STM JOURNALS

Journal of
Artificial Intelligence
Research & Advances

ISSN: 2395-6720
Volume 12, Issue 1, 2025
January–April
DOI Journal: 10.37591/JoAIRA

https://journals.stmjournals.com/joaira

Review JoAIRA

A Survey of Several Machine Learning (ML) Algorithms for Security Solution in Internet of Things (IoT) Networks

Ali H. Wheeb[1,*], Munsifa Firdaus Khan[2]

Abstract

The Internet of Things (IoT) refers to the integration of physical objects with the Internet, allowing for connectivity and monitoring. This idea has garnered immense attention from researchers and users alike, driven by the widespread accessibility of the Internet. It spans a wide range of devices, including smart versions of conventional appliances, innovative tools tailored for Internet-enabled ecosystems, and sensors that leverage connectivity to revolutionize industries such as manufacturing, healthcare, transportation, and everyday living environments. Nevertheless, IoT does have a drawback, though, and that is the absence of strong and reliable security mechanisms. The usage of IoT has a number of potential dangers. These involve the possibility of illegal data accessibility, and other cyberattacks such as ransomware, botnets, denial of service (DoS), and espionage. The main focus outlined below is the application of machine learning (ML) algorithms for detecting network intrusions. When developing intrusion detection systems to identify network abnormalities, ML is a key component. ML algorithms are quite effective in identifying various forms of cyberattacks. The overview of several ML algorithms for detecting intrusions into IoT systems is presented in this research work. Algorithms such as support vector machines, random forests, and neural networks are essential for identifying anomalies in networks. To create intrusion detection systems, many datasets are available, such as CICIDS-2017, KDD-99, UNSW-NB 15, and TON_IoT. These datasets provide information on various kinds of cyberattacks. Further, challenges and security solutions for IoT Networks are discussed.

Keywords: Internet of things (IoT), machine learning (ML) algorithms, security solution, IDS, attack detection

INTRODUCTION

The Internet of Things (IoT) encompasses all devices capable of connecting to the internet to collect, transmit, and process data using integrated sensors, processors, and communication technologies. These devices, often referred to as smart or connected devices, leverage Machine-to-Machine (M2M) communication to interact seamlessly with other connected devices, enhancing their functionality. While humans can interact with these devices to provide commands or retrieve data, they operate autonomously, performing most tasks independently. The proliferation of such devices is largely due to the abundance of small, advanced components found in modern smartphones and the constant connectivity of home and workplace networks to the internet [1]. The application of IoT involves many fields like agriculture [2], healthcare [3], transportation [4], Smart House, etc.

***Author for Correspondence**
Ali H. Wheeb
E-mail: ali.h.wheeb@gmail.com

[1]Associate Professor, Department of Computer Engineering, College of Engineering, University of Baghdad, Iraq
[2]Assistant Professor, Department of Computer Science and Engineering, Assam Downtown University, Guwahati, Assam, India

Received Date: December 14, 2024
Accepted Date: December 20, 2024
Published Date: December 30, 2024

Citation: Ali H. Wheeb, Munsifa Firdaus Khan. A Survey of Several Machine Learning (ML) Algorithms for Security Solution in Internet of Things (IoT) Networks. Journal of Artificial Intelligence Research & Advances. 2025; 12(1): 1–11p.

Figure 1 illustrates the many layers of the Internet of Things, including the sensing, network, data processing, and application layers [5]. The sensing layer is responsible for the collection of data from different sources. This layer primarily consists of actuators and sensors. Sensors are responsible for measuring physical parameters like humidity, temperature etc. and convert them to electrical signals. These are placed at the input port of the system. Actuators use these electrical signals for creating force, motion, sound etc. Both sensors and actuators work simultaneously to complete a task. The network layer manages data transfer across different networks. It assembles the data into packets and ensures their transmission. The data processing layer collects and analyses the data, using which a meaningful insight and decisions can be made. This layer is a sensitive layer as the cyber attackers use this layer to perform cyber-attacks like Man in the Middle attack (MITM) [6], Denial of Service (DOS) [7], and distributed denial of service (DDOS) [8]. The hardware of an IoT device includes components like the microcontroller, firmware, sensors, control unit, and actuators. The network layer involves device APIs and interfaces for network communication, middleware to build the communication stack, and software that handles messages, information, and commands, which are then relayed to the actuators [1]. The data is prepared for additional analysis by the data processing layer. At the top is the application layer, which interacts directly with the user. It gives consumers the ability to manage Internet of Things devices.

Due to their complexity, heterogeneity, and resource limitations, IoT devices are susceptible to a range of security vulnerabilities and attacks. Given how frequently IoT devices are being used, this is a major cause for worry. With the huge growth, cities, healthcare, transportation and other sectors will become smarter. There are more chances of expansion of IoT networks with the introduction of 5G [9] But as there are negative aspects of everything, it can open door to new types of cyber threats. So, the main concern is about security and privacy of IoT devices. The IoT devices lack strong security measures as they have limited capabilities. They do not have robust design which is able to protect IoT devices from cyber-attack. Manufacturers of smart devices are paying very less attention to this aspect as it can increase their cost and there will be an additional overhead. So, the chances of intrusion into IoT devices are very high and it can cause a huge loss of important information. These devices can collect personal and sensitive information from users. This data can be intercepted by unknown hackers without the knowledge of the users and can be misused. An IoT device can serve as a gateway to gain access to a network. Due to their lack of advanced security features, the growing number of IoT devices may give rise to new kinds of cyberattacks. Therefore, it is necessary to implement security methods that can both safeguard IoT devices and boost public confidence in them.

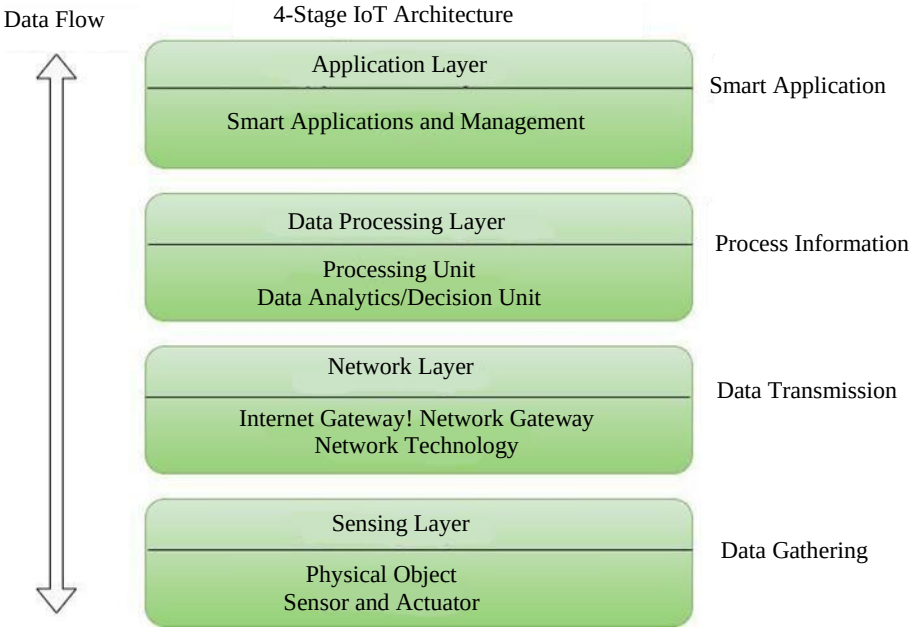

Figure 1. IoT Architecture.

For Internet of Things networks, an intrusion detection system may be put in place that will keep an eye on incoming traffic and effectively identify cyberattacks. The development of intrusion detection systems heavily relies on ML. The three main types of machine learning algorithms are supervised learning, unsupervised learning, and reinforcement learning. The algorithms of ML can detect the patterns of network traffic and can help to detect the attacks. Different types of training models can be formed using different available databases which include information regarding network data. These models can be applied to test the incoming traffic to detect any type of intrusion introduced in the network. These algorithms are used in systems designed to detect intrusions. The following categories apply to the algorithms used to identify cyberattacks [10].

Statistics Based Algorithms

These types of algorithms build statistical model of intrusion patterns. They overcame the limitations of rule based systems and were able to handle noisy data but they are unable to handle large quantities of data.

Rule Based Algorithms

These types of algorithms use prior explicit knowledge of attacks such as corresponding data distribution to create rule based systems and to perform detection. These algorithms are unable to handle noisy and incomplete data and it is very difficult to update them.

Machine Learning Algorithms

These types of algorithms form training models of different types of attacks and use them to detect different types of anomalies in the network. Machine learning algorithms can be categorized as supervised, unsupervised, or reinforcement-based. They are capable of processing vast amounts of data, including noisy datasets, and can improve their performance through experience. They can detect complex intrusions into the network by forming different complex models which are able to detect new types of cyber-attacks.

Scalability problems and the enormous volumes of data produced by an excess of IoT network are beyond the capabilities of traditional intrusion detection systems [11]. Although little work is being done on this front, the growing usage of IoT devices is raising worries about cyber security, which requires quick attention. These electronic devices lack privacy and security features. The rest of the paper is structured as follows: Literature review is explained; Different types of Intrusion Detection System (IDS) and available ML techniques for intrusion detection are explained; IoT security systems issues are explained; Issues and challenges of the current IDS solutions in IoT system are explained; and finally the Conclusion and future works is presented.

LITERATURE REVIEW

Numerous researchers have been working in this area to develop a strong intrusion detection system, commonly referred to as a cyber-attack detection technology. A review of previous studies conducted in this area has been provided in this section. Several ML Algorithms are used to identify network abnormalities.

Maghrabi emphasized on the need of Security solutions requirement for IOT environment [12]. They have tackled the challenges related to performance and class imbalance, which previously hindered accurate intrusion detection. They have proposed an automated network IDS system which used random forest algorithm on UNSW15 NB dataset and achieved accuracy of 90.17%. Data is collected from UNSW-NB 15 dataset. Four steps are performed: Pre-processing to check for missing values, exclusion of redundant packets, and samples of different classes are gathered. Symbolic data is encoded into numeric values. Then data balancing is performed in which training data is resampled by oversampling the minority classes and under sampling the majority classes. Feature selection is done by using three methods: filter method, as it leveraged due to its superior speed. The dataset is divided into training and

testing sets, with the Random Forest model used for training. Feature selection is performed based on Pearson's correlation coefficient. The features with significant correlation of 0.98 are retained while other are excluded. It improves accuracy by 3%. The training data consists of 80% of data and testing data consists of 20% of data. RF has high tolerance for outliers and noise. It is less prone to over fitting. The proposed method has achieved accuracy of 90.17% for unbalanced dataset and 98.77% for balanced dataset which surpasses SOTA (state of the art) approach by 7.34 and .53% respectively. RF improves multiclass classification evaluation metric both for balanced and unbalanced datasets. RF is compared with other algorithms and it is concluded that RF outperforms other algorithms. Introduction of filter reduces the training time. So, combination of RF and Pearson's coefficient of correlation gives more efficient training process and gives robust performance. This work is for only six types of traffic: Exploits, Fizzers, Generic, Normal, Reconnaissance, and DoS. So, this work can be extended for other types of traffic. A real time RF model can be prepared to detect intrusions in IOT networks.

Soundariya *et al*. addressed the problem of noise and irrelevant features into traditional datasets [13]. They proposed a new optimized feature selection method for accurate cyber-attack detection. This approach focuses on identifying the most influential features related to the target variables in order to enhance feature selection and reduction. The CICIDS-2017 data set is used and this method achieves 51% reduction in irrelevant features, increase in detection accuracy to 99.9%, and 50% reduction in model computation time. Data is collected from CICIDS-2017 dataset. Four steps are performed: Data pre-processing, feature selection, model training and optimization, performance evaluation. In pre-processing, redundant values are removed and missing values are filled by using binning method to obtain 70 features. All values such as null, NaN, and infinity are substituted with NaN. To minimize errors, the min-max normalization method is applied. Only features with unique values are selected for normalization. Integer and float values are unchanged and categorical values are encoded. Irrelevant features are reduced using chi-square test. It determines independence of two events by calculating chi-square correlation. A modified chi-rev method is used for feature selection. The comparison is done for binary, multi class and all attack classification. The authors introduced the Chi-Rev technique for feature reduction. It is tuned with various algorithms but it outperforms with random forest classifier. It reached an accuracy of 99.90%, along with nearly 51% fewer features and a 50% decrease in training time when compared to leading methods.

Zhao *et al*. have used a lightweight deep neural network with principal component analysis (PCA), expansion and compression structure, inverse residual structure and channel shuffle operation [14]. This model outperforms with low complexity, small model size and suitable for IOT traffic. Two datasets were used: First is UNSW NB15 dataset, which is used as it overcomes the shortcomings of KDD99 dataset. Raw network packets created by IXIA perfect storm tool for creating hybrid of real mode normal activities and synthetic contemporary attacks. Second is Bot-IoT dataset which is the latest NID data set for IOT which has normal IOT traffic and four attack scenarios: Dos, DDoS, Reconnaissance, and theft. Data pre-processing is performed. PCA algorithm is employed for transforming original high dimensional traffic features into new low dimensional features through linear transformation. The features of training and testing dataset are reduced using PCA algorithms and a new k-dimensional feature space is formed. For binary classification detection, binary cross entropy is used as loss function otherwise use NID loss function.

Bagaa *et al*. have stated that the security issues are increasing with the expansion of IoT in worldwide [15]. Their study presents the model for enhancing security of IoT system using machine learning. A cyber-attack detection solution is developed for IoT devices using ML.

The research employed seven machine learning algorithms to determine the most accurate classifier capable of detecting attack activities and patterns in networks associated with the Internet of Things (IoT). Proposed approach achieved 99.9% accuracy, 99.8% detection rate, 99.9% FI score and AUC

score of 1. So, it achieved overall high execution speed and accuracy. Two datasets were used: First is UNSW NB15 dataset as it overcomes the shortcomings of KDD99 dataset. Raw network packets created by IXIA perfect storm tool for creating hybrid of real modes normal activities and synthetic contemporary attacks. Seven machine learning algorithms were tested on the datasets, and the results showed that the Random Forest (RF), Boosting, AdaBoost, and Ensemble RF-BPNN classifiers performed the best. These models achieved an accuracy of 99.9%, an AUC of 1, and an F1 score of 99.9%.

Ghasemi and Babaie stated that an Intrusion Detection System plays an important role in security and prevents unauthorized users to access network resources by analyzing network patterns [16]. They present a hybrid intrusion detection system that combines Support Vector Machine with Grey Wolf Optimization (GWO) algorithms. Support Vector Machine (SVM) is used to train and differentiate anomaly records from normal records and GWO is used to find kernel function, feature selection and to adjust optimal parameters for SVM to improve the classification. The datasets utilized were the NSL-KDD and TON_IoT datasets. The proposed IDS has been validated through python language on two datasets: NSL-KDD and TON_IoT. The proposed approach excels in detection accuracy, precision, recall, and F-score. It is dataset-independent and demonstrates satisfactory performance on both datasets. The false positive rate of the proposed approach is 0.12 and 1.27 on NSL-KDD and TON_IoT datasets respectively.

Vijayakumar *et al.* emphasized the need to develop strong cyber-attack detection system for internet of healthcare things as IOHT devices are vulnerable to cyber-attacks due to lack of security procedure implementation in these devices [17]. They presented an AI based cyber-attack detection system using deep neural network. The dataset used is ECU-IOHT. The proposed system achieved an accuracy of 99.85%. False positive rate is 0.01. This method has achieved higher detection rate as compared to existing methods. The ECU-IOHT dataset is a newly developed resource that represents various cyber-attacks such as ARP spoofing, DOS attacks, Nmap port scanning, and Smurf attacks. It consists of two phases: the data preparation phase and the DNN-based attack detection phase. Five features are extracted from the dataset, and categorical features are encoded using one-hot encoding. The dataset is labeled into categories: normal, ARP spoofing, DOS, Nmap, and Smurf attacks. It is divided into training and testing sets (80% for training and 20% for testing). The DNN model is trained on the training data using multiclass classification. The trained model is tested using test dataset for predicting the attacks. Five features have been chosen from a set of eleven, including type, source packets, destination packets, protocol type, and length. The extracted features are numerical and categorical. Categorical features are converted into numerical one using one hot encoding algorithm. The proposed model consists of an input layer with five neurons, followed by two dense layers, each containing eight neurons and using the ReLU activation function. The output layer utilizes a softmax activation for classification. The model's performance is assessed through accuracy, precision, recall, F1 score, true positive rate, and false positive rate. Python, along with libraries such as matplotlib, NumPy, pandas, scikit-learn, Keras, and TensorFlow, is used for implementation. The system achieves average values of 99.3% for precision, 96.8% for recall, and 90.3% for the F1 score, demonstrating its superior performance compared to existing methods.

Table 1 shows the summary of the literature review in tabular form. It shows feature selection method, ML technique and the accuracy achieved.

VARIOUS IDS TYPES AND ML ALGORITHMS APPLIED

Numerous kinds of intrusion detection systems are available that employ ML algorithms to identify system invasions. Cyberattack detection is one of the key uses of ML. Cyberattack data may be fed into the ML algorithm to create a training model, which can then be used to identify both new and existing cyber threats. They provide real-time monitoring of network traffic. An overview of the various IDS kinds and ML algorithms is provided in this section.

Various ML Algorithms for intrusions Detection in IoT Networks

Decision Tree

This algorithm is represented through a recursive division of the instance space [18]. It takes the form of a distributed tree, with the root serving as the foundational node, lacking any incoming edges. Other nodes have exactly one incoming edge. The nodes that have outgoing edges are called internal nodes or test node. The rest of the nodes are called leaves. Root node consists of the feature value on the basis of which branching is done. Decision nodes or internal nodes contain the different values of the root node feature on the basis of which branching is done. Each leaf is linked to a specific class, representing the final prediction. This method works well for both classification and regression tasks. The Decision Tree is shown in the Figure 2.

Random Forest (RF)

Random Forest (RF) algorithm forms decision trees by random node splitting and resampling. We can say that it is an ensemble of various trees. The final classification result is voted by multiple trees [19]. The voting technique or averaging technique is applied to reach to the final result. This algorithm provides more accurate results. It is widely used in solving complicated problems. Random Forest algorithm has high accuracy, very less over fitting, can handle large datasets, and can handle missing values. The RF is shown in Figure 3 [20].

Table 1. Summary of literature review.

Literature review	Method for Feature Selection	ML Algorithm Employed	Accuracy
Ref [12] (2024)	Principle Component Analysis (PCA)	Random Forest	90.17%
Ref [13] (2021)	Chi-Rev	Random Forest	99.9%
Ref [14] (2021)	Principle Component Analysis (PCA)	Deep Learning	86.11%
Ref [15] (2020)	Principle Component Analysis (PCA)	Ensemble RF with Neural Network	99.2%
Ref [16] (2024)	Grey Wolf Optimization	SVM	98%
Ref [17] (2023)	Only Five features Selected	Deep Neural Network	99.855%

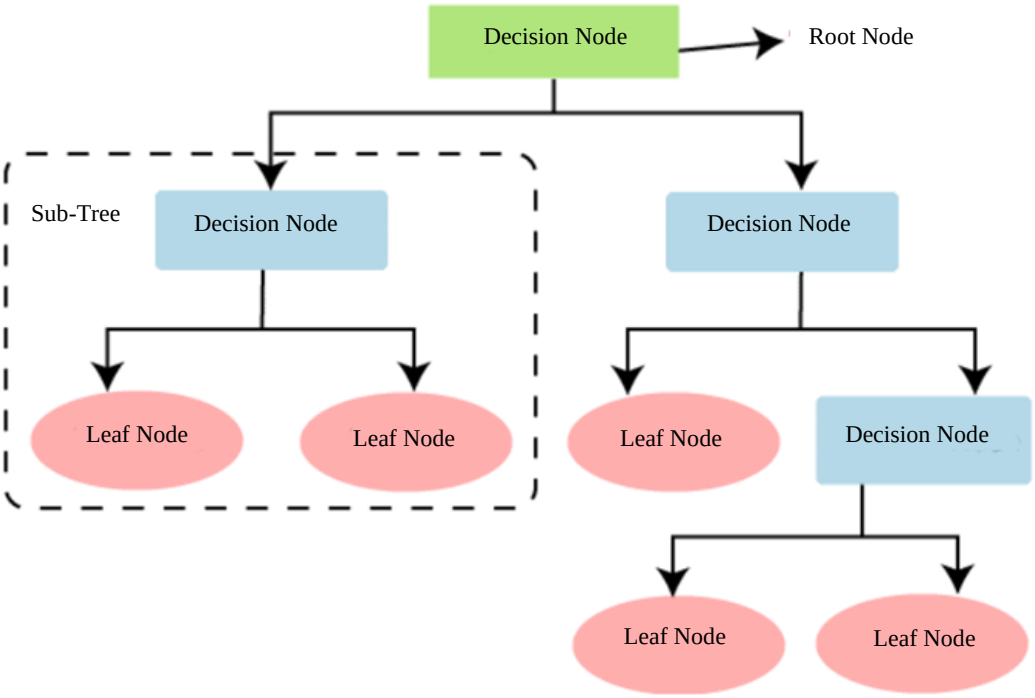

Figure 2. The decision tree algorithm.

Neural Network (NN)

It is a single layer perceptron where the weights are multiplied by a series of inputs before they reach the layer. Then, total is calculated by adding weighted input data together [21]. We can say that it is a network of interconnected nodes with number of layers and it functions like human brain and is able to reform itself from the feedback received. The neural network structure is shown in Figure 4.

Support Vector Machine (SVM)

Support Vector Machine (SVM) algorithm searches for optimal separating surface known as hyper-plane which is equidistant from the classes. This can be applied to both linear and nonlinear data [22]. It is supervised machine learning algorithm and it tries to find linearly separable data points. It is shown in Figure 5.

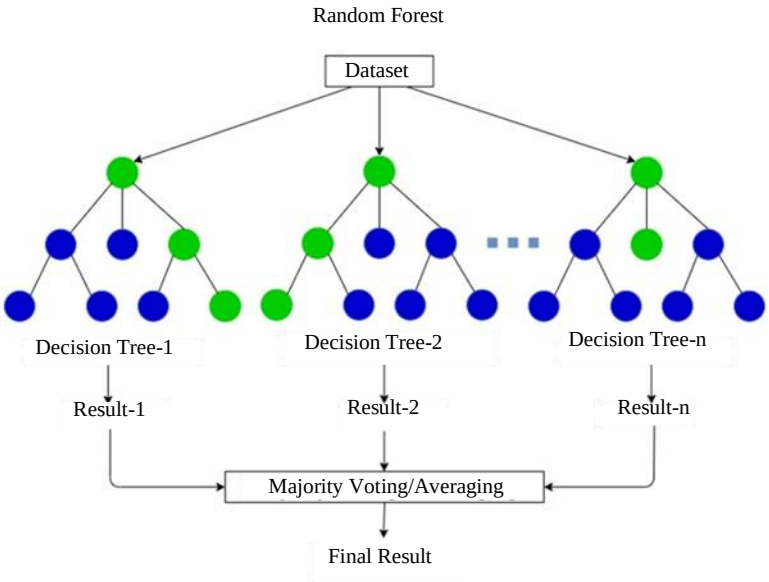

Figure 3. Random forest algorithm.

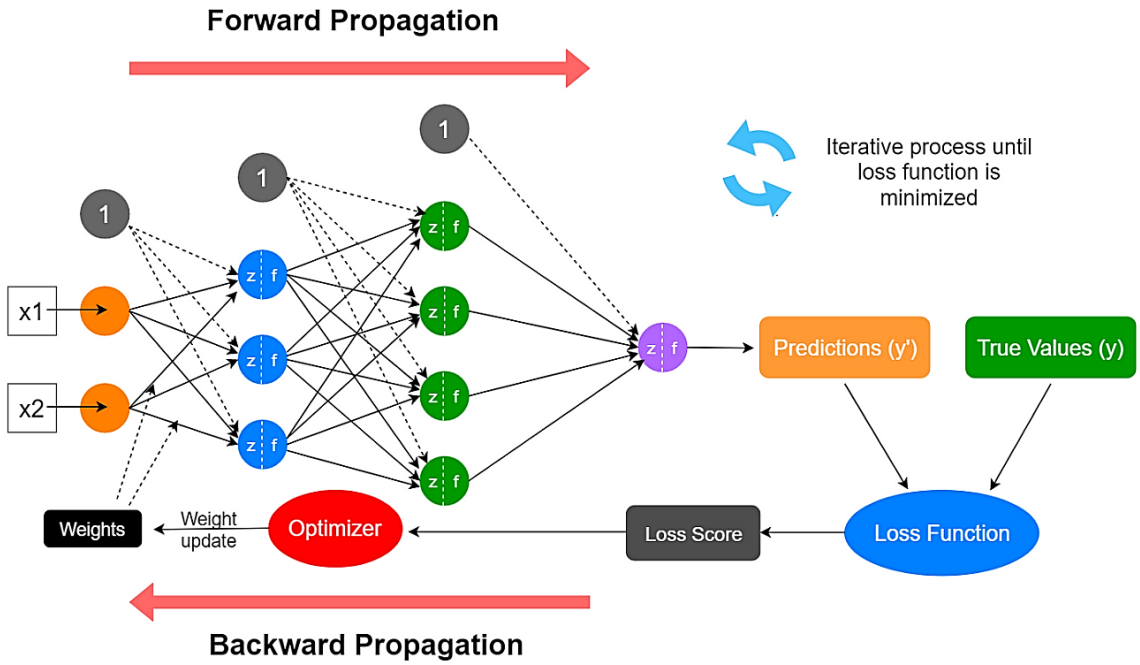

Figure 4. Neural Network (NN).

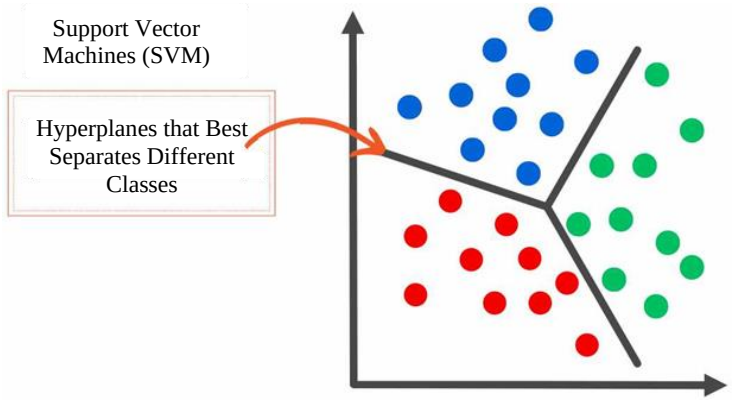

Figure 5. Support vector machine (SVM) algorithm.

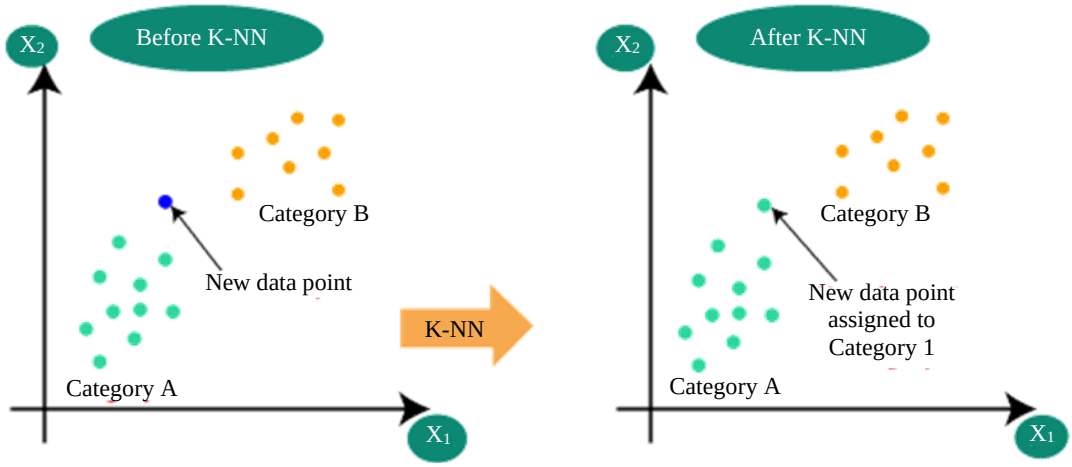

Figure 6. K-Nearest neighbor (KNN) algorithm.

K-Nearest Neighbor (KNN)

It is simple and widely used ML technique for classification and regression problems [23]. It is supervised and non-parametric learning classifier. It involves two types of learnings: Instance based and proximity based learnings. In instance based learning, it memorizes the training data and makes predictions based on its similarity to the stored instances. In proximity based prediction, it assumes that the similar data points (neighbors) exist in close proximity within the feature space. The algorithm involves the following steps: Choosing value of K, calculate distance, find K nearest neighbors and find vote or average. The voting technique is applied to classification problem and average technique is applied to regression problems. KNN method memorizes the whole dataset which makes training fast but prediction becomes slower as the size of data grows. It can handle multi class classification tasks. Figure 6 explains the K-Nearest Neighbor algorithm.

Naïve Bayes

This algorithm is based on Bayes theorem [24]. It is a probabilistic machine learning algorithm. It is a good method for high-dimensional data. Bayes' theorem is applied here with the simplifying assumption that the features are independent of one another. This assumption is not possible for all the cases but it still works well for some sort of problems. P (C|X)=(P (X|C)-P(C))/P(X). Figure 7 shows the Naïve Bayes classifier.

Various IDS Types in IoT Networks

Protocol Based IDS

This type of IDS analyses the different protocols of the system. Here the servers consist of various types of agents on the servers which scrutinize different protocols. This IDS is installed on front end of the server and monitors the HTTP stream [19].

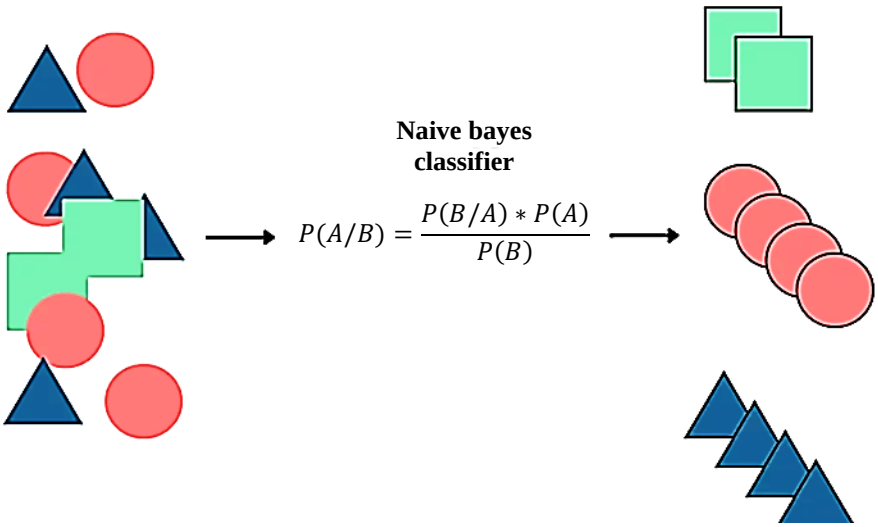

Figure 7. Naïve Bayes classifier.

Host Based IDS

This type of IDS system is installed on every host and it monitors each and every incoming and outgoing network traffic in the host. If any anomaly is detected then an alert is raised. It can detect configuration changes, file modification, system logs, and incorrect client server requests. It follows the rule of string or pattern matching for detection of a threat [25].

Network Based IDS

Network Based IDS (NIDSs) are a crucial tool for identifying and thwarting network-based cyberattacks. They are strategically placed at critical points across the Internet of Things network to track traffic. Intrusion detection systems and signature-based systems are the two primary categories of NIDS. To identify assaults, a signature-based NIDS uses a pre-installed collection of attack signatures that are compared and pattern-matched with the network traffic under observation. Because of this, this kind of NIDS is significantly less successful at identifying new attacks or variations of pre-existing ones, but it may detect known assaults with a comparatively low false alarm rate. On the other hand, intrusion detection-based systems can identify intrusions by identifying changes to the network's typical traffic patterns [26].

IOT NETWORKS' SECURITY ISSUES

IoT usage is growing and improving people's quality of life. It encompasses nearly every industry. However, one of the main issues with this technology is security. It is a significant problem as it may be the primary cause of IoT technology's eventual demise. Safeguarding the linked devices requires rapid attention. As IoT networks have grown and proliferated, the complexity of IoT systems has also increased [27]. There exists issues of scalability and heterogeneity. Apart from this, IoT devices are lacking implementation of sound security standards into the devices due to the limitation of the technology, limited power and high cost of implementing it. The present security measures cannot fit into this new technology. Some of the challenges available with IoT devices are listed below [28]:

1. IoT devices have outdated firmware.
2. Use of weak and default credentials to log in.
3. Lack of encryption.
4. Malware and Ransom ware can affect IoT systems easily.

ISSUES AND CHALLENGES OF THE CURRENT IDS SOLUTIONS ON IOT NETWORKS

The following are shortcomings of the current intrusion detection systems:

1. Various ML algorithms are used in the creation of an IDS system. Traditional, outdated datasets are used in the implementation of several IDSs. To increase efficiency, the authors used the

UNSW-NB-15 dataset, which is relatively old. Therefore, the outdated IDS system is ineffective in identifying novel forms of cyberattacks [12].

2. The Bot-IoT dataset, with training dataset number 364562 and testing dataset number 243043, is also utilized. Increasing the amount of training and testing records will change the outcome and impact efficiency. The implemented methods will result in an ideal IDS and may be used to new datasets with more entries. More training records should be kept, and they should be updated with information on recent cyberattacks.
3. In an IoT establishing, these devices are unable to identify novel cyberattacks. All kinds of novel cyberthreats should be covered in the dataset used to generate the training set. In the current cyber environment, one of the main reasons why intrusion detection systems fail is the extremely old data included in the typical datasets that are now accessible. Since the IoT network has grown complex and the current IDS datasets do not take this into account, the authors' use of the CICIDS2017 and NSL-KDD datasets is not appropriate for identifying novel forms of cyberthreats in the IoT. Accurate datasets that can handle novel threats are required [13, 14].

CONCLUSION AND FUTURE WORKS

The rise in IoT networks usage is largely to blame for the rise in cyberattacks. These assaults must be recognized and prevented. IDS is the answer to this issue. The weaknesses of current IDs must be fixed, and existing IDs should be updated to be able to handle new kinds of attacks in new technologies, in order to identify new and complex cyberattacks. In this study, first of all the overview of the IoT technology is presented. Then related work is presented in the form of literature review. Then the limitations are addressed followed by the solution to cyber security risks. Then challenges and issues of the available IDS are explored. It is concluded that there is a need to develop new intrusion detection systems which are able to detect new types of cyber-attacks for IoT network. The datasets taken for forming different models should be upgraded to address the new types of threats. The existing ML algorithms can be applied to new datasets of IoT along with improved feature selection and classification techniques. Moreover, feature selection methods should be chosen carefully after analyzing the problem. Feature selection is very much helpful in reducing dimensions, improve the speed and increase the comprehensibility of the result. The most commonly used techniques of feature selection are filter method, wrapper method and hybrid methods. Hybrid methods of feature selection can be proven as the best methods by complementing limitations of both the methods. Future research will focus on developing secure and efficient IoT authentication methods in an effort to improve the security of the IoT networks. Further, combining several ML algorithms can also result in outcomes with greater and flawless accuracy.

REFERENCES

1. Hossain MS, Muhammad G. Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. Comput Netw. 2016 Jun 4; 101: 192–202.
2. Farooq MS, Sohail OO, Abid A, Rasheed S. A survey on the role of iot in agriculture for the implementation of smart livestock environment. IEEE Access. 2022 Jan 13; 10: 9483–505.
3. Rejeb A, Rejeb K, Treiblmaier H, Appolloni A, Alghamdi S, Alhasawi Y, Iranmanesh M. The Internet of Things (IoT) in healthcare: Taking stock and moving forward. Internet Things. 2023 Jul 1; 22: 100721.
4. Wu Y, Dai HN, Wang H, Xiong Z, Guo S. A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory. IEEE Commun Surv Tutor. 2022 Mar 10; 24(2): 1175–211.
5. Burhan M, Rehman RA, Khan B, Kim BS. IoT elements, layered architectures and security issues: A comprehensive survey. Sensors. 2018 Aug 24; 18(9): 2796.
6. Cekerevac Z, Dvorak Z, Prigoda L, Cekerevac P. Internet of things and the man-in-the-middle attacks–security and economic risks. MEST J. 2017 Jul; 5(2): 15–25.
7. Ali MH, Jaber MM, Abd SK, Rehman A, Awan MJ, Damaševičius R, Bahaj SA. Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). Electronics. 2022 Feb 8; 11(3): 494.

8. Salim MM, Rathore S, Park JH. Distributed denial of service attacks and its defenses in IoT: a survey. J Supercomput. 2020 Jul; 76: 5320–63.
9. Li S, Da Xu L, Zhao S. 5G Internet of Things: A survey. J Ind Inf Integration. 2018 Jun 1; 10: 1–9.
10. Lansky J, Ali S, Mohammadi M, Majeed MK, Karim SH, Rashidi S, Hosseinzadeh M, Rahmani AM. Deep learning-based intrusion detection systems: a systematic review. IEEE Access. 2021 Jul 14; 9: 101574–99.
11. Benkhelifa E, Welsh T, Hamouda W. A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. IEEE Commun Surv Tutor. 2018 Jun 7; 20(4): 3496–509.
12. Maghrabi LA. Automated Network Intrusion Detection for Internet of Things Security Enhancements. IEEE Access. 2024 Feb 23; 12: 30839–30851.
13. Soundariya RS, *et al*. Effective Feature Selection for Hybrid Wireless IoT Network Intrusion Detection Systems Using Machine Learning Techniques. Ad hoc Sens Wirel Netw. 2021 May 1; 49: 175–206.
14. Zhao R, Gui G, Xue Z, Yin J, Ohtsuki T, Adebisi B, Gacanin H. A novel intrusion detection method based on lightweight neural network for internet of things. IEEE Internet Things J. 2021 Oct 11; 9(12): 9960–72.
15. Bagaa M, Taleb T, Bernabe JB, Skarmeta A. A machine learning security framework for iot systems. IEEE Access. 2020 May 21; 8: 114066–77.
16. Ghasemi H, Babaie S. A new intrusion detection system based on SVM–GWO algorithms for Internet of Things. Wireless Netw. 2024 Feb 1; 30: 2173–2185.
17. Vijayakumar KP, Pradeep K, Balasundaram A, Prusty MR. Enhanced cyber attack detection process for internet of health things (IoHT) devices using deep neural network. Processes. 2023 Apr 3; 11(4): 1072.
18. Ferrag MA, Maglaras L, Ahmim A, Derdour M, Janicke H. Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. Future Internet. 2020 Mar 2; 12(3): 44.
19. Zeeshan M, Riaz Q, Bilal MA, Shahzad MK, Jabeen H, Haider SA, Rahim A. Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets. IEEE Access. 2021 Dec 21; 10: 2269–83.
20. Pramilarani K, Kumari PV. Cost based Random Forest Classifier for Intrusion Detection System in Internet of Things. Appl Soft Comput. 2024 Jan 1; 151: 111125.
21. Almiani M, AbuGhazleh A, Al-Rahayfeh A, Atiewi S, Razaque A. Deep recurrent neural network for IoT intrusion detection system. Simul Model Pract Theory. 2020 May 1; 101: 102031.
22. Akhther P, Maryposonia A, Prasanth VS. Least Square Support Vector Machine based Intrusion Detection System in IoT. In 2023 IEEE 7th International Conference on Intelligent Computing and Control Systems (ICICCS). 2023 May 17; 1545–1550.
23. Mohy-Eddine M, Guezzaz A, Benkirane S, Azrour M. An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. *Multimed Tools Appl.* 2023; 82(15): 23615–23633.
24. Hnamte V, Balram G. Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. J Algebraic Statistics. 2022 Jun 4; 13(2): 2749–57.
25. Martins I, Resende JS, Sousa PR, Silva S, Antunes L, Gama J. Host-based IDS: A review and open issues of an anomaly detection system in IoT. Future Gener Comput Syst. 2022 Aug 1; 133: 95–113.
26. Lo WW, Layeghy S, Sarhan M, Gallagher M, Portmann M. E-graphsage: A graph neural network based intrusion detection system for IOT. In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. 2022 Apr 25; 1–9.
27. Azrour M, Mabrouki J, Guezzaz A, Kanwal A. Internet of things security: challenges and key issues. Secur Commun Netw. 2021; 2021(1): 5533843.
28. Gupta BB, Quamara M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurr Comput: Pract Exp. 2020 Nov 10; 32(21): e4946.

