior, AIDS sends out a warning signal. Moreover, there are several advantages to AIDS. They can first discover dangerous activities going on within. An alert is activated. When a hacker starts using a stolen account to make transactions that aren't consistent with normal user behavior. Second, because the system is built utilizing distinct profiles, it is difficult for a cybercriminal to figure out what regular user behavior is without raising an alarm.
The differences between detection methods based on signatures and anomalies:
The primary distinction between the two is that whereas SIDS can only identify known intrusions, AIDS is capable of identifying zero-day attacks. However, AIDS can result in a high false-positive rate because anomalies might just be the new usual behavior rather than actual invasions. Due to the fact that anomaly-based intrusion detection systems lack a taxonomy.

C. Customized Intrusion Detection System (CIDS)

While customized and AIDS function similarly, this method provides and creates manual definitions and rules to define typical network activities. A network is observed in compliance with the suggested guidelines and directives. It is resistant to novel assault modifications, resulting in a minimum false positive rate. A customized IDS has limitations because of development constraints and complexities, time consumption, and expense.

D. Hybrid intrusion detection System (HIDS)

A hybrid intrusion detection system combines multiple detection techniques, such as signature-based, anomaly-based, and behavior-based approaches, to enhance accuracy and coverage in identifying potential threats. By integrating these methods, it can effectively detect both known attacks through signature matching and unknown attacks through abnormal behavior analysis. This hybrid approach offers improved detection rates and reduces false positives compared to individual detection methods alone, making it more robust in defending against various types of cyber threats.

E. Host-based intrusion detection system (HIDS)

In order to identify suspicious activity or indications of compromise, a host-based intrusion detection system (HIDS) keeps an eye on and evaluates all events and activities on a single host or device. It looks at user behavior, file integrity, and system logs to find unapproved activity or security lapses. On the host, HIDS functions locally, offering thorough insights into possible dangers and facilitating quick action to reduce risks. It's especially helpful in identifying targeted assaults and insider threats against particular systems or applications.

F. Network-based intrusion detection system (NIDS)

An intrusion detection system that is based on the network (NIDS) keeps track on network traffic in order to spot and examine any questionable behavior or possible security risks. It examines packet headers and payloads, looking for patterns indicative of malicious behavior or known attack signatures. NIDS operates at the network perimeter or within the internal network, providing real-time alerts and insights into unauthorized access attempts, malware infections, or other network-based attacks. It complements firewall and router security measures by actively monitoring traffic for anomalies and unauthorized access attempts.[7] The ability to identify unknown attacks is one of the advantages of anomaly-based NIDS that is typically mentioned; yet, the model's training still requires the attack's particular data due to the current design. The majority of NIDS solutions now in use focus on separately extracting features at the flow level while ignoring how those characteristics interact with one another

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

in the network, which affects detection efficiency, is one of their key drawbacks. The author suggests [8] a traffic-aware self-supervised learning system for IoT network intrusion detection systems, or TS-IDS, as a workaround for this problem. Its goal is to record the flow interactions between network entities. It boosts performance by utilizing both edge and node properties [54].

4. Related Work

[14] The proposed deep learning-based intrusion detection system achieved an average accuracy of 93.74% in detecting various types of attacks on IoT devices, including wormhole, DDOS, Opportunistic Service, Sinkhole, and Blackhole attacks. The precision, recall, and F1score of the system were measured to be 93.71%, 93.82%, and 93.47%, respectively, on average The system demonstrated a 93.21% average detection rate, indicating its effectiveness in improving the security of IoT networks

[15]In this work, an anomaly-based Intrusion Detection System (IDS) approach designed for Internet of Things (IoT) contexts is presented. Leveraging the computational power of IoT devices, this approach efficiently analyzes entire network traffic within IoT infrastructures. The suggested approach demonstrates competence in detecting possible breaches and anomalous traffic patterns. Using the NID and BoT-IoT datasets for testing, the model obtains remarkable accuracy rates of 99.51% and 92.85%, respectively.

[16] This study introduces IoTFECNN, a CNN with hybrid layers for improved IoT anomaly detection, coupled with BMECapSA for efficient feature selection, forming CNN-BMECapSA-RF. It surpasses current techniques with 99.99% and 99.85% accuracy when tested on the NSL-KDD and TON-IoT datasets, detecting 27% and 44% of useful characteristics, respectively..

[17] author evaluated binary classification on NSL-KDD, XGBoost-LSTM performed better, with a training time of 225.46 seconds and an accuracy of 88.13% in tests and 99.49% in validations. XGBoost-Simple-RNN obtained 87.07% test accuracy for UNSW-NB15. XGBoost-LSTM and XGBoost-GRU achieved 86.93% and 78.40% accuracy in multiclass classification on UNSW-NB15 and NSL-KDD, accordingly proving the suggested IDS framework's advantage over existing methods.

[18] This article introduces DnRaNN, a lightweight dense random neural network tailored for IoT intrusion detection, showcasing enhanced generalization and distributed capabilities for resource-constrained networks. Extensive experiments on ToN_IoT dataset validate its efficacy across various hyperparameters, yielding promising results across multiple performance metrics. The study offers valuable insights and recommendations for both binary and multiclass intrusion detection scenarios.

[19] This paper introduces MM-WMVEDL, a deep learning model tailored for IDS in IoT, employing a multi-modal architecture to capture intricate relationships within diverse network traffic data. Utilizing wavelet-based feature extraction enhances feature discriminative power, ensuring efficient detection of anomalies.

[20] The paper introduces a DCNN-based IDS featuring 2 convolutional layers and 3 dense layers to enhance performance and reduce computational demands. Evaluation on IoTID20 dataset with metrics including accuracy, precision, recall, and F1-score showcased optimized performance utilizing the optimization methods of Adam, AdaMax, and Nadam.

[21] Using a filter-based feature selection Deep Neural Network (DNN) model, which drops strongly correlated features and is modified with many parameters an innovative anomaly-based intrusion detection system (IDS) for Internet of Things (IoT) networks is presented in this paper. The model obtained 84% accuracy with the UNSW-NB15 dataset, and 91% accuracy with a balanced dataset when Generative Adversarial Networks (GANs) were used to solve class imbalance.

[22] Three intrusion detection models—CNN, LSTM, and a hybrid CNN + LSTM—are presented in this study for IIoT networks. The UNSW-NB15 and X-IIoTID datasets were used to perform binary and multi-class classifications. The hybrid CNN + LSTM model yielded the best results in the UNSW-NB15 dataset, with multi-class and binary classifications of 92.9% and 93.21%, respectively. Respectively, and 99.84% and 99.80% in the X-IIoTID dataset.

Table 1: Related work and their contributions.

Ref.	Description	Methods used	Dataset	Attacks classified	Result	Limitation
[25]	Reviews AI tools for IoT-based DDoS attack detection from 2019-2023.Discusses	Decision Tree, Naive Bayes, Support Vector Machine.	TON-IoT dataset , Edge-IIoT dataset ,IoTID20 dataset,	DDOS Attack	CNN and LSTM model have highest	Exclusion of non-conference and non-journal

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

Ref.	Description	Methods used	Dataset	Attacks classified	Result	Limitation
	real datasets, AI techniques, and ML/DL modeling software.		MedBIoT dataset		accuracy: 99.03%	research studies
[26]	Study compares machine learning methods for detecting cyber anomalies in IoT.Neural network outperformed other models in detecting cyber anomalies	SVM, ANN, DT, LR, k-NN.	ToN-IoT and BoT-IoT datasets	DoS ,DDoS and Ransomware	Neural Network outperforms other models in detecting cyber anomalies.	Current ML models in IoT may inaccurately detect anomalies
[27]	Research focuses on Hybrid CNN-LSTM model for IoT threat detection. Model achieves high accuracy on IoT-23, N-BaIoT, and CICIDS2017 datasets. Incorporates PCA, model quantization, and pruning for efficient deployment.	Hybrid CNN-LSTM model Ensemble classifiers and deep learning techniques	N-BaIoT, CICIDS2017, and IoT-23	21 type of attacks classified	Model achieves 95% accuracy on IoT-23 and 99% on N-BaIoT datasets.	Model not tested in real-time IoT ecosystem.Lower computational efficiency compared to other models.
[28]	Hybrid method detects botnet attacks in IoT devices effectively.Proposed system outperformed other methods by 3% in both classifications.	KNN, DT, RF, AdaBoost, and Bagging models used for intrusion detection	UNSW-NB15 dataset	botnet attacks	RF model achieved an accuracy of 95.11% in binary classification.	The paper does not explicitly mention limitations.
[29]	Paper focuses on detecting brute force attacks on IoT networks. Utilizes deep learning with high accuracy for intrusion detection.	Deep Neural Networks, Support Vector Machines, and Decision Trees are used.	MQTT-IoT-IDS2020	Brute force attacks	Deep learning model achieved over 99% accuracy in attack detection	Limited to detecting brute force attacks on MQTT-IoT networks

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

Ref.	Description	Methods used	Dataset	Attacks classified	Result	Limitation
[30]	Proposed anomaly-based IDS system for IoT networks using Deep Learning. Used GANs to generate synthetic data, resolved class imbalance.	Deep Neural Network (DNN) model for IoT network intrusion detection.CNN, DNN, MLP, and autoencoder models for IoT network security	UNSW-NB15 dataset.	Four attack classes classified in the proposed IDS model.	GANs improved accuracy to 91% by generating synthetic minority attack data.	No specific limitations mentioned in the provided contexts.
[31]	Proposed lightweight IDS model using SFOA-LASSO for SD-IoT security.ML-based IDS model with optimal feature selection for high performance.	Proposed model uses Sheep Flock Optimization Algorithm and Least Absolute Shrinkage.XGBoost, KNN, RF, SVM, and LR are ML algorithms analyzed	SD-IoT dataset	DoS, DDoS, Port Scanning attacks are classified	Achieved accuracy rates of 98.1%	Hit-and-trial method used for feature selection without hyper-parameter tuning
[32]	ELG-IDS enhances IoT network security against RPL internal attacks.ELG-IDS achieves high accuracy rates for various RPL attacks.	Ensemble learning models outperform traditional methods in detecting IoT attacks	Includes Decreased Rank (DR) attack dataset, DIS attack dataset, Version Number (VN) attack dataset	RPL attacks, Insider attack, DoS attacks.	ELG-IDS accuracy rates: 99.18% and Stacking model accuracy: 99.38%	ANN, MLP not adequate for IoT devices
[33]	Efficient IoT device classification and attack detection using SDN-enabled FiWi IoT. Proposed models enhance bandwidth allocation, device identification, and attack detection	CNN model , Proposed SADCAE model	UNSW-NB15, KDDCup99, NSL-KDD Dataset	DoS,SMURF, and Neptune attacks		No data balancing techniques used for IoT classification and attack detection
[34]	Lightweight mini-batch FL approach for IoT attack detection with privacy preservation. Proposed mechanism achieves 98.85% attack detection accuracy with minimal resources	Lightweight mini-batch federated learning	TON-IoT dataset	malicious attacks	Proposed mechanism achieves an overall attack detection accuracy of 98.85%	Federated learning mechanisms have high computational complexities and federation rounds.

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

Ref.	Description	Methods used	Dataset	Attacks classified	Result	Limitation
[35]	IoT security enhanced by machine learning to detect DDoS attacks.Framework integrates SDN and IoT for improved security and access control.	Naive Bayes, Decision Tree, Support Vector Machine.	-	DDOS attack	97.4% accuracy for Naive Bayes, Decision Tree model achieved 98.1% accuracy, SVM classifier achieved 96.1% accuracy	Naive Bayes fails with large datasets and attribute-related data sets
[36]	RRIoT uses RL to detect attacks on IoT devices effectively.Utilizes SAGE to determine feature importance in model performance	RRIoT, DQN, AE-RL, AE-Dueling DQN, RIoT are models	TON-IoT dataset	Attacks classified include scanning, password guessing, and password spraying	Accuracy ranged from 70.95 to 79.94 across different models.	No universal improvements observed when adding a recurrent layer
[37]	Investigates machine learning in IIoT security against cyber-attacks and risks.Reviews vulnerability detection methods and machine learning algorithms for IIoT.	Neural network,Unsupervised learning	NSL-KDD dataset	Side-channel attacks and Network attacks	BLSTM-RNN model has high accuracy with Mirai attack. Proposed architecture claims an accuracy rate of up to 98.50.	High accuracy with Mirai attack, but poor performance on ack attack
[38]	Paper explores ML for IoT security, highlighting trends, challenges, and future vision.Focuses on Generative AI and large language models for enhanced security.	Clustering, supervised learning, Naive Bayes,	Bot-IoT ,CICIDS-2017 ,NSL-KDD ,KDD'99 cup dataset	DDoS, DoS, Heartbleed, PortScan, Bot, and more		Long runtimes during learning, and overfitting risks.
[39]	Proposed intrusion detection method for injection attacks in IoT applications. Utilized feature selection techniques and	Support Vector Machine, Random Forest, Decision Tree	AWID dataset	Injection attacks	Injection attacks classified using decision tree with 99% accuracy	Security solutions for wireless networks have vulnerabilities.

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

Ref.	Description	Methods used	Dataset	Attacks classified	Result	Limitation
	machine learning classifiers for detection. Achieved 99% accuracy using decision tree classifier with 8 features					

Using strong cybersecurity protections to prevent cyberattacks on IoT devices may be the solution. Artificial Neural Networks (ANN), decision trees, and Random Forests (RF) are a few machine learning algorithms that have demonstrated superior accuracy in identifying cyberattacks. RF has been found to be the most optimal technique. Furthermore, high level of precision and accuracy for identifying anomalies in IoT networks has been successfully achieved by deep learning models that incorporate LSTM, BiLSTM, and GRU techniques. Future research may investigate deeper ensemble techniques, federated learning approaches, and deep learning methods to improve anomaly detection in Internet of Things networks.

5. Machine learning techniques for IDS

Modern intrusion detection systems (IDS) rely heavily on machine learning techniques since they can automatically identify and react to cyber threats. Machine learning algorithms can detect unusual patterns suggestive of harmful activity by examining system logs and network data, allowing for proactive security mechanisms. Because of the enormous scale and variety of these deployments, cloud-based centralized architectures show numerous issues from the perspective of [9] ML model training infrastructure in IoT scenarios. excessive bandwidth usage, network resource congestion, load balancing issues, and other issues can result in packet loss, transmission delays, excessive latency, and traffic peaks, all of which can negatively impact training or even render cloud training impossible. Furthermore, the centralization of data may give rise to privacy problems and the necessity of adhering to legislation like the General Data Protection Regulation (GDPR). We find that there is room for improvement in terms of precision, effectiveness, and flexibility when it comes to detecting malicious activity in network data as we continue to explore the field of machine learning-driven intrusion detection. IDS can transform from static rule-based systems to dynamic, intelligent defences that can keep one step ahead of cyber threats by utilizing machine learning [55].

The following are a few typical machine learning methods applied to intrusion detection systems:

A. Supervised Learning Algorithms

- SVM: SVM referred to as support vector machines SVMs are useful in high-dimensional spaces for class separation. By examining features taken from system logs, network traffic, or other data sources, SVMs are trained to differentiate between typical and abnormal behavior. Support Vector Machines (SVMs) create a hyperplane that maximizes the margin between two classes, effectively separating them in the feature space, by training on labeled instances of both harmful and normal activities. By acting as an evaluation boundary, this hyperplane enables SVMs to categorize new instances as either potentially intrusive or normal. Due to unbalanced data, poor feature representation, or subpar hyperparameter tuning, SVM may not be able to detect intrusions with high accuracy, making it impossible to distinguish between legitimate and intrusive instances in the feature space.

- Decision Trees: IDS categorization tasks are a good fit for decision trees because they divide the feature space according to attribute values. DT models are highly adaptable machine learning models that may be used for both regression and classification tasks [40]. The DT model divides the data using a hierarchical structure to allow for precise dataset predictions [41]. Using decision rules, the algorithm iteratively splits the input data into smaller subsets until each subset is associated with a particular class or value.[42] If the number of decision trees increases, a lot more storage is required. Normalization or scaling of the data is not required in Decision Tree [10] when applied to known traffic patterns, decision tree conditions help classify samples and offer a high degree of attack detection accuracy; however, this method is not appropriate for irregular traffic patterns [25]. Three methods can be used to calculate Impurity Measure:- Classification Error, Entropy, and Gini Index.

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

- Neural Networks: In order to use neural networks for intrusion detection in Internet of Things devices, a multi-layered network must be trained to identify patterns of both benign and bothersome behavior from labeled data [57]. The input, hidden, and output layers are made up of interconnected nodes that make up these networks. The input layer uses features that are taken from system logs, network traffic, or sensor data, and the output layer predicts the class label (normal or intrusive). In order to reduce prediction errors during training, the network uses backpropagation to modify its weights and biases. Neural networks provide efficient detection skills by recognizing intricate links in data and adapting to changing threats. Nevertheless, if regularized or validated improperly, they may experience overfitting and necessitate significant computational resources for training.

B. Unsupervised Learning Algorithms

- KNN: A straightforward yet powerful method for detecting intrusions in Internet of Things devices is K-Nearest Neighbours (KNN). In order to classify an instance, KNN first determines how far away it is from other instances in the training dataset. Then, it uses the majority vote of its k nearest neighbours to determine the class label.[44] The measured accuracy values of the ML models RF, NB, and KNN, to detect attacks, are 89%, 75%, and 90%, respectively. The findings demonstrate that the KNN model is superior to other models in terms of accuracy when it comes to detecting assaults with the UNSW-NB15 dataset. However, in large-scale datasets, its accuracy and efficiency can be impacted by the curse of dimensionality, the value of k, and the choice of distance metric [61].

- Autoencoders: Autoencoders are neural network architectures used for unsupervised feature learning. They can reconstruct input data and identify deviations from normal patterns. The input data is compressed into a lower-dimensional latent space representation by an encoder network, and the input data is then reconstructed from this representation by a decoder network. Throughout the training process, the autoencoder gains the ability to reduce the reconstruction error for typical cases. Slight deviations from the reconstructed version when compared to fresh data point to abnormalities or incursions. Due to their lack of reliance on labeled intrusion data, autoencoders are useful for identifying new or undiscovered intrusions [48]. This model will be trained using the genetic algorithm by the sequences of data that represent the normal behavior of the system. And so the model will learn what the normal data looks like so that it can detect abnormal behavior. With the auto-coding approach, author was able to detect new threats with 85% accuracy. Nevertheless, they may have trouble with extremely unbalanced datasets and need meticulous hyperparameter adjustments. However, their capacity to recognize complex patterns and identify anomalies makes them advantageous for detecting intrusions in Internet of Things environments.

C. Ensemble Techniques

- Boosting: Boosting [19] is a recurring procedure that involves adjusting the present weight values based on the values from the past. Algorithms such as AdaBoost enhance overall performance by combining several weak classifiers into one strong classifier. In contrast to SVM and KNN, [43] this work clearly shows that XGBoost and LightXGBoost are better models for detecting spoofing attacks on military IoT devices. This is because these models are not only accurate and detectable, but also require a relatively small amount of memory and detection time—two factors that are crucial for IoT devices operating in combat environments.

- Stacking: To improve detection accuracy, stacking entails training several base models and then merging their predictions using a meta-learner.

- Random Forests: In order to increase the dataset's predicted accuracy, it applies multiple decision trees to different input dataset subgroups and aggregates the outcomes.[47] The RF techniques generate many DTS, each of which is trained with a different subset of the input data and input features. Individual trees each forecast a fresh set of data. Location in the forest, and a majority vote among all the trees determines the final forecast.[45] In comparison to SVM and KNN, which had accuracy rates of 92.80% and 94.7%, respectively, the system discovered that RF had the highest accuracy, at 97.7%. In order to handle high-dimensional data, Random Forest [11] examines the significance of features in resolving overfitting and stability problems, hence decreasing the variance. Because of this, the random forest method can be used to identify and classify dangerous attacks. For noisy data, the random forest is both missing-value aware and resistant to outliers

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

D. Deep Learning Architectures

The deep learning model performs better in highly imbalanced datasets but has a longer training period than the machine learning model that is currently in use [13].

- Artificial Neural Network (ANN): ANNs consist of interconnected nodes organized into layers, with each node performing simple computations. In intrusion detection, ANNs can learn complex patterns from labelled data, such as network traffic or system logs, to distinguish between normal and intrusive behavior. Since ANNs can handle many kinds of data and have flexible model architectures, they are a good choice for identifying a wide range of attacks in Internet of Things contexts. To attain optimal performance, ANNs need to be trained with enough labelled data and have their hyperparameters carefully adjusted. Nevertheless, ANNs are useful for intrusion detection in Internet of Things devices because of their capacity to learn from raw data and adjust to changing threats. ANN [49] achieved a test accuracy of 99.4% in predicting attacks and anomalies on IoT systems

- Long Short-Term Memory (LSTM) and Recurrent Neural Networks (RNNs): These designs can be used for network traffic analysis since they are good at modelling sequential data. Both Long Short-Term Memory (LSTM) networks and Recurrent Neural Networks (RNNs) are useful for detecting intrusions in Internet of Things devices. In order to process sequential input and learn temporal connections in the data, RNNs keep track of information from prior time steps in a hidden state. The vanishing gradient issue, however, makes it difficult for conventional RNNs to capture long-term dependencies. Memory cells and gating mechanisms, which enable them to retain information over longer sequences, are introduced by LSTMs to overcome this problem. LSTMs provide more sophisticated memory retention and are more suited for detecting small anomalies in lengthy data sequences, while RNNs offer a simpler method that might be limited in its capacity to capture long-term dependencies [56].

- Convolutional Neural Networks (CNNs): CNNs excel at extracting hierarchical features from data, which can be valuable in detecting complex intrusion patterns in network packets or logs. Since the CNN model uses the weights from every filter for the full input, it is more efficient than regular neural networks. The model is lighter and requires less memory when it shares weights with a regular neural network rather than establishing a full end-to-end connection since there are fewer learnable parameters.

It's critical to take into account elements like the availability of labelled training data, computational resources, scalability, and the dynamic nature of cyber threats when adopting machine learning algorithms for intrusion detection systems. Additionally, to remain successful in the face of changing attack techniques, models must be continuously updated and monitored

6. Obstacles

Because of the peculiarities of IoT contexts, intrusion detection systems (IDS) for the Internet of Things (IoT) encounter a number of difficulties [59]. These are a few of the main obstacles.

- Heterogeneity: IoT devices are available in a variety of sizes, forms, and features. They may run on different operating systems, have diverse communication protocols, and utilize a range of hardware architectures. Creating a universal IDS solution that can effectively monitor and detect threats across this heterogeneous landscape is challenging.
- Scalability: IoT ecosystems often comprise a massive number of interconnected devices, ranging from sensors and actuators to smart appliances and industrial machines. Scalability becomes a significant concern for IDS, as they must efficiently handle the increasing volume of data generated by these devices without compromising on detection accuracy or performance. IoT devices frequently have processing capacity issues. Additionally, there are a number of services in smart cities that must meet Quality-of-Service standards for availability and integrity.
- Resource Constraints: Many IoT devices have limited memory, processing power, and energy resources. It's possible that traditional IDS solutions require too much memory or processing power to operate directly on these devices. Therefore, designing lightweight IDS algorithms that consume minimal resources while still providing adequate protection is crucial.
- Dynamic Environment: IoT networks are highly dynamic, with devices constantly joining, leaving, or moving within the network. This dynamic nature poses challenges for IDS in maintaining an accurate understanding

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

of the network topology and device behavior. IDS must adapt to these changes in real-time to effectively detect intrusions and anomalies.

- Encrypted Traffic: With the increasing adoption of encryption protocols to secure IoT communications, IDS face the challenge of inspecting encrypted traffic for signs of malicious activity. While decryption can enable deeper inspection, it raises privacy concerns and may not be feasible for resource-constrained devices.
- Data Privacy and Compliance: IoT devices often collect sensitive data about users and their environments. IDS must balance the need for effective threat detection with privacy concerns and regulatory compliance requirements, such as GDPR or HIPAA. This entails developing mechanisms to anonymize or encrypt data without compromising the effectiveness of intrusion detection.
- Zero-Day Attacks: Traditional signature-based IDS may struggle to detect zero-day attacks that exploit previously unknown vulnerabilities. Behavioural and anomaly-based detection techniques are essential for identifying novel threats in IoT environments, but they may also lead to higher false positive rates if not properly tuned.
- Integration with IoT Platforms: IDS solutions need to seamlessly integrate with IoT platforms and management systems to facilitate centralized monitoring, alerting, and response. However, achieving interoperability and compatibility with diverse IoT platforms can be challenging due to proprietary protocols and vendor-specific implementations [60].

Addressing these challenges requires a multidisciplinary approach that combines expertise in networking, cybersecurity, data analytics, and IoT system design. Researchers and practitioners are actively working on developing innovative solutions to enhance the security of IoT ecosystems through improved intrusion detection capabilities.

7. Conclusion

This paper has discussed security concerns at several IoT layers, as well as end-to-end IoT environment security solutions. Various security attacks pertaining to the network, perception, and application layers have been discussed. We also addressed about intrusion detection and the many intrusion detection solutions that it may offer to Internet of Things devices in order to preserve the availability, confidentiality, and integrity of information while also safeguarding the privacy of its users. Afterwards talked about the solutions that researchers have suggested for resolving IoT security issues with machine learning algorithms, emphasizing the reasons behind security issues in IoT-enabled environments. The study's conclusions highlight how critical it is to use machine learning approaches to strengthen IoT system security and shield critical data and infrastructure from dangers. This survey will serve as a roadmap for improving IoT application security.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] Y. Cao, Z. Wang, H. Ding, J. Zhang, and B. Li, “An intrusion detection system based on stacked ensemble learning for IoT network,” Computers and Electrical Engineering, vol. 110, Sep. 2023, doi: 10.1016/j.compeleceng.2023.108836

[2] Praveen, G. Pandian, D. F., C. "IntelliCare: Integrating IoT and Machine Learning for Remote Patient Monitoring in Healthcare: A Comprehensive Framework," Journal of Journal of Cognitive Human-Computer Interaction, vol. 7, no. 2, pp. 50-59, 2024. DOI: https://doi.org/10.54216/JCHCI.070205

[3] M. A. Elsadig, “Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach,” IEEE Access, vol. 11, pp. 83537–83552, 2023, doi: 10.1109/ACCESS.2023.3303113.

[4] N. Prazeres, R. L. de C. Costa, L. Santos, and C. Rabadão, “Engineering the application of machine learning in an IDS based on IoT traffic flow,” Intelligent Systems with Applications, vol. 17, Feb. 2023, doi: 10.1016/j.iswa.2023.200189

[5] S. H. Khan et al., “A new deep boosted CNN and ensemble learning based IoT malware detection,” Comput Secur, vol. 133, Oct. 2023, doi: 10.1016/j.cose.2023.103385.

[6] R. Ahmad, I. Alsmadi, W. Alhamdani, L. Tawalbeh, A deep learning ensemble approach to detecting unknown network attacks, J. Inform. Secur. Appl. 67 (2022) 103196

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

[7] X. H. Nguyen and K. H. Le, “Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model,” Internet of Things (Netherlands), vol. 23, Oct. 2023, doi: 10.1016/j.iot.2023.100851.

[8] H. Nguyen and R. Kashef, “TS-IDS: Traffic-aware self-supervised learning for IoT Network Intrusion Detection,” Knowl Based Syst, vol. 279, Nov. 2023, doi: 10.1016/j.knosys.2023.110966

[9] X. Sáez-de-Cámara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, “Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks,” Comput Secur, vol. 131, Aug. 2023, doi: 10.1016/j.cose.2023.103299

[10] A., A. "Linear Regression and K Nearest Neighbors Machine Learning Models for Person Fat Forecasting," Journal of International Journal of Advances in Applied Computational Intelligence, vol. 3, no. 2, pp. 38-47, 2023. DOI: https://doi.org/10.54216/IJAACI.030204

[11] G. G. Gebremariam, J. Panda, and S. Indu, “Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models,” Alexandria Engineering Journal, vol. 82, pp. 82–100, Nov. 2023, doi: 10.1016/j.aej.2023.09.064

[12] A. Khraisat and A. Alazab, “A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges,” Cybersecurity, vol. 4, no. 1, Dec. 2021, doi: 10.1186/s42400-021-00077-7.

[13] R. K. Muna, M. I. Hossain, M. G. R. Alam, M. M. Hassan, M. Ianni, and G. Fortino, “Demystifying machine learning models of massive IoT attack detection with Explainable AI for sustainable and secure future smart cities,” Internet of Things (Netherlands), vol. 24, Dec. 2023, doi: 10.1016/j.iot.2023.100919.

[14] A. Awajan, “A Novel Deep Learning-Based Intrusion Detection System for IoT Networks,” Computers, vol. 12, no. 2, Feb. 2023, doi: 10.3390/computers12020034

[15] 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, Apr. 2022, doi: 10.1016/j.compeleceng.2022.107810

[16] H. Asgharzadeh, A. Ghaffari, M. Masdari, and F. Soleimanian Gharehchopogh, “Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced Capuchin Search Algorithm,” J Parallel Distrib Comput, vol. 175, pp. 1–21, May 2023, doi: 10.1016/j.jpdc.2022.12.009.

[17] S. M. Kasongo, “A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework,” Comput Commun, vol. 199, pp. 113–125, Feb. 2023, doi: 10.1016/j.comcom.2022.12.010

[18] S. Latif et al., “Intrusion Detection Framework for the Internet of Things Using a Dense Random Neural Network,” IEEE Trans Industr Inform, vol. 18, no. 9, pp. 6435–6444, Sep. 2022, doi: 10.1109/TII.2021.3130248

[19] P. Sanju, “Enhancing intrusion detection in IoT systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks,” Journal of Engineering Research, p. 100122, Jun. 2023, doi: 10.1016/j.jer.2023.100122.

[20] S. Ullah et al., “A New Intrusion Detection System for the Internet of Things via Deep Convolutional Neural Network and Feature Engineering,” Sensors, vol. 22, no. 10, May 2022, doi: 10.3390/s22103607

[21] 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, Apr. 2023, doi: 10.1016/j.compeleceng.2023.108626.

[22] H. C. Altunay and Z. Albayrak, “A hybrid CNN + LSTMbased intrusion detection system for industrial IoT networks,” Engineering Science and Technology, an International Journal, vol. 38, Feb. 2023, doi: 10.1016/j.jestch.2022.101322.

[23] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, “Enhancing IoT network security through deep learning-powered Intrusion Detection System,” Internet of Things (Netherlands), vol. 24, Dec. 2023, doi: 10.1016/j.iot.2023.100936.

[24] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, “Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications,” Sensors, vol. 21, no. 11. MDPI AG, Jun. 01, 2021. doi: 10.3390/s21113654

[25] B. Bala and S. Behal, “AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges,” Computer Science Review, vol. 52. Elsevier Ireland Ltd, May 01, 2024. doi: 10.1016/j.cosrev.2024.100631.

[26] 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, p. 101162, Jul. 2024, doi: 10.1016/j.iot.2024.101162.

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

[27] A. Nazir et al., “A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem,” Ain Shams Engineering Journal, 2024, doi: 10.1016/j.asej.2024.102777.

[28] H. Y. Alshaeaa and Z. M. Ghadhban, “Developing a hybrid feature selection method to detect botnet attacks in IoT devices,” Kuwait Journal of Science, vol. 51, no. 3, Jul. 2024, doi: 10.1016/j.kjs.2024.100222.

[29] A. F. Otoom, W. Eleisah, and E. E. Abdallah, “Deep Learning for Accurate Detection of Brute Force attacks on IoT Networks,” in Procedia Computer Science, Elsevier B.V., 2023, pp. 291–298. doi: 10.1016/j.procs.2023.03.038.

[30] 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, Apr. 2023, doi: 10.1016/j.compeleceng.2023.108626.

[31] C. Kumar and M. S. A. Ansari, “An explainable nature-inspired cyber attack detection system in Software-Defined IoT applications,” Expert Syst Appl, vol. 250, Sep. 2024, doi: 10.1016/j.eswa.2024.123853.

[32] M. Osman, J. He, N. Zhu, and F. M. M. Mokbal, “An ensemble learning framework for the detection of RPL attacks in IoT networks based on the genetic feature selection approach,” Ad Hoc Networks, vol. 152, Jan. 2024, doi: 10.1016/j.adhoc.2023.103331.

[33] P. Malini and D. K. R. Kavitha, “An efficient deep learning mechanisms for IoT/Non-IoT devices classification and attack detection in SDN-enabled smart environment,” Comput Secur, vol. 141, Jun. 2024, doi: 10.1016/j.cose.2024.103818.

[34] M. S. Ahmad and S. M. Shah, “A lightweight mini-batch federated learning approach for attack detection in IoT,” Internet of Things (Netherlands), vol. 25, Apr. 2024, doi: 10.1016/j.iot.2024.101088.

[35] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, “Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks,” Eng Appl Artif Intell, vol. 123, Aug. 2023, doi: 10.1016/j.engappai.2023.106432.

[36] C. Rookard and A. Khojandi, “RRIoT: Recurrent reinforcement learning for cyber threat detection on IoT devices,” Comput Secur, vol. 140, May 2024, doi: 10.1016/j.cose.2024.103786.

[37] C. Ni and S. C. Li, “Machine learning enabled Industrial IoT Security: Challenges, Trends and Solutions,” Journal of Industrial Information Integration, vol. 38. Elsevier B.V., Mar. 01, 2024. doi: 10.1016/j.jii.2023.100549.

[38] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, “Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models,” Internet of Things and Cyber-Physical Systems, vol. 4. KeAi Communications Co., pp. 167–185, Jan. 01, 2024. doi: 10.1016/j.iotcps.2023.12.003.

[39] T. Gaber, A. El-Ghamry, and A. E. Hassanien, “Injection attack detection using machine learning for smart IoT applications,” Physical Communication, vol. 52, Jun. 2022, doi: 10.1016/j.phycom.2022.101685.

[40] A. Nazir et al., “Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets,” Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 10. King Saud bin Abdulaziz University, Dec. 01, 2023. doi: 10.1016/j.jksuci.2023.101820.

[41] Y.-Y. Song, L. Ying, Decision tree methods: applications for classification and prediction, Shanghai Arch. Psychiatry 27 (2) (2015) 130.

[42] IBM, What is machine learning and machine learning techniques, 2023, https: //www.ibm.com/topics/machine-learning, [Online Accessed : 25 Nov 2023].

[43] H. El Alami, K. Hall, and D. B. Rawat, “Comparative Study of Machine Learning Techniques for Detecting GPS Spoofing Attacks on Mission Critical Military IoT Devices,” in 2023 IEEE International Conference on Communications Workshops: Sustainable Communications for Renaissance, ICC Workshops 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 512–517. doi: 10.1109/ICCWorkshops57953.2023.10283613

[44] A. Sharma, H. Babbar, and A. K. Vats, “Detection of Attacks in Smart Healthcare deploying Machine Learning Algorithms,” in 2023 4th International Conference for Emerging Technology, INCET 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/INCET57972.2023.10170367

[45] A. Sharma and H. Babbar, “LUFlow: Attack Detection in the Internet of Things Using Machine Learning Approaches,” in 2nd IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, ICDCECE 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICDCECE57866.2023.10150813

[46] P. A. A. Resende and A. C. Drummond, “A survey of random forest based methods for intrusion detection systems,” ACM Computing Sur veys (CSUR), vol. 51, no. 3, pp. 1–36, 2018.

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024

[47] A. Sharma and H. Babbar, “Machine Learning-Based Anomaly Detection in the Internet of Things,” in 2023 3rd Asian Conference on Innovation in Technology, ASIANCON 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ASIANCON58793.2023.10270100.

[48] A. Khamoun, R. M. Ziani, O. Salem, and A. Mehaoua, “Using Genetic Algorithms to Detect Intrusions for IoT Systems,” in 2023 IEEE International Conference on E-Health Networking, Application and Services, Healthcom 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1–6. doi: 10.1109/Healthcom56612.2023.10472377

[49] M. Hasan, M. Milon Islam, M. Ishrak Islam Zarif, and M. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” 2019, doi: 10.1016/j.iot.2019.10.

[50] O. Embarak, M. Algrnaodi, “Deep Learning Fusion for Attack Detection in Internet of Things Communications”, Journal of Fusion: Practice and Applications, vol. 9, no. 2, pp. 27-47, 2023. doi: https://doi.org/10.54216/FPA.090203.

[51] E. Kazia, “Machine learning for False Information Detection in Social Internet of Things”, Journal of Fusion: Practice and Applications, vol. 10, no. 1, pp. 38-77, 2023. doi : https://doi.org/10.54216/FPA.100103.

[52] Mahmoud Zaher, Nabil M. Eldakhly, “Secured Intrusion Detection in Adhoc Networks”, International Journal of Wireless and Ad Hoc Communication, Vol. 5, No. 2, pp. 30-49. 2023. doi : https://doi.org/10.54216/IJWAC.050203

[53] Mahmoud A. Zaher , Nabil M. Eldakhly, “Cyber Attack Detection in Wireless Adhoc Network using Artificial Intelligence”, International Journal of Wireless and Ad Hoc Communication, Vol. 6 , No. 2 , pp. 18-33. 2023. doi : https://doi.org/10.54216/IJWAC.060202

[54] S.P. Samyuktha , Dr.P. Kavitha , V.A Kshaya , P. Shalini , R. Ramya, “A Survey on Cyber Security Meets Artificial Intelligence: AI– Driven Cyber Security”, Journal of Cognitive Human-Computer Interaction, Vol. 2, No. 2, pp. 50-55, 2022. doi : https://doi.org/10.54216/JCHCI.020202

[55] Gande Akhila , Hemachandran K , Juan R Jaramillo, “Indian Premier League Using Different Aspects of Machine Learning Algorithms”, Journal of Cognitive Human-Computer Interaction, Vol. 1, No. 1, pp. 01-07, 2022. doi : https://doi.org/10.54216/JCHCI.010101

[56] Mahmoud A. Zaher , Nabil M. Eldakhly, “Brain Storm Optimization with Long Short Term Memory Enabled Phishing Webpage Classification for Cybersecurity”, Journal of Cybersecurity and Information Management, Vol. 9, No. 2, pp. 20-30, 2022. doi : https://doi.org/10.54216/JCIM.090202

[57] Nagamalla, V. karkee, J. Kumar, R. "Integrating Predictive Big Data Analytics with Behavioral Machine Learning Models for Proactive Threat Intelligence in Industrial IoT Cybersecurity," Journal of International Journal of Wireless and Ad Hoc Communication, vol. 7, no. 2, pp. 08-24, 2023. DOI: https://doi.org/10.54216/IJWAC.070201

[58] Ossama H. Embarak, Raed Abu Zitar, “Securing Wireless Sensor Networks Against DoS attacks in Industrial 4.0”, Journal of Intelligent Systems and Internet of Things, Vol. 8, No. 1, pp. 66-74, 2023. doi : https://doi.org/10.54216/JISIoT.080106

[59] Reem Atassi, Aditi Sharma, “Intelligent Traffic Management using IoT and Machine Learning”, Journal of Intelligent Systems and Internet of Things, Vol. 8, No. 2, pp. 08-19, 2023. doi : https://doi.org/10.54216/JISIoT.080201

[60] Ahmed Mohamed Zaki, Abdelaziz A. Abdelhamid, Abdelhameed Ibrahim, Marwa M. Eid, El-Sayed M. El-Kenawy, “Metaheuristic Optimization for Enhancing Cyber Security Index Prediction: A DTO+FGW Approach with MLP Integration”, International Journal of Advances in Applied Computational Intelligence, Vol. 4 ,No. 2,pp. 15-25, 2023. doi : https://doi.org/10.54216/IJAACI.040202

[61] Alshaimaa A. Tantawy, “Linear Regression and K Nearest Neighbors Machine Learning Models for Person Fat Forecasting”, International Journal of Advances in Applied Computational Intelligence, Vol. 3 , No. 2 , pp. 38-47, 2023, doi : https://doi.org/10.54216/IJAACI.030204

DOI: https://doi.org/10.54216/JCIM.140227
Received: January 30, 2024 Revised: April 11, 2024 Accepted: July 14, 2024