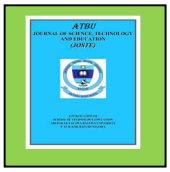
JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(2), JUNE, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net



Intelligent Attack Detection and Network Intrusion based on Cyber Attack Invasion in Data Security: Review and Open Issues from Machine Learning Perspective

Sunday Ochigbo, Souley Boukary, Sani Abba
Department of Mathematical Sciences,
Abubakar Tafawa Balewa University Bauchi, Nigeria

ABSTRACT

Network security is closely related to computers, networks, programs, various data, and so forth, where the purpose of defense is to prevent unauthorized access and modification. However, the growing number of internet-connected systems in finance, E-commerce, and military makes them become targets of network attacks, resulting in large quantity of risk and damage. Essentially, it is necessary to provide effective strategies to detect and defend attacks and maintain network security. Furthermore, different kinds of attacks are usually required to be processed in different ways. How to identify different kinds of network attacks thus becomes the main challenge in domain of network security to be solved, especially those attacks never seen before. To overcome this problem, a lot of efforts have been devoted to modeling the attack or anomaly by using machine learning techniques. Machine learning is successfully used in many areas of computer science such as image processing and intrusion detection. Hence, this research survey intelligent attack detection and network intrusion based on multi-channel invasion in data security. The research surveys the existing literature covering their contributions and limitations respectively. Base on the review, we identified the research opportunities that can be utilized by researches to enhance security in information with high integrity.

ARTICLE INFO
Article History
Received: March, 2023
Received in revised form: April, 2023
Accepted: May, 2023
Published online: June, 2023

KEYWORDS
Autoencoder, Deep Learning, Distributed Denial of Service, K-Means, Machine Learning, Network Intrusion Traffic, Support Vector Machine and Random Forest

INTRODUCTION

Recent years, network attack detection attracts increasing interest in social networking information security as the increasing security threats including cross-site scripting, clickjacking, DDOS, probe and identity theft. The aim of network attack detection is to distinguish the hostile activities from the network traffic. To synchronize with new or variant attacks, the detection must be accomplished in a smart and effective way. Traditional attack detection methods attempt to model all kind of attacks or anomalies, which detect the attacks based on the known knowledge. However, new types of attack have already made great damages before they are detected. As new attacks appear over time, modeling all kinds of attacks and detect the attacks accurately before the large-scale damage are difficult to achieve(Jiang et al., 2018).

As computer networks and information systems become more critical and complex, researchers are looking for new techniques to protect these assets(Servin & Kudenko, 2005). the continuous development and extensive usage of Internet benefit numerous network users from a quantity of aspects. Meanwhile, network security becomes much more important with wide usage of network. Network security is closely related to computers, networks, programs, various data, and so forth, where the purpose of defense is to prevent unauthorized access and modification(Wu, Wei, & Feng, 2020). However, the growing number of internet-connected systems in finance, E-commerce, and military

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

makes them become targets of network attacks, resulting in large quantity of risk and damage. Essentially, it is necessary to provide effective strategies to detect and defend attacks and maintain network security. Furthermore, different kinds of attacks are usually required to be processed in different ways. How to identify different kinds of network attacks thus becomes the main challenge in domain of network security to be solved, especially those attacks never seen before(Wu et al., 2020).

Network security is one of the most important security issues facing cloud computing, with frequent cyber-attacks and cyber intrusions, such as a DDoS attack by a botnet controlled by the malware Mirai in October 2016 which caused widespread outages on the East Coast of the United States. The ransomware software WannaCry, which broke out in May 2017, exploited system vulnerabilities to poison the computers of hundreds of thousands of users in several countries around the world. In China, the annual losses caused by digital crimes such as pseudo-base-stations and malware extortion amount to tens of billions of yuan. the above examples show that network security not only affects the development of national economy but also affects social stability and national security(Liu & Zhang, 2020).

The Internet of Things (IoT) is one of today's most rapidly growing technologies. It is a technology that allows billions of smart devices or objects known as "Things" to collect different types of data about themselves and their surroundings using various sensors. They may then share it with the authorized parties for various purposes, including controlling and monitoring industrial services or increasing business services or functions. However, the Internet of Things currently faces more security threats than ever before(Haji & Ameen, 2021).

To overcome this problem, a lot of efforts have been devoted to modeling the attack or anomaly by using machine learning techniques. Machine learning is successfully used in many areas of computer science such as image processing and intrusion detection(Jiang et al., 2018), for example,(Doshi, Apthorpe, & Feamster, 2018) applied machine learning DDoS Detection for consumer internet of things devices, (Nivaashini & Thangaraj, 2018) proposed Intrusion Detection System (IDS) using hybrid machine learning technique by combining K-means clustering and Support Vector Machine (SVM) classification. They reduced features according to the influence toward classification of attacks, but the performance was similar to the result which used the original features.(Alsamiri & Alsubhi, 2019) evaluate various machine learning algorithms that can be used to quickly and effectively detect IoT network attacks using a new dataset (Bot-IoT). Although these methods have attracted a lot of interest, the detection accuracy rate is not high as desired.

We have seen from the literature that machine learning is one of the popular fields of artificial intelligence that is successfully used in solving various computational problems of different areas. Now a days it is extended to more deep networks such as deep learning, extreme learning, deep extreme learning networks etc(Dixit, Kohli, Acevedo-Duque, Gonzalez-Diaz, & Jhaveri, 2021). It is believed that some characteristics in most of the novel attacks can be derived from the known attacks. The relationships are difficult to describe and represent. Deep learning is suitable to model complex non-linear relationships by learning multiple levels of data representations that correspond to different levels of abstraction. A deep neural network consists of a cascade of many layers of non-linear processing units for feature extraction and transformation, which is a promising method for detecting attacks in social networks(Jiang et al., 2018).

Deep learning (DL) approaches are an excellent solution to stable IoT programs. DL is an innovative tool for artificial intelligence, which cannot be complicated and can surpass complex networks. A wide range of attacks and a safety plan is developed using the DL methods to train a machine. Furthermore, deep learning developments appear promising in detecting and intelligent handling of new threats via learning skills. Future IoT device security protocols would also make DL algorithms more reliable and accessible than before (Haji & Ameen, 2021).
Hence, this research survey intelligent attack detection and network intrusion based on multi-

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

channel invasion in data security. The remainder of this article has the following structure: Section 2 provides an overview of different types of network intrusion attacks and its impact on data security; Section 3 related work including various types of learning algorithms and IoT security solutions; Section 4 an overview and discussion of the reviewed papers and provides research gaps and future trend in the context of data security attacks and intrusion detections;

Advantage and Motivation

As new attacks appear over time, modeling all kinds of attacks and detect the attacks accurately before the large-scale damage is very crucial in many aspects. These includes:

1. the growing number of internet-connected systems in finance, E-commerce, and military makes them become targets of network attacks, resulting in large quantity of risk and damage. Essentially, it is necessary to provide effective strategies to detect and defend attacks and maintain network security.
2. Network security is closely related to computers, networks, programs, various data, and so forth, where the purpose of defense is to prevent unauthorized access and modification.
3. The traditional methods were time-consuming, less efficient, and giving average performance and cannot fit for providing the solution for complex, multi objective, or real-world problems. Hence, the necessity for efficient attack detection systems can reduce the harmful effects of cyber threats. This can support the users, and different applications by ensuring efficient computation and maintaining the quality of service over the network.

LITERATURE REVIEW

Overview of Network Intrusion Attacks and Its Impact on Data Security

IoT system has seen various attacks over the past few years, making manufacturers and consumers more aware of IoT products This section outlines multiple types of attacks, effects, and IoT surfaces. The Attacks in IoT are divided into two types: cyber and physical. Cyberattacks include both passive and active attacks(Haji & Ameen, 2021), as shown in Fig. 1 A cyber-attack threat targets multiple IoT device by hacking and operations in a wireless network (stealing, erasing, changing, or destroying) the user's data. Physical assaults, on the other hand, cause physical harm to IoT devices Here, no network is required to attack the device. Such attacks are also subject to physical IoT devices, such as mobile devices, cameras, sensors, routers, etc. however, in this study, we focus more on the cyber-attacks including both active and passive.

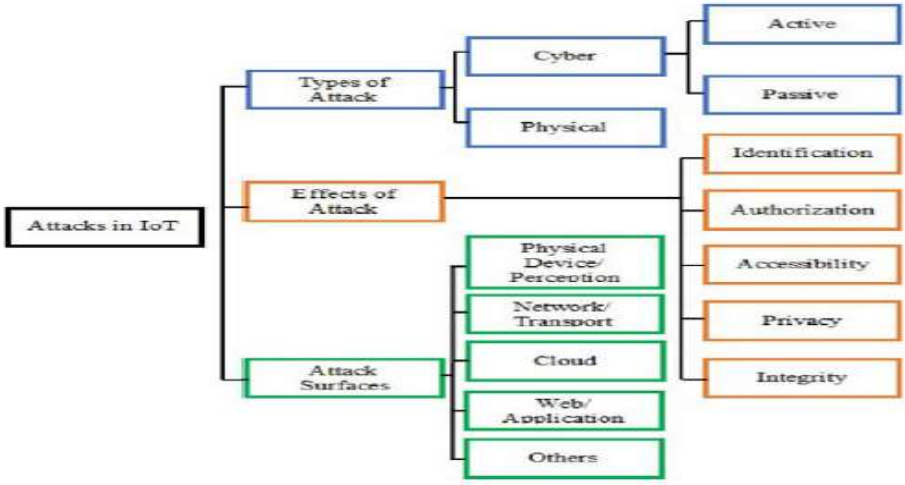


Fig. 1 complete list of IoT attacks, including various attacks, attack surfaces and attack effects (Haji & Ameen, 2021)

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(2), JUNE, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

Active IoT Attacks

An active attack happens when a network attacker accesses the interface settings and disconnects certain services of IoT devices may be attacked in various ways, including interruption, interventions, and changes in active attacks. Fig. 2 describes active attacks, e.g., DoS, middle-hand attacks, Sybil attacks, spoofing, hole attacks, jamming, selective Forwarding, malicious inputs, data tampering, etc.(Tahsien, Karimipour, & Spachos, 2020)

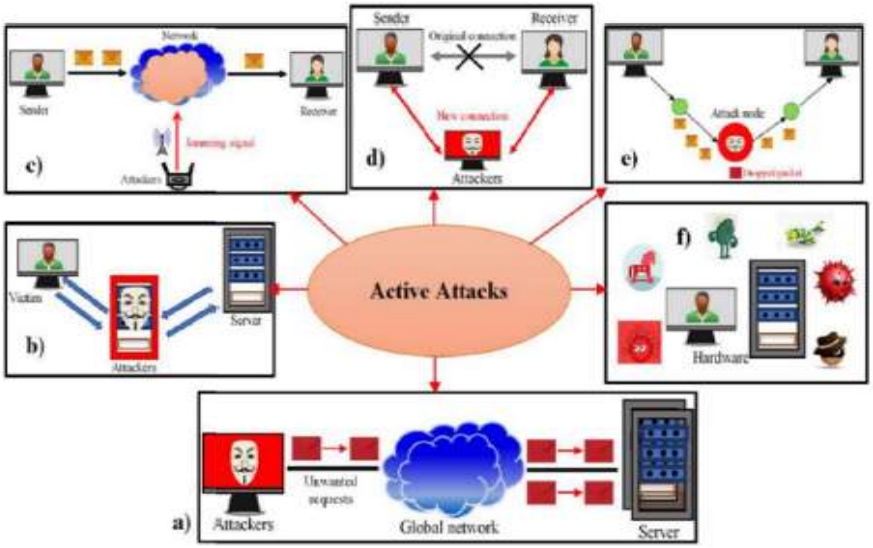


Fig. 2 different forms of cyber-attacks base on active attack (Haji & Ameen, 2021)

Denial of service (DoS) Attacks

DoS attacks are primarily responsible for disabling system services by generating many repetitive demands, as shown in Fig.2.2 As a result, the user cannot navigate and connect to the IoT device, making informed decision-making impossible. Furthermore, DoS attacks keep IoT devices turned on all the time, reducing battery life(Haji & Ameen, 2021). A distributed denial of service (DDoS) attack occurs as several attacks are initiated from different IP addresses to generate various requests to hold the server busy. This makes distinguishing between natural and malicious traffic impossible. In recent years, a specific IoT botnet virus known as Mirai has been responsible for initiating disruptive DDoS attacks, causing thousands of IoT computers to malfunction due to interferences.(Tahsien et al., 2020)

Data Tampering

Data tampering is a severe threat not just to corporations but also to people's lives and property. As a result, companies must take precautions to avoid such assaults and reduce whatever damage they may inflict as seen in Fig.2.2 (Haji & Ameen, 2021).

Spoofing and Sybil attacks

These types of attacks are mainly used to gain unauthorized access to IoT systems by targeting user identification (RFID and MAC address), as seen in Fig.2.2. The TCP/IP suite lacks a robust security protocol, making IoT devices more vulnerable, mainly spoofing attacks. Furthermore, these two attacks initiate additional extreme attacks, such as manin-the-middle attacks and denial-of-service (DoS)(Tahsien et al., 2020).

They were jamming attacks

Continuous communication in a wireless network through transmitting undesirable signals to IoT devices, causing problems for users by keeping the network constantly busy, as shown in Fig.2.2 Furthermore, this type of attack reduces

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(2), JUNE, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

the performance of IoT systems by using more memory, bandwidth, and so on (Tahsien et al., 2020).

Man-in-the-middle attacks

Man-in-the middle attacks are carried out by network members directly linked to another user interface, as shown in Fig. 2.2 As a result, it is simple to disrupt communications by adding bogus and incorrect data to hack original data (Abdulraheem et al., 2020).

Selective Forwarding attacks

The transmission attack functions as a node of the communication device, which can be dropped to create a networking hole, as seen in Fig.2.2 during transmission. It is hard to detect and stop this kind of attack (Tahsien et al., 2020).

Passive IoT Attacks

Passive attacks are designed to collect information about the user without their knowledge and decode their private, encrypted data. Eavesdropping and traffic monitoring are the two most popular techniques for conducting a passive attack on an IoT network(Haji & Ameen, 2021).

Eavesdropping

The attacker listens in on messages sent and received by two entities. The traffic must not be encrypted for the attack to be effective. The attacker can obtain any unencrypted information, such as a password supplied in response to an HTTP request.

Traffic analysis

The attacker examines the metadata transmitted in traffic to derive traffic information, e.g., exchanged traffic and the involved entities (rate, duration, etc.). If encrypted data is employed, traffic analyses can also lead to cryptanalysis assaults, leading to the attacker obtaining information or successful traffic unencrypted.

Impact of Cyber-Attack to Data Security

To protect users' privacy, authentication, and permission, the impact of IoT attacks is threatening for the network. Figure 3 provides a complete list of various forms of attacks, including their effects on IoT devices. When designing a security protocol for the IoT device's attacks, the following features must be considered.

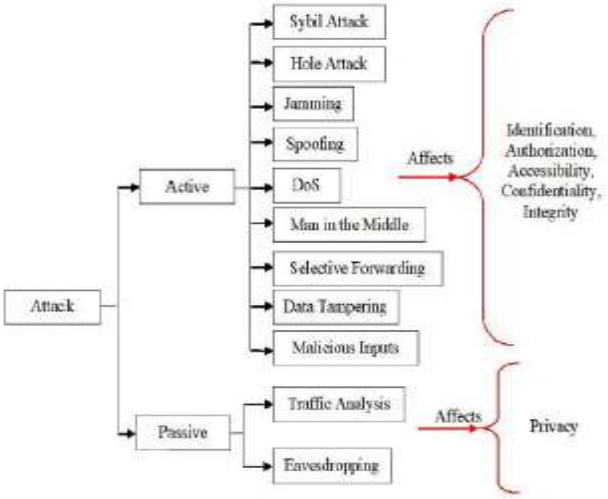


Fig. 3 Cyber-attacks and their corresponding impact on data security.

When designing a security protocol for the IoT device's attacks, the following impact of attack must be considered due to their immense impact to data security. These includes authentication, authorization, accessibility,

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

confidentiality, integrity and privacy(Haji & Ameen, 2021).

Overview of Intelligent Attack Detection Techniques Base on Artificial Learning Algorithms

These sections discussed the intelligent attack detection techniques base on artificial intelligence algorithms, specifically machine learning and deep learning algorithms.

Machine Learning Algorithms Attack Detection

Machine Learning can be described as an intelligent device's ability to modify or automate a knowledge-based state or behavior, which is considered a critical part of an IoT solution. ML has the ability to infer helpful knowledge from data generated by devices or humans, and ML algorithms are used in tasks such as regression, and classification. Likewise, in an IoT network, ML can be used to provide security services. The use of machine learning in attack detection problems is becoming a hotly pursued subject, and ML is being used more and more in different applications in the cybersecurity field. Although many studies in the literature have used ML techniques to discover the best ways to detect attacks, only limited research exists on efficient detection methods suitable for IoT environments(Alsamiri & Alsubhi, 2019). The following supervised machine learning algorithms were used to develop classifiers for botnet activity detection: decision tree, random forest and SVM

Decision Tree

A sequential decision process in which an input data point's attribute values are consecutively tested to determine the data point's classification. A decision tree is composed of a root node, internal nodes, and leaf nodes that contain the possible class labels. Within each internal node, the value of the attribute assigned to the node is tested to determine the next node to progress to along the tree's path. Once a leaf node is reached, its label will represent the input data point's identified classification (Hegde, Kepnang, Al Mazroei, Chavis, & Watkins, 2020).

Random Forest

The random forest classification algorithm is an ensemble learning method in which multiple decision trees are constructed, and the mode value of the classes predicted by the individual trees is used to classify the input data point. Each decision tree in the forest considers a random subset of features and only has access to a random subset of the training data, thereby increasing diversity and potentially resulting in more robust classification predictions compared to individual decision tree classifiers (Hegde et al., 2020).

K-Nearest Neighbour (KNN)

Simplest and most effective supervised learning algorithm. It is used for searching through the available dataset to associate new data points with similar existing points. KNN, which provides good performance over multidimensional data and is a fast algorithm during the training phase, is relatively slow in the estimation stage(Alsamiri & Alsubhi, 2019).

Naïve Bayes (NB)

The NB is a widely used supervised algorithm, and is famous for its simple principles. The Naïve Bayes method is based on the work of Thomas Bayes. For instance, NB might be utilized to categorize traffic as normal or anomalous for intrusion detection. The traffic classification features used are handled independently by the NB classifier despite the fact that these features may depend on each other. Many attributes make NB user-friendly, like its simplicity, low sample requirement, and ease of implementation. On the other hand, NB deals with features independently and is therefore unable to obtain valuable information from the communication and relationships between features(Alsamiri & Alsubhi, 2019).

Artificial Neural Network

Artificial neural networks (ANNs) are a machine learning method that takes inspiration from the way the human brain works, like learning and deriving new information (Alsamiri & Alsubhi, 2019). The two-class neural network classification algorithm is a set of interconnected layers of nodes that perform binary classification. In concept, a neural network consists of an input layer, any

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

number of hidden layers, and an output layer. This design has activation nodes at each layer, and this is done over iterations. Input layers use input vectors, hidden layers calculate weighted values, and the output layer generates a weighted sum from each input data point. The identified classification is determined after all iterations complete. One of the main benefits with this neural network is that it decreases the number of false positives in larger datasets, making it a strong selection for needle-in-the-haystack datasets (Hegde et al., 2020)

Considering the current deep learning methods for attack detection and following the categorization of the previous works, we roughly divide them into three categories as well, that is, unsupervised (e.g., autoencoder (AE), deep belief network (DBN), and generative adversarial network (GAN)), supervised (e.g., deep neural network (DNN), convolutional neural network (CNN), and recurrent neural network (RNN)), and other hybrid methods(Wu et al., 2020); we show the details of categorization in Fig. 4 Essentially, there exist other classification criterions.

Deep learning Algorithms for Attack Detection

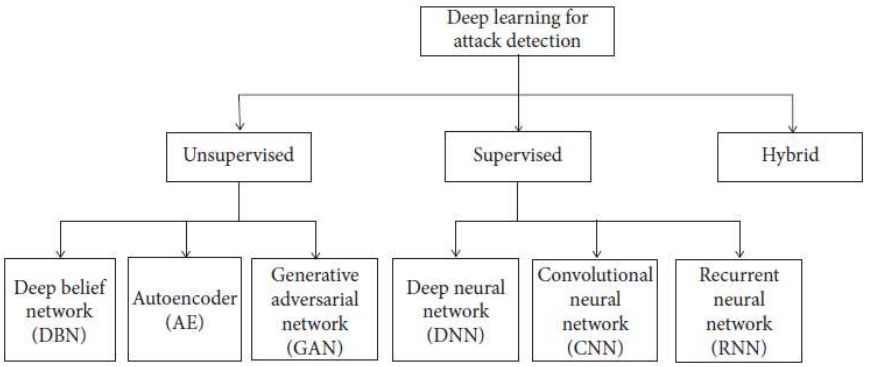


Fig. 4 Categorization of the current deep learning methods for attack detection. Source: (Wu et al., 2020)

Adopting different kinds of deep learning algorithms could bring variant advantages for attack detection methods. Supervised learning-based methods often result in high accuracy, due to quantity of information provided by manually labeled samples. Without sufficient knowledge from labeled data, unsupervised learning-based methods are generally low in performance. However, manually labelling is a time-consuming task, especially for complex attacks. there even exist cases that cannot be described by a simple label, due to the inherent complexity of real-world network attacks. therefore, unsupervised learning-based methods could perform well without prior knowledge of attacks, which is an obvious advantage. Hybrid methods decrease the number of training samples and maintain a relatively high performance, which is suitable to deal with variant attack situations. However, it is generally complex in structure and high in computing time, which prevents its wide usage(Wu et al., 2020).

Auto Encoder (AE)

Let us first introduce the architecture of AE, which can be regarded as a data compression algorithm with neural network structure. In fact, it is capable of firstly compressing the input into feature space representation and then reconstructing representation into the output. Since AE can be regarded as a typical representing learning algorithm, it is widely used for dimension reduction and outlier detection. Researchers in cybersecurity also adopt AE to represent abnormal behaviors in its compressed feature space, which brings the advantage of dynamical representation for unknown(Wu et al., 2020).
category of attacks.

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

Long Short-Term Memory (LSTM)

Recurrent neural network (RNN) is a basic deep learning model used for malicious file detection. RNNs are mainly employed to process sequential information, such as language translation. RNNs have the disadvantage that the longer the input sentence, the smaller the influence of the preceding words. This is known as the vanishing gradient problem.

Although RNN can effectively deal with nonlinear time series data, there are still two problems: (1) due to gradient vanishing and gradient explosion, RNN cannot process long time series data and (2) the training of the RNN model needs to determine the intercept length, and its optimal parameters are difficult to obtain by experience. LSTM can effectively solve these problems. LSTM and RNN have the same input and output, but the difference is the internal structure of the hidden layer. LSTM is an improved recurrent neural network and is mainly to overcome the defect of RNN that is difficult to deal with long-distance dependence in practical application, which is the most popular RNN at present. LSTM has made milestone achievements in many fields such as speech recognition, image description, and natural language processing(Huang, 2021).

Convolutional Neural Network (CNN)

CNN involves convolution computation and depth structure, which is a representative and commonly used techniques in deep learning domain. Specifically, CNN uses multilayer perception variant design requiring minimal preprocessing. the basic structure of CNN is composed of input and output layers and multiple hidden layers which include convolution, pooling, and full connection layer. Compared with other classification algorithms, CNN uses relatively less preprocessing and is independent of feature design containing prior knowledge, which are its main advantages. Convolutional neural network has been applied to network security field with much promising progress(Wu et al., 2020).

RELATED WORK

An increasing number of Internet of Things (IoT) devices are connecting to the Internet, yet many of these devices are fundamentally insecure, exposing the Internet to a variety of attacks. Botnets such as Mirai have used insecure consumer IoT devices to conduct distributed denial of service (DDoS) attacks on critical Internet infrastructure. This motivates the development of new techniques to automatically detect consumer IoT attack traffic and Solve denial of service (DDoS) attacks on critical Internet infrastructure (Doshi et al., 2018) proposed Machine Learning DDoS detection for consumer internet of things devices. The results indicate that home gateway routers or other network middleboxes could automatically detect local IoT device sources of DDoS attacks using low-cost machine learning algorithms and traffic data that is flow-based and protocol-agnostic. However, it will be interesting to experiment with additional features and more complex machine learning techniques beyond those discussed in the study. We believe that there is great potential for the application of deep learning to anomaly detection in IoT networks, especially for detecting attacks that are more subtle than DoS floods. However, the deep learning algorithms required immense number of datasets to perform at optimal standard. In order to mitigate malicious events, in particular botnet attacks against DNS, HTTP and MQTT protocols utilized in IoT networks, (Moustafa, Turnbull, & Choo, 2018) proposed an ensemble intrusion detection technique based on statistical flow features for protecting network traffic of internet of things. The proposed ensemble technique provides a higher detection rate and a lower false positive rate compared with each classification technique included in the framework and three other state-of-the-art techniques. However, the study fails to collect relevant features from other IoT protocols in order to build a dynamic profile of normal and attack patterns. Such a database of features can be used to facilitate the detection of existing and zero-day attacks using the proposed ensemble method.

To solve the non-accessibility of real datasets, (Nivaashini & Thangaraj, 2018) proposed intrusion detection system (IDS) using hybrid machine learning technique by combining K-means clustering and Support Vector Machine (SVM) classification. Experimental results show

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

that the proposed model achieve low false positive rate with improved detection rate which results in a higher attack detection rate of 95%. However, the research fails to improvised the datasets to facilitate studies which may relate to producing future IPv6 network attacks detection technique and to get better accuracy of IDS with more robust Machine Learning and Deep Learning algorithms. Similarly, More so, (Alsamiri & Alsubhi, 2019) evaluate various machine learning algorithms that can be used to quickly and effectively detect IoT network attacks using a new dataset (Bot-IoT) the achieved performance ratios according to F-measure are as follows: F-measure had a value between 0 and 1; Naive Bayes was 0.77; QDA was 0.86; Random Forest was 0.97; ID3 was 0.97; AdaBoost was 0.97; MLP was 0.83; and K Nearest Neighbours was 0.99. However, the research focuses only on supervised learning algorithms, hence, it would be interesting to evaluate the performance of some unsupervised algorithms. Furthermore, the various machine learning algorithms were applied independently from each other. This different machine learning algorithms can be combined as a multi-layered model or deep learners to improve the detection performance.

Deep learning developments appear promising in detecting and intelligent handling of new threats via learning skills. Future IoT device security protocols would also make DL algorithms more reliable and accessible than before. For example, (Jiang et al., 2018) proposed multi-channel intelligent attack detection method based on long short term memory recurrent neural networks (LSTM-RNNs). Experimental results validate that the proposed attack detection method greatly outperforms several attack detection methods that use feature detection and Bayesian or SVM classifiers. Base on the authors recommendation, this study should inspire other researchers to design better deep neural networks for intelligent attack detection along this orientation.

Similarly, (Yang et al., 2020) propose spam transaction attack detection model based on deep recurrent GRU and WGAN-div. The proposed models can distinguish between normal and abnormal transaction behaviours with an accuracy reaching to 99.86%. additionally, (Ullah et al., 2019) combined deep learning approach using CNN to detect the pirated software and malware infected files across the IoT network. The experimental results indicate that the classification performance of the proposed deep learning solution to measure the cyber security threats in IoT are better than the state-of-the-art methods.
To overcome the problem of cybersecurity threats and attacks (Rashid, Kamruzzaman, Hassan, Imam, & Gordon, 2020) explore an attack and anomaly detection technique based on machine learning algorithms (LR, SVM, DT, RF, ANN and KNN) to defend against and mitigate IoT cybersecurity threats in a smart city. Experimental results with the recent attack dataset demonstrate that the proposed technique can effectively identify cyberattacks and the stacking ensemble model outperforms comparable models in terms of accuracy, precision, recall and F1-Score. However, further insights in stacking of classifiers can better detect cyberattacks in the smart city systems go beyond technical contributions and carry economic and social implications.

Despite the promising results achieved by the aforementioned deep learning algorithms, the problem of IoT botnets and generic confidentiality, integrity, and availability (CIA) attacks remains a threat in data security. To address this problem (Hegde et al., 2020) explores botnet detection by experimenting with supervised machine learning and deep-learning classifiers

experiments have demonstrated incremental improvement in results for accuracy, probability of detection, and probability of false alarm. However, the work is limited to smaller dataset and can be extended to consider a wider range of IoT devices, larger datasets, and the use of unsupervised learning classifiers.

To solve resource constraints and the complexity, (Liang et al., 2020) focusses on the design, implementation and testing of an intrusion detection system which uses a hybrid placement strategy based on a multi-agent system, blockchain and deep learning algorithms. The results demonstrate the efficiency of deep learning algorithms when detecting attacks from the transport layer. Although the accuracy rate of DNN model on distinguishing different attack types is quite high, some rare attack types cannot be

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

detected accurately. The lengthy learning period of agents and the need for large training sets need to be resolved in future.

Therefore, identifying the pattern and characteristics of this attack is a crucial step in mitigating these attacks. Hence, for effectively detection of network attack behaviour (Liu & Zhang, 2020) proposed network intrusion detection based on convolutional neural network. The experimental results show that the multiclassification network intrusion detection model proposed in the study improves the accuracy and check rate, reduces the false positive rate, and also obtains better test results for the detection of unknown attackseffectively. However, the accuracy of the model proposed in the study in multiclass experiments need to be improved; in particular, the classification results of unknown different attack types still have room for improvement, which needs to be explored in future work.

As new attacks are constantly increasing recently as more IoT devices are being install in the cloud infrastructure, adapting with new attacks become another crucial step in preventing future security attacks. To solve the problem of adaptability to the new characteristics in IoT attacks, (Gu et al., 2020) uses entropy-based attack detection framework integrating the reinforcement learning model. Extensive experiments over a real IoT attack dataset demonstrate the proposed IoT attack detection approach's efficiency. However, the size of the datasets used is small.

Recently, in 2021 (Huang, 2021) proposed network intrusion detection based on an improved long-short-term memory model in combination with multiple spatiotemporal structures. Experimental verification shows that the accuracy and false alarm rate of the intrusion detection model based on the neural network are significantly better than those of other traditional model's network intrusion detection. However, the model only works well in the simulation dataset but needs to be tested in the actual network environment to verify the real performance of the model.

While machine learning can benefit from the massive amount of IoT data, privacy concerns and communication costs have caused data silos. Although the adoption of blockchain and federated learning technologies addresses the security issues related to collusion attacks and privacy leakage in data sharing, the "free-rider attacks" and "model poisoning attacks" in the federated learning process require auditing of the training models one by one.

To developed credible intrusion detection and defense mechanism on the device. A trusted feature aggregator federated learning for distributed malicious attack detection was proposed by(Hei, Yin, Wang, Ren, & Zhu, 2020). The proposed model was compared with important machine learning algorithms, and considerable test scores were obtained. however, the study fails to explore the efficiency of RSP alarm analysis in real scenarios to meet the application requirements of IoT devices. This increases the communication cost of the entire training process.

Hence, to address the problem of increased communication cost due to node security verification in the blockchain-based federated learning process (Xuan et al., 2021) a blockchain-based optimized solution for the counterattacks in the internet of federated learning systems. Experimental comparisons verify that the proposed model effectively reduces the communication cost of the node security verification in the blockchain-based federated learning process. Summary of related work is further presented in Table 2 below.

Comparative Analysis of The Intrusion Detection Techniques in Data Security

This section enumerated a comparison of most closely related works done by researchers using machine learning and deep learning for detecting data intrusion and their limitations. The Table below presents in chronological order, authors, proposed approach, findings, problem solve and research trend in the state-of-the-art literatures that have been reviewed.

Table 1: Major Literatures Reviewed

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

Reference	Proposed Approach	Findings	Problem address	Research gaps
(Doshi et al., 2018)	Machine Learning DDoS detection for consumer internet of things devices	The results indicate that home gateway routers or other network middleboxes could automatically detect local IoT device sources of DDoS attacks using low-cost machine learning algorithms and traffic data that is flow-based and protocol-agnostic	Solve denial of service (DDoS) attacks on critical Internet infrastructure	It will be interesting to experiment with additional features and more complex machine learning techniques beyond those discussed in this paper. We believe that there is great potential for the application of deep learning to anomaly detection in IoT networks, especially for detecting attacks that are more subtle than DoS floods.
(Nivaashini & Thangaraj, 2018)	Intrusion Detection System (IDS) using hybrid machine learning technique by combining K-means clustering and Support Vector Machine (SVM) classification	achieve low false positive rate with improved detection rate which results in a higher attack detection rate of 95%.	Solve the non-accessibility of real datasets	Fail to improvised the datasets to facilitate studies which may relate to producing future IPv6 network attacks detection technique and to get better accuracy of IDS with more robust Machine Learning and Deep Learning Algorithms
(Moustafa et al., 2018)	an ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things	The proposed ensemble technique provides a higher detection rate and a lower false positive rate compared with each classification technique included in the framework and three other state-of-the-art techniques	mitigate malicious events, in particular botnet attacks against DNS, HTTP and MQTT protocols utilized in IoT networks	Fail to collect relevant features from other IoT protocols in order to build a dynamic profile of normal and attack patterns. Such a database of features can be used to facilitate the detection of existing and zero-day attacks using the proposed ensemble method

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

(Jiang et al., 2018)	multi-channel intelligent attack detection method based on long short term memory recurrent neural networks (LSTM-RNNs)	Experimental results validate that the proposed attack detection method greatly outperforms several attack detection methods that use feature detection and Bayesian or SVM Classifiers	information security	This should inspire other researchers to design better deep neural networks for intelligent attack detection along this orientation
(Ullah et al., 2019)	combined deep learning approach using CNN to detect the pirated software and malware infected files across the IoT network	The experimental results indicate that the classification performance of the proposed solution to measure the cyber security threats in IoT are better than the state-of-the-art methods	Software piracy and malware attacks	only considers the influence of the current input without considering information from the previous and future time
(Alsamiri & Alsubhi, 2019)	evaluate various machine learning algorithms that can be used to quickly and effectively detect IoT network attacks using a new dataset (Bot-IoT)	The achieved performance ratios according to F-measure are as follows: F-measure had a value between 0 and 1; Naive Bayes was 0.77; QDA was 0.86; Random Forest was 0.97; ID3 was 0.97; AdaBoost was 0.97; MLP was 0.83; and K Nearest Neighbours was 0.99.	detection of attacks in IoT networks	it would be interesting to evaluate the performance of some unsupervised algorithms. Furthermore, the various machine learning algorithms were applied independently from each other. This different machine learning algorithms can be combined as a multi-layered model to improve the detection performance
(Yang et al., 2020)	Spam transaction attack detection model based on GRU and WGAN-div	The proposed models can distinguish between normal and abnormal transaction behaviours with an accuracy reaching to 99.86%.	solve the inadequate training problems of unbalanced samples and small samples that traditional	Fail to optimized the training time

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

			threat perception methods are faced with	
(Gu et al., 2020)	entropy-based attack detection framework integrating the reinforcement learning model	extensive experiments over a real IoT attack dataset demonstrate the proposed IoT attack detection approach's efficiency	adaptability to the new characteristics in IoT attacks	Advanced deep learning algorithms could be explored to improve the performance of system
(Liu & Zhang, 2020)	network intrusion detection based on convolutional neural network	the experimental results show that the multiclassification network intrusion detection model proposed in this paper improves the accuracy and check rate, reduces the false positive rate, and also obtains better test results for the detection of unknown attacks	effectively detection of network attack behaviour	accuracy of the model proposed in this paper in multiclass experiments need to be improved; in particular, the classification results of unknown different attack types still have room for improvement, which needs to be explored in future work.
(Liang et al., 2020)	focusses on the design, implementation and testing of an intrusion detection system which uses a hybrid placement strategy based on a multi-agent system, blockchain and deep learning algorithms	The results demonstrate the efficiency of deep learning algorithms when detecting attacks from the transport layer	resource constraints and the complexity	Although the accuracy rate of DNN model on distinguishing different attack types is quite high, some rare attack types cannot be detected accurately. The lengthy learning period of agents and the need for large training sets need to be resolved in future
(Rashid et al., 2020)	explore an attack and anomaly detection technique based	Experimental results with the recent attack dataset demonstrate that the proposed technique can effectively identify cyberattacks and the	cybersecurity threats and attacks	further insights in stacking of classifiers can better detect cyberattacks in the smart city systems go beyond technical

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

	on machine learning algorithms (LR, SVM, DT, RF, ANN and KNN) to defend against and mitigate IoT cybersecurity threats in a smart city	stacking ensemble model outperforms comparable models in terms of accuracy, precision, recall and F1-Score		contributions and carry economic and social implications
(Hegde et al., 2020)	explores botnet detection by experimenting with supervised machine learning and deep-learning classifiers	experiments have demonstrated incremental improvement in results for accuracy, probability of detection, and probability of false alarm	IoT botnets and generic confidentiality, integrity, and availability (CIA) attacks	The work is limited to smaller dataset and can be extended to consider a wider range of IoT devices, larger datasets, and the use of unsupervised learning classifiers
(Hei et al., 2020)	A trusted feature aggregator federated learning for distributed malicious attack detection	The proposed model was compared with important machine learning algorithms, and considerable test scores were ob- tained.	credible intrusion detection and defense mechanism on the device	Fail to explore the efficiency of RSP alarm analysis in real scenarios to meet the application requirements of IoT devices
(Huang, 2021)	network intrusion detection based on an improved long-short-term memory model in combination with multiple spatiotemporal structures	Experimental verification shows that the accuracy and false alarm rate of the intrusion detection model based on the neural network are significantly better than those of other traditional models	network intrusion detection	The model only works well in the simulation dataset but needs to be tested in the actual network environment to verify the real performance of the model
(Xuan et al., 2021)	a blockchain-based optimized solution for the counterattacks	experimental comparisons verify that the proposed model effectively reduces the communication cost of	increased communication cost due to node security verification in	Fail to optimize the feedback training process

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

	in the internet of federated learning systems	the node security verification in the blockchain-based federated learning process	the blockchain-based federated learning process	
(Dixit et al., 2021)	enhancement security frameworks for the detection of cyberattacks, and prevention by using different machine learning and optimization techniques in the domain of cybersecurity	High performance for detection, mitigation, and identification of cyberattacks and provide a security mechanism over the network	detection and mitigation of cyberattack	Advanced deep learning algorithms could be explored to improve the performance of system

DISCUSSION CHALLENGES AND FUTURE DIRECTION

Inside the summary of continuous investigation to build up a knowledge/multi-operator framework focused towards intelligent intrusion detection attack in data security using machine learning specifically deep learning technique discoveries. This research surveys the existing literature covering their contributions and limitations respectively. Base on the review, we identified the following research opportunities. Based on the speed with which the ML-based systems respond and versatility, they balance a wide variety of IoT network vulnerabilities. ML research for all types of applications is highly stimulated. There are good evidence points that show the value of ML specifically deep learning algorithms as an emerging technology. Thereby, the performance of the proposed intelligent attack detection method can be significantly improved by deep learning methods, which will inspire other researchers to design better deep neural networks for intelligent attack detection along this orientation(Jiang et al., 2018).

The study in (Nivaashini & Thangaraj, 2018) have shown that hybrid machine learning such as K-mean + SVM algorithms, has resulted in a higher attack detection rate of 95%. however, the dataset produced need to be improvised to facilitate studies related to producing future IPv6 network attacks detection technique and to get better accuracy with more machine learning base on deeper learning algorithms such as auto encoders (AE), deep belief network (DBN) and Bi-LSTM algorithms. Thereby, advanced deep learning algorithms could be explored to improve the performance of system(Liang et al., 2020).

We have notice that the existing work uses small datasets for evaluations purposes (Hegde et al., 2020), hence, future work could be extended to consider a wider range of IoT devices, larger datasets, and the use of unsupervised learning classifiers (Hegde et al., 2020). Collecting a larger dataset would also allow us to see how DoS detection accuracy is affected by the amount and diversity of IoT traffic(Doshi et al., 2018).

More so, the existing research only considered network activity from three devices, although many more smart-home devices exist and are continuing to be manufactured. There is motivation to perform anomaly detection on specific brands of the same IoT devices; this would provide insight into network and application layers of the specific IoT devices. Additionally, the existing research only considered training from a labeled dataset; additional work could consider the

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

implementation of unsupervised learning techniques on unlabeled data, to detect malicious activity.

Additionally, combining different machine learning algorithms to form a multi-layered model to further improve the detection performance is another interesting research opportunities(Alsamiri & Alsubhi, 2019).

Acknowledgment

We wish to thank research our supervisors Prof. Souley Boukary and Dr. Sani Abba for their immense contribution and academic guidance towards the success of this research work.

REFERENCES

Abdulraheem, A. S., Salih, A. A., Abdulla, A. I., Sadeeq, M., Salim, N., Abdullah, H., . . . Saeed, R. A. (2020). Home automation system based on IoT.

Alsamiri, J., & Alsubhi, K. (2019). Internet of Things cyber attacks detection using machine learning. *Int. J. Adv. Comput. Sci. Appl, 10*(12), 627-634.

Dixit, P., Kohli, R., Acevedo-Duque, A., Gonzalez-Diaz, R. R., & Jhaveri, R. H. (2021). Comparing and Analyzing Applications of Intelligent Techniques in Cyberattack Detection. *Security and Communication Networks, 2021*.

Doshi, R., Apthorpe, N., & Feamster, N. (2018). *Machine learning ddos detection for consumer internet of things devices.* Paper presented at the 2018 IEEE Security and Privacy Workshops (SPW).

Gu, T., Abhishek, A., Fu, H., Zhang, H., Basu, D., & Mohapatra, P. (2020). *Towards Learning-automation IoT Attack Detection through Reinforcement Learning.* Paper presented at the 2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM).

Haji, S. H., & Ameen, S. Y. (2021). Attack and anomaly detection in iot networks using machine learning techniques: A review. *Asian Journal of Research in Computer Science*, 30-46.

Hegde, M., Kepnang, G., Al Mazroei, M., Chavis, J. S., & Watkins, L. (2020). *Identification of Botnet Activity in IoT Network Traffic Using Machine Learning.* Paper presented at the 2020 International Conference on Intelligent Data Science Technologies and Applications (IDSTA).

Hei, X., Yin, X., Wang, Y., Ren, J., & Zhu, L. (2020). A trusted feature aggregator federated learning for distributed malicious attack detection. *Computers & Security, 99*, 102033.

Huang, X. (2021). Network Intrusion Detection Based on an Improved Long-Short-Term Memory Model in Combination with Multiple Spatiotemporal Structures. *Wireless Communications and Mobile Computing, 2021*.

Jiang, F., Fu, Y., Gupta, B. B., Liang, Y., Rho, S., Lou, F., . . . Tian, Z. (2018). Deep learning based multi-channel intelligent attack detection for data security. *IEEE transactions on Sustainable Computing, 5*(2), 204-212.

Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., . . . Idris, N. B. (2020). Intrusion detection system for the internet of things based on blockchain and multi-agent systems. *Electronics, 9*(7), 1120.

Liu, G., & Zhang, J. (2020). CNID: research of network intrusion detection based on convolutional neural network. *Discrete Dynamics in Nature and Society, 2020*.

Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2018). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet of Things Journal, 6*(3), 4815-4830.

Nivaashini, M., & Thangaraj, P. (2018). *A framework of novel feature set extraction based intrusion detection system for internet of things using hybrid machine learning algorithms.* Paper presented at the 2018 international conference on computing, power and communication technologies (GUCON).

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques. *International Journal of Environmental Research and Public Health, 17*(24), 9347.

Servin, A., & Kudenko, D. (2005). Multi-agent reinforcement learning for intrusion detection *Adaptive Agents and Multi-Agent Systems III. Adaptation and Multi-Agent Learning* (pp. 211-223): Springer.

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

Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. *IEEE Access, 7*, 124379-124389.

Wu, Y., Wei, D., & Feng, J. (2020). Network attacks detection methods based on deep learning techniques: a survey. *Security and Communication Networks, 2020*.

Xuan, S., Jin, M., Li, X., Yao, Z., Yang, W., & Man, D. (2021). DAM-SE: A Blockchain-Based Optimized Solution for the Counterattacks in the Internet of Federated Learning Systems. *Security and Communication Networks, 2021*.

Yang, J., Li, T., Liang, G., Wang, Y., Gao, T., & Zhu, F. (2020). Spam transaction attack detection model based on GRU and WGAN-div. *Computer Communications, 161*, 172-182.

Corresponding author: Sunday Ochigbo
ochigbosunday76@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.