Asian Journal of Research in Computer Science

9(4): 12-34, 2021; Article no.AJRCOS.69594
ISSN: 2581-8260

A State of the Art Survey of Machine Learning Algorithms for IoT Security

Alan Fuad Jahwar[1*] and Subhi R. M. Zeebaree[1]

[1]Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.

Authors' contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v9i430226
Editor(s):
(1) Dr. G. Sudheer, GVP College of Engineering for Women, India.
Reviewers:
(1) Rafamantanantsoa Fontaine, University of Fianarantsoa , Madagascar.
(2) G.Singaravel, K.S.R.College of Engineering (Autonomous), India.
(3) Mateus Mendes, University of Coimbra – ISR, Portugal.
Complete Peer review History: http://www.sdiarticle4.com/review-history/69594

Review Article

Received 10 April 2021
Accepted 14 June 2021
Published 16 June 2021

ABSTRACT

The Internet of Things (IoT) is a paradigm shift that enables billions of devices to connect to the Internet. The IoT's diverse application domains, including smart cities, smart homes, and e-health, have created new challenges, chief among them security threats. To accommodate the current networking model, traditional security measures such as firewalls and Intrusion Detection Systems (IDS) must be modified. Additionally, the Internet of Things and Cloud Computing complement one another, frequently used interchangeably when discussing technical services and collaborating to provide a more comprehensive IoT service. In this review, we focus on recent Machine Learning (ML) and Deep Learning (DL) algorithms proposed in IoT security, which can be used to address various security issues. This paper systematically reviews the architecture of IoT applications, the security aspect of IoT, service models of cloud computing, and cloud deployment models. Finally, we discuss the latest ML and DL strategies for solving various security issues in IoT networks.

Keywords: Deep learning; intrusion detection; network attacks; intrusion datasets.

**Corresponding author: E-mail: alan.jahwar@dpu.edu.krd;*

1. INTRODUCTION

The IoT is an internet-connected network of semi-autonomous computers, each equipped with low-cost computation, networking, sensing, and action in the physical world. The deployment of IoT devices continues to accelerate, with the total expected to reach approximately 75 billion by 2025 [1]. However, 70% of all IoT devices do not use encryption. The most frequently cited reasons are the following: 1) restricted onboard computing capability; 2) prohibitively high implementation costs for the manufacturer; and 3) issues of scalability related to deployment and management [2].

With the advancement of information technology, IoT technology has increasingly evolved and is now commonly used in various fields, including manufacturing, agriculture, and the military. Due to the IoT's widespread adoption and technical diversity, different devices are constantly being incorporated into the IoT, IoT terminals, or IoT branches [3,4]. As an open system on the internet, IoT faces dynamic and varied threats from outside. The identification of security problems in IoT, therefore, needs to be improved. There are security gateways, firewalls, code signatures, and data encryption among the current security technologies. However, all of these are passive security protection mechanisms incapable of performing active detection and response [5,6].

Cloud computing has grown in popularity as a network access model due to its open and pervasive sharing environment for a wide range of computing resources [7]. Cloud Computing provides users with large virtualized computing tools on-demand, making it very appealing for various industrial application domains [8]. Therefore, companies' and consumers' communication with IT services would shift using cloud computing [9]. Given the complexity of a cloud system's components: (a) user application/workload efficiency, (b) Virtual Machine (VM)/host performance, (c) power consumption, (d) resource contention and scheduling, and (e) network communication, it is impossible to accurately model all of the system's components [10,11].

The ML has been implemented successfully in various fields, including image processing, Natural Language Processing (NLP), and self-driving vehicles [12]. Emerging hardware has increased computer capability, and as a result, the number of training data handled by ML has significantly increased. The DL, in particular, has made considerable strides in improving decision-making for a variety of identification, classification, and prediction tasks [13]. As a practice, ML can make more accurate decisions in areas such as facial recognition [14,15,16], natural language understanding (including social media, which does not strictly adhere to grammar rules), medical image [17,18], identifying traffic signals for self-driving cars, and defeating professional gamers in traditional games (e.g., Google's AlphaGo) and computer games [13]. Also, Industry Prediction, industry maintenance, and inventory.

The organization of the rest of the paper is as follows: Section II describes various algorithms of Machine Learning. Section III discusses different algorithms of Deep Learning. In section, IV describes the Cloud System. Section V describes the Internet of Things. Section VI describes Literature Review. In Section VII Discussion and Comparisons. Finally, Section VIII produces the Conclusion and Future work suggestions.

2. MACHINE LEARNING AND IDS

The ML is a data analysis method that automates the process of developing analytical models. It is a subset of Artificial Intelligence (AI) based on the principle that systems can learn from data, recognize patterns, and make decisions with little human intervention. On large datasets, ML algorithms use mathematical techniques to create models of human behavior. Additionally, ML allows the capability to learn without being specifically programmed. The main types of ML including supervised and unsupervised [19]. Fig. 1 illustrates many ML algorithms used to secure IoT systems [20]. The most common supervised learning methods, called classification and regression, are popular in the classification or prediction of a security problem in the future. Unsupervised learning, alternatively referred to as descriptive learning, identifies patterns in unfamiliar objects by grouping related objects together [21].

Additionally, ML applications in IoT security in a variety of domains can be used to detect intelligent attacks on IoT devices and to establish a robust defense strategy, communication standards in IoT [22], Face recognition for forensics, Malicious code identification, Distributed Denial of Service (DDoS) detection and other [23]. In the following, we discuss the most common and famous methods for solving ML tasks and their relationship to IoT security tasks.

2.1 Support Vector Machine (SVM)

SVM is a method for supervised learning that is used to analyze data using regression and classification processing. Between two classes, SVM generates a plane called a hyperplane. The hyperplane's objective is to optimize the distance between each class that defines each class with the least amount of error at the maximum margin. If the hyperplane becomes nonlinear due to the analysis, SVM transforms the kernel function into a linear hyperplane using new features. Often, an optimal kernel function is hard to use in SVM [24]. SVM, while highly accurate, is a good fit for IoT protection such as intrusion detection, malware detection, and intelligent grid attacks [25]. As shown in Fig. 2

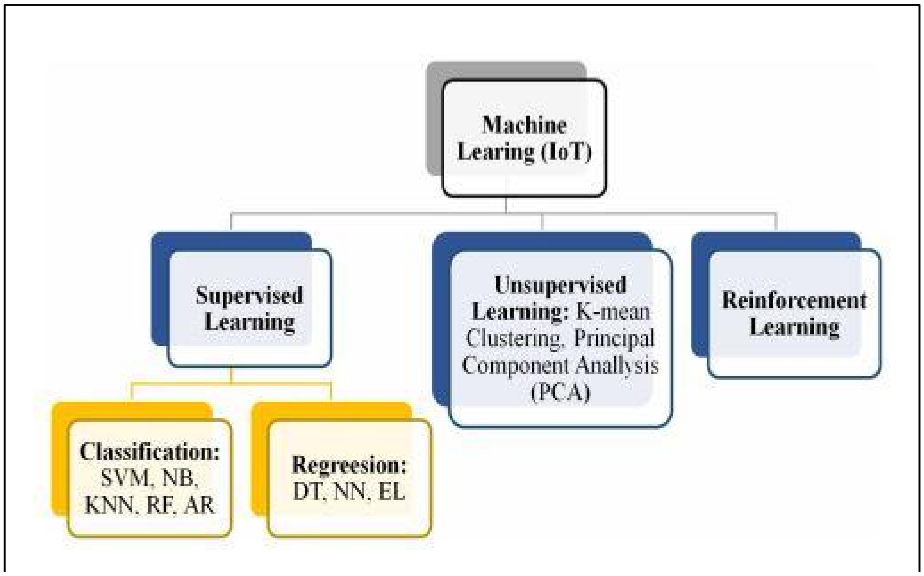
Machine Learing (IoT)
Supervised Learning
Unsupervised Learning: K-mean Clustering, Principal Component Anallysis (PCA)
Reinforcement Learning
Classification: SVM, NB, KNN, RF, AR
Regreesion: DT, NN, EL

Fig. 1. Classification of general machine learning algorithms [20]

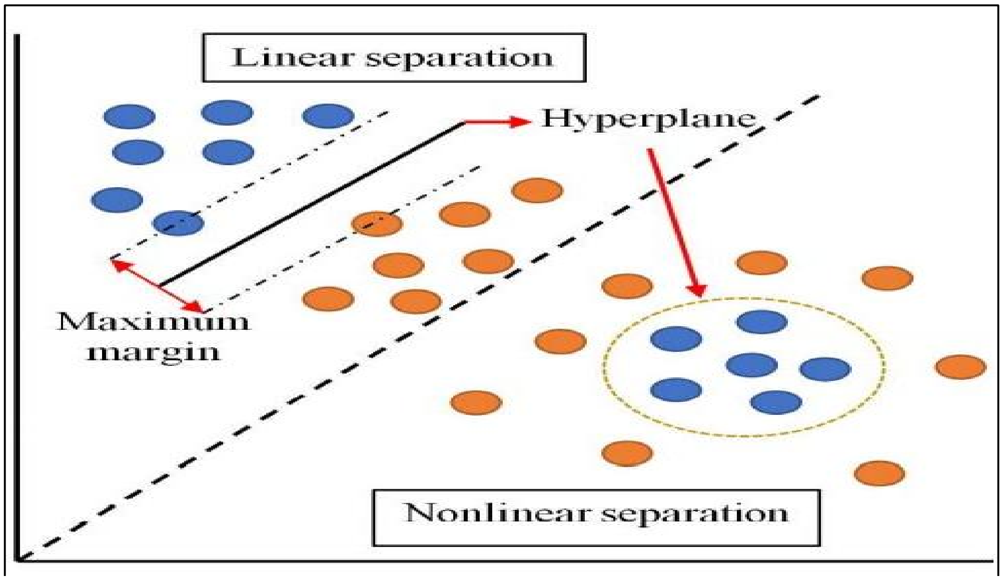

Fig. 2. Illustration of SVM class separation techniques for both linear and nonlinear groups [26]

2.2 K-Nearest Neighbor (K-NN)

K-NN is a supervised learning technique that uses Euclidean distance as a distance metric [27]. In K-NN, the Euclidian distance between two nodes defines the average value of the unknown node, which is the sum of its k-NN. Observe Fig. 3. [28]. For example, if a node is lost, the nearest neighbor's average value can be used to predict the loss. Although this value is inaccurate, it aids in identifying the possible missing node. The K-NN approach is used for Intrusion Detection (ID), malware detection, and anomaly detection in the Internet of Things [29]. The K-NN algorithm is simple, inexpensive, and quick to implement [30].

2.3 Decision-Tree (DT)

DT is a method for supervised learning, one of the most common classification and prediction techniques based on a structure similar to a flow chart [31]. In a DT, there are two nodes, which are the Decision Node and Leaf Node, as shown in Fig. 4. The CART, Iterative Dichotomies 3 (ID3), and C4.5 algorithms are the most commonly used DT algorithms. The C4.5 algorithm is a modified version of the ID3 algorithm that uses the knowledge gain ratio to determine which attributes have the best split [32,33].

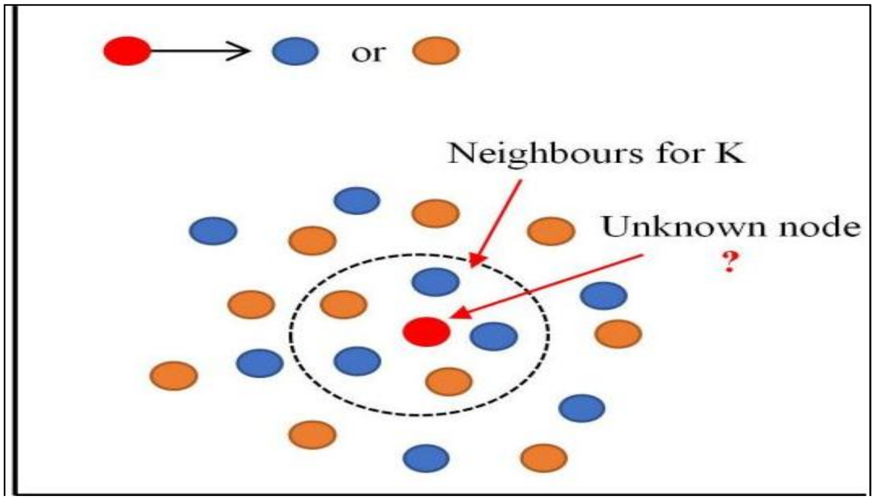

Fig. 3. Illustration of KNN learning [28]

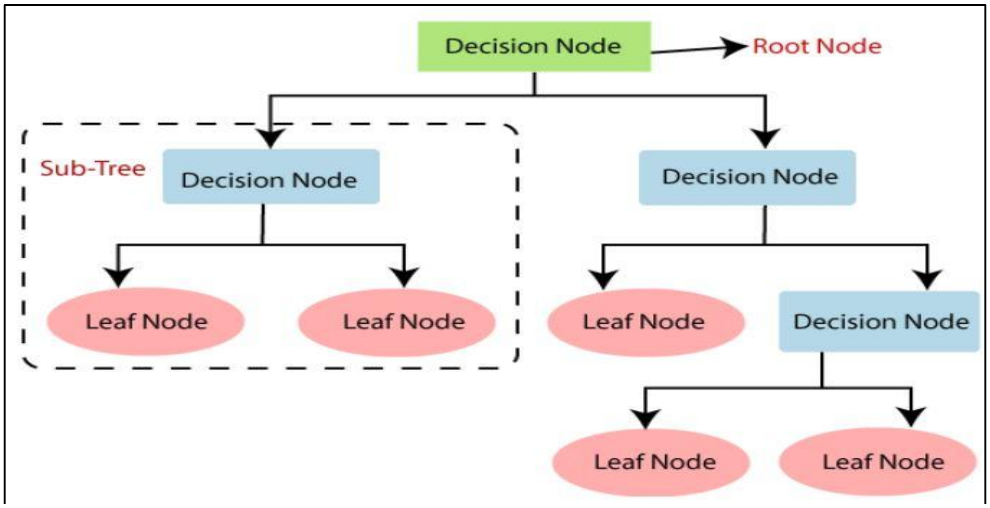

Fig. 4. DT structure [32]

In addition, to the most popular ML algorithms mentioned above, several other ML techniques exist in the field for various purposes. For instance, Random forest (RF) is a multiple DT which is usually more accurate in a learning model than a single DT. The advantages of RF include its ability to handle broad and expansive data sets, its robust system for estimating missing data, and its ability to retain accuracy in the absence of a large proportion of data [34]. Regression analysis consists of various ML algorithms that allow the prediction of a continuous (y) outcome variable based on the values of one or more (x) predictor variables [35]. Some well-known regression methods include logistic, linear, polynomial, lasso, and ridge regression [36]. Cluster analysis, alternatively referred to as clustering, is an unsupervised ML algorithm used to identify and group similar data points in large datasets without concern for the particular outcome. Clustering can be used in a variety of different fields of IoT [37]. For example, an FCM-based clustering algorithm can be used to extend the network lifetime and conserve energy in wireless sensor networks (WSNs) for IoT applications [38], complicated clustering techniques for big data analytics [39]. The most common clustering algorithms are K-means and Dbscan [40,41,42].

3. DEEP LEARNING

The DL is a subfield of ML in Artificial Intelligence (AI) that allows the use of neural networks capable of unsupervised learning from unstructured or unlabeled data. Also known as "deep neural learning" or "Deep Neural Network" (DNN) [43]. The network consists of multiple neurons that are linked by weighted connections. It uses a large number of hidden layers to extract higher-level features from the input [44]. One of the limitations of DL algorithms is the increased training time required. With increasing amounts of training data, the training time increases. However, DL algorithms require a large amount of training data to perform well. The DL model's basic architecture is depicted in Fig. 5. It consists of a single input layer followed by several hidden layers that feed data to the output layer [45]. DL uses multi-layer neural networks to discover hidden relationships and features among a variety of data sets.

Nonetheless, to obtain highly accurate results using equivalent DL models, appropriate data and computing power are needed [46,47]. In IoT security, DL approaches may be used for a variety of purposes. For instance, the IoT devices in a smart home will communicate automatically to create an intelligent home [48]. In the following section, we will discuss the most common neural network and DL algorithms in the context of IoT, including the Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), and long-short term memory (LSTM) network [49,50].

3.1 Convolutional Neural Network (CNN)

A convolutional neural network (CNN, or ConvNet) is a deep neural network used in deep learning [51]. The use of CNNs in computer vision (CV) and NLP applications is well-known [52]. This type of network has been successfully used to recognize images [53] and video, classification, and text processing. In general, CNN often consists of multiple layers: input layer, convolutional layer, pooling layer, fully connected layers, and an output layer [52], as illustrated in Fig. 6 [54]. Convolutional layers are used to extract features, and pooling layers are used to improve the generalizability of the extracted features [52]. Though CNNs are most frequently used for visual image analysis, which can be used for IoT applications. It has been used for tasks like intrusion detection in IoT Networks [55], CNN-based Applications on IoT Edge Devices [56]. However, counting people detect objects in general.

3.2 Restricted Boltzmann Machine (RBM)

RBM is a well-known algorithm for unsupervised learning. RBM can use in many applications like classification, regression, dimensionality reduction, collaborative filtering, feature learning, and topic modeling [57,58]. RBMs have two main layers: visible and hidden, as shown in Fig. 7. The visible layer contains the known input, while the hidden layer comprises several layers containing latent variables. Since no two nodes in the same layer share a link, an RBM is called "restricted". RBM has two phases Forward Pass and Backward Pass. RBM takes the inputs and converts them to a series of numerical values (forward pass). After that, these numbers can be used to recreate the inputs (backward pass) [59,60].

3.3 Autoencoder (AE)

Autoencoders (AE) is a subclass of Artificial Neural Networks (ANNs) used to learn effective data encodings unsupervised [61]. The purpose of an AE is to train the network to ignore signal "noise" in order to discover an encoding (representation) for a collection of data, usually for dimensionality reduction. Along with the reduction side, a reconstructing side is taught [62]. The autoencoder tries to represent the original input as similar to the original as possible from the reduced encoding, as illustrated in Fig. 8 [63]. The AE module is composed of two components: an encoder and a decoder. The encoder discovers the fundamental characteristics of a process. Typically, these characteristics are of a reduced dimension. From these underlying features, the decoder can reconstruct the original data [64].

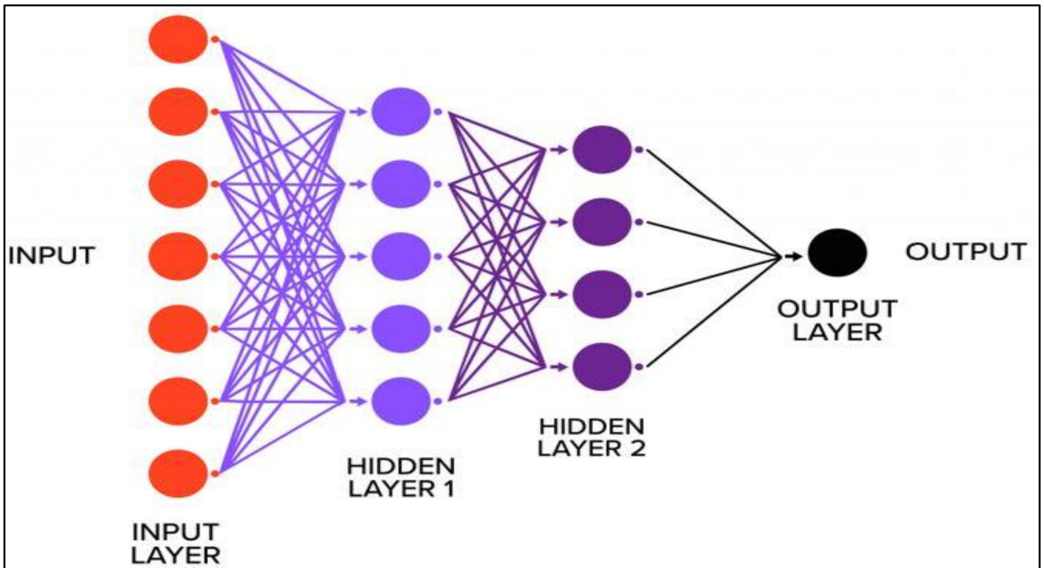

Fig. 5. The architecture of deep learning model [45]

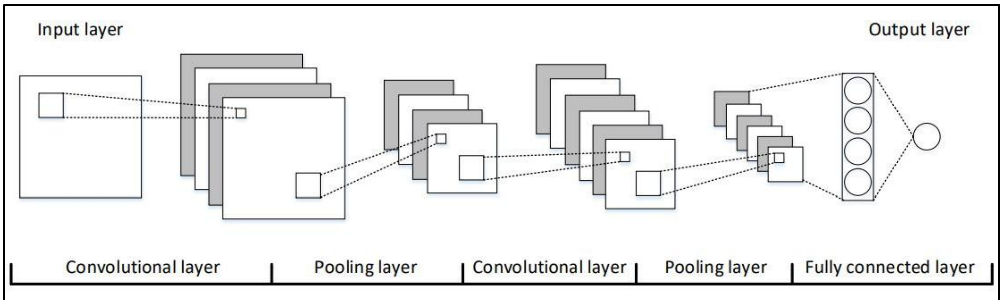

Fig. 6. The structure CNN [54]

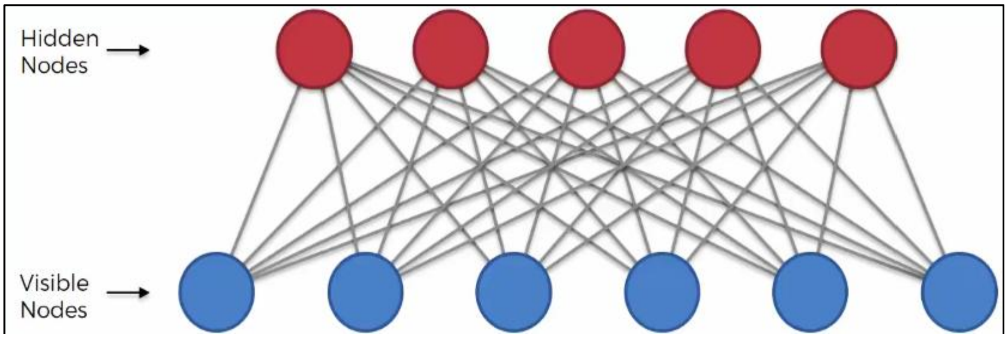

Fig. 7. RBM Structure [59]

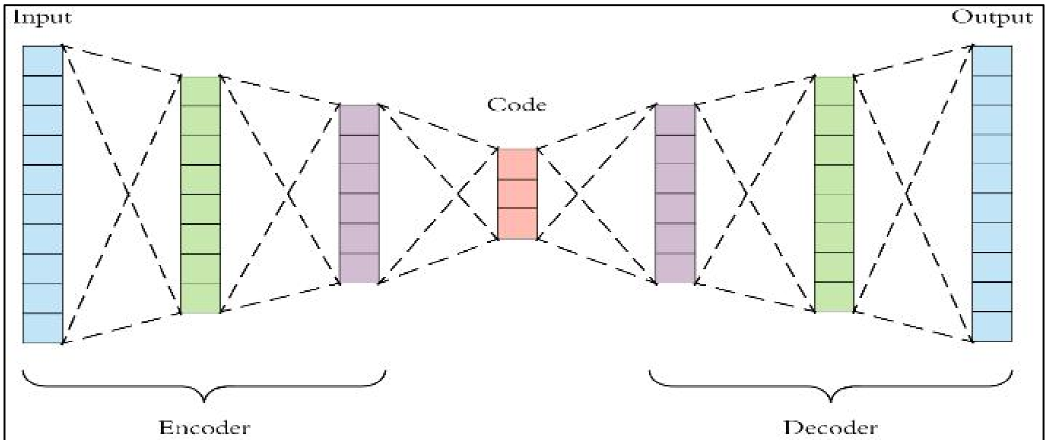

Fig. 8. The autoencoder neural network [63]

As mentioned above most popular DL methods, many other deep learning approaches exist in the field for various purposes. For example, the Self-Organizing Map (SOM) is a form of ANN that uses unsupervised learning to convert high-dimensional data to a two-dimensional grid map, thereby achieving dimensionality reduction [65,66]. A Deep Belief Network (DBN) is a DNN unsupervised network similar to RBM or autoencoders. It is also a type of Backpropagation Neural Network (BPNN) [67]. A Generative Adversarial Network (GAN) is a form of DL network that can generate new data with properties similar to the original data input [68]. Additionally, GANs are commonly used in natural image synthesis, medical image processing, bioinformatics, data augmentation, video generation, and voice generation, among other applications. Additionally, it is beneficial in the field of IoT [69].

4. CLOUD SYSTEMS

Cloud computing is a set of hardware and software technologies that work together to create a network for delivering on-demand services over the internet [70]. Traditionally, a user's computer's hardware and software are entirely enclosed within it, and you can access your data and programs exclusively from the user's computer. Rather than storing data and programs on a user's personal computer or server, cloud storage allows you to access them through software, databases, email, and file services. This means that users can access online services that are generally accessible from any computer with an internet connection, regardless of the user's location, as illustrated in Fig. 9 below [50,71,72,73]. Cloud computing is classified into two models: service models and deployment models; in the following subsection, we will discuss both [74].

4.1 Cloud Computing of Service Models

The availability of cloud computing resources has facilitated the creation of customized cloud service models. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are the three models (IaaS). The service models are depicted in Fig. 10, and a discussion follows [75,76].

Infrastructure as a Service (IaaS): The Cloud makes the data available to the customers [77]. The data are presented in a business- and user-friendly format. The data and information distribution system is essentially a standardized method for efficiently representing and disseminating data and information [78]. IAS's primary objective is to present impressions derived from analyzed and processed data and information derived from experience or a credible source [79].

Platform as a Service (PaaS): In this model, Cloud providers users with development environment resources enable them to create and run their applications. Programming language environments, Operating systems, databases, and web servers are all examples of utilities [80].

Software as a Service (SaaS): The Cloud provides users with access to cloud-based developer applications in this model [81]. Cloud clients have access, and cloud users do not have to manage the infrastructure on which the application operates, removing the need for cloud users to install and run their computers [82]. These services are available on a demand basis. For a specified period, the user can access these services as desired. These services are managed by service providers or companies such as Amazon, Google, and IBM [83].

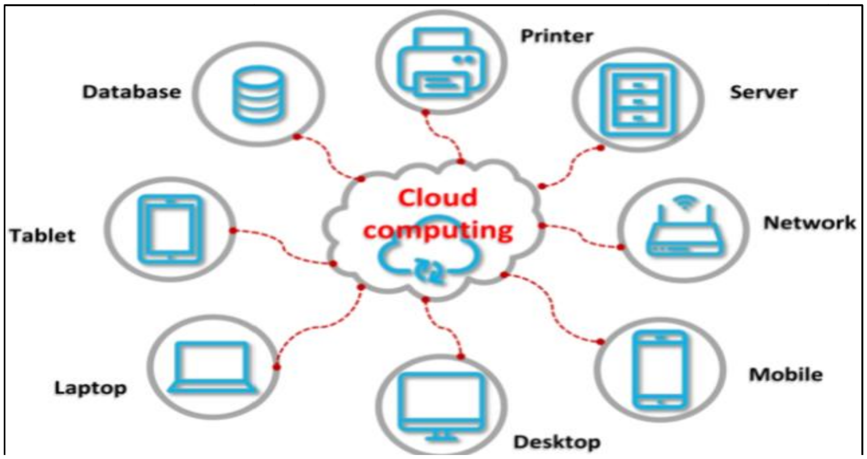

Fig. 9. Cloud computing [50]

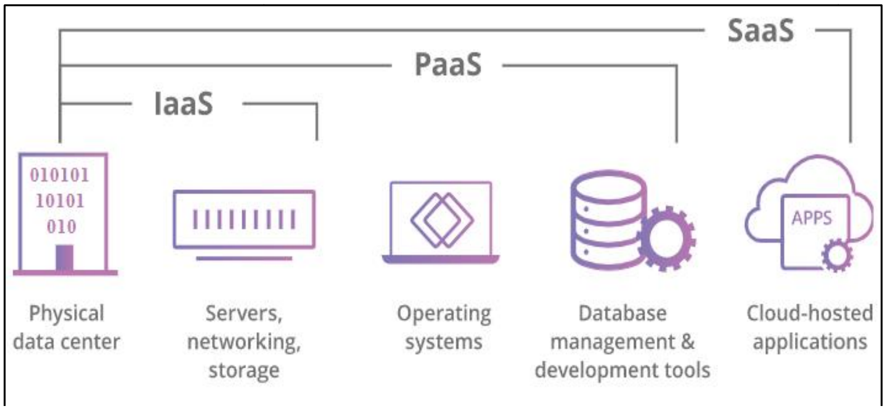
SaaS
PaaS
IaaS
010101
10101
010
APPS
Physical data center
Servers, networking, storage
Operating systems
Database management & development tools
Cloud-hosted applications

Fig. 10. Service model [75]

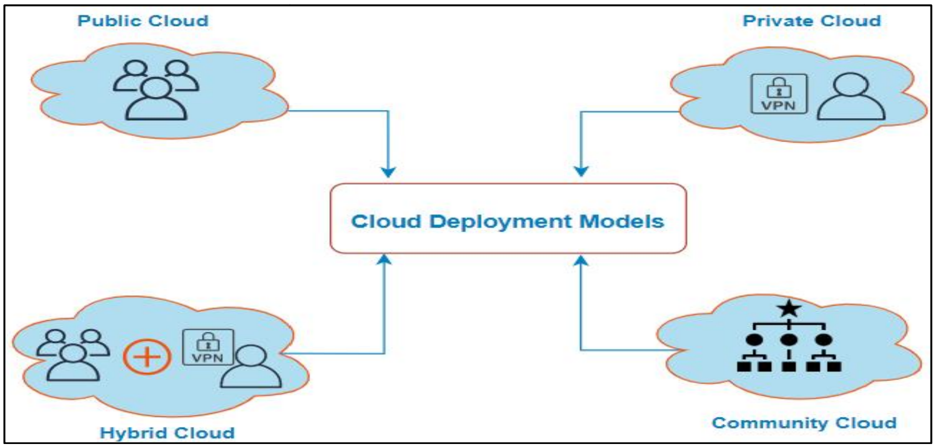

Fig. 11. Type of cloud deployment models [85]

4.2 Cloud Deployment Models

Cloud computing services are delivered via the internet. Cloud integrators can be critical in determining the optimal cloud direction for a particular company. As illustrated in Fig. 11, Public cloud, private Cloud, hybrid Cloud, and community cloud are the four most common cloud deployment models [84,85].

Public Cloud: are accessible to those interested in using infrastructures such as computing resources (Amazon Ec2), storage, and database services. The public Cloud employs a multi-tenancy model, which enables users to scale resources as required [86]. It is a large enterprise. The following are some of the advantages of public clouds [87]:

- Adaptability
- Excellent scalability
- Energy efficiency at a low cost
- Reliability and quality
- Geographical independence

Private Cloud: is more costly than public Cloud, but it gives companies greater control over their security and privacy. Private Cloud offers the same advantages as public Cloud, but the cloud infrastructure is dedicated to a single tenant/organization. Many companies do not have access to infrastructure resources [88]. Private clouds can be handled on-premise or by a cloud service provider. The advantages of private cloud computing are as follows [89]:

- Increased protection
- Increased reliability
- Increased control
- Cost-effectiveness

Community Cloud: deployment model is somewhat similar to a private cloud, but the key difference is that data is shared between organizations [89]. In a community cloud environment, organizations with similar backgrounds share infrastructure, resources, and data [90]. For instance, a country's government can have several entities within it, but they must share specific data [91].

A hybrid cloud is a cloud computing enterprise or environment that uses public, private, and community computing foundations. With a hybrid cloud, service provider companies can use third-party cloud providers in various ways, increasing cloud computing's adaptability and versatility [92]. The following are some of the advantages of hybrid cloud architecture [93]:

- Adaptability
- Economic performance
- Safety
- Adaptability

5. INTERNET OF THINGS AND SECURITY

The Internet of Things (IoT) is a relatively new technology that has grown in popularity over the last few years [94]. The IoT is described as a network of physical objects, computers, cars, and buildings embedded with electronics, software, sensors, and network connectivity to collect and exchange data. IoT developed in a permanent universal link between people and things. The diverse range of IoT system applications is often classified into numerous categories [95], including smart home, smart city [96], health care and medical, transportation, home automation and building, agriculture, manufacturing, energy conservation, and environmental monitoring as military applications. The IoT enables people to thrive and function more efficiently and complete control over their lives [97,98].

However, due to the limited resources available to IoT devices, high-complexity tasks, and vast data storage volumes are often managed by the resource-rich cloud model, significantly improving their performance. For example, IoT devices produce large volumes of data, putting a significant strain on the IoT. The Cloud can be used to process and store large amounts of data produced by IoT devices, thus increasing the overall efficiency of a cloud-based IoT environment [99]. Fig. 12 depicts the cloud-based IoT architecture [100].

5.1 Architecture of Internet of Things

There are several viewpoints on the Internet of Things architecture. However, several researchers have considered the IoT's three-layer architecture. The Perception, Network, and Application layers are referred to like these three layers [101]. Each layer plays a unique role in the IoT system, as illustrated in Fig. 13 [102].

Perception Layer: is primarily responsible for data collection and transmission to the Network layer. Numerous sensors embedded in IoT devices can detect and record meaningful physical Temperature, humidity, light intensity, and sound are all examples of physical quantities. Before transmission, data may be preprocessed in the Perception layer. Additionally, the Perception layer can allow devices to collaborate through short-range networks. The capture of nodes, Injection of Malicious Code, Injection of False Data, and Booting Attacks are all significant security threats that can occur at the perception layer.

Network Layer: is responsible for routing and transmitting the Perception Layer's data through the network layer. The data is transmitted through the Internet to other computers or IoT hubs. WiFi, Bluetooth, 3G/LTE, Zigbee, and Lora are only a few examples of commonly used network technologies. The most common security concerns at the network layer are Phishing Site Attacks, Access Attacks, DDoS/DoS Attacks, Data Transit Attacks, and Routing Attacks.

Application Layer: is the IoT framework's top layer, and it is responsible for achieving the final objective of supporting the world. Smart City, Smart Home, and Smart Factory are all examples of this layer. The Application layer collects data transmitted over the Network Layer and processes it to accomplish the ultimate purpose of delivering the IoT infrastructure's intended service. Data Theft, Access Control Attacks, Service Interruption Attacks, Injection of Malicious Code Attacks, Sniffing Attacks, and reprogram Attacks are the application layer encounters' primary security problems.

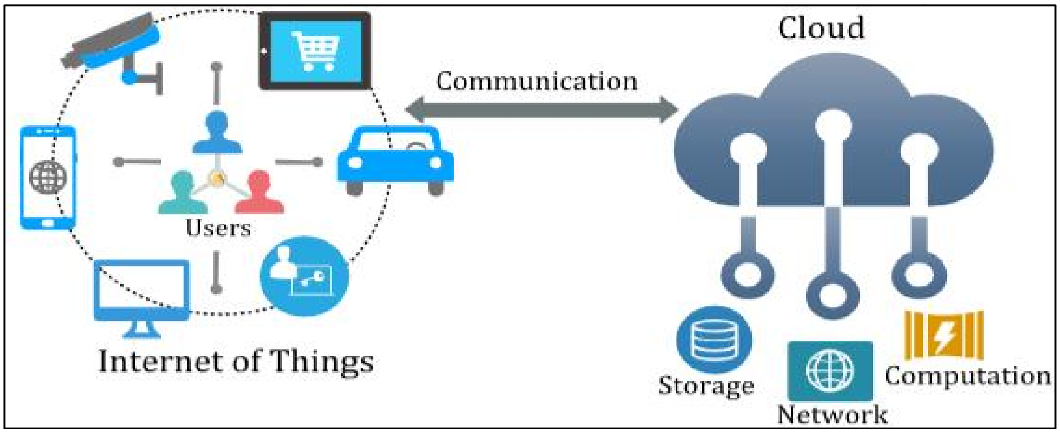

Fig. 12. Cloud-based IoT context [100]

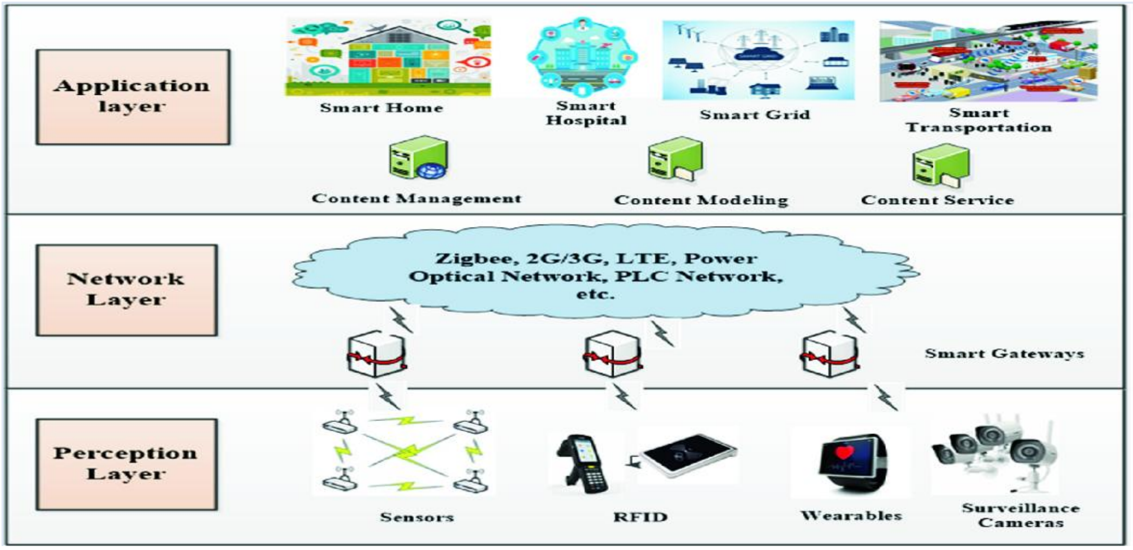

Fig. 13. Layers in IoT system [102]

5.2 Security Aspects of IoT Devices

Security and privacy are two critical aspects of commercializing IoT services and applications [103]. The modern Internet is a prime target for security threats ranging from simple hacks to well-coordinated corporate-level security breaches that have harmed various healthcare and industry industries. The limitations of IoT devices and the world in which they work create additional challenges for application and system protection. Until now, security and privacy concerns have focused on system design, network access, and the data collected by IoT devices [104].

5.3 Security Issues for IoT

A variety of different groups created ioT, and as a result, it takes on a variety of different types and implementations. There is still no agreement on the exact meaning of the Internet of Things, and many individuals and organizations have their perspectives. Consequently, During the early stages of IoT development, no predefined security was available standards between various groups, which has caused considerable concern about security issues in recent years. IoT devices and sensors have the potential to capture and distribute private and confidential data that include personally identifiable information. As a consequence, it is critical to include security services that provide the CIA triad. Due to the many specific characteristics of IoT, delivering IoT security services is a difficult challenge. One explanation is that since many IoT platforms are unique, it is challenging to develop universal and homogeneous protection systems applied to various IoT platforms. The other explanation is that the size of IoT networks is so large that attempting to monitor the entire network of devices simultaneously can introduce many complications. The primary security objectives of the IoT will include the following [105,106,107]:

- Confidentiality, Integrity, and Availability.
- Authentication, authorization, and accounting.
- Energy Efficiency.
- Heterogeneity.
- Network policy

6. LITERATURE REVIEW

Many pieces of research have analyzed the Deep Learning and Machine Learning Algorithms for Internet of Things Security, Wei. Y and et al. [108] A fingerprint indoor positioning system aided by the IoT and an SVM classifier has been suggested. The support vector classification technique is used in conjunction with kernel tricks to solve the multi-class classification problem in indoor fingerprint positioning. Three distinct kernel functions are examined and compared using data from an experiment conducted in a real-world indoor environment. The results indicate that a support vector classifier with a Gaussian RBF kernel function has the highest accuracy for positioning.

Fatayer. T and Azara. M [109] Classification of IoT networks using SVM. This classification aims to distinguish malicious from regular traffic. The proposed approach classifies traffic into four distinct categories: periodic, event, query, and malicious. After identifying malicious traffic, it must be blocked immediately to prevent network congestion.

Additionally, separate channels may be created to carry different types of traffic to minimize latency. The model is evaluated using a confusion matrix, a receiver operating characteristic curve, and a classification report. The Author used 1777 records to train the SVM model initially and archived training accuracy of 78.51% and testing accuracy of 78.32%. Later, the number of records was increased to 14216, and the training accuracy was increased to 79.08%, while the testing accuracy was increased to 72.57%.

Jiahao. Y and et al. [110] To suggested a method for detecting faults in the GS-IoT system using a combination of SVM and BiLSTM by analyzing the OM and ES communication to emotional expression. The Author evaluated the data in real-time and identified the fault forms using a dynamic approach. To deal with the BiLSTM algorithm's complex and deep structure, to proposed first entered the data into an SVM to differentiate between normal and fault conditions, and then used the data in the BiLSTM to accurately locate the type of failure. The accuracy of the proposed fault detection system in this article is 99.12%, satisfying the gas station's criteria for fault detection accuracy.

Sugi. S and Ratna. S [111] Suggested that the LSTM and KNN algorithms detect security and privacy concerns in IoT networks. The attack detection module's deep learning and machine learning algorithms are analyzed using a bot-IoT dataset. The obtained results indicate that the recurrent neural network outperforms the kappa statistic values in terms of accuracy. In the IoT paradigm, LSTM is effective at detecting attacks.

Dior and et al. [112] proposed a DL-based IDS for defending against DoS attacks on IoT networks. Based on the NSLKDD dataset, the proposed model is evaluated. The authors compared the proposed IDS to the more conventional shallow model approach. Additionally, the proposed IDS employs a centralized and distributed detection strategy. The comparison results indicate that the distributed attack detection system is more accurate than the centralized attack detection scheme. Similarly, the deep model produces superior accuracy, precision, recall, and F1 test compared to the shallow model.

Spantidi. P and et al. [113] have introduced a solution for implementing a large-scale CNN on a heterogeneous IoT computing framework systematically. The Author has developed a framework that investigated the device's operating frequencies, prunes the system design, and selects the best computer configuration according to the system's objectives (low power/high performance). The proposed framework improves efficiency by an average of 33.4% and up to 66.3% compared to the system's default governor and operation mode, thus reducing power consumption by an average of 42.8% and up to 61.5%.

Su. J and et al. [114] To suggested a novel lightweight method for detecting DDoS malware in the Internet of Things (IoT) environments. The author extracted malware images (i.e., a one-channel gray-scale image changed from a malware binary) and classified their families using a lightweight CNN algorithm with the original 500 malware samples dataset. The experimental results indicate that the proposed method can categorize goodware and DDoS malware with an accuracy of 94.0% and goodware and two prominent malware families with an accuracy of 81.8%.

Doshi. R and et al. [115] The Author has, claimed there were almost 15 times as many attack packets as ordinary ones due to the flooding nature of the DoS attacks. As a result, a simple baseline prediction algorithm that assumes all packets are harmful will achieve a baseline accuracy of 0.93. It made use of machine learning at the packet stage.

Shakeel. P and et al. [116] The Author has used, Deep-Q-Network (DQN) to analyze security issues in IoT health applications, including authentication, malware detection, and access control. The proposed approach authenticates the system first and then extracts traffic characteristics, channel impulse response, an indicator of received signal strength, channel state information, and received signal strength from the request to be stored in databases trained using defined DQN for detecting malware attacks in IoT health data transactions in networks. The evaluation result indicates that the error rate is 0.12%, and the accuracy rate is 98.79%.

Han. G and et al. [117] To suggested the k-means cluster-based location privacy (KCLP) scheme for protecting location privacy in wireless sensor networks (WSNs) for the Internet of Things. A fake source and sink are used to cover the location of the natural source and sink. The author has used, k-means cluster, the routing path can be extended, thus increasing the safety time. Finally, the difference in routing patterns between the fake and actual packets will help minimize network latency. The results of the experiments indicate that the KCLP scheme outperforms the SLP and RBR schemes in terms of safety time and delay.

Jang. S and Ahn. B [118] That used facial recognition and eye-blink recognition technologies. The proposed machine learning was used to predict drowsiness and develop drowsiness prediction. The Author utilized an Internet of Things (IoT) sensor (CO2) chip to determine additional drowsiness. Additionally, speech recognition technology can be used to perform Speech to Text (STT), enabling a driver to request music or make a call-in to prevent drowsiness while driving.

Ahn. H and Park. N [119] To proposed a deep RNN-based short-term forecast for photovoltaic power. The proposed model takes advantage of the on-site IoT data and power data obtained in real-time to represent the effects of weather changes. To investigate various parameters of the proposed deep RNN-based forecast model and their interaction with weather parameters to develop an effective prediction model. The experimental results indicated that the forecasting accuracy for 5 and 15 minutes ahead of PV power generation using three RNN layers with 12-time steps was 98.0% and 96.6%, respectively, based on the normalized root mean square error. Their R2-values were 0.988 and 0.949, respectively. Their accuracies were 94.8% and 92.9 percent, respectively, in experiments conducted one and three hours ahead of forecasts for photovoltaic power generation.

Additionally, their R2-scores were 0.963 and 0.927, respectively. The experiments demonstrated that the proposed deep RNN-based short-term forecast algorithm improved prediction accuracy. In the same work, [120] proposes a multi-layer RNN algorithm for forecasting photovoltaic (PV) power collected via on-site IoT (Internet of Things) sensors in the short term. The experimental results indicated that short-term PV power prediction accuracy using three RNN layers with 12-time steps was 98.02% and 96.58%, respectively, based on the normalized root mean square error. These experiments established that the proposed short-term prediction algorithm, which is based on a multi-layer RNN model, can respond to short-term PV fluctuation.

T. J. Sheng et al. [121] The authors demonstrated an intelligent waste management system that incorporates integrated sensors, the LoRa communication protocol for transmitting data to the server, and a TensorFlow implementation for training deep learning model capable of real-time object detection and classification. Similarly, In [122], The author proposed a System of smart bins focused on deep learning and image processing and the Internet of Things. This approach uses a CNN to classify and separate waste into various categories, including metal, glass, paper, and plastic. To train the network, 400 to 500 images containing the four distinct groups are used. TensorFlow and Keras are used to implement the CNN. Eight layers comprise the network. For each class, the train/validation split is 350-400/50-100, for a total of 50 epochs. The system, which utilizes image processing on the Raspberry Pi microcontroller, is capable of identifying and classifying waste with an accuracy of approximately 84%.

Vu. L and Nguyen. Q [123] The authors proposed a new ensemble model for learning the latent representation in IoT anomaly detection that combines Tanh and Rectified Linear Unit (Relu) functions in AEs. The proposed model is called Latent Representation Ensemble (ELR). Additionally, the author analyzed the properties of three common AFs, Sigmoid, Tanh, and Relu, to determine why Tanh and Relu are better suited for learning characteristics of IoT anomaly data than Sigmoid. The demonstrator conducted extensive simulations on IoT botnet datasets using four traditional classifiers: SVM, PCT, NCT, LR. The results of the experiments have shown that our proposed model significantly improves the precision of IoT anomaly detection by 19,9% relative to the originals with a curve region.

Bao. J and et al. [124] The Author presented a hybrid supervised and unsupervised learning approach for secondary classification of unseen system types in this article. Our technology combines a deep neural network with clustering to permit both the classification of visible and invisible devices. It uses automatic encoding technology to minimize dataset dimension, thus providing a good balance between overview and accuracy of classification.

Mohapatra. S and et al. [125] The authors proposed a new technique for predicting soil type and providing accurate information to farmers through audio for improvised cultivation. It collects various soil parameters such as temperature, moisture, and nitrogen, phosphorous, and potassium (NPK) values present in the soil using multiple sensors and uses RF Classifier, SVM, and Linear Regression Algorithms to predict the soil type. After comparing all of the ML algorithms listed previously, it is determined that RF Classifier provides the best soil type prediction with the lowest Root Mean Square Error (RMSE) value. The predicted soil type information, provided in text format, is converted to an audio format easily understood by farmers using the AWS technique.

Panda. S and Panda. G [126] The author presented a machine learning-based classification solution to the network nodes. The proposed method aims to provide an intelligent multimedia traffic classification scheme for IoT applications involving consumer recognition in healthcare. To present a performance comparison of three machine learning-based classification methods: DT, NB, and RF. The Parkinson's disease-related voice data set is collected by digital home virtual assistants and transmitted via a complex global network infrastructure (IoT) to track patients at network nodes.

Fan. C and et al. [127] described a solution to excessive data and undue Pressure of cloud computing IoT by using cloud-based collaborative architecture. This approach synchronizes the raw data obtained at the edge

Table 1. A summary of IoT-related machine learning and deep learning algorithms

Ref	Years	Datasets	Algorithms	Attacks	Proposed Applications	Results / Accuracy
[108]	2020	3.5 lakh dataset	ANN	DoS Malicious Control Malicious Operation Probing Spying Scan Wrong Setup	To anomaly detection for IoT Network	The data is split into two groups, training, and test. An ANN achieves 99.4% accuracy for the first case, while the second case achieves 99.99% accuracy.
[109]	2020	41 Features	Deep Learning Algorithms	breakthroughs in domains, object and voice recognition	Intrusion detection systems	Accuracy = 99%
[110]	2020	Temperature Humidity Soil moisture	DT	No	IoT based Smart Agriculture	As a result, through the DT algorithm, an email alert is sent to farmers, assisting them in making informed decisions regarding water supply in advance.
[111]	2020	Generation dataset	RNN	Malicious	A novel approach to detect IoT malware	Increased accuracy has been reached for the smallest possible number of epochs.
[112]	2020	TAO Stock HPC	KNN	No	KNN-Based Approximate Outlier Detection	The results verify the efficiency and accuracy of GAAOD
[113]	2020	NSL KDD	SVM	DoS Data leakage	Framework Machine Learning Security for IoT Systems	The detection accuracy of anomalies achieved 99.71%
[114]	2020	CIDDS-001 UNSWNB15 NSL-KDD	RF CART MLP AB GBM XGB ETC	DoS	Intrusion detection systems	Classification and regression trees, along with extreme gradient boosting classifiers, yield the best combination of

Ref	Years	Datasets	Algorithms	Attacks	Proposed Applications	Results / Accuracy
						prominent metrics and response time, making them both ideal for creating IoT-specific anomaly-based IDS.
[115]	2020	NSL NB15 BoT-IoT BoTNeTIoT	PCA RF filter-based dimensionality reduction	No	Dimensionality Reduction in IoT IDS	PCA results in the greatest size reduction.
[116]	2020	Real-world IoT dataset	SAE	Man in the Middle Recon DoS Botnet Malware	Novel ERID scheme	With an overall accuracy rate of 83.3 percent, the findings indicated that ERID has a wide range of application possibilities.
[117]	2020	IoT botnet dataset	Gaussian NB LDA LR DT RF	Normal DoS Scan	New botnet dataset for ID in IoT networks	The author has chosen the five most excellent classifiers based on accuracy, precision, recall, and F scores for binary, category, and subcategory classes.
[118]	2020	IoT Network Intrusion Dataset	LR SVM KNN RF XGBOOST	Malicious cyberattacks	Develop an anomaly-based IDS	99.9% -100.0% accuracy while maintaining a high level of performance
[119]	2019	MNIST	CNN	No	Smart parking based on IOT	The accuracy = 98.5%
[120]	2019	KDD CUP 99	ANN MLP RBF	DoS U2R R2L Probing	To Detecting IoT attacks using ANN Classification Algorithms	MLP achieves the best accuracy (99.86%).
[121]	2019	ATM	CNN	No	Face Occlusion Recognition	The occlusions in faces accuracy 98.89% and occlusion verification accuracy 97.25%

Ref	Years	Datasets	Algorithms	Attacks	Proposed Applications	Results / Accuracy
[122]	2019	1241 Rows	DT KNN	No	To improve the existing crowd management controlling system in hajj by using an E-wrist belt.	The KNN algorithm provided better accuracy in the result than the Decision tree algorithm.
[123]	2019	Real traffic data	SVM	Blackhole Sinkhole Selective forward	Anomaly detection model to detect abnormalities within the IoT	Accuracy=100% for known topology Accuracy=81% for unknown topology
[124]	2019	Synthetic data from the virtual environment	LR DT SVM ANN RF	DoS Data Type Spying Wrong Setup Malicious Operation Scan Malicious Control Probing	To predict attacks and anomalies on the IoT systems	LR=98.3% DT=99.4% SVM=98.2% ANN=99.4% RF=99.4%
[125]	2019	UNSW-NB 15	RF	Cyberattacks	Anomaly Detection IoT (AD-IoT) system	99.34%
[126]	2019	MNIST	CNN	NO	Smart parking based on IoT	98% accuracy for license plate detection
[127]	2019	KDDCUP	DBN GA	DoS R2L Probe U2R	A Novel ID Method for IoT.	99%

layer, utilizes the random forest algorithm to classify, process, and feed the results back to the system. Simultaneously, the data is uploaded to the Cloud through the edge layer, organized, and stored using the LSTM-FCN data classification model. The LSTM-FCN algorithm described in this article is significantly more accurate than the other two algorithms, with an average accuracy of approximately 94%.

7. COMPARISON AND DISCUSSION

Our work examines many academic IoT studies based on ML and DL, as illustrated in Table 1. In this paper, we reviewed most of the ML and DL algorithms for IoT security. At the current, the field of IoT and its significance are penetrating every door. Additionally, the security of IoT has garnered interest from a variety of network and device researchers. To implement ML algorithms effectively in IoT systems, appropriate data sets are needed, which are frequently difficult to collect depending on the system's ability to recognize threats and take necessary actions. Furthermore, for cryptanalysis by attackers, ML and DL methods have been considered a possible challenge to the IoT scheme. While cryptography is generally difficult to break, advanced ML algorithms such as SVM and RF are used to break down a robust cryptographic framework. We first discuss some issues related to the performance and security tradeoff observed from the experimental results.

In this review, we realize that most of them are having good accuracy. However, some research has higher accuracy through the literature in Table (1) ML and DL technique with variance datasets. Some previous works proposed that the data is split into two parts, training and testing. In the first case, an ANN algorithm achieves 99.4% accuracy, while the second case achieves 99.99% accuracy, which realized the excellent result. Other works proposed uses the learning anomaly detection model of the Support Vector Machine (SVM) to detect anomalies on the Internet of Things. When tested with anonymous information from the same topology as qualified networks and 81% with an unknown topology, the model achieves up to 100% accuracy. On the other hand, the author research offered a thorough overview of unsupervised algorithms for DL. 99% detection accuracy is shown in the simulation studies, also show us the deep learning algorithm has enough capacity to extract powerful result with the internet of things security. As well as another research proposed an intelligent parking model to reduce the wastage of time using the internet of thing and google Cloud through an Android application and also utilized one of the Deep Learning algorithms (CNN) for the user verification process and navigated, in there results from they are got 98% accuracy and wastage of time by 50% the result show as the better performance the traditional methods. While, other authors proposed a novel ML-based security architecture that automatically addresses the growing security concerns associated with the IoT. In Addition, some researchers addressed several ML models to predict IoT systems attacks and abnormalities reliably. The Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), and Artificial Neural Network (ANN) algorithms were used in this work (ANN). The method achieved a test accuracy of 99.4 percent for Decision Tree, Random Forest, and ANN. While both methods are accurate, other metrics demonstrate that Random Forest performs significantly better. However, some previous works proposed model is an intelligent irrigation system that uses ML algorithms to predict crop water requirements. The three most important parameters for determining the water quantity needed in any agricultural area are moisture, temperature, and moisture. This researcher employed a machine-efficient learning algorithm applied to data sensed from the field to predict performance effectively. As we show in this review, the ML and DL algorithms got an excellent result with the field of internet of things security but still lack of study to increase the accuracy.

8. CONCLUSION

While we have focused on time in this systematic literature review, the relative number of research publications has shown that it is a hot field of research. This research area combines many increasingly increasing areas, including the Internet of Things, machine learning, deep learning with the dataset. The IoT will transform the future and put global issues into our hands. We expect that this field of research will remain intensely concentrated for many years. Vertically and horizontally, the evolution and growth of IoT devices and use will continue. At a similar rate, attacks will continue to increase on such networks and computers. As future work, it can be suggested to depend on autonomous and real-time detection of such attacks. A large scale of intelligence will be mandatory. Also, it is recommended to merge the developed ML algorithms with the sixth generation of IoT to provide enhance systems in this field.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Hassan RJ, et al. State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions. Asian J. Res. Comput. Sci. 2021; 32–48.
2. Reising D, Cancelleri J, Loveless TD, Kandah F, Skjellum A. Radio identity verification-based IoT security using RF-DNA fingerprints and SVM. IEEE Internet Things J; 2020.
3. Yang G, Zhang Q, Liang YC. Cooperative ambient backscatter communications for green Internet-of-Things. IEEE Internet Things J. 2018;5(2)1116–1130.
4. Yahia HS, et al. Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling. Asian J. Res. Comput. Sci. 2021;1–16.
5. Halder S, Ghosal A, Conti M. LiMCA: An optimal clustering algorithm for lifetime maximization of internet of things. Wirel. Networks. 2019;25(8):4459–4477.
6. Ageed ZS, et al. A survey of data mining implementation in smart city applications. Qubahan Acad. J. 2021;1(2):91–99.
7. Qureshi KN, Bashir F, Iqbal S. “Cloud computing model for vehicular ad hoc networks,” in 2018 IEEE 7th International Conference on Cloud Networking (CloudNet). 2018;1–3.

8. Abdulqadir HR, et al., A study of moving from cloud computing to fog computing. Qubahan Acad. J. 2021;1(2):60–70.
9. Mubeen S, Asadollah SA, Papadopoulos AV, Ashjaei M, Pei-Breivold H, Behnam M. Management of service level agreements for cloud services in IoT: A systematic mapping study. IEEE access. 2017;6:30184–30207.
10. Bambrik I. A survey on cloud computing simulation and modeling. SN Comput. Sci. 2020;1(5):1–34.
11. Ageed ZS, et al. A state of art survey for intelligent energy monitoring systems. Asian J. Res. Comput. Sci. 2021;46–61.
12. Shukur H, Zeebaree S, Zebari R, Zeebaree D, Ahmed O, Salih A. Cloud computing virtualization of resources allocation for distributed systems. J. Appl. Sci. Technol. Trends. 2020;1(3):98–105.
13. Sagduyu YE, Shi Y, Erpek T. “IoT network security from the perspective of adversarial deep learning,” in 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). 2019;1–9.
14. Abdulrazaq MB, Mahmood MR, Zeebaree SRM, Abdulwahab MH, Zebari RR, Sallow AB. “An analytical appraisal for supervised classifiers’ performance on facial expression recognition based on relief-F feature selection,” in Journal of Physics: Conference Series. 2021;1804(1):12055.
15. Mahmood MR, Abdulrazzaq MB, Zeebaree SR, Ibrahim AK, Zebari RR, Dino HI. Classification techniques’ performance evaluation for facial expression recognition. Indones. J. Electr. Eng. Comput. Sci. 2021;21(2):176–1184.
16. Dino H, et al. Facial expression recognition based on hybrid feature extraction techniques with different classifiers. TEST Eng. Manag. 2020;83:22319–22329.
17. Zebari DA, Haron H, Zeebaree SRM, Zeebaree DQ. “Enhance the mammogram images for both segmentation and feature extraction using wavelet transform,” in 2019 International Conference on Advanced Science and Engineering (ICOASE). 2019;100–105.
18. Jahwar A, Ahmed N. Swarm intelligence algorithms in gene selection profile based on classification of microarray data: A review. J. Appl. Sci. Technol. Trends. 2021;2(01):1–9.
19. Liang F, Hatcher WG, Liao W, Gao W, Yu W. Machine learning for security and the internet of things: The good, the bad, and the ugl. IEEE Access. 2019;7:158126–158147.
20. Tahsien SM, Karimipour H, Spachos P. Machine learning based solutions for security of internet of things (IoT): A survey. J. Netw. Comput. Appl. 2020;161:102630.
21. Agrawal P, Trivedi B. “Machine learning classifiers for Android malware detection,” in Data Management, Analytics and Innovation, Springer. 2021;311–322.
22. Abdulla AI, et al. Internet of things and smart home security. Technol. Rep. Kansai Univ. 2020;62(5):2465–2476.
23. Hussain F, Hussain R, Hassan SA, Hossain E. Machine learning in IoT security: Current solutions and future challenges. IEEE Commun. Surv. Tutorials. 2020;22(3):1686–1721.
24. Hosseinzadeh M, Rahmani AM, Vo B, Bidaki M, Masdari M, Zangakani M. Improving security using SVM-based anomaly detection: Issues and challenges. Soft Comput. 2020;1–29.
25. Karimipour , Dinavahi V. “On false data injection attack against dynamic state estimation on smart power grids,” in 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE). 2017;388–393.
26. Ioannou C, Vassiliou V. “Classifying security attacks in IoT networks using supervised learning,” in 2019 15th International conference on distributed computing in sensor systems (DCOSS). 2019;652–658.
27. Durga S, Nag R, Daniel E. “Survey on machine learning and deep learning algorithms used in internet of things (IoT) healthcare,” in 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). 2019;1018–1022.
28. Quek YT, Woo WL, Thillainathan L. IoT load classification and anomaly warning in ELV DC picogrids using hierarchical extended ${k} $-nearest neighbors. IEEE Internet Things J. 2019;7(2):863–873.
29. Abdulraheem AS, et al. Home automation system based on IoT; 2020.
30. Salih AA, Zeebaree SRM, Abdulraheem AS, Zebari RR, Sadeeq MAM, Ahmed OM. Evolution of mobile wireless communication to 5G revolution. Technol. Reports Kansai Univ. 2020;62(5):2139–2151.

31. Taghavinejad SM, Taghavinejad M, Shahmiri L, Zavvar M,. Zavvar MH. “Intrusion detection in IoT-based smart grid using hybrid decision tree,” in 2020 6th International Conference on Web Research (ICWR). 2020;152–156.
32. Lucky G, Jjunju F, Marshall A. “A lightweight decision-tree algorithm for detecting DDoS flooding attacks,” in 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C). 2020;382–389.
33. Dino HI, et al. Impact of process execution and physical memory-spaces on OS performance; 2020.
34. Ageed ZS, et al. Comprehensive survey of big data mining approaches in cloud systems. Qubahan Acad. J. 2021;1(2):29–38.
35. Yazdeen AA, Zeebaree SRM, Sadeeq MM, Kak SF, Ahmed OM, Zebari RR. FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review. Qubahan Acad. J. 2021;1(2):8–16.
36. Abdulrahman LM, et al. A state of art for smart gateways issues and modification. Asian J. Res. Comput. Sci. 2021;1–13.
37. Haji SH, et al. Comparison of software defined networking with traditional networking. Asian J. Res. Comput. Sci. 2021;1–18.
38. Bensaid R, Ben Said M, Boujemaa H. “Fuzzy C-means based clustering algorithm in WSNs for IoT applications,” in 2020 International Wireless Communications and Mobile Computing (IWCMC). 2020;126–130.
39. Ahmed M, Barkat A. “Performance analysis of hard clustering techniques for big IoT data analytics,” in 2019 Cybersecurity and Cyberforensics Conference (CCC). 2019;62–66.
40. Mondal MA, Rehena Z. “Identifying traffic congestion pattern using K-means clustering technique,” in 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). 2019;1–5.
41. Zeebaree DQ, Haron H, Abdulazeez AM, Zeebaree SRM. Combination of K-means clustering with genetic algorithm : A review. 2017;12(24):14238–14245.
42. Jahwar AF, Abdulazeez AM. Meta-Heuristic algorithms For K-means clustering: A review. PalArch’s J. Archaeol. Egypt/Egyptology. 2020;17(7):12002–12020.
43. Malallah H, et al. A comprehensive study of kernel (issues and concepts) in different operating systems. Asian J. Res. Comput. Sci. 2021;16–31.
44. Malik S, Chauhan R. “Securing the internet of things using machine learning: A review,” in 2020 International Conference on Convergence to Digital World-Quo Vadis (ICCDW). 2020;1–4.
45. Roopak M, Tian GY, Chambers J. “Deep learning models for cyber security in IoT networks,” in 2019 IEEE 9th annual computing and communication workshop and conference (CCWC). 2019; 452–457.
46. Liu X, Yu W, Liang F, Griffith D, Golmie N. Towards deep transfer learning in industrial internet of things. IEEE Internet Things J; 2021.
47. Zeebaree SR, Ahmed O, Obid K. “CSAER net: An efficient deep learning architecture for image classification,” in 2020 3rd International Conference on Engineering Technology and its Applications (IICETA). 2020;122–127.
48. Li H, Ota K, Dong M. Learning IoT in edge: Deep learning for the internet of things with edge computing. IEEE Netw. 2018; 321):96–101.
49. Yasin HM, et al., IoT and ICT based smart water management, monitoring and controlling system: A review. Asian J. Res. Comput. Sci. 2021;42–56.
50. Ibrahim IM. Task scheduling algorithms in cloud computing: A review. Turkish J. Comput. Math. Educ. 2021;12(4):1041–1053.
51. Zebari IMI, Zeebaree SRM, Yasin HM. “Real time video streaming from multi-source using client-server for video distribution,” in 2019 4th Scientific International Conference Najaf (SICN). 2019;109–114.
52. Thompson WL, Talley MF. “Deep Learning for IoT communications: Invited presentation,” in 2019 53rd Annual Conference on Information Sciences and Systems (CISS).; 2019;1–4.
53. Abdullah SMSA, Ameen SYA, Sadeeq MAM, Zeebaree S. Multimodal emotion recognition using deep learning. J. Appl. Sci. Technol. Trends. 2021;2(02):52–58.
54. Du J, Shen M, Du Y. “A distributed in-situ CNN inference system for IoT applications,” in 2020 IEEE 38th

International Conference on Computer Design (ICCD). 2020;279–287.

55. Susilo B, Sari RF. Intrusion detection in IoT networks using deep learning algorithm. Information. 2020;11(5):279.

56. Castro-Godínez J, Hernández-Araya D, Shafique M, Henkel J. “Approximate acceleration for CNN-based applications on IoT edge devices,” in 2020 IEEE 11th Latin American Symposium on Circuits & Systems (LASCAS). 2020;1–4.

57. Yasin HM, Zeebaree SRM, Zebari IMI. “Arduino based automatic irrigation system: Monitoring and SMS controlling,” in 2019 4th Scientific International Conference Najaf (SICN). 2019;109–114.

58. Zeebaree SR, Yasin HM. Arduino based remote controlling for home: power saving, security and protection. Int. J. Sci. Eng. Res. 2014;5(8):266–272.

59. Hwang S, Jeong J, Kang Y. “SVM-RBM based predictive maintenance scheme for IoT-enabled smart factory,” in 2018 Thirteenth International Conference on Digital Information Management (ICDIM). 2018;162–167.

60. Zeebaree SR, Zebari IM. Multilevel client/server peer-to-peer video broadcasting system. Int. J. Sci. Eng. Res. 2014;5(8).

61. Zebari SRM, Yaseen NO. Effects of parallel processing implementation on balanced load-division depending on distributed memory systems. J. Univ. Anbar Pure Sci. 2011;5(3):50–56.

62. Izadeen GY, Ameen SY. Smart android graphical password strategy: A review. Asian J. Res. Comput. Sci. 2021;59–69,.

63. Provotar OI, Linder YM, Veres MM. “Unsupervised anomaly detection in time series using lstm-based autoencoders,” in 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). 2019;513–517.

64. Khalifa IA, Zeebaree SRM, Ataş M, Khalifa FM. Image steganalysis in frequency domain using co-occurrence matrix and Bpnn. Sci. J. Univ. Zakho. 2019;7(1):27–32.

65. Qu X, et al. A survey on the development of self-organizing maps for unsupervised intrusion detection. Mob. networks Appl. 2019;1–22.

66. Aziz ZAA, Ameen SYA. Air pollution monitoring using wireless sensor networks. J. Inf. Technol. Informatics. 2021;1(1):20–25.

67. Wei P, Li Y, Zhang Z, Hu T, Li Z, Liu D. An optimization method for intrusion detection classification model based on deep belief network. IEEE Access. 2019;7:87593–87605.

68. Amanuel SVA, Ameen SYA. Device-to-device communication for 5G security: A Review. J. Inf. Technol. Informatics. 2021;1(1):26–31.

69. Yin C, Zhu Y, Liu S, Fei J, Zhang H. “An enhancing framework for botnet detection using generative adversarial networks,” in 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD). 2018;228–234.

70. Khalid LF, Ameen SY. Secure Iot integration in daily lives: A review. J. Inf. Technol. Informatics. 2021;1(1):6–12.

71. Taryana U, Fajar AN, Utama DN. “Information as a service on cloud computing technology: A review,” in 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). 2018;39–42.

72. Samann FEF, Zeebaree SRM, Askar S. IoT provisioning QoS based on cloud and fog computing. J. Appl. Sci. Technol. Trends. 2021;2(01):29–40.

73. Sadeeq MAM, Zeebaree SRM, Qashi R, Ahmed SH, Jacksi K. “Internet of things security: A survey,” in 2018 International Conference on Advanced Science and Engineering (ICOASE). 2018;162–166.

74. Sharif KH, Ameen SY. “A review of security awareness approaches with special emphasis on gamification,” in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;151–156.

75. Mohammed CM, Zebaree SRM. “Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review,” Int. J. Sci. Bus. 2021;5(2):17–30.

76. Al Janaby AO, Al-Omary A, Ameen SY, Al-Rizzo H. Tracking and controlling high-speed vehicles via CQI in LTE-A systems. Int. J. Comput. Digit. Syst. 2020;9(6):1109–1119.

77. Zeebaree S, Ameen S, Sadeeq M. Social media networks security threats, risks and recommendation: A case study in the kurdistan region. Int. J. Innov. Creat. Chang. 2020;13:349–365.

78. Hamed ZA, Ahmed IM, Ameen SY. “Protecting windows OS against local threats without using antivirus,” relation. 2020;29(12s):64–70.

79. Siddeeq Y, Ameen Ali O, Mohammed Al Janaby. An enhancement of LTE networks performance efficiency. Noor Publ; 2020.
80. Fawzi LM, Alqarawi SM, Ameen SY, Dawood SA. Two Levels alert verification technique for smart oil pipeline surveillance system (SOPSS). Int. J. Comput. Digit. Syst. 2019;8(02):115–124.
81. Haji SH, Ameen SY. Attack and anomaly detection in IoT networks using machine learning techniques: A review. Asian J. Res. Comput. Sci. 2021;30–46.
82. Jijo BT, et al. A comprehensive survey of 5G mm-wave technology design challenges. Asian J. Res. Comput. Sci. 2021;1–20.
83. Kareem FQ, et al. A survey of optical fiber communications: challenges and processing time influences. Asian J. Res. Comput. Sci. 2021;48–58.
84. Kolte MSA, Ajmire PE. A survey-cloud computing. Int. J. Adv. Res. Comput. Commun. Eng. 2016;4.
85. Nowrin IN, Khanam FK. “Importance of cloud deployment model and security issues of software as a service (SaaS) for cloud computing,” in 2019 International Conference on Applied Machine Learning (ICAML). 2019;183–186.
86. Omer MA, et al. Efficiency of malware detection in android system: A survey. Asian J. Res. Comput. Sci. 2021; 59–69.
87. Maulud DH, Zeebaree SRM, Jacksi K, Sadeeq MAM, Sharif KH. State of art for semantic analysis of natural language processing. Qubahan Acad. J. 2021; 1(2):21–28.
88. Sadeeq MM, Abdulkareem NM, Zeebaree SRM, Ahmed DM, Sami AS, Zebari RR. IoT and Cloud computing issues, challenges and opportunities: A review. Qubahan Acad. J. 2021;1(2):1–7.
89. Shukur H, et al. A state of art survey for concurrent computation and clustering of parallel computing for distributed systems. J. Appl. Sci. Technol. Trends. 2020;1(4):148–154.
90. Sadeeq MAM, Abdulazeez AM. “Neural networks architectures design, and applications: A review,” in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;199–204.
91. Ageed ZS, Ibrahim RK, Sadeeq MAM. Unified ontology implementation of cloud computing for distributed systems. Curr. J. Appl. Sci. Technol. 2020;82–97.
92. Sadeeq MA, Abdulla AI, Abdulraheem AS, Ageed ZS. Impact of electronic commerce on enterprise business. Technol. Rep. Kansai Univ. 2020;62(5):2365–2378.
93. Alzakholi O, Shukur H, Zebari R, Abas S, Sadeeq M. Comparison among cloud technologies and cloud performance. J. Appl. Sci. Technol. Trends. 2020;1(2):40–47.
94. Sallow AB, et al. An investigation for mobile malware behavioral and detection techniques based on android platform. IOSR J. Comput. Eng. 2020;22(4):14–20.
95. Sulaiman MA, Sadeeq MA, Abdulraheem AS, Abdulla AI. Analyzation study for gamification examination fields. Technol. Rep. Kansai Univ. 2020;62(5):2319–2328.
96. Saleem SI, Zeebaree SR, Zeebaree DQ, Abdulazeez AM. “Building smart cities applications based on IoT technologies: A review. Technol. Reports Kansai Univ. 2020;62(3):1083–1092.
97. Sallow AB, Zeebaree SR, Zebari RR, Mahmood MR, Abdulrazzaq MB, Sadeeq MA. Vaccine tracker. SMS Remind. Syst. Des. Implement; 2020.
98. Nayak J, et al. Intelligent computing in IoT-enabled smart cities: A systematic review. Green Technol. Smart City Soc. 2021;1–21.
99. Sadeeq MAM, Zeebaree S. Energy management for internet of things via distributed systems. J. Appl. Sci. Technol. Trends. 2021;2(02):59–71.
100. Li X, Wang Q, Lan X, Chen X, Zhang N, Chen D. Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach. IEEE Access. 2019;7:9368–9383.
101. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access. 2019;7:82721–82743.
102. Wala T, Chand N, Sharma AK. “Energy efficient data collection in smart cities using iot,” in Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario’s, Springer. 2020;632–654.
103. Peña MAL, Fernández IM. “SAT-IoT: An architectural model for a high-performance fog/edge/cloud IoT platform,” in 2019 IEEE

5th World Forum on Internet of Things (WF-IoT). 2019;633–638.

104. Siboni S, et al. Security testbed for Internet-of-Things devices. IEEE Trans. Reliab. 2019;68(1):23–44.

105. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. 2018;82:395–411.

106. Shin H, Lee HK, Cha HY, Heo SW, Kim H. "IoT security issues and light weight block cipher," in 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). 2019;381–384.

107. Dorobantu OG, Halunga S. "Security threats in IoT," in 2020 International Symposium on Electronics and Telecommunications (ISETC). 2020;1–4.

108. Wei Y, Hwang SH, Lee SM. "IoT-aided fingerprint indoor positioning using support vector classification," in 2018 International Conference on Information and Communication Technology Convergence (ICTC). 2018;973–975.

109. Khedkar SP, Aroul Canessane R. "Machine learning model for classification of iot network traffic," in 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). 2020;166–170.

110. Jiahao Y, Jiang X, Wang S, Jiang K, Yu X. SVM-BiLSTM: A fault detection method for the gas station IoT system based on deep learning. IEEE Access. 2020;8:203712–203723.

111. Sugi SSS, Ratna SR. "Investigation of machine learning techniques in intrusion detection system for IoT network," in 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS). 2020;1164–1167.

112. Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. Futur. Gener. Comput. Syst. 2018;82: 761–768.

113. Spantidi O, Galanis I, Anagnostopoulos I. "Frequency-based power efficiency improvement of CNNs on heterogeneous IoT computing systems," in 2020 IEEE 6th World Forum on Internet of Things (WF-IoT). 2020;1–6.

114. Su J, Vasconcellos DV, Prasad S, Sgandurra D, Feng Y, Sakurai K. "Lightweight classification of IoT malware based on image recognition," in 2018 IEEE 42Nd annual computer software and applications conference (COMPSAC). 2018;2:664–669.

115. Doshi R, Apthorpe N, Feamster N. "Machine learning ddos detection for consumer internet of things devices," in 2018 IEEE Security and Privacy Workshops (SPW). 2018;29–35.

116. Shakeel PM, Baskar S, Dhulipala VRS, Mishra S, Jaber MM. Maintaining security and privacy in health care system using learning based deep-Q-networks. J. Med. Syst. 2018;42(10):1–10.

117. Han G, Wang H, Guizani M, Chan S, Zhang W. "KCLP: A k-means cluster-based location privacy protection scheme in WSNs for IoT," IEEE Wirel. Commun. 2018;25(6):84–90.

118. Jang SW, Ahn B. Implementation of detection system for drowsy driving prevention using image recognition and IoT. Sustainability. 2020;12(7):3037.

119. Ahn HK, Park N. Deep RNN-based photovoltaic power short-term forecast using power IoT sensors. Energies. 2021;14(2):436.

120. Park N, Ahn HK. "Multi-layer RNN-based short-term photovoltaic power forecasting using IoT dataset," in 2019 AEIT International Annual Conference (AEIT). 2019;1–5.

121. Sheng TJ, et al. An internet of things based smart waste management system using LoRa and tensorflow deep learning model. IEEE Access. 2020;8:148793–148811.

122. Hulyalkar S, Deshpande R, Makode K, Kajale S. Implementation of smartbin using convolutional neural networks. Int. Res. J. Eng. Technol. 2018;5(4).

123. Vu L, Nguyen QU. "An ensemble of activation functions in auto encoder applied to IoT anomaly detection," in 2019 6th NAFOSTED Conference on Information and Computer Science (NICS). 2019;534–539.

124. Bao J, Hamdaoui B, Wong WK. "Iot device type identification using hybrid deep learning approach for increased iot security," in 2020 International Wireless Communications and Mobile Computing (IWCMC). 2020;565–570.

125. Mohapatra S, Mohapatra A, Patil A. "Soil Analysis and its type prediction with speech enabled output using IoT and AWS," in 2020 IEEE 17th India Council International Conference (INDICON). 2020;1–4.

126. Panda S, Panda G. “Intelligent classification of IoT traffic in healthcare using machine learning techniques,” in 2020 6th International Conference on Control, Automation and Robotics (ICCAR). 2020; 581–585.

127. Fan C, Lu Y, Leng X, Luan W, Gu J, Yang W. “Data classification processing method for the Power IoT based on cloud-side collaborative architecture,” in 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC). 2020;9: 684–687.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/69594