Foundation University Journal of Engineering and Applied Sciences

FUJEAS
Vol. 4, Issue 2, 2023.
DOI:10.33897/fujeas.v4i2.779

Review Article

Article Citation:
Soofi et al. (2023). "Securing the Internet of Things: A Comprehensive Review of Security Challenges and Artificial Intelligence Solutions". *Foundation University Journal of Engineering and Applied Sciences*
DOI:10.33897/fujeas.v4i2.779

Published by
Foundation University
Islamabad.
Web: https://fui.edu.pk/

Securing the Internet of Things: A Comprehensive Review of Security Challenges and Artificial Intelligence Solutions

Aized Amin Soofi [a], Muhammad Tahir [b, *], Naeem Raza [a]

[a] Department of Computer Science, NUML Faisalabad Campus, Faisalabad, Pakistan
[b] Department of Engineering and Computer Science, NUML Faisalabad Campus, Faisalabad, Pakistan

* **Corresponding author**: dr.tahir@numl.edu.pk

Abstract:

One of the major needs and challenges of this century is the use of cutting-edge technology considering the industry 4.0 revolution. The Internet of Things (IoT) falls in the category of a cutting-edge example of such innovation in the computing and information industry. In IoT compared to classical networking methods practically; every device we employ is accessible at any time from any location. Nevertheless, IoT continues to encounter several security challenges, and the magnitude of cyber-physical security risks is escalating alongside the widespread use of IoT technologies considering Moore's laws expected to be 30 billion devices by 2025. IoT will continue to face vulnerabilities and risks unless there is a comprehensive understanding and proactive approach towards tackling its security concerns. To ensure both the cyber and physical security of IoT devices during data gathering and sharing, it is imperative to evaluate security considerations, identify instances of cyber-attacks, and implement effective security protocols at multiple layers for making highly secured IoT. Conventional security measures like data classification, strict access controls, monitoring privileged account access, encrypting sensitive data, security awareness training, network segregation, segmentation cloud security, application security, patch management, and physical security employed in the realm of IoT are inadequate in light of the current security difficulties posed by the proliferation of sophisticated attacks and threats. Utilization of artificial intelligence (AI) techniques, especially machine and deep learning models is becoming a compelling and effective approach to enhance security of the IoT devices. This research article presents a comprehensive review of the key aspects of IoT security, including the challenges, potential opportunities, and AI-driven solutions. The primary goal of this article is to provide technical resources for cybersecurity experts and researchers working on IoT initiatives.

Keywords: Internet of Things; IoT Security; Artificial Intelligence; Deep Learning; Machine Learning; Cyber and Physical Security; Industry 4.0.

1. Introduction

IoT is a decentralized network. It connects devices and humans. This connection is via the internet. IoT makes device connectivity possible. Any object reachable via IoT is a "thing". Even home appliances can be "things". "Things" can communicate via IoT. They provide useful data. Sensors and machine learning are IoT subsets [1], [2]. They enable real-time analysis. Smart devices share collected data. This data helps in daily tasks. Figure 1 shows the IoT concept. It connects people and objects.

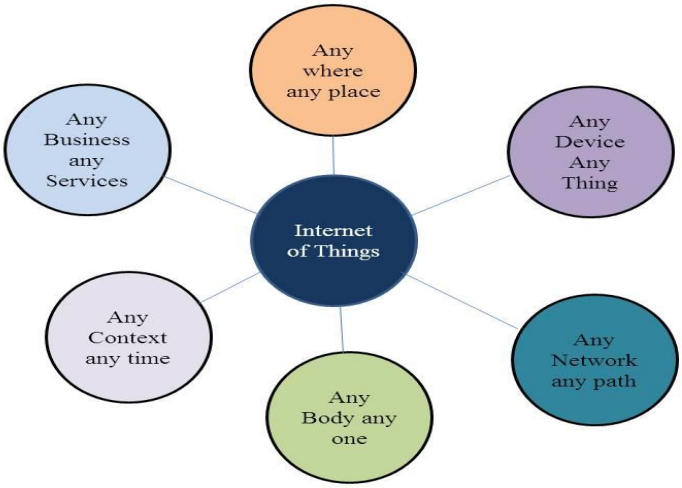

Figure 1: IoT definition [20]

There are no time or place limits. "IoT security" is a term used. It refers to IoT system safety [3]. These systems are internet-dependent. Hence, they are hacker targets. IoT implementation needs network security. IoT networks are large-scale. They pose new challenges. Data management is one such challenge. IoT security is crucial. It protects sensitive data. This data is sent by IoT devices [4], [5], [6]. It prevents data theft. It also prevents privacy breaches. Strong security measures are needed. They prevent cyberattacks. They also prevent breaches. Such incidents can disrupt IoT systems. They can cause substantial damages. Healthcare has widespread IoT implementations. Transportation is another such area [7], [8]. Energy grids also use IoT. These systems need reliable security measures. Organizations must follow security standards. They must also follow laws. This ensures legal compliance. It also reduces related risks [9], [10], [11]. Inadequate IoT security has severe consequences. Data breaches are one such consequence. Financial setbacks are another one. It can harm reputation. It can lead to legal responsibilities. It can also risk public safety [12], [13], [14]. Therefore, it is crucial to establish and give priority to security measures for the IoT to promote the durability and long-term viability of IoT ecosystems in a world that is becoming more networked and digital [15].

Some of the potential attacks that need to be addressed for secure IoT systems include; spoofing, eavesdropping, tampering, jamming, denial of service (DOS), etc. [16]. Traditional methods of handling security incidents are ineffective because of the recent surge in sophisticated menaces and invasions and the complexity of these incidents. Therefore, protecting the IoT system requires a powerful security system utilizing cutting-edge technologies that can handle the challenges. As a key component of the 4.0 industrial revolution; AI provides the most promising avenues for creating smart systems [17]. To provide a dynamic and up-to-date security solution for the IoT; we can take leverage of artificial intelligence (AI) knowledge, specifically machine learning (ML) and deep learning (DL), to identify anomalies or undesirable malicious activities. The security of data is analyzed using ML or DL models, which offers a collection of regulations, protocols, and complex mathematical functions for transferring data [18]. Well-known AI techniques like ML and DL models like artificial neural network (ANN), and convolutional neural network (CNN) can aid IoT devices in learning from experiences represented as data and adapting their behavior accordingly [6, 19].

Typically, an IoT network or system operates at different layers, Section 2 has covered the three primary levels of IoT architecture. Different types of cyber and physical threats are associated with each layer of IoT. Practically multiple AI techniques can be adopted to ensure IoT security like classification, regression, clustering, rule-based, DL, and hybrid models. In this article, an attempt is made to discuss the different security threats in IoT environments with their AI-based available solutions in the literature.

The subsequent sections of this research article are structured as follows; IoT architecture has been discussed in section 2, and characteristics of IoT networks are presented in section 3. In section 4 role

of ML and DL techniques in IoT security has been discussed. Classification strategies for the security of IoT have been addressed in section 5 while regression techniques have been discussed in section 6. Section 7 contains the discussion about clustering techniques for IoT security. Section 8 of the document has covered the application of DL techniques for enhancing security in the IoT. Potential challenges and opportunities have been addressed in section 9. Table 6 specifically summarizes the AI techniques with their advantages and disadvantages in IoT environments with security applications. Table 1 depicts a list of notations used and their definitions used in this research.

Table 1: List of notations used in securing IoT

Notation	Definition	Notation	Definition
IoT	Internet of Things	WSN	Wireless Sensor Network
ANN	Artificial Neural Network	DNN	Deep Neural Network
CNN	Convolutional Neural Network	MLP	Multi-Layer Perception
ML	Machine Learning	NS2	Network Simulator-2
DL	Deep Learning	NIDS	Network Intrusion Detection System
AI	Artificial Intelligence	DSRC	Dedicated Short-Range Communication
M2M	Machine to Machine	RNN	Recurrent Neural Network
M2G	Machine to Gateway	D2D	Device-to-Device Communication
M2C	Machine to Cloud	KNN	K-Nearest Neighbor
SVM	Support Vector Machine	LR	Logistic Regression
DDoS	Distributed Denial of Service	GMM	Gaussian Mixture Model
DoS	Denial of Service	IDS	Intrusion Detection System
RF	Random forest	BLR	Binary Logistic Regression
RR	Ridge Regression	DT	Decision Tree

2. IoT Architecture

IoT signifies a significant change in the world of information technology. The phrase "Internet of Things," often shortened to IoT, combines two critical terms: "Internet" and "Things." In this context, "Things" refers to intelligent gadgets or objects. Many companies and research organizations explain IoT and smart environments in various ways and from various angles.

IoT, as described in [21], refers to a combination of physical hardware components and a digital transmission of data that relies on RFID tags. According to the Institute of Electrical and Electronics Engineers (IEEE) [22], the IoT is defined as a network of interconnected things equipped with sensors that are connected to the Internet. Because no universally accepted model for the IoT architecture has been developed, many models have recently been presented [23]. A three-tier generic architecture for IoT has been depicted in Figure 2 which contains a perception layer, network layer, and application layer.

The perception layer is the foundational layer of the architecture of the IoT paradigm and is mostly called the brain of three-layered architecture, but in real terms, it is a physical layer. This layer in IoT design is of utmost importance as it acts as the interface connecting the physical and digital domains [24]. It enables the smooth integration of data from the physical environment into digital systems. The

perception layer consists of sensors, actuators, and data-collecting devices that allow for the real-time capture of contextual information about the surrounding environment, objects, and events [25]. The primary function of this layer is to serve as the sensory component of IoT systems, collecting a wide range of data including temperature, motion, sound, and light intensity [26, 27].

In the network layer, data is transferred and processed based on what was sensed from objects in the perception layer. It is the glue that binds the IoT together, linking up computers, servers, and other smart devices [28]. Machine-to-machine (M2M), machine-to-gateway (M2G), machine-to-cloud (M2C), and backend data sharing are all facilitated by this layer [29]. The network layer also serves as the fundamental framework of IoT infrastructure, incorporating a wide array of networking technologies, protocols, and standards designed to meet the specific needs of IoT ecosystems, such as scalability, dependability, and energy efficiency [30]. The application layer is the highest-level layer of the IoT structure [31] responsible for intelligent services at a high level delivered by this layer to meet the requirements of the customers [32]. This layer functions as the visible interface and coordinator of capabilities in IoT architecture [33, 34]. It converts raw data into practical insights and provides value-added services to end-users. Furthermore, it facilitates smooth incorporation with current corporate procedures and IT systems, unlocking fresh sources of income, improving customer experiences, and promoting digital transformation in many sectors [35].

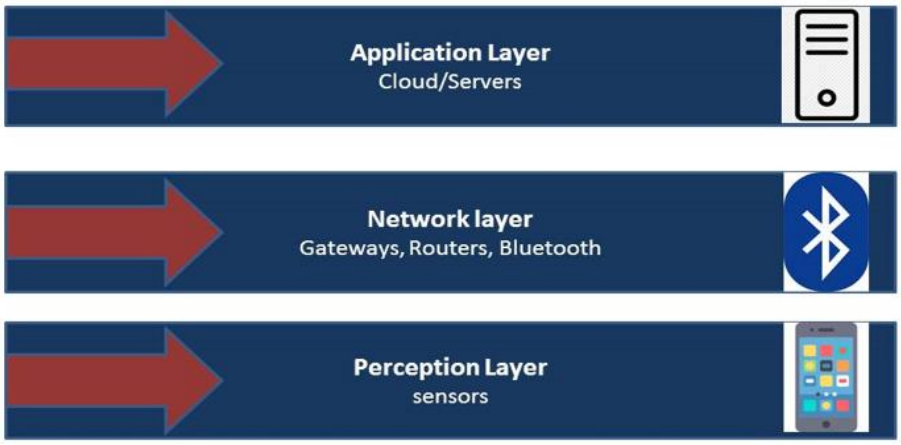

Figure 2: Three-Tier IoT architecture

3. Characteristics of IoT Networks

Security and privacy measures that have been used in traditional networks may not be effective on IoT networks due to the constantly changing and connected nature of IoT poses unique security challenges because of the following characteristics described here.

3.1. Massive Scale Deployment

There is a belief that the numerous interconnected devices approximately in billions communicating with each other through the Internet will eventually outstrip the existing Internet's capabilities. Implementing IoT on a massive scale also presents difficulties, such as creating networking and storage infrastructure for smart devices, developing effective data communication standards, identifying and safeguarding against malicious attacks, standardizing technologies, and creating consistent device and application interfaces [36].

3.2. Heterogeneity

Within an IoT network, many distinct devices possess various capabilities, characteristics, and communication protocols exists. These devices may employ different communication standards, and communication paradigms, and may have varying limitations on their hardware resources creating

problems from smaller scale to larger scale on different layers [37].

3.3. Intelligence

The capability of IoT to make wise judgments quickly and intelligently is one of its most alluring aspects. To extract meaning from the data generated by IoT devices and take action based on the processed data, it must be processed in a meaningful way [38].

3.4. Efficient and Affordable Communication

In order to achieve optimal network performance for IoT devices, it is necessary to implement solutions that have both ultra-low power consumption and cheap cost. These solutions require due to the massive connectivity involved and that is only possible by designing efficient protocols for routing of data on the network layer and by designing applications considering web 3.0 development.

3.5. Safety

Alongside other characteristics, ensuring safety is crucial for the effective operation of IoT networks. Both customers and devices must take safety precautions due to the proliferation of IoT devices, which might potentially jeopardize the security of personal data transmitted through these devices. Furthermore, the safety and secrecy of the gadgets themselves are also crucial considerations.

3.6. Dynamic Changes

Efficient management of a vast number of devices is necessary for IoT. These devices operate dynamically, adjusting to the needs of the application. Factors such as the device's sleep/wake time, internet usage, and direct communication must also be incorporated into IoT networks.

3.7. Proximal Communication

Another notable characteristic of the IoT is the ability for devices to communicate with one another in close proximity, without the need for a central authority like base stations. Device-to-device communication (D2D) makes use of the inherent characteristics of communication from device to device, which include Dedicated Short-Range Communication (DSRC) and similar innovations. The conventional architecture of the internet largely emphasizes network-centric interaction. The division of service providers and networks has made it easier for devices and content to communicate with one another, expanding the range of services available in the IoT [39].

3.8. Interconnectivity

The term IoT describes the linking of devices and their ability to communicate with each other, much like a dialogue. As a result, networks connected to the IoT may be accessible whenever and anywhere, day or night [40].

4. Securing IoT with ML and DL Techniques

The utilization of AI techniques, specifically ML and DL, is widely recognized as a means for IoT devices to acquire knowledge from data and subsequently adjust their behavior accordingly. Learning models utilized for this purpose usually consist of a collection of principles, methodologies, or advanced transfer functions that can be applied to identify significant security incident patterns in IoT data to predict and detect behavior [41]. Consequently, in the realm of IoT, both ML and DL can function effectively within ever-changing IoT networks without the need for human intervention or involvement. Figure 3 depicts how ML and DL techniques have the potential to create a data-focused model for IoT security intelligence. Various ML techniques can be employed to gain insights from IoT security data, such as

regression and classification analysis, rule-based methods, clustering, and feature optimization methods [42, 43].

DL techniques that rely on artificial neural networks (ANN), such as convolutional networks, multi-layer perceptron networks, and recurrent networks, can also be utilized to secure IoT networks from different types of attacks [44, 45]. A significant utilization of DL algorithms is mostly for the purpose of anomaly identification, whereby they instantly detect and stop any breaches or cyber threats by analyzing real-time network traffic and device behavior [46]. Moreover, these models exhibit outstanding proficiency in detecting and examining coding patterns and network linkages, therefore bolstering the IoT devices' security against malicious software. The DL expertise encompasses verification along with access control, bolstering safety protocols by employing biometric identification, and behavioral evaluation to strengthen defense against illegal access [47]. DL approaches are utilized to strengthen the security of communication amongst IoT devices through the implementation of encryption and decryption strategies. This guarantees the preservation of data confidentiality and integrity.

The subsequent section will address the application of various machine and DL methods in the field of security solutions inside the IoT framework. Various techniques have been discussed with their primary aim, dataset, and accuracy. The utilization of ML and DL techniques in IoT applications also presents novel challenges. These challenges are multifaceted, including the difficulty of creating an appropriate model to process data from various IoT applications. Likewise, accurately categorizing incoming data is consequently a tedious operation [48]. Another obstacle is the utilization of a limited amount of labeled data throughout the learning process. Deploying these models on IoT devices with limited resources presents additional problems since it is crucial to minimize processing and storage overhead.

5. Classification Techniques in IoT Security

Classification is one of the popular ML approaches in which an object can be placed into one of several predetermined classes using its attributes [49, 50]. Classification techniques serve as an effective protective mechanism [51]. Through the analysis of network traffic and device activity, classification algorithms are capable of identifying unauthorized devices, classifying lawful ones based on their purpose, and detecting irregularities that indicate potential security risks [52]. This enables the implementation of focused security protocols, the automatic identification of potential risks, and the enforcement of restricted access privileges [53]. Classification enhances IoT security by providing it with the ability to discern between regular and malicious activities, thus protecting the entire network [54]. A summary of classification techniques used for IoT security has been presented in Table 2. In IoT security, a classification task typically entails forecasting a defined discrete value or category, such as normal or anomaly data, and type of attack such as attack-1, attack-2, attack-3, etc. A few commonly used classification techniques include k-nearest neighbors(KNN) [55], support vector machines (SVM) [56], naive bayes [57], random forest (RF) [58], and decision trees [59]. These techniques can be applied to classify security incidents and mitigate various IoT security concerns, such as detecting intrusions or attacks, analyzing malware, and identifying anomalies or fraudulent behavior within IoT systems. KMANB algorithm [60] was designed to secure an IoT network from anomalies like trojans, worms, passwords, backdoors and DDoS attacks. In the proposed approach K-means clustering algorithm was used to group the anomalies data and the naive bayes algorithm was used to detect the anomalies. The anomaly detection accuracy of the proposed algorithm on the ToN_IoT dataset was between 90% to 100%. Statistical results also show the improved speed, accuracy, flexibility and scalability of the proposed technique.

In [61] a technique named NBC-MAIDS was introduced in which Naive Bayes classification algorithm was applied in IDSs to overcome the Distributed Denial of Service (DDOS) attacks in IoT networks. Naive Bayesian distinguisher model was presented in [62] in which the packet loss state was captured and classify the packet loss type in an IoT network. In this approach, NS2 simulator was used that showed up to 95% classification accuracy with improved throughput and friendliness in the network. IoT-based cyber security of drones was ensured in [63] for the prevention of DoS, jamming, and

spoofing attacks. In this approach, a Naive Bayes algorithm was used with the KDD'99 dataset and experimental results showed 96.3% accuracy. Although this approach provides 96.3% accuracy but one of the problems with this approach is that it uses two layers of processing that cause the independence between information in predicting items.

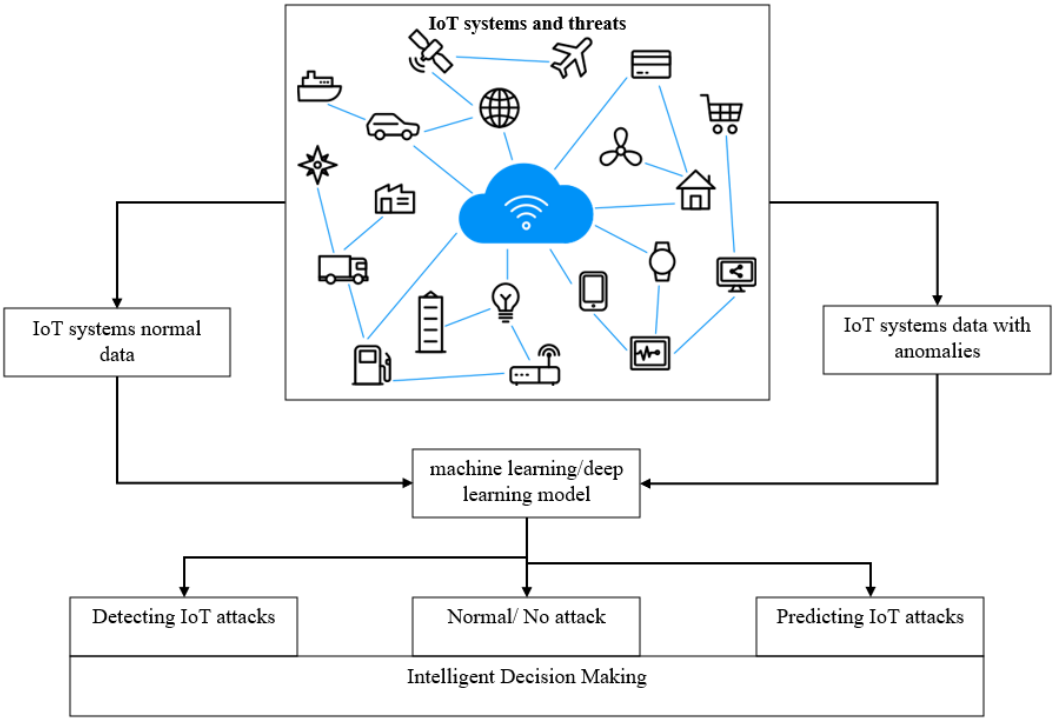

Figure 3: Potential role of the ML and DL modeling for IoT security intelligence

Digital identification techniques have been introduced in [64] to prevent digital ID spoofing attacks in IoT devices. In the proposed technique signals were collected from eighteen WiMAX radio devices. This technique defeats spoofing attacks through feature-reduced RF-DNA fingerprints and an SVM (Support Vector Machine) classifier with a true verification accuracy of 97.8%. In [65] a model was proposed that provides detection against DDoS attacks in IoT networks using Naive Bayes and the KNN classifier. The proposed model was trained on the BoT-IoT dataset in which two data sets were used, one was a real-time dataset and the second was a class-balanced dataset. The accuracy of Naïve bayes algorithm on real time dataset and class balanced dataset was 99.4% and 55.1% respectively. The accuracy of KNN algorithm on real time dataset and class balanced dataset was 99.6% and 92.1% respectively.

Table 2: Classification techniques in IoT security

Author	AI approach	Security objective	Dataset/data collection	Accuracy
[60]	Naive Bayes	anomaly detection	ToN_IoT dataset	90-100%
[61]	Naive Bayes	DDOS attack prevention	realtime	-
[62]	Naive Bayesian	Packet loss detection	NS2 simulator	95%
[66]	Naive Bayes	anomaly detection	UNSW-NB15 dataset	92.48%

[63]	Naive Bayes	Prevent DoS attacks, jamming and spoofing	Drone KDD'99 dataset	96.3%
[65]	KNN, Naive Bayes	DDoS attack prevention	BoT-IoT dataset	99.6% & 99.4%
[64]	SVM	digital ID spoofing attacks	Multiple WiMAX radio	97.8%
[67]	SVM	Malware attack	14 different malware	98.9 % – 99.8%
[68]	SVM	Abnormal behavior profiling	Mica2Dot sensors	93.7 %
[69]	SVM	Secure data sharing platform	BCWD and HDD	90.35% and 93.89%
[70]	RF	Intrusion detection	NSL-KDD, UNSW-NB15, and GPRS	95.5%
[71]	RF	DDOS attack prevention	Real-time traffic by using Raspberry Pi v3	99%
[72]	KNN	Detect unauthorized access	Bot IoT dataset	92.29%
[73]	KNN/SVM/RF	Malware and intrusion detection	Aposemat IoT-23	89.80% to 92.96%
[74]	Decision tree (DT)	Intrusion detection	NSL-KDD	83.14%

To detect a malware attack on Android devices an experimental approach was used [67] in which fourteen different malware were analyzed by using different ML algorithms. The results show that the proposed SVM approach provides 99.8% accuracy on DroidKungFu and zitmo malware and 98.9% on FakeInst malware. Abnormal behavior profiling of IoT devices was performed in [68] by considering four factors including temperature, humidity, light, and voltage. The data was collected by deploying Mica2Dot sensors in a real-time environment. The SVM algorithm was used to train normal and abnormal datasets. The results show 93.7% accuracy in normal datasets and 69.5% accuracy in abnormal datasets when the malicious user modified data. In [69] SVM training scheme named secureSVM was proposed to build a secure data-sharing platform for IoT network's homomorphic cryptosystems. In which the SVM algorithm is applied to two real-world datasets, namely the Heart Disease Data Set (HDD) and the Breast Cancer Wisconsin Data Set (BCWD). The accuracy of the proposed algorithm was 90.35% in the case of the BCWD dataset and 93.89 in the case of the HDD dataset. This proposed technique helped overcome the challenges of data integrity and data privacy in the transmission of data in IoT networks.

In [70] a parameterized, efficient RF classifier was presented to enhance anomaly detection in IoT networks. The experiment included three different data sets (NSL-KDD, UNSW-NB15, and GPRS) and ten different classifiers (each of which was assessed based on the number of trees in its ensemble). Statistical analysis showed that RF-800 outperformed competing classifiers with 95.5% accuracy. DDoS detection using an RF classifier was performed in [71]. The premise upon which the selection of characteristics was based was that consumer IoT devices generate network traffic that is fundamentally

different from that generated by the well-studied but non-IoT networked devices. An experimental consumer IoT device network's regular and DoS attack traffic was used to evaluate five different ML classifiers including RF. The accuracy on the test set was greater than 99% for all five algorithms.

A KNN approach was proposed [72] to detect vulnerabilities in IoT networks. The attack detection module employs a DL and ML technique, and this approach was evaluated using a bot-IoT dataset with an accuracy of 92.29%. In [73] three classification techniques were implemented and tested on the Aposemat IoT-23 dataset. Accuracy levels for intrusion detection attained by the RF, SVM, and KNN were 92.96%, 86.23%, and 91.48%, while those for malware detection were 92.27%, 83.52%, and 89.80%, respectively. Three decision trees were utilized in a hybrid categorization system [74] in which results were compared with SVM and KNN. The result showed that the proposed approach perform better with an accuracy of 83.14% for intrusion detection as compared to the other two approaches but in [70] RF approach has been applied on the same dataset with 95.5% accuracy.

5.1. Review of classification techniques in IOT security

We can conclude that the performance of KNN, Naive Bayes, and RF-based classification approaches are best for DDOS attack prevention on both data sets i.e.; real-time and previously available. While the SVM approach is good for intrusion detection and some specific types of malwares but SVM-based models are complex and challenging to understand and interpret. Additionally, decision trees and RF techniques can be used to classify IoT data and predict potential security threats. The building nature of DT necessitates vast storage facilities. Using only a small number of DTs makes DT-based approaches straightforward to grasp. These techniques can be used in conjunction with other security measures, such as encryption and authentication, to enhance the overall security of IoT systems.

6. Regression Techniques in IoT Security

Most of the time, regression analyses are used to make forecasts and predictions, which is a big part of the field of ML. In some cases, regression analysis can also be used to figure out how the independent and dependent variables are related to each other [75]. Through the examination of patterns in sensor data, regression models have the capability to forecast potential device failures, allowing for preemptive maintenance and the avoidance of security weaknesses [76]. Furthermore, they contribute to the optimization of resources by efficiently allocating resources such as power and bandwidth based on device activity. A summary of regression techniques in IoT security has been presented in Table 3. In [77] a Network Intrusion Detection System (NIDS) is tailored to resource-limited WSN (Wireless Sensor Network) and IoT nodes. In which the offline training stage involved the creation of detection modules using Binary Logistic Regression (BLR). These modules were trained using benign local node activity and malicious behavior from two typical routing attacks. The authors determined that utilizing training data from a single network topology was enough for identifying assaults in comparable network topologies, taking into account their size and network density. Accuracy ratings of the proposed system ranged from 96% to 100% throughout the real-time evaluation phase.

In [78] several different ML methods were used on the data. The dataset was subjected to five rounds of cross-validation testing with each method. It was proved with experiments that the logistic regression (LR) approach performed well in the first two-fold testing phases after that its performance became weak. The average efficiency of linear regression was 98.3%. A Smart Cybersecurity Framework [79] for IoT-Empowered Drones was presented in which LR and RF techniques were merged to provide better security on a collected dataset. The accuracy of the proposed framework was 98.58% while the accuracy of simple LR and RF approaches was 92.23% and 92.36% respectively.

Modeling of DDoS attacks [80] in IoT networks using ML has been performed. Researchers looked at how well and quickly several ML methods (supervised, unsupervised, and semi-supervised) could spot DDoS threats in IoT. The DARPA dataset was used for experimental purposes. The result shows 97.93% accuracy in the case of RR and 98.60% accuracy in the case of LR. A LogitRegTrust model [81] was proposed to ensure authentication and prevent black hole attacks in IoT networks. Reputation score was used in this approach to compute trust and the indirect trust value of the node was computed

Table 3: Regression techniques in IoT security

Author	AI approach	Security objective	Dataset/data collection	Accuracy
[77]	BLR	Intrusion detection (Blackhole attack)	Run-Time Monitoring Tool (RMT)	96% - 100%
[78]	LR	Multiple anomaly detection	Open-source dataset	98.3%
[79]	LR & RF	Detection of DoS and probe attacks	IoT data from drones, sensors, and network information	98.58%
[80]	RR and LR	DDOS attack prevention	DARPA	RR: 97.93% LR: 98.60%
[81]	LR	Blackhole attack detection	COOJA simulator	-
[82]	Nonlinear regression	Malware detection (botnet attacks)	Malware analysis for 1425 files was conducted.	98.75%

using local trust in the Trust-based RPL while using global trust in the proposed model. In a laboratory setting, [82] deliberately infected nine commercial IoT devices using two well-known IoT-based botnets, Mirai and BASHLITE. The projected results demonstrated the recommended strategy's ability to accurately and swiftly detect the assaults as they were being launched from the compromised IoT devices that were part of a botnet. The tests demonstrate a remarkable accuracy of 98.75%.

6.1. Review of Regression Techniques in IoT Security

Regression techniques can play a role in IoT security by helping to identify patterns and relationships in IoT data that can indicate security threats or vulnerabilities. For example, linear and LR can be used to analyze IoT sensor data and identify unusual patterns or anomalies that may indicate a security breach. Regression techniques are good for attack detection and mitigation, malware analysis, anomaly and intrusion detection.

7. Clustering Techniques in IoT Security

Clustering is a process of grouping similar data points into clusters. The goal of clustering is to discover natural groupings or patterns in the data, without any prior knowledge about the groupings. Clustering results in data partitioning. Each cluster contains similar data points. Clustering is an unsupervised learning method. It discovers patterns in unlabeled data. Hidden patterns can be revealed by clustering. It helps identify IoT anomalies. Table 4 summarizes IoT security clustering. A method was proposed in [83]. It examines network attack patterns. It suggests an IoT intrusion detection technique. A node authority management approach based on traffic restriction was suggested to increase the security of IoT communication and lessen the downsides brought on by algorithm detection failures. A data intrusion detection technique was developed, which is based on K-means clustering and is highly efficient.

In [84] three scenarios were used in the experiments employing wireless communication: regular traffic, attack traffic, and mixed normal-attack traffic. A related dataset was produced for each scenario. Datasets were then divided into the normal and assault clusters. The clustering outcomes were generated using the K-Means technique with an efficiency of 99.94%. In [85] the data was divided into

Table 4: Clustering techniques in IoT security

Author	AI approach	Security objective	Dataset/data collection	Accuracy
[83]	K-means	Network intrusion detection	sensors	-
[84]	K-means	ping flood attack pattern recognition	sensors	99.94%
[85]	Fuzzy clustering	Intrusion detection	-	99%
[86]	GMM	DDOS attack detection	CIC-IDS2017 CIC-DDoS2019	94%
[87]	GMM	Anomaly detection	NAB dataset Self-made dataset	-
[88]	GMM	spoofing attack detection	2D feature vector extracted from an estimated channel state vector	98%

high-risk data and low-risk data, which are correspondingly detected by high frequency and low frequency. Both the principal component analysis approach and the suppressed fuzzy clustering algorithm were used simultaneously for the self-adjustment of the detection frequency. It was found that as data amount increases, intrusion detection algorithm accuracy and efficiency gradually decline. The suggested method [86] was effective at identifying known DDoS attacks. However, the system performance suffers greatly when faced with innovative attacks. The proposed technique [87] can perform well in the health system. The real-time anomaly detection algorithm works because it was tested on two different types of datasets. But most of this work is about how to find low-dimensional anomalies. It does not look at how to find high-dimensional or super-high-dimensional anomalies. In [88] successful usage has been found for a two-dimensional feature vector based on the distance and correlation between two channel state vectors. However, other features are feasible, and the use of more than two features should be seriously examined.

7.1. Review of Clustering Techniques in IoT Security

Clustering identifies patterns in IoT data. It also spots anomalies. It helps detect security breaches. Suspicious devices can be isolated. GMM models IoT devices' behavior. It detects anomalies and malicious activity. GMM can analyze sensor data. It spots unusual patterns. Deviations from normal behavior are detected. These could indicate a security breach.

8. Deep Learning Techniques in IoT Security

DL is a subset of ML techniques that are based on ANNs with multiple layers [89]. These techniques are used to automatically learn representations of data, such as images, audio, and text, by training a neural network on a large dataset. DL techniques can learn from IoT security data by passing through layers, which are known as hierarchical learning methods due to their ability to capture knowledge in deep architectures. The proposed architecture and model [90] are both fast and accurate, while also being sensitive to the restricted resources of IoTs. It has also been observed that accuracy starts falling at some point with an increase in the size of the dataset. Table 5 represents the summary of DL techniques in the IoT environment.

Using quantitative measurements for the assessment of images, such as peak signal-to-noise ratio (SNR), structural similarity index, and mean squared error (MSE), the proposed framework [91] by using CNN proved to be superior to existing methods. The technique was applied to the MRI dataset but this

Table 5: DL techniques in IoT security

Author	AI approach	Security objective	Dataset/data collection	Accuracy
[90]	CNN	Malware detection	IoTPoT	95%
[91]	CNN	Medical image security	MRI Dataset	-
[92]	CNN	Malware detection	IoT_Malware dataset	97.93%
[93]	CNN	Malicious data identification	Kitsune network attack database	-
[94]	RNN	Intrusion detection	NSL-KDD	97.35%
[95]	RNN	Intrusion detection	DARPA/KDD Cup '99	98.91%
[96]	DNN	Anomaly detection	IoT-Botnet 2020	99%
[97]	MLP	Botnet attack detection	captured from 9 IoT devices	99%

technique may perform poorly for complex blurred and color images. In addition to recognizing other sorts of attack categories, the model [94] demonstrates excellent sensitivity to DoS attacks, which are one of the most prominent attacks that impede the growth of IoT networks. The outcomes of a proposed method [95] were superior to those of previously published work, and they were truly excellent. This study targeted IoT gadgets with limited processing capabilities and manageable data loads. However, in a scenario, where processing power is high and data amount is vast, this strategy cannot perform better. Proposed technique [96] provides efficiency of 99% in case of anomaly detection but this technique cannot provide higher efficiency in multiclass classification scenarios.

8.1. Review of DL Techniques in IOT Security

DL's primary benefit over conventional machine learning is its higher level of accuracy on massive datasets. DL techniques can be used in IoT security to improve the detection of anomalies and malicious activity, as well as to protect the privacy of IoT device users. However, DL methodologies require massive amounts of data, computing resources, and high hardware specifications.

Table 6: Overview of AI techniques with their advantages and disadvantages in IoT

AI Technique	Advantages	Disadvantages	IoT security applications
Naive Bayes	powerful and efficient algorithm that can be used for IoT security to detect and classify anomalies and predict potential security threats [98].	prone to overfitting the training data when the number of features is too large compared to the size of the dataset [99].	anomaly detection, classification, and prediction.

SVM	robust to noise and can handle data with missing values, making it suitable for analyzing large, real-world datasets generated by IoT devices [100].	sensitive to outliers, which can affect the performance of the algorithm [101]. Outliers in IoT data can be common and difficult to detect, making SVM less suitable in certain situations.	anomaly detection, intrusion detection, malware detection, and physical attack detection.
KNN	simple and easy-to-understand algorithm that requires minimal training, making it a suitable option for IoT security applications [102].	cannot handle missing data and requires complete datasets. In IoT security applications where data can be missing or incomplete, this can be a limitation [103].	anomaly detection
RF	robust to noisy or incomplete data and can handle missing values effectively.	can be less effective when dealing with small datasets, which can be a limitation in IoT security applications where data is limited [104].	device fingerprinting, authentication, botnet detection, vulnerability detection, anomaly detection
DT	can handle both categorical and numerical data, making them suitable for a wide range of IoT security applications.	can be sensitive to noise or outliers in the data, which can result in inaccurate or unreliable predictions [105].	vulnerability detection, intrusion detection, and anomaly detection
BLR	can handle imbalanced data, which may be common in IoT security applications where some types of threats are rare [106].	can overfit the training data, leading to poor generalization performance on new data [77].	spoofing attacks, DOS attacks, malware detection, and physical attacks
LR	produces probabilistic predictions, which can be useful in IoT security applications where understanding the confidence of a prediction is important [107].	requires careful feature selection to avoid overfitting and to ensure that the selected features are relevant to the security threat being detected.	spoofing attacks, DOS attacks, malware detection, and physical attacks
RR	can be used for both regression and classification tasks in IoT security applications, making it a versatile algorithm.	assumes that all input variables are relevant to the prediction task, which may not always be the case in IoT security applications [80].	anomaly detection, intrusion detection, and malware detection
K-means	can identify anomalous patterns in IoT data that may indicate a security threat [108].	requires the number of clusters to be specified in advance, which can be difficult to determine in IoT applications.	anomaly detection, botnet attacks, intrusion detection, and malware detection
Fuzzy clustering	can adapt to changing patterns in IoT data, making it suitable for applications where the underlying data	may not work well for all types of IoT data, particularly if the data is highly skewed or contains outliers that cannot be	network intrusion and anomaly detection

	structure may evolve over time [109].	easily modeled using a fuzzy approach [110].	
CNN	can automatically learn and extract features from IoT data without requiring manual feature engineering.	may not generalize well to new, unseen IoT security scenarios, particularly if the distribution of data is significantly different from the training data [111].	man-in-the-middle attacks, virus detection, breach detection, and DOS attack
RNN	can deal with variable length and size inputs, which is important in IoT where data is noisy and unreliable [112].	can be computationally expensive, particularly when dealing with large datasets, which can limit their practicality in some IoT applications [113].	forecasting and mitigation, malware identification, and detecting intrusions
DNN	can learn complex patterns and relationships in data, making them well-suited for detecting security threats in IoT systems [114].	require labeled data for training, which can be time-consuming and expensive to obtain, particularly in IoT applications where data may be noisy or unlabeled.	botnet detection, intrusion detection, malware detection, and anomaly detection
MLP	relatively simple and easy to implement compared to other neural network architectures, making them a popular choice for many IoT applications [115].	limited capacity to handle complex patterns and may not perform as well as other neural network architectures in some IoT applications [116].	DOS attack, DDOS attack, malware detection, anomaly detection

9. Challenges and Opportunities

The primary emphasis of the present study pertaining to provenance security has revolved around the identification of requirements and the proposition of solutions employing established AI techniques for safeguarding data in IoT environments. It would be of great interest to investigate whether, similar to the realm of privacy, the interplay between data and provenance gives rise to novel security challenges and corresponding remedies. The absence of universally accepted security standards for IoT devices poses challenges in maintaining consistent security measures across various products and vendors. The establishment of reliable security standards still needs the attention of the research community. Moreover, insufficient authentication systems might facilitate unauthorized access by attackers to IoT gadgets and networks. There is limited literature available that uses AI approaches to overcome the issue of authentication. More study is required to identify the strong role of AI in the authentication process for IoT environments.

There exist multiple datasets that are deemed appealing to investigate network intrusion detection. One example of a widely employed dataset for the examination of network IDSs is KDD 99. Nevertheless, it is important to note that there is currently a lack of publicly available datasets specifically focused on pure IoT threats. Certain widely used datasets, like as NSL-KDD, encompass a variety of security attacks. It is worth noting that a significant proportion of the malicious instances present in the NSL-KDD dataset are specifically categorized as DoS attacks. Utilization of these methods for various forms of attacks poses a significant challenge in terms of study and analysis.

10. Concluding Remarks

A comprehensive critical analysis of the existing literature on the topic of IoT security challenges and solutions based on AI techniques, specifically machine learning and DL has been conducted in this research. These techniques can identify anomalous activity or variations from typical patterns in the connectivity of IoT devices. These techniques can also reduce false positive alarms by differentiating between legal and harmful operations using learned patterns and contextual information. This study encompasses several aspects such as the IoT paradigm, IoT-based smart environments, the associated security concerns, and potential solutions that leverage AI. To facilitate the advancement of the argument presented in this paper, an extensive examination of the current status of research on security in the IoT was conducted. The effectiveness and efficiency of an IoT security solution that utilizes ML or DL techniques are greatly influenced by the qualities and features of the data, as well as the performance of the learning algorithms. To effectively identify and mitigate cyberattacks targeting IoT devices and systems, it is imperative to conduct a thorough examination of IoT system architecture. Hence, a concise examination has been conducted to explore the potential use of several machine and DL algorithms in addressing security challenges inside the IoT environment. An effective security framework for the IoT should use machine or DL modeling, as deemed suitable based on the attributes of the data. For the system to facilitate intelligent decision-making, it is imperative to develop a proficient learning algorithm that is grounded in the acquired IoT security information that pertains to the specific application at hand.

We can conclude that the performance of KNN, Naive Bayes, and RF-based classification approaches are best for DDOS attack prevention on both data sets i.e.; real-time and previously available. While the SVM approach is good for intrusion detection and some specific types of malwares but SVM-based models are complex and challenging to understand and interpret. Regression techniques are good for attack detection and mitigation, malware analysis, anomaly and intrusion detection. GMM can be used to model the normal behavior of IoT devices and detect any anomalies or malicious activity. For example, GMM can be used to analyze sensor data and detect any unusual patterns or deviations from the normal behavior of the device, which could indicate a security breach or attack. DL's primary benefit over conventional machine learning is its higher level of accuracy on massive datasets. IoT security may utilize DL approaches to improve the detection of anomalies and malicious activity, as well as to protect the privacy of IoT device users.

Conflict of Interest

There are no conflicts of interest to declare regarding this manuscript.

Data Availability

Data supporting the findings of this study are provided in this manuscript.

Funding Statement

This research study did not receive any funding.

11. References

[1] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015: IEEE, pp. 336-341.

[2] A. Ali, A. Mateen, A. Hanan, and F. Amin, "Advanced Security Framework for Internet of Things (IoT)," *Technologies,* vol. 10(3), p. 60, 2022.

[3] M. Javaid and I. H. Khan, "Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic," *Journal of Oral Biology and Craniofacial Research,* vol. 11(2), pp. 209-214, 2021.

[4] G. Alqarawi, B. Alkhalifah, N. Alharbi, and S. El Khediri, "Internet-of-Things Security and Vulnerabilities: Case Study," *Journal of Applied Security Research,* pp. 1-17, 2022.

[5] S. Haseeb, M. Khalil Afzal, M. Tahir, M. Raza Jafri, and N. Raza, "Energy-efficient selection of relay for UWSNs in the Internet of underwater things," *International Journal of Communication Systems,* vol. 36(18), p. e5619, 2023.

[6] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications,* pp. 1-17, 2022.

[7] 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,* 2024.

[8] A. A. Soofi and H. Ahmad, "Deep Learning for IoT Security: Applications and Challenges," *Emerging Technologies for Securing the Cloud and IoT,* pp. 69-99, 2024.

[9] D. Kolevski and K. Michael, "Edge Computing and IoT Data Breaches: Security, Privacy, Trust, and Regulation," *IEEE Technology and Society Magazine,* vol. 43(1), pp. 22-32, 2024.

[10] M. Adil, M. K. Khan, N. Kumar, M. Attique, A. Farouk, M. Guizani and Z. Jin, "Healthcare Internet of Things: Security Threats, Challenges and Future Research Directions," *IEEE Internet of Things Journal,* 2024.

[11] G. Nissar, R. A. Khan, S. Mushtaq, S. A. Lone, and A. H. Moon, "IoT in healthcare: a review of services, applications, key technologies, security concerns, and emerging trends," *Multimedia Tools and Applications,* pp. 1-62, 2024.

[12] H. Gupta, S. Sharma, and S. Agrawal, "Artificial Intelligence-Based Anomalies Detection Scheme for Identifying Cyber Threat on IoT-Based Transport Network," *IEEE Transactions on Consumer Electronics,* 2023.

[13] C. Ni and S. C. Li, "Machine learning enabled Industrial IoT Security: Challenges, Trends and Solutions," *Journal of Industrial Information Integration,* p. 100549, 2024.

[14] M. Muhammad, S. U. Bazai, S. Ullah, S. A. A. Shah, S. Aslam, A. Amphawan and T. K. Neo, "A systematic literature review on the role of big data in IoT security," *Journal of Telecommunications and the Digital Economy,* vol. 12(1), pp. 39-64, 2024.

[15] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications,* vol. 28(1), pp. 296-312, 2023.

[16] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications,* vol. 161, p. 102630, 2020.

[17] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions," *SN Computer Science,* vol. 2(3), pp. 1-18, 2021.

[18] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big data,* vol. 7(1), pp. 1-29, 2020.

[19] A. A. Soofi, "Exploring Deep Learning Techniques for Glaucoma Detection: A Comprehensive Review," *Journal of Computing & Biomedical Informatics,* vol. 5(02), pp. 220-238, 2023.

[20] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications,* vol. 90(11), 2014.

[21] F. Thiesse and F. Michahelles, "An overview of EPC technology," *Sensor Review,* 2006.

[22] N. J. Kulkarni and J. Bakal, "E-health: Iot based system and correlation of vital stats in identification of mass disaster event," In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018: IEEE, pp. 1-6.

[23] F. Masoodi, S. Alam, and S. T. Siddiqui, "Security & privacy threats, attacks and countermeasures in Internet of Things," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 11, 2019.

[24] E. F. N. Shipena and A. M. Gamundani, "A Review of Internet of Things (IoT) Smart Office Data Security Threats," *Digital Technology and Changing Roles in Managerial and Financial Accounting: Theoretical Knowledge and Practical Application,* pp. 375-381, 2024.

[25] Rishikesh and D. Sinha, "Traditional and Blockchain Based IoT and IIoT Security in the Context of Agriculture: A Survey," *Wireless Personal Communications,* pp. 1-29, 2024.

[26] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016: IEEE, pp. 5772-5781.

[27] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering,* vol. 2017, 2017.

[28] V. Agarwal, P. Mishra, S. Kumar, and E. S. Pilli, "A Review on Attack and Security Tools at Network Layer of IoT," *Optical and Wireless Technologies,* pp. 497-506, 2022.

[29] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson, "Architectural considerations in smart object networking," 2070-1721, 2015.

[30] S. Lakshminarayana, A. Praseed, and P. S. Thilagam, "Securing the IoT Application Layer from an MQTT Protocol Perspective: Challenges and Research Prospects," *IEEE Communications Surveys & Tutorials,* 2024.

[31] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Generation Computer Systems,* vol. 78, pp. 964-975, 2018.

[32] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and Solutions Survey," *Sensors,* vol. 22(19), p. 7433, 2022.

[33] H. G. Hamid and Z. T. Alisa, "Survey on IoT application layer protocols," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 21(3), pp. 1663-1672, 2021.

[34] N. Raza and M. Tariq, "Effect of Node Density over the performance of DSR, TORA, and OLSR Routing Protocols of MANET," *International Journal of Computer Applications,* vol. 177(39), pp. 34-41.

[35] B. Nataraj and P. Duraisamy, "An Investigation on Attacks in Application Layer Protocols and Ransomeware Threats in Internet of Things," In *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2023, vol. 1: IEEE, pp. 668-672.

[36] U. S. Shanthamallu, A. Spanias, C. Tepedelenlioglu, and M. Stanley, "A brief survey of machine learning methods and their sensor and IoT applications," In *2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 2017: IEEE, pp. 1-8.

[37] R. Kollolu, "A Review on Wide Variety and Heterogeneity of IoT Platforms," *The International Journal of Analytical and Experimental Modal Analysis, Analysis,* vol. 12, pp. 3753-3760, 2020.

[38] N. Javaid, A. Sher, H. Nasir, and N. Guizani, "Intelligence in IoT-based 5G networks: Opportunities and challenges," *IEEE Communications Magazine,* vol. 56(10), pp. 94-100, 2018.

[39] B. Panigrahi, H. K. Rath, R. Ramamohan, and A. Simha, "Energy and spectral efficient direct Machine-to-Machine (M2M) communication for cellular Internet of Things (IoT) networks," In *2016 International Conference on Internet of Things and Applications (IOTA)*, 2016: IEEE, pp. 337-342.

[40] S. Li, L. D. Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers,* vol. 17, pp. 243-259, 2015.

[41] S. Dua and X. Du, *Data mining and machine learning in cybersecurity*. CRC Press, 2016.

[42] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *SN computer science,* vol. 2(3), p. 160, 2021.

[43] A. A. Soofi and A. Awan, "Classification techniques in machine learning: applications and issues," *J. Basic Appl. Sci,* vol. 13(1), pp. 459-465, 2017.

[44] I. H. Sarker, "Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective," *SN Computer Science,* vol. 2(3), p. 154, 2021.

[45] I. H. Sarker, "Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions," *SN Computer Science,* vol. 2(6), p. 420, 2021.

[46] H. Liao, M. Z. Murah, M. K. Hasan, A. H. M. Aman, J. Fang, X. Hu and A. U. R. Khan, "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things," *IEEE Access,* 2024.

[47] R. Kumar, G. Joshi, A. K. S. Chauhan, A. K. Singh, and A. K. Rao, "A Deep Learning and Channel Sounding Based Data Authentication and QoS Enhancement Mechanism for Massive IoT Networks," *Wireless Personal Communications,* vol. 130(4), pp. 2495-2514, 2023.

[48] M. Zheng, D. Xu, L. Jiang, C. Gu, R. Tan, and P. Cheng, "Challenges of privacy-preserving machine learning in IoT," In *Proceedings of the First International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things*, 2019, pp. 1-7.

[49] A. O. Adebayo and M. S. Chaubey, "Data mining classification techniques on the analysis of student's performance," *GSJ,* vol. 7(4), pp. 45-52, 2019.

[50] M. Tariq, A. A. Sufi, H. ur Rehman, S. K. Ajmal, D. Riaz, M. Amjad, B. Ahmad and M. H. Raza, "Brain Tumor Classification Using Convolutional Neural Network with Neutrosophy, Super-Resolution and SVM," *Webology (ISSN: 1735-188X),* vol. 18(1), 2022.

[51] W. B. Demilie, "Plant disease detection and classification techniques: a comparative study of the performances," *Journal of Big Data,* vol. 11(1), p. 5, 2024.

[52] M. Aljabri, A. A. Alahmadi, R. M. A. Mohammad, F. Alhaidari, M. Aboulnour, D. M. Alomari and S. Mirza, "Machine learning-based detection for unauthorized access to IoT devices," *Journal of Sensor and Actuator Networks,* vol. 12(2), p.27, 2023.

[53] P. Shukla, C. R. Krishna, and N. V. Patil, "EIoT-DDoS: embedded classification approach for IoT traffic-based DDoS attacks," *Cluster Computing,* vol. 27(2), pp. 1471-1490, 2024.

[54] J. H. Kalwar and S. Bhatti, "Deep Learning Approaches for Network Traffic Classification in the Internet of Things (IoT): A Survey," *arXiv preprint arXiv:2402.00920,* 2024.

[55] P. Cunningham and S. J. Delany, "k-Nearest neighbour classifiers-A Tutorial," *ACM computing surveys (CSUR),* vol. 54(6), pp. 1-25, 2021.

[56] W. S. Noble, "What is a support vector machine?," *Nature Biotechnology,* vol. 24(12), pp. 1565-1567, 2006.

[57] G. I. Webb, E. Keogh, and R. Miikkulainen, "Naïve Bayes," *Encyclopedia of machine learning,* vol. 15, pp. 713-714, 2010.

[58] S. J. Rigatti, "Random forest," *Journal of Insurance Medicine,* vol. 47(1), pp. 31-39, 2017.

[59] S. B. Kotsiantis, "Decision trees: a recent overview," *Artificial Intelligence Review,* vol. 39, pp. 261-283, 2013.

[60] L. Best, E. Foo, and H. Tian, "A Hybrid Approach: Utilising Kmeans Clustering and Naive Bayes for IoT Anomaly Detection," *arXiv preprint arXiv:2205.04005,* 2022.

[61] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," *The Journal of Supercomputing,* vol. 74(10), pp. 5156-5170, 2018.

[62] Y. Chen, L. Lu, X. Yu, and X. Li, "Adaptive method for packet loss types in IoT: an naive Bayes distinguisher," *Electronics,* vol. 8(2), p. 134, 2019.

[63] R. Majeed, N. A. Abdullah, and M. F. Mushtaq, "IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm," *International Journal of Advanced Computer Science and Applications,* vol. 12(7), 2021.

[64] D. Reising, J. Cancelleri, T. D. Loveless, F. Kandah, and A. Skjellum, "Radio identity verification-based IoT security using RF-DNA fingerprints and SVM," *IEEE Internet of Things Journal,* vol. 8(10), pp. 8356-8371, 2020.

[65] S. Pokhrel, R. Abbas, and B. Aryal, "IoT security: botnet detection in IoT using machine learning," *arXiv preprint arXiv:2104.02231,* 2021.

[66] S. Manimurugan, "IoT-Fog-Cloud model for anomaly detection using improved Naive Bayes and principal component analysis," *Journal of Ambient Intelligence and Humanized Computing,* pp. 1-10, 2021.

[67] H. S. Ham, H. H. Kim, M. S. Kim, and M. J. Choi, "Linear SVM-based android malware detection for reliable IoT services," *Journal of Applied Mathematics,* vol. 2014, 2014.

[68] S. Y. Lee, S.-r. Wi, E. Seo, J. K. Jung, and T.-M. Chung, "ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach," In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, 2017: IEEE, pp. 1-6.

[69] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet of Things Journal,* vol. 6(5), pp. 7702-7712, 2019.

[70] R. Primartha and B. A. Tama, "Anomaly detection using random forest: A performance revisited," In *2017 International Conference on Data and Software Engineering (ICoDSE)*, 2017: IEEE, pp. 1-6.

[71] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," In *2018 IEEE Security and Privacy Workshops (SPW)*, 2018: IEEE, pp. 29-35.

[72] S. S. S. Sugi and S. R. Ratna, "Investigation of machine learning techniques in intrusion detection system for IoT network," In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 2020: IEEE, pp. 1164-1167.

[73] S. Strecker, R. Dave, N. Siddiqui, and N. Seliya, "A modern analysis of aging machine learning based IOT cybersecurity methods," *arXiv preprint arXiv:2110.07832,* 2021.

[74] S. M. Taghavinejad, M. Taghavinejad, L. Shahmiri, M. Zavvar, and M. H. Zavvar, "Intrusion detection in IoT-based smart grid using hybrid decision tree," In *2020 6th International Conference on Web Research (ICWR)*, 2020: IEEE, pp. 152-156.

[75] Z. Cui, X. Xu, X. U. E. Fei, X. Cai, Y. Cao, W. Zhang and J. Chen, "Personalized recommendation system based on collaborative filtering for IoT scenarios," *IEEE Transactions on Services Computing,* vol. 13(4), pp. 685-695, 2020.

[76] F. A. M. Solomon, G. W. Sathianesan, and R. Ramesh, "Logistic Regression Trust-A Trust Model for Internet-of-Things Using Regression Analysis," *Computer Systems Science & Engineering,* vol. 44(2), 2023.

[77] C. Ioannou and V. Vassiliou, "An intrusion detection system for constrained WSN and IoT nodes based on binary logistic regression," In *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2018, pp. 259-263.

[78] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things,* vol. 7, p. 100059, 2019.

[79] W. D. Nanda and F. D. S. Sumadi, "LRDDoS Attack Detection on SD-IoT Using Random Forest with Logistic Regression Coefficient," *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi),* vol. 6(2), pp. 220-226, 2022.

[80] P. Machaka, O. Ajayi, H. Maluleke, F. Kahenga, A. Bagula, and K. Kyamakya, "Modelling DDoS Attacks in IoT Networks using Machine Learning," *arXiv preprint arXiv:2112.05477,* 2021.

[81] K. Prathapchandran and T. Janani, "A trust-based security model to detect misbehaving nodes in Internet of Things (IoT) environment using logistic regression," In *Journal of Physics: Conference Series*, 2021, vol. 1850(1): IOP Publishing, p. 012031.

[82] E. Arul, "Deep nonlinear regression least squares polynomial fit to detect malicious attack on IoT devices," *Journal of Ambient Intelligence and Humanized Computing,* vol. 12, pp. 769-779, 2021.

[83] J. Zhu, L. Huo, M. D. Ansari, and M. A. Ikbal, "Research on Data Security Detection Algorithm in IoT Based on K-means," *Scalable Computing: Practice and Experience,* vol. 22(2), pp. 149–159-149–159, 2021.

[84] D. Stiawan, M. E. Suryani, M. Y. Idris, M. N. Aldalaien, N. Alsharif, and R. Budiarto, "Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network," *IEEE Access,* vol. 9, pp. 116475-116484, 2021.

[85] L. Liu, B. Xu, X. Zhang, and X. Wu, "An intrusion detection method for internet of things based on suppressed fuzzy clustering," *EURASIP Journal on Wireless Communications and Networking,* vol. 2018(1), pp. 1-7, 2018.

[86] C.-S. Shieh, W.-W. Lin, T.-T. Nguyen, C.-H. Chen, M.-F. Horng, and D. Miu, "Detection of unknown DDoS attacks with deep learning and gaussian mixture model," *Applied Sciences,* vol. 11(11), p. 5213, 2021.

[87] N. Ding, H. Ma, H. Gao, Y. Ma, and G. Tan, "Real-time anomaly detection based on long short-Term memory and Gaussian Mixture Model," *Computers & Electrical Engineering,* vol. 79, p. 106458, 2019.

[88] X. Qiu, T. Jiang, S. Wu, and M. Hayes, "Physical layer authentication enhancement using a Gaussian mixture model," *IEEE Access,* vol. 6, pp. 53583-53592, 2018.

[89] J. Han, M. Kamber, and J. Pei, "Data mining concepts and techniques third edition," *University of Illinois at Urbana-Champaign Micheline Kamber Jian Pei Simon Fraser University,* 2012.

[90] A. M. Zaza, S. K. Kharroub, and K. Abualsaud, "Lightweight IoT malware detection solution using cnn classification," in *2020 IEEE 3rd 5G World Forum (5GWF)*, 2020: IEEE, pp. 212-217.

[91] S. More, J. Singla, S. Verma, U. Ghosh, J. J. Rodrigues, A. S. Hosen and I. H. Ra, "Security assured CNN-based model for reconstruction of medical images on the internet of healthcare things," *IEEE Access,* vol. 8, pp. 126333-126346, 2020.

[92] M. Asam, S. H. Khan, A. Akbar, S. Bibi, T. Jamal, A. Khan, U. Ghafoor and M. R. Bhutta, "IoT malware detection architecture using a novel channel boosted and squeezed CNN," *Scientific Reports,* vol. 12(1), pp. 1-12, 2022.

[93] Z. Gu, S. Nazir, C. Hong, and S. Khan, "Convolution neural network-based higher accurate intrusion identification system for the network security and communication," *Security and Communication Networks,* vol. 2020, 2020.

[94] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory,* vol. 101, p. 102031, 2020.

[95] M. K. Putchala, "Deep learning approach for intrusion detection system (IDs) in the internet of things (IoT) network using gated recurrent neural networks (GRU)," Master's thesis, Wright State University, 2017.

[96] Z. Ahmad, A. S. Khan, K. Nisar, I. Haider, R. Hassan, M. R. Haque, S. Tarmizi and J. J. Rodrigues, "Anomaly detection using deep neural network for IoT architecture," *Applied Sciences,* vol. 11(15), p. 7050, 2021.

[97] Y. Javed and N. Rajabi, "Multi-layer perceptron artificial neural network based IoT botnet traffic classification," In *Proceedings of the Future Technologies Conference*, 2019: Springer, pp. 973-984.

[98] S. Na, T. Kim, and H. Kim, "A study on the classification of common vulnerabilities and exposures using naïve bayes," In *Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 11th International Conference On Broad-Band Wireless Computing, Communication and Applications (BWCCA–2016) November 5–7, 2016, Korea*, 2017: Springer, pp. 657-662.

[99] M. Jindal, J. Gupta, and B. Bhushan, "Machine learning methods for IoT and their Future Applications," In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 2019: IEEE, pp. 430-434.

[100] A. Al Shorman, H. Faris, and I. Aljarah, "Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection," *Journal of Ambient Intelligence and Humanized Computing,* vol. 11, pp. 2809-2825, 2020.

[101] M. Hosseinzadeh, A. M. Rahmani, B. Vo, M. Bidaki, M. Masdari, and M. Zangakani, "Improving security using SVM-based anomaly detection: issues and challenges," *Soft Computing,* vol. 25, pp. 3195-3223, 2021.

[102] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors,* vol. 20(13), p. 3625, 2020.

[103] Z. Chen, J. Liu, Y. Shen, M. Simsek, B. Kantarci, H. T. Mouftah and P. Djukic, "Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats," *ACM Computing Surveys,* vol. 55(5), pp. 1-37, 2022.

[104] N. S. Akash, S. Rouf, S. Jahan, A. Chowdhury, and J. Uddin, "Botnet detection in IoT devices using random forest classifier with independent component analysis," *Journal of Information and Communication Technology,* vol. 21(2), pp. 201-232, 2022.

[105] A. K. Pathak, S. Saguna, K. Mitra, and C. Åhlund, "Anomaly detection using machine learning to discover sensor tampering in IoT systems," In *ICC 2021-IEEE International Conference on Communications*, 2021: IEEE, pp. 1-6.

[106] B. K. Mohanta, D. Jena, N. Mohapatra, S. Ramasubbareddy, and B. S. Rawal, "Machine learning based accident prediction in secure IoT enable transportation system," *Journal of Intelligent & Fuzzy Systems,* vol. 42(2), pp. 713-725, 2022.

[107] H. Bashir, S. Lee, and K. H. Kim, "Resource allocation through logistic regression and multicriteria decision making method in IoT fog computing," *Transactions on Emerging Telecommunications Technologies,* vol. 33(2), p. e3824, 2022.

[108] S. Kumar, V. Kumar-Solanki, S. Kumar Choudhary, A. Selamat, and R. González-Crespo, "Comparative study on ant colony optimization (ACO) and K-means clustering approaches for jobs scheduling and energy optimization model in internet of things (IoT)," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 6(1), pp.107-116, 2020.

[109] M. D. Alshehri and F. K. Hussain, "A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT)," *Computing,* vol. 101(7), pp. 791-818, 2019.

[110] D. Palani and K. Venkatalakshmi, "An IoT based predictive modelling for predicting lung cancer using fuzzy cluster based segmentation and classification," *Journal of Medical Systems,* vol. 43, pp. 1-12, 2019.

[111] A. Anand, S. Rani, D. Anand, H. M. Aljahdali, and D. Kerr, "An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications," *Sensors,* vol. 21(19), p. 6346, 2021.

[112] I. Ullah and Q. H. Mahmoud, "Design and development of RNN anomaly detection model for IoT networks," *IEEE Access,* vol. 10, pp. 62722-62750, 2022.

[113] C. Gao, S. Braun, I. Kiselev, J. Anumula, T. Delbruck, and S.-C. Liu, "Real-time speech recognition for IoT purpose using a delta recurrent neural network accelerator," In *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2019: IEEE, pp. 1-5.

[114] W. Zhang, D. Yang, H. Peng, W. Wu, W. Quan, H. Zhang and X. Shen, "Deep reinforcement learning based resource management for DNN inference in industrial IoT," *IEEE Transactions on Vehicular Technology,* vol. 70(8), pp. 7605-7618, 2021.

[115] I. Garcia-Magarino, R. Muttukrishnan, and J. Lloret, "Human-centric AI for trustworthy IoT systems with explainable multilayer perceptrons," *IEEE Access,* vol. 7, pp. 125562-125574, 2019.

[116] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019: IEEE, pp. 0452-0457.