2023

Security of Internet of Things (IoT) Using Federated Learning and Deep Learning — Recent Advancements, Issues and Prospects

Vinay Gugueoth
University of the Cumberlands

Sunitha Safavat
Howard University

Sachin Shetty
Old Dominion University, sshetty@odu.edu

Original Publication Citation

Gugueoth, V., Safavat, S., & Shetty, S. (2023). Security of Internet of Things (IoT) using federated learning and deep learning — recent advancements, issues and prospects. *ICT Express, 9*(5), 941-960.
https://doi.org/10.1016/j.icte.2023.03.006

The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 9 (2023) 941–960

www.elsevier.com/locate/icte

Security of Internet of Things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects

Vinay Gugueoth*, Sunitha Safavat, Sachin Shetty

Department of Computer and Information Science, University of the Cumberlands, Williamsburg, USA
Department of Electrical Engineering and Computer Science, Howard University, Washington DC, USA
Department of Computational, Modeling and Simulation Engineering, Old Dominion University, Norfolk, USA

Received 4 December 2022; received in revised form 15 February 2023; accepted 19 March 2023
Available online 21 March 2023

Abstract

There is a great demand for an efficient security framework which can secure IoT systems from potential adversarial attacks. However, it is challenging to design a suitable security model for IoT considering the dynamic and distributed nature of IoT. This motivates the researchers to focus more on investigating the role of machine learning (ML) in the designing of security models. A brief analysis of different ML algorithms for IoT security is discussed along with the advantages and limitations of ML algorithms. Existing studies state that ML algorithms suffer from the problem of high computational overhead and risk of privacy leakage. In this context, this review focuses on the implementation of federated learning (FL) and deep learning (DL) algorithms for IoT security. Unlike conventional ML techniques, FL models can maintain the privacy of data while sharing information with other systems. The study suggests that FL can overcome the drawbacks of conventional ML techniques in terms of maintaining the privacy of data while sharing information with other systems. The study discusses different models, overview, comparisons, and summarization of FL and DL-based techniques for IoT security.

Keywords: Security; Internet of Things (IoT); Machine learning; Deep learning; Federated learning

1. Introduction

IoT is a network of various interconnected devices such as sensors and actuators which collect information at a higher speed. With a system of modest sensors and interconnected things, data assortment on our reality and condition can be accomplished at a higher level. The popularity of IoT is increasing day by day and it is estimated that the number of IoT based applications will be approximately 20.4 billion in 2022 [1]. The rising prominence of IoT is due to its excellent attributes such as automation, reliability, scalability, and robustness. These attributes can transform the future IoT applications and enhance the quality of service (QoS) offered by the IoT applications such as smart cities, smart healthcare [2], industrial automation [3], smart transportation [4].

However, the integration of the IoT system with various devices raises the security concerns in IoT applications. IoT communicates with other connecting devices through a centralized server which increases the privacy and security concerns. The heterogeneous and dynamic nature of IoT devices make them susceptible to different types of threats and security attacks [5]. In addition, the hypersensitivity of IoT devices increases the chances of device spoofing, which makes IoT face serious challenges regarding data security and data privacy. It requires a robust security model which can prevent the IoT system against adversarial attacks. However, it is highly complicated and challenging to design an effective security approach in IoT due to the resource constraints in the IoT system [6]. Most of the IoT devices have restricted resources such as computational overhead, bandwidth and memory which are not compatible with the demands of complex security solutions.

Conventional security techniques such as malware detection, access control, device authentication, and cryptography based methods were proposed previously to maximize IoT security [7–9]. However, identification of different types of

* Corresponding author at: Department of Computer and Information Science, University of the Cumberlands, Williamsburg, USA.

E-mail addresses: vinayg@ieee.org (V. Gugueoth), sunitha.safavat@bison.howard.edu (S. Safavat), sshetty@odu.edu (S. Shetty).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2023.03.006

cyberattacks and security threats using these techniques is highly challenging. In addition, various unsolved and critical operational problems increase the security risks that undermine the trustworthiness of the IoT paradigm. Existing security approaches should be transformed in order to detect novel cyberattacks. It requires a smart and intelligent model to identify different types of attacks in IoT such as denial of service (DoS), distributed DoS (DDoS), flooding attacks, jamming attacks, botnet attacks [10]. Artificial intelligence (AI) based techniques can be used in the design and development of an intelligent attack detection model for securing IoT systems. The proper utilization of AI knowledge, especially machine learning (ML), can help the researchers to detect anomalies or unwanted malicious activities in the IoT, and, as a result, offer a dynamic security solution that is constantly improved and up to date [11]. Specifically, machine or deep learning (DL) models comprise a set of rules, methods, or complex transfer functions that extract useful insights or interesting data patterns from the security data. Thus, it is possible to utilize the resultant security models to train machines to predict threats or risks at an early stage.

However, conventional ML algorithms require a large amount of training data for performing a specific task. Collecting large scale datasets for ML models increases the privacy and security risks. In addition, ML models suffer from the problem of privacy leakage due to the need of transferring the device data to a centralized third party server. It is not feasible to implement centralized ML models for IoT due to the larger data size and training such large models can be computationally expensive [12]. Recently federated learning (FL) is considered as one of the potential alternatives to overcome the limitations associated with conventional ML algorithms [13,14]. Unlike conventional ML models, it is not essential to migrate the data into a central server in federated learning. This minimizes the risk of privacy leakage due to the centralized servers and hence makes it a preferred technique compared to ML algorithms. Another promising technology that is extensively used in the security of IoT systems is deep learning (DL). DL models have shown their efficacy in providing security to IoT systems [15].

Although both FL and DL are essentially a branch of ML, this review discusses these two models as separate sections in order to provide a comprehensive analysis including comparisons and significance in IoT security. The main contributions of this research are summarized as follows:

1. *Investigation of potential vulnerabilities in IoT:* A detailed investigation on the security issues, security challenges and attacks on IoT systems is presented in this paper. This paper discusses different types of security attacks such as Sybil attacks, malware analysis, device spoofing, man-in-the-middle attacks, and denial of service (DoS) attacks for each attack surface.
2. *Comprehensive analysis of ML models:* A broad categorization of ML models such as supervised, unsupervised, and reinforcement learning algorithms is discussed in this paper. In addition, different ML algorithms as security solutions for IoT are also outlined in this review.
3. *Application of FL, and DL for IoT security:* The implementation of federated learning techniques for IoT security is investigated and the concept and taxonomy of FL-based models for IoT security along with evaluation of FL methods. Furthermore, the state of art of DL models is discussed with an emphasis on performance metrics such as classification accuracy, precision, F1 score etc.
4. *Summary and comparison:* A brief summary and comparison of different ML, FL, and DL models is presented in this paper which provides a clear analysis of their application to IoT security.
5. *Challenges related to FL and DL:* The prominent research challenges related to the implementation of FL and DL models for ensuring the privacy and security of IoT is outlined in this paper.

1.1. Related works

In [16] proposed a safe authentication protocol through combining digital signature and encryption methods. The protocol resisted diverse attacks and offered reliable security. In [17] employed a cryptographic encryption with hybrid optimization methodology for securing clinical images in IoT settings. The encryption/decryption procedure's security level was enhanced through optimal key selection using particle swarm optimization and grasshopper optimization approaches. This approach consumed less time for encryption/decryption procedure and offered elevated security. In [18] employed a combined cryptographic scheme for IoT. The authors exploited DES and RSA techniques for offering elevated information security. This hybrid approach offered greater security compared to techniques when exploited alone. In [19] augmented security authentication in IoT through exploiting cryptographic-directed methodologies. The IoT sensitive information was secured through improved homomorphic encryption (IHE) approach. This approach initially categorized the confidential information from the IoT database. Then that confidential information was encrypted and decrypted using IHE. Despite the availability of various surveys, there is still great demand for the research related to IoT security. This is mainly due to the constant transformation and update of security attacks and evolution of different security techniques. In contrast to other review works, this presents a detailed analysis of ML techniques along with the application of federated learning and deep learning for IoT security along with challenges associated with it.

The paper is structured as follows: Section 2 provides a brief overview of Internet of Things Paradigm. Section 3 discusses potential threats and attacks in IoT. Section 4 provides a brief overview of Machine Learning for IoT Security. Section 5 discusses the role of FL for IoT security. Section 6 presents a brief overview of DL models for securing IoT devices. Section 7 outlines the challenges associated with FL and DL models and Section 8 concludes the paper with prominent observations.

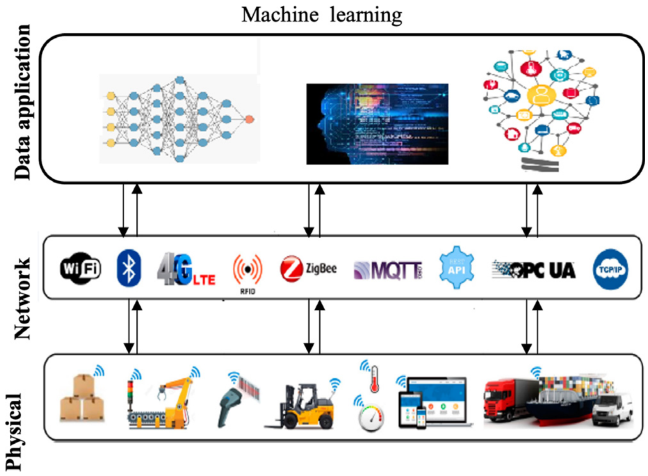

Fig. 1. Three-Layered IoT architecture.

2. The IoT paradigm

A fundamental IoT architecture is a three-layered architecture consisting of a physical resource layer, the network layer, and the data application layer as shown in Fig. 1.

- *Physical layer:* This layer consists of physical resources such as sensors and actuators for obtaining real-time information using various communication devices.
- *Network layer:* In this layer, various networking protocols will be incorporated in order to establish a secure communication between the network devices. This layer allows a Device-to-Device communication for ensuring security and Quality-of-Service (QoS) of the network [20].
- *Application Layer:* This layer delivers application specific services such as smart cities, smart healthcare services etc using ML algorithms. This is an important layer in the IoT network which is vulnerable to security attacks. The ML algorithm deployed in this layer ensures the security and reliability of the IoT network.

In an IoT reference architecture, the sensors and actuators are connected to the application through device gateways and use a rule engine for processing. A device is a hardware component which is connected to sensors through wired or wireless communication. If the devices are not capable of connecting directly with the systems, they use Gateways for communication. In other words, a Gateway is used to communicate or translate the information between devices and other components. The Rule engine in IoT helps in creating simple processing rules without requiring any programming. Here, users can create simple rules which instructs the system to perform necessary action and respond to the incoming events.

2.1. IoT-based smart environments

IoT-based smart environment refers to an integrated system where the IoT devices communicate with other devices through a connected network to improve the QoS. Smart environment in IoT signifies the ability of IoT devices to automate their operation, apply knowledge, and make decisions according to the variations in the external environment [21]. The preliminary objective of the smart environments is to provide services based on the data collected by the sensors using smart techniques. The automation of the service will simplify the business process and hence the smart environments will play a crucial role in modernizing the traditional way of operation [22]. Various factors such as increased number of users, scalability, and handling large scale data affects the adoption of smart environments. These factors must be considered while adopting IoT based smart environment applications.

2.2. Significance of IoT security

The implementation of IoT systems comes with a wide range of security challenges. Addressing the security challenges is a complex and tedious task considering the dynamic nature of the IoT devices. Some of the prominent security challenges that needs to be addressed are as follows:

- *Heterogeneity:* The diversity of IoT devices in terms of size, number, bandwidth, hardware and software requirements makes it difficult for the researchers to design a model which can cope with the heterogeneity.
- *Volume:* IoT collects data from multiple sensors and communication devices. As a result there is a huge volume of data generated in the IoT environment, which is difficult to handle.
- *Susceptibility to attacks:* IoT devices are vulnerable to various security attacks such as cookie theft, cross-site scripting, structured query language injection, session hijacking, and often distributed denial of service.
- *Latency and reliability:* The prominent challenges in most of the IoT networks are related to low-latency and reliability issues. Majority of the technologically advanced applications such as smart healthcare, lane detection and traffic monitoring etc demand a low-latency and high reliability system architecture.
- *Cost effectiveness and resource utilization:* As discussed previously, IoT is a resource constrained environment and it is challenging to achieve a proper tradeoff between the cost effectiveness and resource utilization.

Though most of these challenges are discussed previously in various research works, the resource constraint nature of IoT along with its volatility and complexity of operations have magnified the need for addressing these concerns using more advanced technologies. In this context, this review focuses on the adaptation of FL and DL models for IoT security and discusses the state-of-art, challenges, advantages and limitations of these models.

3. Security attacks in IoT

Integration of IoT with external environments enables a smart and automated interaction between the devices with

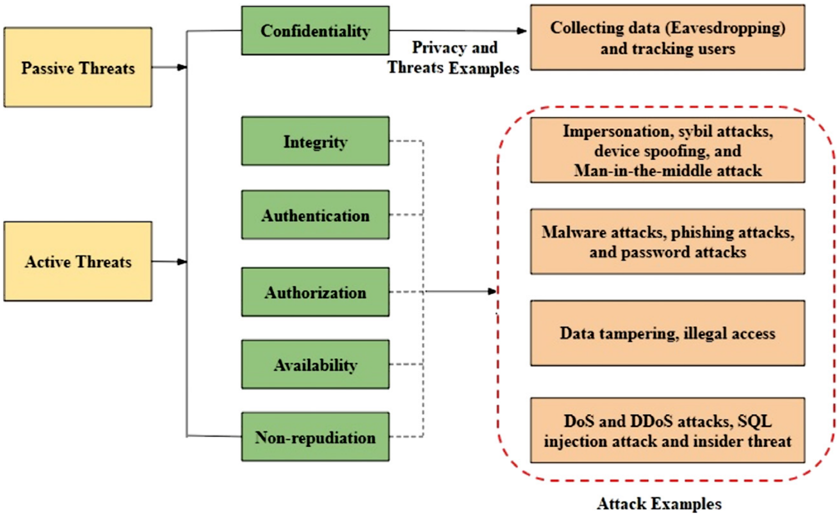
Passive Threats
Active Threats
Confidentiality
Integrity
Authentication
Authorization
Availability
Non-repudiation
Privacy and Threats Examples
Collecting data (Eavesdropping) and tracking users
Impersonation, sybil attacks, device spoofing, and Man-in-the-middle attack
Malware attacks, phishing attacks, and password attacks
Data tampering, illegal access
DoS and DDoS attacks, SQL injection attack and insider threat
Attack Examples

Fig. 2. Potential security attacks and threats in IoT.

its surroundings. In general IoT devices communicate with physical words to perform different tasks. However, the security of these devices require an in-depth analysis of the device attributes and their behavior in cyber and physical environments [23,24]. As discussed previously, designing a robust security framework for identifying different cyber-attacks in IoT is a challenging task. This problem can be more complicated for securing wireless networks. Since most of the IoT devices work in an open and centralized and unattended environment, it becomes easy for the intruders to gain illegal access to these devices and exploit sensitive and confidential information through eavesdropping. In addition, IoT devices are characterized by their limited computation and high resource consumption which adds to the existing challenges and results in potential threats becoming more probable [25]. A threat is defined as an act which can exploit the shortcomings of the security in a system and have a negative impact on it. Threats are basically categorized as active and passive threats [26]. Active threats include Sybil attacks, malware analysis, device spoofing, man-in-the-middle attacks, and denial of service (DoS) attacks. On the other hand, passive threats include eavesdropping, phishing attacks etc. These attacks have a profound effect on the efficacy and trustworthiness of the IoT system.

The potential threats and attacks that affect the privacy and integrity of the IoT system are illustrated in Fig. 2. The prominent security properties that are considered while designing a potential IoT security framework are as follows:

- *Confidentiality:* Confidentiality is one of the crucial parameters in the IoT systems. It is essential to ensure that the important information stored in IoT devices is not accessed by any unauthorized entities. However, in some of the cases such as financial applications, although the communicated data is encrypted and is transferred confidentially, intruders can gain access to the device data and manipulate it. This risks the confidentiality of the system data and restricts the adaptability of IoT devices [27].
- *Integrity:* The integrity of the device information can be strengthened by allowing the access of data only to authorized entities. Since a major portion of data is communicated through wireless networks, the IoT network becomes more susceptible to cyber-attacks. Integrity ensures an efficient verification process for detecting the changes in the communication while communicating over an insecure wireless network. Integrity protects the system from various malicious threats which can introduce SQL injection attacks [28]. Lack of integrity can reduce the operation of the IoT devices if not detected in the early stages.
- *Authentication:* The identity of the user or device should be known before performing any task. However, due to the dynamic behavior of the IoT systems, the authentication process differs from one system to another. Hence it is essential to consider the device attributes and functionalities while designing an appropriate authentication framework. In addition, the design of an authentication system must achieve a proper tradeoff between the system requirements and security constraints in order to develop a robust security approach [29].
- *Authorization:* Data authorization schemes are mainly used for protecting the sensitive information by ensuring an authorized access to the data. Authorization schemes make use of different access policies and tokens to define a specific control action and thereby authorizes the actions performed on IoT applications. In general, authorization schemes are classified as policy based and token based architectures [30]. Policy based authorization schemes are more appropriate for centralized systems which depend on a central server for access control. On the other hand, token based schemes are more suitable for decentralized systems and are more advantageous compared to policy based schemes [31].
- *Availability:* In IoT systems, the data collected from different devices should be available either on the private or public cloud. Availability of the data is important

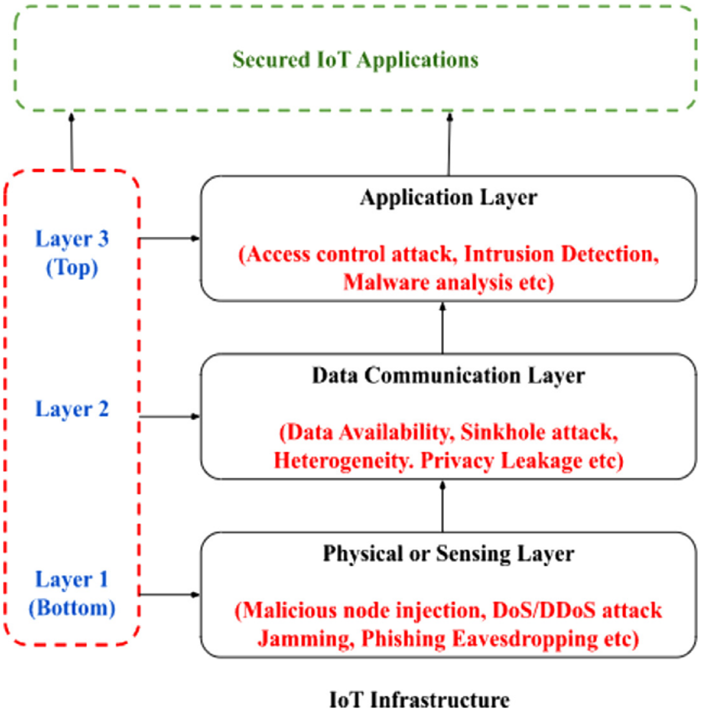
Secured IoT Applications
Layer 3
(Top)
Layer 2
Layer 1
(Bottom)
Application Layer
(Access control attack, Intrusion Detection, Malware analysis etc)
Data Communication Layer
(Data Availability, Sinkhole attack, Heterogeneity. Privacy Leakage etc)
Physical or Sensing Layer
(Malicious node injection, DoS/DDoS attack Jamming, Phishing Eavesdropping etc)
IoT Infrastructure

Fig. 3. Layer-wise security attacks in IoT.

Table 1
Security challenges in IoT.

References	Attacks	Layer	Security challenges
[34]	DoS, DDoS attacks	Network layer	Secure IoT offloading, Access control, Data Availability, and Heterogeneity
[35]	Jamming	Network layer	Identity, Leak of Private Data, Confidentiality
[36]	Phishing	Network layer	Authentication
[37]	Phishing	Network layer	Prediction and Prevention
[38]	Intrusion	Application layer	Access control
[39]	Malware Detection	Application layer	Malware detection and Access control
[40]	Eavesdropping	Physical layer	Confidentiality, Device Integration

since it allows the authorized entities to access their specific information resources. Data availability in IoT systems involves both hardware and software availability where hardware availability means that the data can be readily accessed by the IoT devices and in software availability the service provided to the end users should be authorized before being accessed [32].

- *Non-repudiation:* Non-repudiation secures the reliability and trustworthiness of the data shared between two systems. Non-repudiation assures that the validity of data cannot be denied since it provides the proof of the origin of data, reliability, and integrity of the data [33].

The security attacks on IoT are different for each layer as shown in Fig. 3 and layer-wise security attacks in IoT are discussed in Table 1 Correspondingly, machine learning algorithms for solving the security issues in IoT are presented in Table 2.

4. Machine learning for IoT security

Machine learning and deep learning techniques are based on artificial intelligence which plays an important role in detecting malware and malicious network traffic in IoT systems. In conventional attack detection systems, detection of malicious network traffic and classification of network attack is performed using predefined strategies and feature sets. Hence, these techniques fail to identify new types of attacks and are restricted to attack detection of specific types. This limitation can be resolved using ML algorithms which learn from previous experience instead of depending on certain predefined rules and specifications [57]. Several research works have implemented and validated the effectiveness of ML algorithms for the security of IoT in recent times [58,59]. It can be inferred from these studies that ML algorithms can handle the dynamic behavior of IoT systems without requiring any manual intervention. Hence, ML algorithms can be used for detecting different IoT attacks in the early stage by monitoring

Table 2
Security threats in IoT and ML-based solutions.

References	Security threats/attack	ML-based solutions
[41–43]	Authentication	Deep Neural Network Q- Learning Recurrent Neural Network (RNN)
[44–46]	Attack Detection and Mitigation	Support Vector Machine (SVM) Deep Belief Network (DBN) Random Forest K-Nearest Neighbor (KNN) Extreme Learning Machine (ELM
[47–49]	DoS and DDoS Attack	Random Forest and Decision Tree ResNet Neural Networks Support Vector Machine Deep Learning
[50–53]	Anomaly/Intrusion Detection	Artificial Neural Network (ANN) Naive Bayes Random Forest K-means clustering Federated Learning Deep Learning
[54–56]	Malware Analysis	Deep Convolutional Networks Artificial Neural Network Naive Bayes, and Principal Component Analysis (PCA) Ensemble Learning Recurrent Neural Network

the behavior of the network and are suitable for resource constrained IoT devices.

In general, ML algorithms are broadly categorized into three types namely supervised, unsupervised, and reinforcement learning (RL) algorithms as shown in Fig. 4

4.1. Supervised ML algorithms

Supervised learning is predominantly used in ML algorithms for performing a specific task. In this process, ML models are trained using a learning algorithm and a training dataset, based on which the output is classified. Classification and regression are the two types of process used in supervised learning.

4.1.1. Classification algorithms

Supervised ML algorithms classify the output based on the input data into a particular category such as true or false, real or fake etc. The most prominent supervised ML algorithms used as classifiers are SVM, NB, KNN, and RF.

- *Support Vector Machine (SVM):* SVM algorithm is one of the progressive ML algorithms adopted for classification and regression techniques. SVM uses a supervised learning process to classify different types of security attacks such as DoS/DDoS [60], privacy preservation [61], IoT botnet detection [62], Cipher attacks and plain text attacks in IoT architecture [63]. The classification accuracy of SVM is comparatively higher and hence is a better candidate for securing IoT systems [62]. However, the main drawbacks of SVM are; high generalization, slow convergence speed and high sensitivity to local extrema. Hence the performance efficiency of conventional SVMs are affected by unbalanced samples.
- *Random Forest (RF):* Similar to DTs, the RF algorithm is also a supervised ML based classification algorithm. The RF algorithm creates the forest with a certain number of trees. More the number of trees in the algorithm, more robust is the potential of the algorithm i.e., higher the number of trees in the algorithm leads to higher classification and prediction accuracy. Due to its excellent classification abilities, RF is widely used in different IoT security processes such as anomaly detection [64], user to root attack, and remote to local attack detection etc [65]. However, the performance of RF is affected when the number of trees increases beyond a certain count and this makes the algorithm slow and less effective for real-time classification tasks.
- *K- Nearest Neighbor (KNN):* KNN algorithm uses Euclidean distance as a metric to determine the distance between two nodes which in turn defines the average value of the unknown node, which is the sum of its k-NN. For instance, if a node is lost then the average value of the nearest neighbor can be used to predict the loss. This value helps in identifying the missing node. In IoT, KNN is used for malware detection [66], anomaly detection [67] and intrusion detection [68]. KNN is advantageous in terms of its simplicity, cost effectiveness and flexible implementation. However, KNNs do not work well with larger datasets and are highly sensitive to outliers and missing values.
- *Naive Bayes (NB):* The NB algorithm works based on the principle of Bayesian theorem which uses the probability of statistics theorem for learning. This type of supervised learning helps the NB to generate outputs based on previous information and their probability of learning. In IoT, NB algorithm is used to predict the attacks based on the information learnt in the past and is suitable for detecting anomalies in the network layer [69]. NB is easy to understand, requires fewer data for classification, and is suitable for performing multi-stage classification. One main drawback of NB is the dependency on the interaction between the features which requires past information. This restricts the accuracy of NB as a classifier.
- *Logistic Regression:* Regression analysis is a set of statistical processes used for determining the relationship between dependent and independent variables. Logistic regression employs a generic way to perform statistical analysis using a logistics function. The work proposed by [45] implemented logistic regression for detecting compromised nodes in IoT. A cryptographic technique and trust-based authentication scheme is adopted for

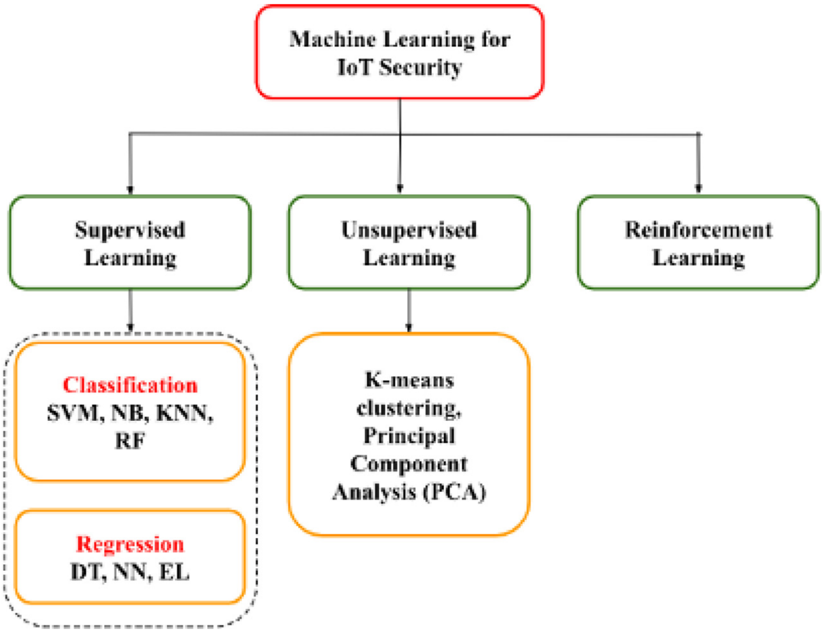

Fig. 4. Taxonomy of ML algorithms for IoT security.

ensuring that the nodes in the IoT network are authenticated by monitoring their behavior. Logistic regression possesses better throughput, average delay and high attack detection rate. However, logistic regression algorithms suffer from overfitting problems and difficulty in analyzing complex relationships between data patterns.

4.1.2. Regression algorithms

Regression algorithms investigate the relationship between independent features (variables) and a dependent variable for predicting the output. The output can either be a continuous value or a real number based on the input. DTs, NNs, and ELs are the types of regression algorithms which are discussed in below points:

- *Decision Trees (DT):* DTs are better classifiers which can also perform regression tasks similar to SVM. DTs can predict the value of a target variable by learning simple decision based rules. These rules are derived from the extracted features. For a given sample, initially an individual decision tree will perform a random selection process through the bootstrap resampling mechanism and the obtained samples will be employed for constructing a decision tree. In a decision tree, each leaf node is provided with a class label and the non terminal nodes which consists of internal and root nodes, are incorporated with certain feature test constraints to distinguish different features with different characteristics. DTs are widely used in IoT security to classify different types of attacks such as intrusion detection [70], user centric security solutions [71] and interference recognition [72]. One of the prominent drawbacks of DTs is associated with its stability. DTs are highly unstable and they fail to handle continuous variables and hence generate less effective results.
- *Linear Regression:* Linear regression (LR) is used for analyzing the relationship between different input and output variables. LR models predict a target value based on independent variables. One of the prominent prerequisites for LR algorithm is the Markov property which states that the present instance is dependent on the previous instances. The preliminary aim of the LR model is to achieve an accurate estimation of the LR parameters by reducing the error between the estimated value and the actual value [73]. LR algorithms are simple to implement and are less complex compared to other ML models. However, the performance of LR models is affected by the presence of outliers. Besides, LR models assume a linear relationship between the input and output variables, which is not suitable for practical applications.
- *Neural Networks:* The architecture of NNs resembles the structure of the neurons in the human brain. NNs can handle complex and nonlinear data without affecting the performance efficiency [74]. Neural network models are either connected in a hierarchical manner or are interconnected with other layers in the network. In general, NNs consist of three main layers namely an input layer, hidden layers and an output layer. There can be multiple hidden layers in a single network and the function of NNs depends on these layers. NNs are characterized by their fast response time and superior performance in IoT systems. However, the computational complexity of NNs is too high and it is challenging to adapt them in a heterogeneous IoT system.
- *Ensemble Learning (EL):* EL integrates two or more ML algorithms for generating a desired output with high performance efficiency. Since EL is a combination of multiple learning algorithms, it is suitable for solving

most of the complex problems in IoT such as network monitoring, attack detection, intrusion detection, botnet detection and anomaly detection [75,76].

4.2. Unsupervised ML algorithms

Unsupervised algorithms can discover hidden patterns and analyze unlabeled datasets without depending on any training datasets. Since these algorithms work on unlabeled data, they try to evaluate the similarities between the data samples and the input variables and classify the samples into individual groups known as clusters. Several, unsupervised ML algorithms are implemented for strengthening the privacy and security of IoT devices [77]. K-means clustering, PCA, Hierarchical Clustering, Fuzzy K-means Clustering, and Gaussian Mixture Models (GMMs) are the most widely used unsupervised ML algorithms.

- *K-means clustering:* K-Means clustering algorithm intends to cluster 'n' number of objects into 'k' number of clusters where each object belongs to the cluster with the nearest mean [78]. This method generates exactly 'k' different clusters of greatest possible distinction with each center having a centroid. The best number of clusters 'k' leading to the greatest separation (distance) is not known as a priori and must be computed from the data. The main goal is to evaluate the centroid for all the clusters and then select a node which is placed at a nearest distance to the centroid. This process is continued till all nodes are connected. K-means algorithm works effectively on unlabeled data and its simple implementation makes it an ideal candidate for IoT systems [79]. However, this algorithm underperforms compared to supervised learning algorithms. Most commonly, K-means is used for detecting anomalies and sybil attacks in IoT.
- *Principal Component Analysis (PCA):* PCA is used as a dimensionality reduction technique which extracts relevant features and converts a large dataset into a smaller dataset without losing any information. As a result, PCA improves the computational speed and reduces the complexity of the attack detection models. PCA improves the performance of ML algorithms by selecting features related to attack detection in IoT [80]. However, it is difficult to interpret the correlation between the features using PCA and it assumes a linear relationship between two features. In addition, PCA is not robust against any outliers and this affects the performance of PCA.
- *Hierarchical clustering:* Hierarchical cluster analysis (HCA) algorithm creates a hierarchy of clustered data samples. The clusters are obtained by decomposing or segmenting the data samples based on their hierarchy. Unlike K-means clustering, HCA does not require any predefined number of clusters for analysis [81]. There are two types of hierarchical clustering namely agglomerative and divisive clustering approaches [82]. Agglomerative employs a bottom-up method, wherein each dataset is considered as a single cluster and the closest cluster pairs are grouped together. The process is continued till all clusters are merged into a single cluster. On the other hand, the divisive method is the reverse of the agglomerative approach, which uses a top-down approach. HCA is advantageous since it is independent of predefined number of samples. One of the major drawbacks of HCA is its inability to work with mixed data types and its performance deteriorates when used for handling large scale datasets.
- *Fuzzy K-means Clustering (FCM) algorithm:* The FCM algorithm is a soft clustering approach which uses the principles of fuzzy logic for clustering the multidimensional data wherein each data point is assigned with a probability score belonging to a particular cluster [83]. The FCM algorithm is more effective when compared with conventional clustering techniques where each data point is assigned to an exact label.
- *Gaussian Mixture Models (GMMs):* GMM is a probabilistic technique which assumes that all the data samples are generated from a mixture of a finite number of Gaussian distributions with unknown parameters [84]. GMM models are classified into hard and soft clustering algorithms. Mixture models employ a probabilistic approach as soft clustering wherein each clauser represents a probability distribution in a 'd' dimensional space wherein each data point represents the samples formed by the probability distribution

4.3. Reinforcement learning (RL)

RL algorithms allow the system to learn from the interaction with the external environment based on certain actions. RL models incorporate an efficient Q-learning mechanism which allows the system parameters to make decisions automatically without requiring any previous knowledge of the environment. In RL, the actions are performed dynamically for performing any task and use trial and error process for identifying the appropriate action to gain maximum reward. Different RL algorithms such as Q-learning, deep Q network (DQN) etc are used in detecting security attacks in IoT [85]. RL algorithms can overcome the limitations of conventional machine learning algorithms such as; high computational time, requirement of larger parameters for training, poor accuracy, inability to handle complex problems etc. RL suffers from the problem of high computation overload since it requires a lot of data for computation.

The performance of different ML algorithms for IoT security is evaluated with respect to its accuracy of attack detection.

Table 3 discusses the performance evaluation of ML algorithms. As observed from the analysis, most of the ML algorithms achieve better performance in terms of classification and detection accuracy. SVM, DT, KNN, K-means algorithm and RF achieves superior performance with more than 99% of detection accuracy.

However, ML algorithms suffer from certain limitations which limits their performance efficiency. ML algorithms are

Table 3
Performance of different ML algorithms for IoT security.

ML algorithm	Attack detection in IoT	Accuracy of detection	Reference
Supervised learning			
Support Vector Machine (SVM)	Malware detection	99.96%	[86]
	Malicious node detection	90.00%	[87]
	Data Authentication	99.40%	[88]
Random Forest	Anomaly detection	99.6%	[89]
	DDoS attack detection	99.63%	[90]
K- Nearest Neighbor (KNN)	Classification of IoT devices	85%	[91]
	Security of IoT data	95%	[92]
Naive Bayes (NB)	Cyber security in IoT	96.3%	[93]
	Intrusion detection and DDoS attacks	78%	[94]
Decision Trees (DT)	Multiclass attack detection	99.92%	[95]
	Botnet detection	99.89%	[96]
Ensemble Learning	Anomaly detection	99.8%	[97]
	Malware detection	99.98%	[98]
	Cyberattack detection	96.35%	[99]
Unsupervised learning			
K-Means clustering	Intrusion detection	99.94%	[100]
PCA	DDoS attack detection	95.24%	[101]
Reinforcement learning			
Q-Learning	Malware detection	Improves the accuracy by 40%	[102]

trained using a large number of training samples and this increases the computational burden on the IoT system and risk of privacy leakage. This restricts the adaptability of ML algorithms for IoT applications. To overcome the limitations of conventional ML algorithms, Federated learning (FL) is used as an alternative since they are not computationally intensive. Thus, this section discusses the role of Federated Learning and Deep Learning as a solution for security problems in IoT.

5. Federated learning

Federated learning is an effective solution for decentralized systems which require on-device training without compromising on the privacy of the data [13]. Recently, FL has become one of the extensively employed solutions for maintaining the privacy and integrity of the data with low latency [103–106]. FL overcomes the drawbacks of centralized paradigms and over performs conventional ML techniques in terms of maintaining the privacy of data while sharing information with other systems. An exceptional strategy is used by FL models which allows them to share a trained ML model with multiple devices and the trained ML model will help these devices to learn from the surrounding environment utilizing the available computational resources. With its superior attributes and operational concepts, FL offers various advantages as discussed in below points:

- *Privacy Enhancement:* FL does not require raw data for training the model. Hence, the chances of leaking confidential information to a third party entity is very minimum and therefore the privacy of the data is maintained. This privacy enhancement mechanism makes FL an appropriate candidate for developing a robust security approach for IoT systems.
- *Low latency communication:* Since it is not required to transmit the IoT data to the server, the application of FL helps in reducing the communication latency caused due to the data offloading. Correspondingly, FL also reduces the computational burden and minimizes the utilization of network resources.
- *Improved Learning Quality:* FL can improve the convergence rate and quality of learning to achieve desired accuracy [107] which is not possible using conventional ML techniques. In addition, the distributed learning ability of FL enhances the scalability of the IoT networks.

These distinctive advantages of FL makes it one of the most extensively used techniques in several IoT applications. Although FL is researched widely in previous literary works, there is a lack of dedicated research which signifies the application of FL for IoT security. Hence this research focuses on highlighting the adoption of FL for IoT security. The taxonomy of FL models for security of IoT networks is discussed in Table 4.

5.1. Concepts of federated learning

The concept of FL in IoT involves two main components namely data clients and an aggregation server. Here, data clients are represented as IoT devices and the server is located at the base station (BS) as shown in Fig. 4. Let $P = (1, 2, \ldots., P)$ be the set of IoT users who collectively adopt a FL model for performing a specific task in IoT. In the FL process, each user shares a trained ML model by using their own dataset D_p. Further, the FL model is trained using the local data available and once the model is trained, it is uploaded by the users to the base station and then aggregates all the models to develop a shared model. This aggregated model is called the global model wG. Since IoT devices are distributed in nature, the aggregated server at the base station can enhance the training process without compromising on the privacy and integrity of the user data. The architecture of the FL-IoT model is illustrated in Fig. 5.

As shown in Fig. 5, the process involved in federated learning includes three main stages namely; system initialization and device selection, local training and update, and model aggregation as discussed in below points:

- *System Initialization and device selection:* During system initialization, the aggregator selects to perform certain IoT tasks and trains the model using learning parameters. The aggregator also selects the IoT devices which can

Table 4
Taxonomy of FL-based models for IoT security.

Security issues	Reference	IoT use cases	Specification of FL	Limitations
Attack Detection in IoT	[108]	Attack defense	A FL-based attack defense network is proposed for industrial IoT networks	The effect of communication latency is not considered
	[109]	Attack detection	A FL model for detecting security attacks in IoT	The issue of data privacy is not addressed
	[110]	Attack detection	Federated attack detection in industry 4.0 using FL	Scalability issue is not investigated
	[111]	Intrusion detection	An intrusion detection model is developed using FL for IoT	A fundamental FL model is considered and its performance is not empirically analyzed.
	[112]	Intrusion detection	Scalable detection of intrusion in IoT using FL	The performance of FL is not validated by comparing with ML and DL approaches.
	[113]	Malware detection	Detecting malware in android applications using FL	The convergence of learning process is not addressed.
	[114]	Intrusion detection	A FL based IDS is developed for detecting intrusions in agricultural IoT.	The model is tested for closed and centralized models. There is a need to test the FL-based IDS for decentralized models.
	[115]	Intrusion detection	A comprehensive review of FL techniques for detecting intrusions are discussed.	Coordination between different IoT devices is a major bottleneck and needs a deeper investigation.
	[116]	Data breaching	FL is used for identifying and preventing data breaching in industrial IoT.	The performance of FL needs to be tested for larger datasets.
Security and Privacy of IoT	[117]	Privacy Preservation	A FL-based privacy preserving model for vehicular IoT	The convergence performance is not evaluated.
	[118]	Privacy Preservation	A FL-based differential privacy approach for strengthening privacy in IoT	The issue of communication latency is not considered while sharing data with the cloud
	[119]	Privacy Preservation	A privacy preservation model for crowdsourcing systems in IoT	The effect of Blockchain mining on IoT is not evaluated
	[120]	Anomaly Detection in IoT	A multitasking FL approach for detecting anomalies in IoT networks	Detailed experimentation is not conducted
	[121]	Malware detection in IoT devices	Security enhancement in IoT using FL	Energy performance and learning ability is not discussed
	[122]	Anomaly Detection in IoT	decentralized FL is implemented for protecting data security in IoT.	The performance of FL with respect to neural networks needs more validation.
	[123]	Privacy Preservation	FL is implemented for privacy preservation in IoT-based healthcare system using Blockchain.	The issue of communication latency and intensive computation is not discussed.

participate in the federated learning process and updates the learning process through local computation for each device [106].

- *Local training and update:* Once the system is initialized, the configuration is trained and a new model is initialized by the server which is denoted as w_G^0 and the model data is transmitted to the users for initiating distributed training. Each user trains the local model using their dataset D_p and then updates the training data w_p and thereby minimize the loss function $F(w_p)$ as shown in below equation:

$$W_p^* = argmin F(w_p),\ p \in P \tag{1}$$

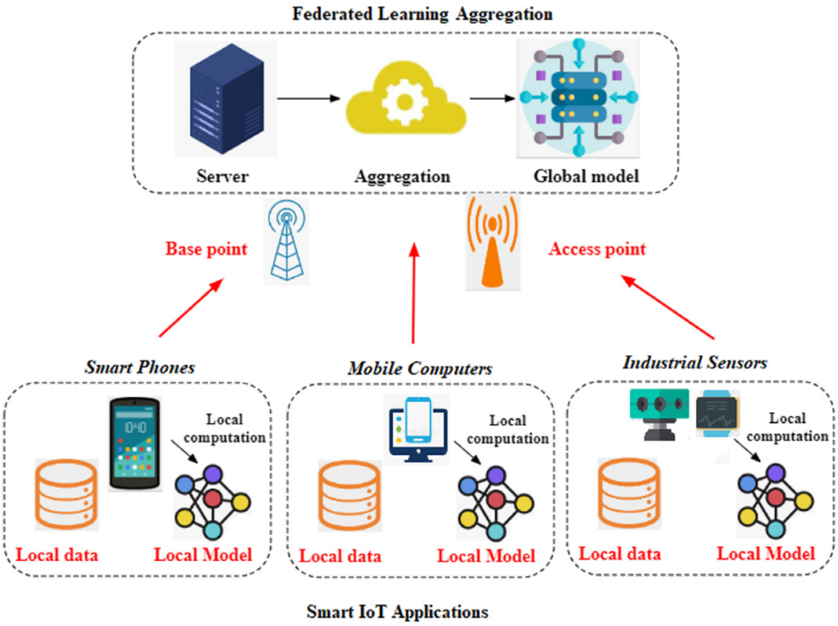

Fig. 5. Integrated architecture and communication process for FL-IoT.

The loss function can be different for different FL processes and for each process the client p updates their computed value w_p in the server for aggregation.

- *Model Aggregation:* After training and updating the model by the local clients, the server aggregates the model and then computes the new model for the global model as shown in Eq. (2):

$$w_G = \frac{1}{p \in P|D_p|} \sum_{p=1}^{P} |D_p| w_p \tag{2}$$

Further, the loss function can be minimized by solving the optimization problem as shown in below equation:

$$P_1 = min_{w_p \in P} \frac{1}{P} \sum_{p=1}^{P} F(w_p) \tag{3}$$

Where F is the loss function which represents the accuracy of the FL process [124]. The constraint (P1) ensures that the same learning model is shared by the clients and the server throughout the FL process after each training session. After aggregation, the server shares the new update value w_G for the global model with all the clients. The local model is further optimized in the next learning stage. The process is continued till an optimized global value is obtained which helps in achieving the desired accuracy.

The constraint (P1) ensures that the same learning model is shared by the clients and the server throughout the FL process after each training session. After aggregation, the server shares the new update value w_G for the global model with all the clients. The local model is further optimized in the next learning stage. The process is continued till an optimized global value is obtained which helps in achieving the desired accuracy.

5.2. State of art of FL for IoT security

The increasing significance and adaptability of IoT applications has increased the susceptibility of IoT devices towards adversarial attacks and security threats that affect the ML, FL, and DL models. These threats tamper the data inputs and modify the network parameters to generate an erroneous output [125]. Several research works have discussed the implementation of FL to develop potential solutions for IoT security. Techniques such as ensemble or adversarial training [126] are proposed for securing IoT systems. However, these techniques work for only specific types of attacks that are not scalable enough when applied for distributed networks. FL can cope with the distributed nature of the IoT network and is capable of detecting an extensive range of security threats and attacks and can play an important role in developing robust defense solutions. Based on the privacy enhancement properties of FL, the security frameworks are designed in such a way that each IoT device can run a neural network model in parallel to strengthen the security model against different adversaries. The integration of FL with IoT expedites the learning process and accelerates the attack detection mechanism while minimizing the risks. In a heterogeneous learning environment such as IoT, it is essential to develop an attack detection module inside the FL environment. One such attack detection framework is presented in [127] for ensuring a safe and reliable FL process. In simple words, a dynamic model is designed for evaluating the aggregated parameters which is tuned to mitigate the attacks in IoT while interacting with the FL. This research motivates the researchers to develop novel and unique solutions for detecting and preventing different types of attacks incorporating FL as discussed in [128]. In this research, an efficient anomaly detection process is developed and deployed at the global server for identifying rare and distinct updates by removing the malicious data instances and keeping only important and relevant data features. In real time scenarios, IoT devices can contain malicious information and this data can be updated at the global server. In such cases, it is important to identify and detect malicious nodes to ensure the safety of IoT devices in the FL environment [129]. It can be inferred from previous works that there is a requirement of a pre-trained attack detection model which can identify the unusual behavior of the users and IoT devices by monitoring the network and by updating the models continuously at the global server. As a consequence, the vicious attacks and unauthorized users can be identified and prevented using the FL process [130]. In addition, FL models can also be trained to detect unauthorized users in dynamic IoT networks [131]. FL models also expedite the identification of compromised (malicious) IoT devices in FL networks. However, communication bottleneck is one of the serious issues in the FL-based IoT environment which increases the communication delay. A survey of different works done to alleviate communication bottleneck is presented in [132]. The communication congestion can be created due to the increased number of participating devices, network bandwidth, limited edge node computation, and heterogeneity. The study states that this limitation can be resolved by updating the model, selecting clients to restrict the number of participating devices and ease the communication load, by performing decentralized training and Peer-to-Peer learning. The authors [133] addressed the issue of communication bottleneck by implementing a generic decentralized FL (DFL) approach. The DFL can operate in both synchronous (Sync-DFL) mode and asynchronous (Async-DFL) mode to mitigate communication congestion around the central server. The Async-DFL is the first DFL to introduce a generic FL-framework which is asynchronous and can avoid waiting periods. This results in the effective training of the distributed model in a heterogeneous IoT environment. In addition to the communication bottleneck, another concern with respect to FL-based IoT is the intermittent connectivity of the IoT devices which affects the stability of the communication process. The connectivity issue in FL-based IoT is discussed in [134] by proposing a novel framework developed using a Message Queue Telemetry Transport (MQTT) protocol and the Open Mobile Alliance (OMA) Lightweight Machine-to-Machine (LwM2M) semantics to strengthen FL model while handling IoT devices. The feasibility of the protocol in improving the connectivity and communication efficiency is discussed and is compared with existing Proof-of-Concept (PoC) to validate the scalability. A brief evaluation of the FL process for IoT is discussed in Table 5.

Considering the advancements and sophistication of security attacks, it is highly complicated to identify them using the current models which can recognize the attacks by identifying the variations from the normal behavior of the network and IoT devices with a lower false alarm rate and detection time [135]. Along with FL, this section also discusses the role of deep learning (DL) models in the security of IoT systems.

6. Deep learning for IoT security

Deep learning (DL) is the most advanced technique used for exploring the data to study the ‘normal’ and ‘abnormal’ functioning of the IoT components based on device interactions within the IoT environment [136]. DL models are capable of anticipating new attacks by taking a cue from previous attacks and they also brilliantly predict new future attacks by learning from previous instances. It must be noted that, with the increase in the attacker’s strength and resources, conventional machine learning techniques used for attack detection becomes ineffective in detecting complex cyber attacks. These techniques fail to identify the changes in the variants of the threats and attacks and cannot extract relevant features to distinguish novel attacks or variants from benign. Deep learning-based neural networks can overcome this problem since they are capable of handling complex classification and attack detection tasks [137]. An illustration of the potential of DL models for IoT security is shown in Fig. 6 The workflow of the DL process in the attack detection process is summarized in below points:

- *Data Preprocessing:* Data preprocessing is one of the preliminary stages involved in the attack detection process. Preprocessing is performed to filter out the uncertainties present in the data in the form of external noise, missing data, null values, redundant data etc. The raw input data will be processed in order to make it suitable for classification. The uncertainties present in the input data will affect the classification accuracy and hence they must be eliminated in order to achieve better detection and classification of attacks in IoTs.
- *Feature Extraction:* It is one of the important steps in the attack detection process. In general, feature extraction is a process wherein only relevant and important features are extracted from the input data. Extraction of only important features will reduce the dimensionality since most of the features are not contributing enough to the overall attack detection process. Reducing unwanted and redundant features will also reduce the computational time and improve the overall performance of the attack detection process.
- *Attack Detection and Classification:* In this process, the extracted features are given as input to the DL model for identifying the security attacks. After detecting the attacks from the input data, the classifier will classify different types of attack such as DoS and DDoS attacks etc based on the extracted attack-related features. Here, the DL models will be trained to monitor the network continuously in order to identify any abnormal changes in the behavior of the network. Once the changes are detected, the model will classify the data as normal or malicious.
- *Performance Evaluation:* The performance of the DL models is evaluated in terms of different performance metrics such as accuracy, precision, recall, f1 score and support.

Table 5
Evaluation of FL process for IoT security.

Evaluation metrics	Description	Advantages of FL
Privacy and Security	Privacy and security deals with the protection of IoT systems from malicious attacks.	Enhanced privacy protection, Trustworthy verification and learning process Secure data transmission
Scalability	Scalability is a measure that defines the ability of a FL model which can operate with more number of users and provide better accuracy	High FL accuracy Robust connectivity
Sparsification	This metric helps the FL model to select appropriate IoT devices for performing a specific task	Low convergence time High accuracy of learning
Robustness	Robustness defines the ability of the FL process which can swiftly learn from the external environment and prevent the possibility of failure	Cost optimization Accurate FL model
Quantization	This metric necessitate the need for reducing the size of the local learning process to minimize the convergence time	Fast FL convergence High accuracy due to learning process

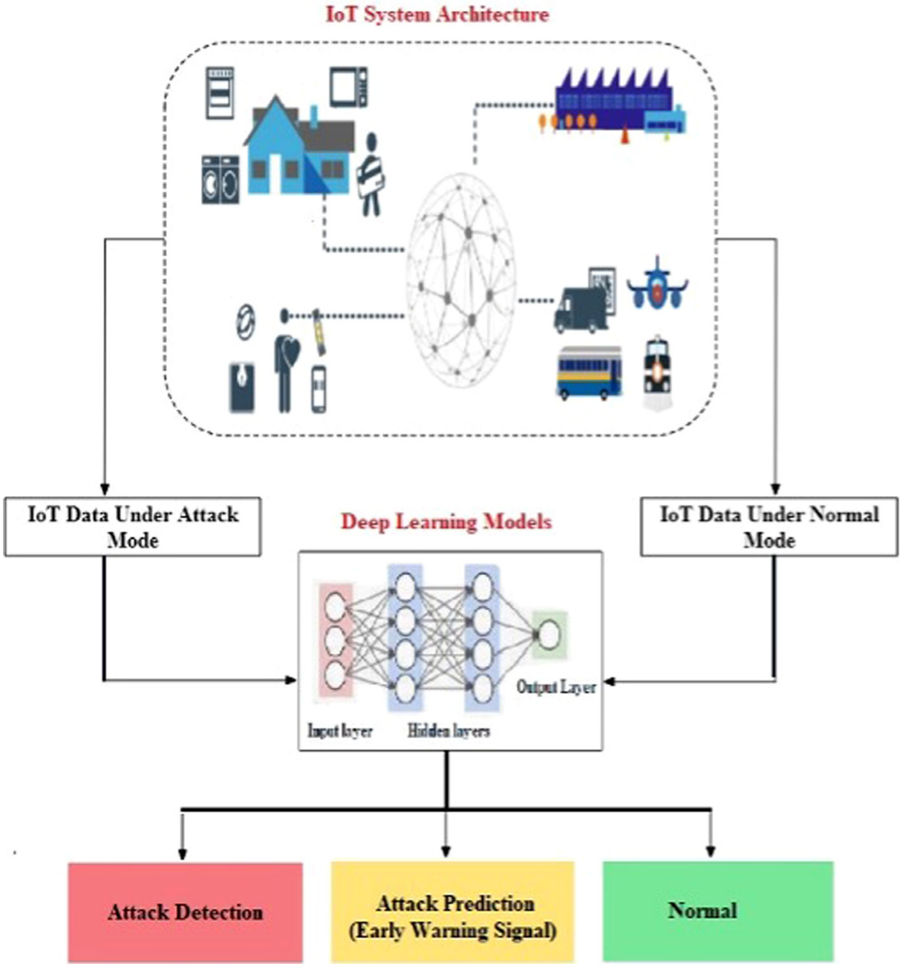

Fig. 6. An illustration of DL model for IoT security.

Table 6
DL models for securing IoT systems.

DL models	Working principle	Advantages	Limitations	Application for IoT security
Deep Neural Networks [138]	DNN is a type of artificial neural network (ANN) which uses a nonlinear transformation method for evaluating the input and then creates a statistical model for generating the output based on its learning ability.	DNNs are capable of modeling complex and nonlinear models for creating computational models which can handle large scale data with high accuracy.	DNN suffers from vanishing gradient problems which usually occur in the layers present at the bottom of the network	Intrusion detection
Recurrent Neural Networks (RNN) [139]	RNN belongs to the class of neural networks wherein the output of the network from the previous step is fed as input to the current step for computing the output.	RNNs have the capacity of automatic learning and sequence prediction based on the previous data with high prediction capability.	Training of RNN is a slow and complex task. Besides, it is also difficult to process longer sequences.	Malware detection
Deep Reinforcement Learning (DRL) [140,141]	The DRL algorithm employs an efficient Q-learning mechanism which allows the system parameters to make decisions automatically without requiring any previous knowledge of the environment.	DRL can overcome the limitations of conventional ML algorithms such as; high computational time, requirement of larger parameters for training, poor accuracy, inability to handle complex problems etc.	The performance of the DRL algorithm can be affected due to sampling efficiency problems	Attack detection and Intrusion detection
Generative Adversarial Networks (GANs) [142,143]	GAN consists of two individual neural networks such as: a Generator ‘P’ that includes a random noise vector n and creates a synthetic data P (n) and a discriminator Q that considers an input x or P (n) to generate an output of a probability Q(x) or Q (P(n)). This distinguishes whether the input is obtained from the synthetic data P (n) or from true data distribution	GANs are capable of generating additional data from the available training dataset and are simple to train.	GANs suffer from the problem of slow convergence or non-convergence and diminishing gradient	Securing data privacy, attack detection and Intrusion detection
Deep Belief Networks (DBNs) [144]	DBN is constituted using two types of neural networks such as Belief networks and another one is the Restricted Boltzmann Machines (RBM) wherein every single layer is RBM which is stacked to each other to develop DBN	DBN is highly accurate and efficient when dealing with complex	DBN incorporate complex mathematical computation and training DBN using complex and large scale data can be computationally expensive	Intrusion detection, and preventing security breach
Convolutional Neural Networks (CNN) [145] [146]	CNNs operate by extracting features from the images automatically without manual intervention. The structure of CNN differs from other neural networks (NNs) with respect to the shape and function of the layers.	CNNs require less preprocessing compared to other algorithms and can learn the features even from handmade filters with proper training	The performance of CNN is affected due to the issues such as signal down sampling and low spatial consistency	Real-time attack detection, and Anomaly detection in IoT

6.1. State of art of DL models for IoT security

DL models are the subset of ML algorithms which capture hierarchical representations in the neural network architecture. Their ability to handle large scale data without increasing the complexity of the networks makes them a popular candidate for developing security solutions for IoT systems. Some of the prominent models used in IoT security and their performance evaluation are discussed in Table 6 and Table 7 respectively.

The performance of the DL model in terms of different evaluation metrics is discussed in Table 7. As observed, DL models achieve phenomenal accuracy in terms of detecting

Table 7
Performance evaluation of DL models for security of IoT.

Reference	DL model	IoT application	Performance metric used
[147]	Deep CNN	Cybersecurity threat detection	Classification accuracy = 97.46%
[148]	RNN-based Long Short Term Memory (LSTM)	IoT architecture for smart cities	Precision = 0.7244, Recall = 0.7078, F1 score = 0.7118, with high scalability
[149]	Feed-Forward Deep Neural Network (FFDNN) based on feature extraction	Wireless computer networks, vehicular networks, and cyber physical systems	Binary classification accuracy = 99.66% and Multiclass classification accuracy = 99.77%
[150]	Text-CNN and Gated Recurrent Unit (GRU)	Intrusion Detection System for IoT systems	F1 score = 0.98
[151]	Long Short Term Memory (LSTM)	Intrusion Detection System for IoT systems	Prediction accuracy = 99.5% for NSL-KSS dataset, 99.3% for CIDDS-001 dataset and 99.1% for UNSWNB15 dataset
[152]	Depp CNN model	Identification of cyber-attacks in IoT communication networks	Binary classification accuracy = 99.30% and Multiclass classification accuracy = 98.20%

Table 8
Comparison of FL and DL for IoT security.

Federated learning	Deep learning
FL is used for distributed training of classical ML algorithms on different edge devices without exchanging training data	DL is a subset of ML algorithms, which forms a neural network with two or more layers
FL models can train the model without revealing the sensitive information to a central cloud server	The data is collected and the model is trained on a single server, which increases the risk of privacy when the data is shared with a central cloud server
The implementation of FL for edge devices is restricted by the resource constraint behavior of IoT devices. However, FL models are less intensive	DL models are computationally intensive, which imposes strict requirements on hardware and results in low training efficiency in edge devices
The models in FL are updated continuously and allow client input. Hence there is no need of data aggregation	DL models require aggregation of user data in IoT in a centralized location, which increases the chances of data breaching

intrusions and different cyber-attacks. Results validate the application of DL models for IoT security. Although the DL model exhibits excellent performance, there are certain aspects which makes it indistinct from the FL models. A brief comparison of FL and DL is discussed in the Table 8.

7. Challenges associated with FL and DL models

A comprehensive analysis of the ML based security approaches is discussed in the previous section with an emphasis on FL and DL. Despite the availability of several security frameworks there are certain challenges and issues which need to be addressed.

1. *Security and Privacy Issues in FL:* Though FL minimizes the risk of privacy protection in IoT, the vulnerabilities associated with FL are still a critical challenge [153]. This is due to the changes that the end users can alter the data features of inject a compromised set of data into the original dataset aiming to tamper the objective of the end application. This is also called backdoor attacks. This issue needs significant attention since it affects the integrity of the FL models.
2. *Convergence Problems in FL-IoT:* The implementation of FL-IoT suffers from the problem of learning and communication convergence. This problem is because of the sensitivity in IoT networks owing to different sensing environments.
3. *Optimal Management of Resources:* The integration of FL with IoT requires a scalable platform which can enable the on-device training before aggregating the learning parameters at the global server. In order to obtain a synchronized update, the IoT devices must have enough storage and computation resources for training. However, it is difficult to satisfy this demand owing to the resource constraint nature of IoT [154]. This results in the increased delay and affects the synchronization of IoT devices.

4. *Computational Complexity and High energy consumption in DL:* As discussed previously, the resource constraintment in IoT offers a significant challenge in the deployment of DL models. Most of the existing solutions for computation offloading requires a high energy overhead and this results in the increased computational burden. To overcome this problem, most of the DL models are deployed alongside GPUs [155]. However, GPUs consume more energy and thereby depreciates the energy efficiency of the IoT systems.
5. *Security tradeoffs in IoT:* It is difficult to achieve a better tradeoff between other parameters of IoT and security. Parameters such as safety, energy efficiency, cost effectiveness, availability pose a significant challenge to achieve high security since most of the existing models compromise on any of the above stated parameters to achieve better security in IoT. There is a need to balance these parameters and provide better security without compromising on any other aspects.

8. Conclusion

This review paper focuses on the application of ML algorithms with an emphasis on federated learning and deep learning for IoT security. The study reviews various FL and DL techniques for identifying different security threats and potential attacks on IoT. Both FL and DL can be used to provide robust security against various malicious attacks since it can handle the resource constrained nature and heterogeneity of IoT devices. This review also outlines the recent techniques proposed in existing works and presents a thorough analysis on the layer-wise attacks in IoT which is essential to detect for protecting the system against the adversarial attacks. Consequently, the study also explored different types of ML algorithms for providing a solution against security attacks. Based on the characteristics and functionalities of IoT devices, the security model should be designed using an appropriate DL or FL model and the security model should be trained to make intelligent decisions in a real-time environment by learning from available instances. Finally, the study also discusses and addresses the issues, challenges associated with the implementation of ML-based security approaches for IoT systems. The challenges that are highlighted in this research can be considered as promising research directions for further research in IoT security.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work is supported in part by DoD Center of Excellence in AI and Machine Learning (CoE-AIML) under Contract Number W911NF-20-2-0277 with the U.S. Army Research Laboratory.

References

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on IoT security: Application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.

[2] T.M. Ghazal, M.K. Hasan, M.T. Alshurideh, H.M. Alzoubi, M. Ahmad, S.S. Akbar, B. Al Kurdi, I.A. Akour, IoT for smart cities: Machine learning approaches in smart healthcare—A review, Future Internet 13 (8) (2021) 218.

[3] V. Lesi, Z. Jakovljevic, M. Pajic, Security analysis for distributed IoT-based industrial automation, IEEE Trans. Autom. Sci. Eng. (2021).

[4] J. Zhang, Y. Wang, S. Li, S. Shi, An architecture for IoT-enabled smart transportation security system: A geospatial approach, IEEE Internet Things J. 8 (8) (2020) 6205–6213.

[5] W.H. Hassan, et al., Current research on Internet of Things (IoT) security: A survey, Comput. Netw. 148 (2019) 283–294.

[6] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2702–2733.

[7] Q.-D. Ngo, H.-T. Nguyen, V.-H. Le, D.-H. Nguyen, A survey of IoT malware and detection methods based on static features, ICT Express 6 (4) (2020) 280–286.

[8] I. Ali, S. Sabir, Z. Ullah, Internet of Things security, device authentication and access control: A review, 2019, arXiv preprint arXiv:1901.07309.

[9] M. Khari, A.K. Garg, A.H. Gandomi, R. Gupta, R. Patan, B. Balusamy, Securing data in Internet of Things (IoT) using cryptography and steganography techniques, IEEE Trans. Syst. Man Cybern.: Syst. 50 (1) (2019) 73–80.

[10] E. Džaferović, A. Sokol, A.A. Almisreb, S.M. Norzeli, DoS and DDoS vulnerability of IoT: A review, Sustain. Eng. Innov. 1 (1) (2019) 43–48.

[11] B.K. Mohanta, D. Jena, U. Satapathy, S. Patnaik, Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology, Internet Things 11 (2020) 100227.

[12] V. Mothukuri, P. Khare, R.M. Parizi, S. Pouriyeh, A. Dehghantanha, G. Srivastava, Federated-learning-based anomaly detection for IoT security attacks, IEEE Internet Things J. 9 (4) (2021) 2545–2554.

[13] M. Aledhari, R. Razzak, R.M. Parizi, F. Saeed, Federated learning: A survey on enabling technologies, protocols, and applications, IEEE Access 8 (2020) 140699–140725.

[14] V. Mothukuri, R.M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, G. Srivastava, A survey on security and privacy of federated learning, Future Gener. Comput. Syst. 115 (2021) 619–640.

[15] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M.A. Latif, F. Al-Turjman, L. Mostarda, Cyber security threats detection in Internet of Things using deep learning approach, IEEE Access 7 (2019) 124379–124389.

[16] S. Izza, M. Benssalah, K. Drouiche, An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment, J. Inf. Secur. Appl. 58 (2021) 102705.

[17] M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maseleno, N. Arunkumar, Hybrid optimization with cryptography encryption for medical image security in Internet of Things, Neural Comput. Appl. 32 (15) (2020) 10979–10993.

[18] A. Kumar, V. Jain, A. Yadav, A new approach for security in cloud data storage for IoT applications using hybrid cryptography technique, in: 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and Its Control, PARC, IEEE, 2020, pp. 514–517.

[19] G. Kalyani, S. Chaudhari, An efficient approach for enhancing security in Internet of Things using the optimum authentication key, Int. J. Comput. Appl. 42 (3) (2020) 306–314.

[20] M. Litoussi, N. Kannouf, K. El Makkaoui, A. Ezzati, M. Fartitchou, IoT security: Challenges and countermeasures, Procedia Comput. Sci. 177 (2020) 503–508.

[21] I.H. Sarker, A.I. Khan, Y.B. Abushark, F. Alsolami, Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions, Mob. Netw. Appl. (2022) 1–17.

[22] D. Kumawat, B. Umamaheswari, Internet of Things IoT based smart environment integrating various business applications and recent research directions, Int. J. Trend Sci. Res. Dev 3 (2019) 422–425.

[23] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, E. Bartocci, A roadmap toward the resilient Internet of Things for cyber-physical systems, IEEE Access 7 (2019) 13260–13283.

[24] M. Krishna, S.M.B. Chowdary, P. Nancy, V. Arulkumar, A survey on multimedia analytics in security systems of cyber physical systems and IoT, in: 2021 2nd International Conference on Smart Electronics and Communication, ICOSEC, IEEE, 2021, pp. 1–7.

[25] K. Tabassum, A. Ibrahim, S.A. El Rahman, Security issues and challenges in IoT, in: 2019 International Conference on Computer and Information Sciences, ICCIS, IEEE, 2019, pp. 1–5.

[26] S. Bhatt, P.R. Ragiri, et al., Security trends in Internet of Things: A survey, SN Appl. Sci. 3 (1) (2021) 1–14.

[27] J. Zhang, H. Chen, L. Gong, J. Cao, Z. Gu, The current research of IoT security, in: 2019 IEEE Fourth International Conference on Data Science in Cyberspace, DSC, IEEE, 2019, pp. 346–353.

[28] M. Gowtham, H. Pramod, Semantic query-featured ensemble learning model for SQL-injection attack detection in IoT-ecosystems, IEEE Trans. Reliab. (2021).

[29] J. Zhang, C. Shen, H. Su, M.T. Arafin, G. Qu, Voltage over-scaling-based lightweight authentication for IoT security, IEEE Trans. Comput. 71 (2) (2021) 323–336.

[30] S. Ravidas, P. Karkhanis, Y. Dajsuren, N. Zannone, An authorization framework for cooperative intelligent transport systems, in: International Workshop on Emerging Technologies for Authorization and Authentication, Springer, 2019, pp. 16–34.

[31] A.Y.F. Alsahlani, A. Popa, LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment, J. Netw. Comput. Appl. 192 (2021) 103177.

[32] P.M. Chanal, M.S. Kakkasageri, Security and privacy in IOT: A survey, Wirel. Pers. Commun. 115 (2) (2020) 1667–1693.

[33] F. Chen, J. Wang, J. Li, Y. Xu, C. Zhang, T. Xiang, TrustBuilder: A non-repudiation scheme for IoT cloud applications, Comput. Secur. 116 (2022) 102664.

[34] F. Hussain, S.G. Abbas, M. Husnain, U.U. Fayyaz, F. Shahzad, G.A. Shah, IoT DoS and DDoS attack detection using ResNet, in: 2020 IEEE 23rd International Multitopic Conference, INMIC, IEEE, 2020, pp. 1–6.

[35] B. Upadhyaya, S. Sun, B. Sikdar, Machine learning-based jamming detection in wireless IoT networks, in: 2019 IEEE VTS Asia Pacific Wireless Communications Symposium, APWCS, IEEE, 2019, pp. 1–5.

[36] M.N. Alam, D. Sarma, F.F. Lima, I. Saha, S. Hossain, et al., Phishing attacks detection using machine learning approach, in: 2020 Third International Conference on Smart Systems and Inventive Technology, ICSSIT, IEEE, 2020, pp. 1173–1179.

[37] S. Naaz, Detection of phishing in Internet of Things using machine learning approach, Int. J. Digit. Crime Forensics (IJDCF) 13 (2) (2021) 1–15.

[38] M. Ahmad, Q. Riaz, M. Zeeshan, H. Tahir, S.A. Haider, M.S. Khan, Intrusion detection in Internet of Things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set, EURASIP J. Wireless Commun. Networking 2021 (1) (2021) 1–23.

[39] W. Yaokumah, J.K. Appati, D. Kumah, Machine learning methods for detecting Internet-of-Things (IoT) malware, Int. J. Cogn. Inf. Nat. Intell. (IJCINI) 15 (4) (2021) 1–18.

[40] T.M. Hoang, T.Q. Duong, H.D. Tuan, S. Lambotharan, L. Hanzo, Physical layer security: Detection of active eavesdropping attacks by support vector machines, IEEE Access 9 (2021) 31595–31607, http://dx.doi.org/10.1109/ACCESS.2021.3059648.

[41] J.M. McGinthy, L.J. Wong, A.J. Michaels, Groundwork for neural network-based specific emitter identification authentication for IoT, IEEE Internet Things J. 6 (4) (2019) 6429–6440, http://dx.doi.org/10.1109/JIOT.2019.2908759.

[42] N.D. Kathamuthu, A. Chinnamuthu, N. Iruthayanathan, M. Ramachandran, A.H. Gandomi, Deep Q-learning-based neural network with privacy preservation method for secure data transmission in Internet of Things (IoT) healthcare application, Electronics 11 (1) (2022) 157.

[43] J.M. Ackerson, R. Dave, N. Seliya, Applications of recurrent neural network for biometric authentication & anomaly detection, Information 12 (7) (2021) 272.

[44] H. Zhang, Y. Li, Z. Lv, A.K. Sangaiah, T. Huang, A real-time and ubiquitous network attack detection based on deep belief network and support vector machine, IEEE/CAA J. Autom. Sin. 7 (3) (2020) 790–799, http://dx.doi.org/10.1109/JAS.2020.1003099.

[45] K. Prathapchandran, T. Janani, A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest–RFTRUST, Comput. Netw. 198 (2021) 108413.

[46] S. Pokhrel, R. Abbas, B. Aryal, IoT security: Botnet detection in IoT using machine learning, 2021, CoRR abs/2104.02231, arXiv:2104.02231.

[47] M.H. Aysa, A.A. Ibrahim, A.H. Mohammed, IoT DDoS attack detection using machine learning, in: 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT, 2020, pp. 1–7, http://dx.doi.org/10.1109/ISMSIT50672.2020.9254703.

[48] F. Hussain, S.G. Abbas, M. Husnain, U.U. Fayyaz, F. Shahzad, G.A. Shah, IoT DoS and DDoS attack detection using ResNet, in: 2020 IEEE 23rd International Multitopic Conference, INMIC, 2020, pp. 1–6, http://dx.doi.org/10.1109/INMIC50486.2020.9318216.

[49] X. Tang, R. Cao, J. Cheng, D. Fan, W. Tu, DDoS attack detection method based on V-support vector machine, in: International Symposium on Cyberspace Safety and Security, Springer, 2019, pp. 42–56.

[50] K. Wehbi, L. Hong, T. Al-salah, A.A. Bhutta, A survey on machine learning based detection on DDoS attacks for IoT systems, in: 2019 SoutheastCon, 2019, pp. 1–6, http://dx.doi.org/10.1109/SoutheastCon42311.2019.9020468.

[51] R. Gopi, V. Sathiyamoorthi, S. Selvakumar, R. Manikandan, P. Chatterjee, N. Jhanjhi, A.K. Luhach, Enhanced method of ANN based model for detection of DDoS attacks on multimedia Internet of Things, Multimedia Tools Appl. 81 (19) (2022) 26739–26757.

[52] S.A. Rahman, H. Tout, C. Talhi, A. Mourad, Internet of Things intrusion detection: Centralized, on-device, or federated learning? IEEE Netw. 34 (6) (2020) 310–317, http://dx.doi.org/10.1109/MNET.011.2000286.

[53] S. Sriram, R. Vinayakumar, M. Alazab, S. KP, Network flow based IoT botnet attack detection using deep learning, in: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, 2020, pp. 189–194, http://dx.doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162668.

[54] S. Manimurugan, IoT-fog-cloud model for anomaly detection using improved Naive Bayes and principal component analysis, J. Ambient Intell. Humaniz. Comput. (2021) 1–10.

[55] Z. Ren, H. Wu, Q. Ning, I. Hussain, B. Chen, End-to-end malware detection for android IoT devices using deep learning, Ad Hoc Netw. 101 (2020) 102098.

[56] M. Woźniak, J. Siłka, M. Wieczorek, M. Alrashoud, Recurrent neural network model for IoT and networking malware threat detection, IEEE Trans. Ind. Inform. 17 (8) (2020) 5583–5594.

[57] S. Chesney, K. Roy, S. Khorsandroo, Machine learning algorithms for preventing IoT cybersecurity attacks, in: Proceedings of SAI Intelligent Systems Conference, Springer, 2020, pp. 679–686.

[58] M. Bagaa, T. Taleb, J.B. Bernabe, A. Skarmeta, A machine learning security framework for IoT systems, IEEE Access 8 (2020) 114066–114077.

[59] S.M. Tahsien, H. Karimipour, P. Spachos, Machine learning based solutions for security of Internet of Things (IoT): A survey, J. Netw. Comput. Appl. 161 (2020) 102630.

[60] A. Mubarakali, K. Srinivasan, R. Mukhalid, S.C. Jaganathan, N. Marina, Security challenges in Internet of Things: Distributed denial of service attack detection using support vector machine-based expert systems, Comput. Intell. 36 (4) (2020) 1580–1592.

[61] M. Shen, X. Tang, L. Zhu, X. Du, M. Guizani, Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities, IEEE Internet Things J. 6 (5) (2019) 7702–7712, http://dx.doi.org/10.1109/JIOT.2019.2901840.

[62] A. Al Shorman, H. Faris, I. Aljarah, Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection, J. Ambient Intell. Humaniz. Comput. 11 (7) (2020) 2809–2825.

[63] D. Samanta, A.H. Alahmadi, M.P. Karthikeyan, M.Z. Khan, A. Banerjee, G.K. Dalapati, S. Ramakrishna, Cipher block chaining support vector machine for secured decentralized cloud enabled intelligent IoT architecture, IEEE Access 9 (2021) 98013–98025, http://dx.doi.org/10.1109/ACCESS.2021.3095297.

[64] R. Primartha, B.A. Tama, Anomaly detection using random forest: A performance revisited, in: 2017 International Conference on Data and Software Engineering, ICoDSE, 2017, pp. 1–6, http://dx.doi.org/10.1109/ICODSE.2017.8285847.

[65] S. Nakhodchi, A. Upadhyay, A. Dehghantanha, A comparison between different machine learning models for IoT malware detection, in: Security of Cyber-Physical Systems, Springer, 2020, pp. 195–202.

[66] P. Amangele, M.J. Reed, M. Al-Naday, N. Thomos, M. Nowak, Hierarchical machine learning for IoT anomaly detection in SDN, in: 2019 International Conference on Information Technologies, InfoTech, IEEE, 2019, pp. 1–4.

[67] P. Amangele, M.J. Reed, M. Al-Naday, N. Thomos, M. Nowak, Hierarchical machine learning for IoT anomaly detection in SDN, in: 2019 International Conference on Information Technologies, InfoTech, 2019, pp. 1–4, http://dx.doi.org/10.1109/InfoTech.2019.8860878.

[68] Z.H. Abdaljabar, O.N. Ucan, K.M. Ali Alheeti, An intrusion detection system for IoT using KNN and decision-tree based classification, in: 2021 International Conference of Modern Trends in Information and Communication Technology Industry, MTICTI, 2021, pp. 1–5, http://dx.doi.org/10.1109/MTICTI53925.2021.9664772.

[69] I.S. Thaseen, V. Mohanraj, S. Ramachandran, K. Sanapala, S.-S. Yeo, A hadoop based framework integrating machine learning classifiers for anomaly detection in the Internet of Things, Electronics 10 (16) (2021) 1955.

[70] S.M. Taghavinejad, M. Taghavinejad, L. Shahmiri, M. Zavvar, M.H. Zavvar, Intrusion detection in IoT-based smart grid using hybrid decision tree, in: 2020 6th International Conference on Web Research, ICWR, 2020, pp. 152–156, http://dx.doi.org/10.1109/ICWR49608.2020.9122320.

[71] D. Puthal, S. Wilson, A. Nanda, M. Liu, S. Swain, B.P. Sahoo, K. Yelamarthi, P. Pillai, H. El-Sayed, M. Prasad, Decision tree based user-centric security solution for critical IoT infrastructure, Comput. Electr. Eng. 99 (2022) 107754.

[72] S. Mugunthan, Decision tree based interference recognition for fog enabled IoT architecture, J. Trends Comput. Sci. Smart Technol. (TCSST) 2 (01) (2020) 15–25.

[73] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, W. Song, System statistics learning-based IoT security: Feasibility and suitability, IEEE Internet Things J. 6 (4) (2019) 6396–6403.

[74] J. Pacheco, V.H. Benitez, Z. Pan, Security framework for IoT end nodes with neural networks, Int. J. Mach. Learn. Comput. 9 (4) (2019) 381–386.

[75] A. Rezaei, Using ensemble learning technique for detecting botnet on IoT, SN Comput. Sci. 2 (3) (2021) 1–14.

[76] U. Ahad, Y. Singh, P. Anand, Z.A. Sheikh, P.K. Singh, Intrusion detection system model for IoT networks using ensemble learning, J. Interconnect. Netw. (2022) 2145008.

[77] N. Banerjee, T. Giannetsos, E. Panaousis, C.C. Took, Unsupervised learning for trustworthy IoT, in: 2018 IEEE International Conference on Fuzzy Systems, FUZZ-IEEE, IEEE, 2018, pp. 1–8.

[78] S. Kumar, Z. Raza, A K-means clustering based message forwarding model for internet of things (IoT), in: 2018 8th International Conference on Cloud Computing, Data Science & Engineering, Confluence, IEEE, 2018, pp. 604–609.

[79] J. Zhu, L. Huo, M.D. Ansari, M.A. Ikbal, Research on data security detection algorithm in IoT based on K-means, Scalable Comput.: Pract. Exp. 22 (2) (2021) 149–159.

[80] B. Purnama, E.A. Winanto, D. Stiawan, D. Hanapi, M.Y. bin Idris, R. Budiarto, et al., Features extraction on IoT intrusion detection system using principal components analysis (PCA), in: 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics, EECSI, IEEE, 2020, pp. 114–118.

[81] J. Shuja, M.A. Humayun, W. Alasmary, H. Sinky, E. Alanazi, M.K. Khan, Resource efficient geo-textual hierarchical clustering framework for social IoT applications, IEEE Sens. J. 21 (22) (2021) 25114–25122.

[82] C. Guyeux, S. Chrétien, G. Bou Tayeh, J. Demerjian, J. Bahi, Introducing and comparing recent clustering methods for massive data management in the Internet of Things, J. Sensor Actuator Netw. 8 (4) (2019) 56.

[83] P. Kashyap, A. Jaiswal, M. Kumar, Fuzzy K-means clustering (FKmC) to maximize the energy efficiency in sensor-enabled Internet of Things, in: 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies, GUCON, IEEE, 2021, pp. 1–6.

[84] V. Vashishth, A. Chhabra, D.K. Sharma, GMMR: A Gaussian mixture model based unsupervised machine learning approach for optimal routing in opportunistic IoT networks, Comput. Commun. 134 (2019) 138–148.

[85] T. Gu, A. Abhishek, H. Fu, H. Zhang, D. Basu, P. Mohapatra, Towards learning-automation IoT attack detection through reinforcement learning, in: 2020 IEEE 21st International Symposium on “a World of Wireless, Mobile and Multimedia Networks”, WoWMoM, IEEE, 2020, pp. 88–97.

[86] T.-L. Wan, T. Ban, S.-M. Cheng, Y.-T. Lee, B. Sun, R. Isawa, T. Takahashi, D. Inoue, Efficient detection and classification of Internet-of-Things malware based on byte sequences from executable files, IEEE Open J. Comput. Soc. 1 (2020) 262–275.

[87] L. Liu, J. Yang, W. Meng, Detecting malicious nodes via gradient descent and support vector machine in Internet of Things, Comput. Electr. Eng. 77 (2019) 339–353.

[88] A. El-Rahiem, M. Hammad, et al., A multi-fusion IoT authentication system based on internal deep fusion of ECG signals, in: Security and Privacy Preserving for IoT and 5G Networks, Springer, 2022, pp. 53–79.

[89] B.A. Tama, K.-H. Rhee, An integration of pso-based feature selection and random forest for anomaly detection in IoT network, in: MATEC Web of Conferences, Vol. 159, EDP Sciences, 2018, p. 01053.

[90] M.B. Farukee, M. Shabit, M. Haque, A. Sattar, et al., DDoS attack detection in IoT networks using deep learning models combined with random forest as feature selector, in: International Conference on Advances in Cyber Security, Springer, 2020, pp. 118–134.

[91] M.O. Arowolo, R.O. Ogundokun, S. Misra, J. Oluranti, A.F. Kadri, K-nearest neighbour algorithm for classification of IoT-based edge computing device, in: Artificial Intelligence for Cloud and Edge Computing, Springer, 2022, pp. 161–179.

[92] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, W. Song, Secure and efficient {K} nearest neighbor query over encrypted uncertain data in cloud-IoT ecosystem, IEEE Internet Things J. (2019) 9868–9879.

[93] R. Majeed, N.A. Abdullah, M.F. Mushtaq, IoT-based cyber-security of drones using the Naïve Bayes algorithm, Int. J. Adv. Comput. Sci. Appl. 12 (7) (2021).

[94] A. Mehmood, M. Mukherjee, S.H. Ahmed, H. Song, K.M. Malik, NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks, J. Supercomput. 74 (10) (2018) 5156–5170.

[95] T.T. Huong, T.P. Bac, D.M. Long, B.D. Thang, T.D. Luong, N.T. Binh, An efficient low complexity edge-cloud framework for security in iot networks, in: 2020 IEEE Eighth International Conference on Communications and Electronics, ICCE, IEEE, 2021, pp. 533–539.

[96] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, F. Aloul, Botnet attack detection using machine learning, in: 2020 14th International Conference on Innovations in Information Technology, IIT, IEEE, 2020, pp. 203–208.

[97] E. Tsogbaatar, M.H. Bhuyan, Y. Taenaka, D. Fall, K. Gonchigsumlaa, E. Elmroth, Y. Kadobayashi, DeL-IoT: A deep ensemble learning approach to uncover anomalies in IoT, Internet Things 14 (2021) 100391.

[98] D. Vasan, M. Alazab, S. Venkatraman, J. Akram, Z. Qin, MTHAEL: Cross-architecture IoT malware detection based on neural network advanced ensemble learning, IEEE Trans. Comput. 69 (11) (2020) 1654–1667.

[99] P. Kumar, G.P. Gupta, R. Tripathi, An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks, Comput. Commun. 166 (2021) 110–124.

[100] D. Stiawan, M.E. Suryani, M.Y. Idris, M.N. Aldalaien, N. Alsharif, R. Budiarto, et al., Ping flood attack pattern recognition using a K-means algorithm in an Internet of Things (IoT) network, IEEE Access 9 (2021) 116475–116484.

[101] S. Salaria, S. Arora, N. Goyal, P. Goyal, S. Sharma, Implementation and analysis of an improved PCA technique for DDoS detection, in: 2020 IEEE 5th International Conference on Computing Communication and Automation, ICCCA, IEEE, 2020, pp. 280–285.

[102] G. Han, L. Xiao, H.V. Poor, Two-dimensional anti-jamming communication based on deep reinforcement learning, in: 2017 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP, IEEE, 2017, pp. 2087–2091.

[103] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, W. Pan, Intrusion detection for wireless edge networks based on federated learning, IEEE Access 8 (2020) 217463–217472.

[104] W.Y.B. Lim, N.C. Luong, D.T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, C. Miao, Federated learning in mobile edge networks: A comprehensive survey, IEEE Commun. Surv. Tutor. 22 (3) (2020) 2031–2063.

[105] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, W. Pan, Intrusion detection for wireless edge networks based on federated learning, IEEE Access 8 (2020) 217463–217472, http://dx.doi.org/10.1109/ACCESS.2020.3041793.

[106] W.Y.B. Lim, N.C. Luong, D.T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, C. Miao, Federated learning in mobile edge networks: A comprehensive survey, IEEE Commun. Surv. Tutor. 22 (3) (2020) 2031–2063, http://dx.doi.org/10.1109/COMST.2020.2986024.

[107] D.C. Nguyen, M. Ding, Q.-V. Pham, P.N. Pathirana, L.B. Le, A. Seneviratne, J. Li, D. Niyato, H.V. Poor, Federated learning meets blockchain in edge computing: Opportunities and challenges, IEEE Internet Things J. 8 (16) (2021) 12806–12825, http://dx.doi.org/10.1109/JIOT.2021.3072611.

[108] Y. Song, T. Liu, T. Wei, X. Wang, Z. Tao, M. Chen, FDA^3: Federated defense against adversarial attacks for cloud-based IIoT applications, IEEE Trans. Ind. Inform. 17 (11) (2021) 7830–7838, http://dx.doi.org/10.1109/TII.2020.3005969.

[109] T.D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, A.-R. Sadeghi, D IoT: A federated self-learning anomaly detection system for IoT, in: 2019 IEEE 39th International Conference on Distributed Computing Systems, ICDCS, 2019, pp. 756–767, http://dx.doi.org/10.1109/ICDCS.2019.00080.

[110] T.V. Khoa, Y.M. Saputra, D.T. Hoang, N.L. Trung, D. Nguyen, N.V. Ha, E. Dutkiewicz, Collaborative learning model for cyberattack detection systems in IoT industry 4.0, in: 2020 IEEE Wireless Communications and Networking Conference, WCNC, 2020, pp. 1–6, http://dx.doi.org/10.1109/WCNC45663.2020.9120761.

[111] B. Cetin, A. Lazar, J. Kim, A. Sim, K. Wu, Federated wireless network intrusion detection, in: 2019 IEEE International Conference on Big Data, Big Data, 2019, pp. 6004–6006, http://dx.doi.org/10.1109/BigData47090.2019.9005507.

[112] D.C. Attota, V. Mothukuri, R.M. Parizi, S. Pouriyeh, An ensemble multi-view federated learning intrusion detection for IoT, IEEE Access 9 (2021) 117734–117745, http://dx.doi.org/10.1109/ACCESS.2021.3107337.

[113] R. Galvez, V. Moonsamy, C. Díaz, Less is more: A privacy-respecting android malware classifier using federated learning, 2020, CoRR abs/2007.08319, arXiv:2007.08319.

[114] O. Friha, M.A. Ferrag, L. Shu, L. Maglaras, K.-K.R. Choo, M. Nafaa, FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things, J. Parallel Distrib. Comput. 165 (2022) 17–31.

[115] E.M. Campos, P.F. Saura, A. González-Vidal, J.L. Hernández-Ramos, J.B. Bernabé, G. Baldini, A. Skarmeta, Evaluating federated learning for intrusion detection in Internet of Things: Review and challenges, Comput. Netw. 203 (2022) 108661.

[116] A. Makkar, T.W. Kim, A.K. Singh, J. Kang, J.H. Park, Secureiiot environment: Federated learning empowered approach for securing IIoT from data breach, IEEE Trans. Ind. Inform. 18 (9) (2022) 6406–6414.

[117] Y. Lu, X. Huang, Y. Dai, S. Maharjan, Y. Zhang, Federated learning for data privacy preservation in vehicular cyber-physical systems, IEEE Netw. 34 (3) (2020) 50–56, http://dx.doi.org/10.1109/MNET.011.1900317.

[118] Y. Zhao, J. Zhao, M. Yang, T. Wang, N. Wang, L. Lyu, D. Niyato, K.-Y. Lam, Local differential privacy-based federated learning for Internet of Things, IEEE Internet Things J. 8 (11) (2021) 8836–8853, http://dx.doi.org/10.1109/JIOT.2020.3037194.

[119] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, Y. Liu, Privacy-preserving blockchain-based federated learning for IoT devices, IEEE Internet Things J. 8 (3) (2021) 1817–1829, http://dx.doi.org/10.1109/JIOT.2020.3017377.

[120] Y. Zhao, J. Chen, D. Wu, J. Teng, S. Yu, Multi-task network anomaly detection using federated learning, in: Proceedings of the Tenth International Symposium on Information and Communication Technology, 2019, pp. 273–279.

[121] V. Rey, P.M.S. Sánchez, A.H. Celdrán, G. Bovet, Federated learning for malware detection in IoT devices, Comput. Netw. 204 (2022) 108693.

[122] Z. Lian, C. Su, Decentralized federated learning for Internet of Things anomaly detection, in: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, 2022, pp. 1249–1251.

[123] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, B. Yoon, A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology, Future Gener. Comput. Syst. 129 (2022) 380–388.

[124] M. Chen, Z. Yang, W. Saad, C. Yin, H.V. Poor, S. Cui, A joint learning and communications framework for federated learning over wireless networks, IEEE Trans. Wireless Commun. 20 (1) (2021) 269–283, http://dx.doi.org/10.1109/TWC.2020.3024629.

[125] H. Wang, K. Sreenivasan, S. Rajput, H. Vishwakarma, S. Agarwal, J.-y. Sohn, K. Lee, D. Papailiopoulos, Attack of the tails: Yes, you really can backdoor federated learning, Adv. Neural Inf. Process. Syst. 33 (2020) 16070–16084.

[126] S. Wang, Z. Qiao, Robust pervasive detection for adversarial samples of artificial intelligence in IoT environments, IEEE Access 7 (2019) 88693–88704, http://dx.doi.org/10.1109/ACCESS.2019.2919695.

[127] Y. Fraboni, R. Vidal, M. Lorenzi, Free-rider attacks on model aggregation in federated learning, in: International Conference on Artificial Intelligence and Statistics, PMLR, 2021, pp. 1846–1854.

[128] S. Li, Y. Cheng, W. Wang, Y. Liu, T. Chen, Learning to detect malicious clients for robust federated learning, 2020, CoRR abs/2002.00211, arXiv:2002.00211.

[129] S. Li, Y. Cheng, Y. Liu, W. Wang, T. Chen, Abnormal client behavior detection in federated learning, 2019, CoRR abs/1910.09933, arXiv:1910.09933.

[130] L. Wang, S. Xu, X. Wang, Q. Zhu, Eavesdrop the composition proportion of training labels in federated learning, 2019, CoRR abs/1910.06044, arXiv:1910.06044.

[131] N.R. Barroso, E. Martínez-Cámara, M.V. Luzón, G. González-Seco, M.Á. Veganzones, F. Herrera, Dynamic federated learning model for identifying adversarial clients, 2020, CoRR abs/2007.15030, arXiv:2007.15030.

[132] O. Shahid, S. Pouriyeh, R.M. Parizi, Q.Z. Sheng, G. Srivastava, L. Zhao, Communication efficiency in federated learning: Achievements and challenges, 2021, arXiv preprint arXiv:2107.10996.

[133] P. Pinyoanuntapong, W.H. Huff, M. Lee, C. Chen, P. Wang, Toward scalable and robust AIoT via decentralized federated learning, IEEE Internet Things Mag. 5 (1) (2022) 30–35.

[134] C. Campolo, G. Genovese, G. Singh, A. Molinaro, Scalable and interoperable edge-based federated learning in IoT contexts, Comput. Netw. (2023) 109576.

[135] D.C. Nguyen, M. Ding, P.N. Pathirana, A. Seneviratne, J. Li, H. Vincent Poor, Federated learning for Internet of Things: A comprehensive survey, IEEE Commun. Surv. Tutor. 23 (3) (2021) 1622–1658, http://dx.doi.org/10.1109/COMST.2021.3075439.

[136] M. Roopak, G. Yun Tian, J. Chambers, Deep learning models for cyber security in IoT networks, in: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC, 2019, pp. 0452–0457, http://dx.doi.org/10.1109/CCWC.2019.8666588.

[137] P.K. Keserwani, M.C. Govil, E.S. Pilli, P. Govil, A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model, J. Reliab. Intell. Environ. 7 (1) (2021) 3–21.

[138] T. Alladi, A. Agrawal, B. Gera, V. Chamola, B. Sikdar, M. Guizani, Deep neural networks for securing IoT enabled vehicular ad-hoc networks, in: ICC 2021 - IEEE International Conference on Communications, 2021, pp. 1–6, http://dx.doi.org/10.1109/ICC42927.2021.9500823.

[139] M. Woźniak, J. Siłka, M. Wieczorek, M. Alrashoud, Recurrent neural network model for IoT and networking malware threat detection, IEEE Trans. Ind. Inform. 17 (8) (2021) 5583–5594, http://dx.doi.org/10.1109/TII.2020.3021689.

[140] W. Liang, W. Huang, J. Long, K. Zhang, K.-C. Li, D. Zhang, Deep reinforcement learning for resource protection and real-time detection in IoT environment, IEEE Internet Things J. 7 (7) (2020) 6392–6401, http://dx.doi.org/10.1109/JIOT.2020.2974281.

[141] B. Abd El-Rahiem, M. Hammad, A multi-fusion IoT authentication system based on internal deep fusion of ECG signals, Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions (2022) 53–79.

[142] C. Huang, S. Chen, Y. Zhang, W. Zhou, J.J.P.C. Rodrigues, V.H.C. de Albuquerque, A robust approach for privacy data protection: IoT security assurance using generative adversarial imitation learning, IEEE Internet Things J. (2021) 1, http://dx.doi.org/10.1109/JIOT.2021.3128531.

[143] L. Nie, Y. Wu, X. Wang, L. Guo, G. Wang, X. Gao, S. Li, Intrusion detection for secure social Internet of Things based on collaborative edge computing: A generative adversarial network-based approach, IEEE Trans. Comput. Soc. Syst. 9 (1) (2022) 134–145, http://dx.doi.org/10.1109/TCSS.2021.3063538.

[144] N. Balakrishnan, A. Rajendran, D. Pelusi, V. Ponnusamy, Deep belief network enhanced intrusion detection system to prevent security breach in the Internet of Things, Internet Things 14 (2021) 100112.

[145] M.V. de Assis, L.F. Carvalho, J.J. Rodrigues, J. Lloret, M.L. Proença Jr., Near real-time security system applied to SDN environments in IoT networks using convolutional neural network, Comput. Electr. Eng. 86 (2020) 106738.

[146] I. Ullah, Q.H. Mahmoud, Design and development of a deep learning-based model for anomaly detection in IoT networks, IEEE Access 9 (2021) 103906–103926, http://dx.doi.org/10.1109/ACCESS.2021.3094024.

[147] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M.A. Latif, F. Al-turjman, L. Mostarda, Cyber security threats detection in Internet of Things using deep learning approach, IEEE Access 7 (2019) 124379–124389, http://dx.doi.org/10.1109/ACCESS.2019.2937347.

[148] S.K. Singh, Y.-S. Jeong, J.H. Park, A deep learning-based IoT-oriented infrastructure for secure smart city, Sustainable Cities Soc. 60 (2020) 102252.

[149] S.M. Kasongo, Y. Sun, A deep learning method with wrapper based feature extraction for wireless intrusion detection system, Comput. Secur. 92 (2020) 101752.

[150] M. Zhong, Y. Zhou, G. Chen, Sequential model based intrusion detection system for IoT servers using deep learning methods, Sensors 21 (4) (2021) 1113.

[151] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, A. Robles-Kelly, Deep learning-based intrusion detection for IoT networks, in: 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing, PRDC, IEEE, 2019, pp. 256–25609.

[152] Q. Abu Al-Haija, S. Zein-Sabatto, An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks, Electronics 9 (12) (2020) 2152.

[153] L. Lyu, H. Yu, Q. Yang, Threats to federated learning: A survey, 2020, CoRR abs/2003.02133, arXiv:2003.02133.

[154] M. Tsukada, M. Kondo, H. Matsutani, A neural network-based on-device learning anomaly detector for edge devices, IEEE Trans. Comput. 69 (7) (2020) 1027–1044, http://dx.doi.org/10.1109/TC.2020.2973631.

[155] M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for Internet of Things (IoT) security, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1646–1685, http://dx.doi.org/10.1109/COMST.2020.2988293.