International Journal of Advances in
Soft Computing and Intelligent Systems (IJASCIS)
2025, Vol 04, Issue 01, 74-97
ISSN: 3048-4987

Science Transactions © 2025

Original Paper

A Review of Intrusion detection Schemes in Fog computing using Machine and Deep Learning techniques: concepts, challenges and open issues.

Anita Seth[a],[*]

[a]DAVV University, IET, Khandwa Road, Indore, 452009, India.

[a] aseth@ietdavv.edu.in

ABSTRACT

Internet of Things (IoT) is emerging as new computing paradigm that is exhibiting enormous growth with the development of wireless communication technologies. The unprecedented growth of IoT devices has led to rapid increase in the generated data and computational load. Though cloud computing has unlimited data storage and processing capability. However, sending all the data directly to the cloud server for processing is not a suitable architecture for applications involving real time processing. In this regard, technologies including Edge Computing (EC) and Fog Computing (FC) have been developed to overcome these challenges. This review work aims to recapitulate the existing state of the security aspects in fog and edge computing and cover the machine learning and deep learning techniques for overcoming the associated threats. In this work, an attempt is made to review the studies using machine and deep learning techniques to address security problems in fog and edge computing. The paper discusses different types of attacks associated with fog and edge computing and corresponding mitigating technologies. Further, brief review of intrusion detection system is also presented. Finally, research challenges and open issues are discussed and possible solutions for the same are proposed.

KEYWORDS

Internet of things, Security, Fog computing, Edge computing.

1. Introduction

Internet of things (IoT) is a communication paradigm which enables the devices having limited computation, storage and communication capabilities (such as sensors and actuators) to collect, process and exchange the data. The basic objective is to make human life more valuable and productive by overcoming the adversities associated with the living environment [5]. There has been unprecedented increase in application of IoT in edge of networks for real time applications such as e-Healthcare, smart city etc. [30]. Though cloud computing has unlimited data storage and processing capability. However, sending all the data directly to the cloud server for processing is not a suitable architecture for applications involving real time processing such as e-healthcare system [43]. Transferring all the data to the cloud for processing would enhance the load on communication networks as well as increase the transmission latency due to the data transfer over large distance. In this regard, technologies including Edge Computing (EC) and Fog Computing (FC) have been proposed to overcome these challenges. This would enable to perform part of the computation on the device itself or on a node that is close to the source of data. Fog computing is a novel distributed computing paradigm where fog nodes/devices reside physically close to the end user devices [5]. These devices have in built processing capability to process the data in a limited way in order to reduce the latency.

Fog computing involves multiple fog nodes in the fog layer. Fog nodes may consist of variety of computing resources such as servers, routers, wireless access devices, mobile devices etc. These devices have the capacities of computing, network communication and security storage [5]. While, edge devices may include sensors, smart mobile phones and other IoT devices etc. Edge computing involves various devices like smart phones, sensors etc. connected to an edge server. Edge servers reside on the edge of the network and acts as a connection between a private network and internet [63]. They can be used for data and computation offloading as well as for multimedia content provision. Some amount of data computation is performed on the edge servers and the reduced data is sent to the fog and cloud for further processing. This new paradigm of edge computing has been recently proposed to complement cloud computing by performing certain data processing tasks at the edge of the network. However, it is a challenging task to implement classification models on edge devices as these have constrained resources and do not have enough storage and processing capabilities.

Fog computing enables to overcome the problem of resource scarcity in IoT as costly storage, computation and networking might be offloaded to nearby fog nodes. However, as a new computing paradigm, the security problem of fog computing cannot be underestimated [7]. In the architecture of fog computing, fog nodes lie in between the cloud and IoT device. Furthermore, fog nodes process crucial information which can be related to personal data. It would be disastrous if such confidential information gets into the hands of an intruder. Once the attacker gets access to such information, the stored data can be modified. In other case, an attacker may also launch denial of service (DoS) or distributed denial of service (DDoS) attacks to make the resources unavailable to authorized users. Though fog computing can offer a distributed and parallel architecture for managing services and resources, a robust security mechanism is needed for its protection. While the new paradigm of fog and edge computing has shown a significant reduction in the system running time, memory cost, and energy consumption for various applications as compared to conventional cloud computing. However, these solutions don’t operate within the controlled and secure environment and these interfaces posses additional security risks [38].

Machine Learning is a subfield of artificial intelligence that enables systems to learn from data and make predictions or decisions without being explicitly programmed. In several previous studies, researchers have used ML techniques to solve networking problems such as routing, resource allocation, security and traffic engineering [12, 21]. Deep Learning is a subset of Machine Learning that uses artificial neural networks to model and solve complex problems. Deep learning models are able to learn from large volumes of data, and are capable of achieving high accuracy in tasks such as image and speech recognition, natural language processing, and anomaly detection. These techniques can also be extended to fog and edge computing for performing autonomous and intelligent tasks relating to security. In the last few years, machine learning techniques have been extensively used on fog and edge computing [62, 67, 33]. Thus, discussing ML within the context of fog and edge computing assumes importance [13]. Various studies discussed the security and privacy issues in fog computing; however most of these studies overlooked detailed review on intrusion detection in fog computing and use of various machine learning and deep learning techniques to handle it. Besides, most of the previous review work have not provided the focused details in this area. Thus, this review work aims to recapitulate the existing state of the security aspects in fog and edge computing and cover the machine learning and deep learning techniques for overcoming the associated threats.

In this work, an attempt is made to review the studies using ML techniques to address security problems in fog and edge computing paradigm. Some of the major contributions of this study are listed below:

(i) Highlight different types of attacks associated with fog and edge computing and corresponding mitigating technologies.

(ii) Detailed review of Intrusion Detection System is presented.

(iii) Review of various machine learning and deep learning techniques for handling intrusion detection in fog and edge computing is presented.

(iv) Finally, research challenges and open issues are discussed and possible solutions for the same are proposed.

Fig. 1 depicts the roadmap of the review work conducted.

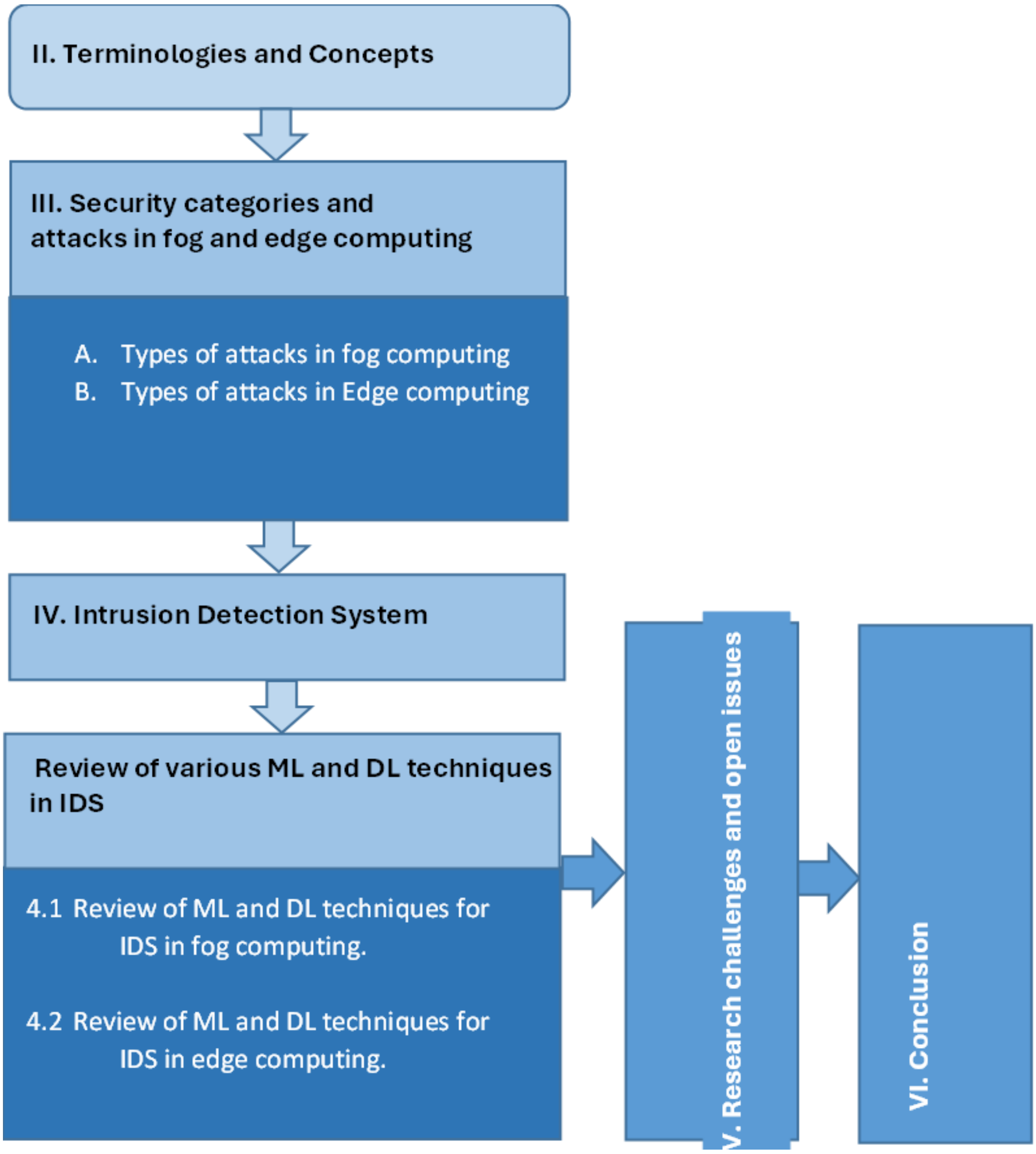
II. Terminologies and Concepts
III. Security categories and attacks in fog and edge computing
A. Types of attacks in fog computing
B. Types of attacks in Edge computing
IV. Intrusion Detection System
Review of various ML and DL techniques in IDS
4.1 Review of ML and DL techniques for IDS in fog computing.
4.2 Review of ML and DL techniques for IDS in edge computing.
V. Research challenges and open issues
VI. Conclusion

Fig. 1. Roadmap of conducted review work.

2. OVERVIEW OF KEY BACKGROUND TERMINOLOGIES AND CONCEPTS

This section gives an overview of key concepts relating to cloud, fog and edge computing in order to further enhance the understanding.

2.1 Cloud, Fog, Edge computing; Fog, Edge and cloud characteristics

Cloud is a technique that deals with storage and processing of data. The rapid growth of technology has contributed to increase of devices connected to the cloud and thus generating huge amount of data. Cloud computing as described by NIST (National Institute of Standards and Technology) [47], is ‘‘a model for enabling convenient, resource pooling, ubiquitous, on-demand access which can be easily delivered with different types of service provider interaction.” With the extensive growth in today’s technological era, cloud computing is being used to address the data storage and processing requirements. However, it suffers from the limitations of higher latency and more bandwidth requirement for transmitting the desired information. The cloud layer consists of various data centers that are meant for storage and processing of data. For extending the widespread usage of IoT applications, there is a need for the shift from cloud-based paradigm towards fog computing.

The concept of fog computing was introduced by Cisco in 2010 to bring the methodical arrangement of computation, storage and network resources between regular clouds and the end points [14]. Fog computing is a novel paradigm through which the cloud platform model can be extended by using network edges to back up computing resources. Similar to the cloud platform, fog computing provides data storage and application services [36]. Fog computing does not replace cloud computing but it supplements it. The characteristics of fog such as geo-distribution, support for mobility, support for heterogeneity, platform for ubiquitous access, low latency, location awareness presents the basic provisions for a wide range of IoT systems and applications [16]. Fog nodes comprise of edge servers or devices with communication and computing capability [8]. The terms "fog computing" and "edge computing" are used interchangeably in industry and academia. However, there is a distinction between the two terms.

Fog computing and architecture

The typical fog computing architecture comprises of three layers namely, the device layer, the fog layer and the cloud layer as depicted in Figure 2. In this hierarchical architecture, the lowest layer is the device layer which comprises of various smart devices including mobile phones, wearable devices, tablets and other IoT devices. The next layer comprises of fog layer, at which the data is aggregated from various IoT devices and then forwarded to the cloud. There can be multiple fog nodes in the fog layer comprising of servers, routers, smart devices etc. Further, the cloud layer is used for storing huge amount of data generated by various IoT applications. It also provides shared access, data offloading and processing.

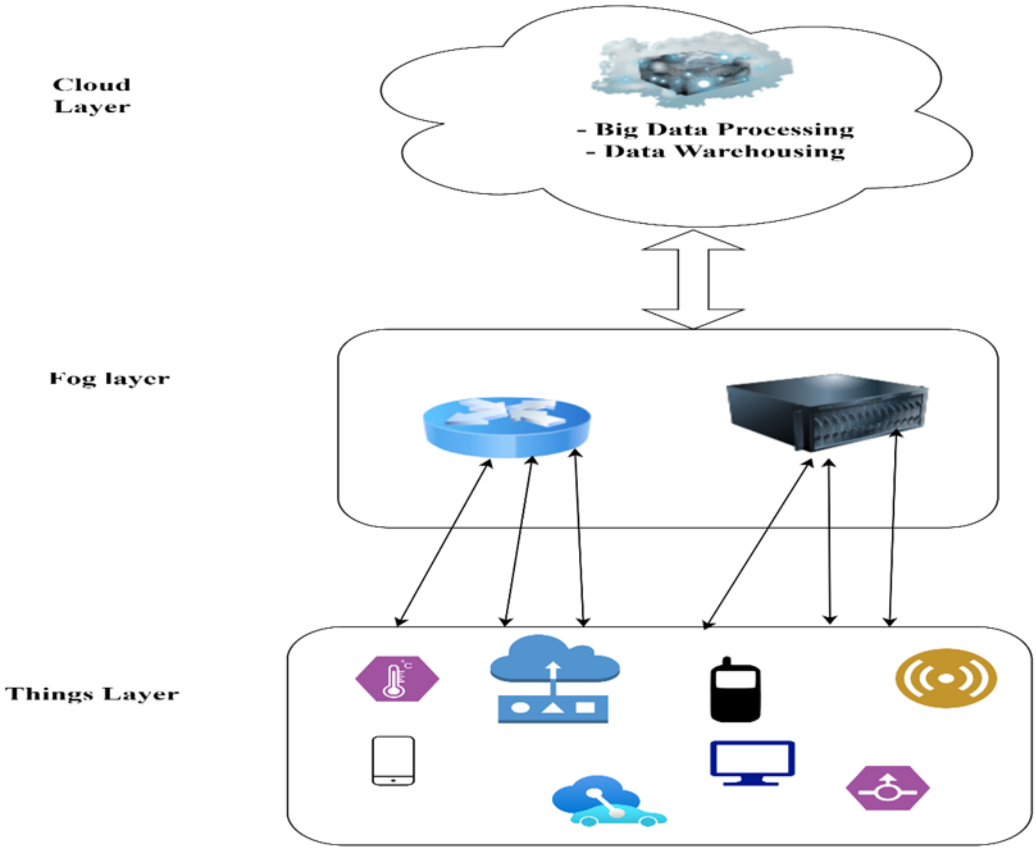

Fig. 2. Fog computing architecture.

Edge computing

The concept of edge computing (EC) has emerged as an innovative architecture where the cloud computing capabilities are extended to the edge of the network. It involves enhancing the computational capabilities at the network edge to ensure that processing occurs close to source of information. This may significantly reduce the latency experienced in the cloud computing framework and provides seamless integration with various application service providers and vendors [45]. This may enhance the performance of IoT network by reducing the response time and energy consumption of IoT networks. In the EC environment, edge servers are attached to the base stations and access points, which are further linked to edge devices. Edge servers provide the internet connectivity and covers a specific geographic area. An edge device like a smart phone links sensors in wearable devices, or sensors implanted on patient’s body to the edge servers. However, this architecture faces various security and privacy related challenges. The security related challenges comprise of wireless network security, authentication and trust issues, access control and intrusion detection.

3. SECURITY CATEGORIES AND ATTACKS IN FOG AND EDGE COMPUTING

Security is a critical concern in Fog and Edge computing due to the distributed nature of the architecture and the proximity of Edge devices to sensitive data sources. The unique characteristics of fog computing presents novel security challenges. In order to deal with these challenges, it is important to understand the various categories of security threats. Following types of security domains pertaining to fog computing have been identified and are summarized in Table 1.

Table 1. Various security categories in fog computing.

Category no.	Security category	Description	Issues
C1	Security standards	This category deals with security policies defined by regulatory bodies to ensure safe working environment.	Trust
C2	Network security	This category involves security problems related to network links.	-Intrusion detection in the network link. -detection of new attacks.
C3	Access control	It is user driven and involves problems relating to authentication and authorization.	-authentication mechanisms.
C4	Data security	It deals with problems relating to data integrity and privacy.	-loss of data and data leakage. -privacy of data. -recovery of data -accessibility of data.

3.1 Types of Attacks in Fog computing

The fog layer comprises of fog nodes that receive data from terminal devices at the network edge. Some of the fog nodes may be compromised by malicious nodes and become corrupted. These corrupted fog nodes may work together with external attackers to eavesdrop confidential data or temper with private data. In such a situation the integrity and accuracy of data is affected. It is important to categorize the attacks and understand how they affect data integrity, availability and confidentiality. According to the type of attacks, appropriate response system can be designed and implemented. Further, the fog nodes are vulnerable to various types of attacks as well as privacy leakage. Some of these attacks are presented below:

i. Impersonation Attacks

It is a type of phishing attack and does not involve malware. Fog computing networks are vulnerable to impersonation attacks because of the wireless interface between the fog nodes and end users. A malicious or spoofing node impersonate a legal device using its identity such as medium access control (MAC) address and gain illegal access into the network. It can further launch other attacks such as man-in-the-middle attack as well as DoS attacks.

ii. Denial of Service Attack (DoS)

DoS attack can be launched when devices connected to IoT network request for infinite processing/ storage services. Under this attack, the legitimate users are denied the system services. Since majority of the devices are not mutually authenticated, so this attack can be launched easily. The intensity of such an attack increases manifold when multiple nodes make repeated and fake requests.

iii. Distributed Denial of Service Attack (DDoS)

It is a major security threat that adversely affect service availability in Fog computing. In this DDoS attack, the attacker creates a network of bots or zombie machines by infecting machine over the internet [39]. Then these compromised machines further perform attacks on the victim nodes. In this way, huge traffic from so many compromised machines is directed towards a single victim node. As a result of which, the victim node resources including bandwidth, CPU, memory etc. starts getting depleted. The infected sever machine services are no longer available to request from legitimate users. In 2016, a massive DDoS attack was launched which was identified as Mirari botnet. This malware infects IoT smart devices and turns them into a network of remotely controlled bots or zombies. This network of bots which is often called as botnet is used to launch DDoS attack.

iv. Man in the middle attack (MiTM): It is type of eavesdropping in which the attacker secretly intercepts and controls the communication between the sender and receiver. It poses a serious threat to online security as the attacker is able to capture and manipulate sensitive information such as log in credentials, account details etc. in real time. In order to gain access to devices and sensitive information, IP spoofing is one of the ways to conduct MiTM attack.

v. IP spoofing attack: It takes place when the source address of IP packets is altered in order to hide the identity of the sender. Such as when the cybercriminals modify the source IP address of a website, email address or device for the purpose of masking it.

Table 2. Summary of the surveys covering different types of attacks in fog computing.

Author (year)	Problem	Types of attack	Technique	Security domain
[61]	Overcoming the issue of impersonation attacks.	Impersonation attacks	Q-learning algorithm.	Network security
[24]	Secure authentication scheme specifically for fog centric IoT environment.	Man-in the middle attack, impersonation attack. Fog device captured attack.	Light weight authentication scheme.	Data security
[23]	Processed data may be tampered by some malicious nodes while the data is transferred or aggregated.	Man-in-the middle attack, single node attack and collusion attack.	Secure data query framework based on data aggregation trees.	Data security
[3]	Identifying a spoofed IP packet	IP spoofing in DDoS attack	Active and passive operating system fingerprinting	Network security
[4]	Securing the access channel to IoT devices.	DDoS attack	Challenge response authentication	Data and network security
[17]	Addressed the problem of DDoS attack	DDoS	Proposed a framework in which DDoS attack traffic is generated and is made to pass through fog defender to cloud.	Network security
[46]	Attack detection in fog computing	Intrusion detection	Various ML techniques such as Decision tree, K means, and Random Forest algorithm.	Network security

3.2 Types of Attacks in Edge computing

Edge computing associated with IoT applications is vulnerable to various malicious attacks. These attacks can be introduced during three phases of data analytics that include data collection from edge devices, computation in edge servers and storage in edge/cloud servers [10]. Various types of attacks possible at edge computing are described below:

(i) Distributed Denial of Service Attack (DDoS)

DDoS attack in the EC environment is often coordinated via the control of mobile and IoT devices. An IoT based DDoS attack not only targets the cloud servers but also edge servers deployed around mobile and IoT devices. This may exhaust the processing capabilities of the edge server and disrupt the applications running on it and thus causing significant economic loss and severe social impact. For example, a malware named Mirai can be used to connect as many as 400,000 compromised smart devices into a controlled” zombies” network to launch a DDoS attack [15].

(ii) Collision attack

In this attack, the cybercriminal injects malicious nodes into the network and thus affecting the information gathered at the edge server. The malicious node combines two or more copies of information communicated by trusted edge node to produce a completely new copy. It is quite difficult to detect collusion attacks in IoT environment due to large number of devices connected into the network and continuous mobility of IoT devices. Authors [56] proposed the solution to this problem by encrypting the communicated messages with symmetric AES cryptographic technique. At each instance of communication process, new AES keys are used for encrypting the message.

(iii) Replay attack

In this attack, the third-party intercept the information sent by the genuine edge entity and transmit it to another legitimate edge entity as if it is being transmitted from the original sender. Various researchers [22, 69] have dealt with replay attack by incorporating a timestamp to the signed message used for authenticating the communication between the edge entities.

(iv) Malware Injection Attack

In this the attacker injects some malicious software code into the vulnerable program that changes the course of execution of the program [10]. The successful launch of this attack poses threat to the system as it can result into data loss, service denial etc. These types of attacks are generally prevalent in legacy applications. It is often found in XML parser, NoSQL queries, LDAP, program arguments and HTTP/SMTP headers etc.

(v) Physical attacks and Tampering

Many edge devices make use of semi-conductor chips that are prone to physical attacks and tampering. These types of attacks are based on establishing connection with electrical signals from chips, which may lead to stealing sensitive information stored in the chip. In order to overcome such attacks, inbuilt security in the chip can be enhanced.

Table 3 covers some of the studies that focused on these attacks and proposed solutions using different techniques.

Table 3. Summary of the surveys covering different types of attacks in edge computing.

Author (year)	**Problem**	**Types of attack**	**Technique**	**Security domain**
[44]	Leakage of privacy of medical data	--	Light weight privacy preserving XGBoost framework.	Data security
[49]	Improving the scalability and efficiency of collision attack.	Collision attack	AES implementation with first order resistant masking scheme.	Data security
[18]	Improving the efficiency of collision attack when applied to masked AES in edge computing.	Collision attack	Relation between Euclidean distance between traces and hamming distance between values and AES implemented with mask.	Data security
[68]	Reducing the attack traffic, reserving user traffic and reducing inspection delays.	DDoS	Reinforcement learning framework	Network security
[42]	Mutual authentication in the smart grid based on edge computing.	Side channel attack	Blockchain	Data security
[62]	Security challenges with multi access edge computing.	DoS	Software defined Perimeter framework.	Network security
[26]	Edge DDoS mitigation	DDoS	Game theoretical approach	Network security
[62]	Resource constrains in edge nodes constricts the deployment of network intrusion detection system based on deep learning model.	DDoS	Recurring Neural Network	Network security

Some of the security threats in fog and edge computing are highlighted below:

- Data interception and eavesdropping: Fog and Edge Computing systems transmit and store large amounts of data, making them vulnerable to interception and eavesdropping. Attackers can intercept data packets and use them to steal sensitive information, such as user credentials, financial data, or intellectual property.
- Malware attacks: Malware attacks are a significant threat to Fog and Edge Computing systems. Malware can compromise the security of the system by infecting devices, stealing data, or disrupting the system's operation.
- Denial of Service (DoS) attacks: DoS attacks can disrupt the availability of Fog and Edge Computing systems by overwhelming the system with requests or flooding the system with traffic, making it unable to respond to legitimate requests.
- Physical attacks: Fog and Edge Computing systems are vulnerable to physical attacks, such as theft, vandalism, or destruction of the devices or infrastructure. These attacks can compromise the integrity and availability of the system.

- Insider threats: Insider threats are a significant risk to the confidentiality, integrity, and availability of Fog and Edge Computing systems. Insiders with privileged access can intentionally or unintentionally cause damage to the system by stealing data, introducing malware, or disrupting the system's operation.
- Unauthorized access: Unauthorized access to Fog and Edge Computing systems can compromise the confidentiality, integrity, and availability of the system. Attackers can gain access to the system by exploiting vulnerabilities or by stealing user credentials.

To address these threats, it is important to develop a comprehensive security framework that includes implementing intrusion detection system and intrusion response system.

4. A BRIEF OVERVIEW OF INTRUSION DETECTION SYSTEM

As IoT is gaining widespread usage, more and more devices are getting connected to internet. It is forecasted that is going to generate huge amount of traffic which may even exceed the previous levels. In such a scenario, detecting malicious traffic and taking immediate action is needed. In this respect, the design of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) gains importance. In fog computing, malicious activities and attacks can adversely impact the performance and the services provided to the end users. It is vulnerable to numerous malicious attacks such as worms, denial-of-service (DoS) attacks, distributed denial of service (DDoS) attacks, Remote to Local (R2L), PROBE, User to Root (U2R) etc. Though several defensive techniques such as cryptography, firewalls etc. have been developed, such anti-threat systems still possess the limitations of detecting various attacks [11]. Thus, there is a need to implement a robust security system that can detect such attacks and take preventive measures.

Intrusion is a set of actions that violate security policies including integrity and confidentiality of data and availability of services [32]. In the literature, there are three major solutions for preventing the attacks. These include Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and Intrusion Response System (IRS). An IDS is a well-established approach to detect the presence of intruders in the network. It is usually hardware or software-based system that monitors events occurring in a computer system and identifies intrusions.

Based on the monitoring environment, IDS can be classified into network based and host-based system. Network based IDS monitor and analyze the external computer system state, i.e. the network traffic. Host based IDS monitors the host system log file [11]. Further, based on the detection approach, IDS can also be categorized into three types namely anomaly detection, misuse detection and hybrid detection. Anomaly based detection involves building a model using machine learning or statistical based algorithms. Any deviation between the observed behavior and model is interpreted as an anomaly. Anomaly detection is mainly used for unknown attacks. The existing defense strategies that have been devised for other types of networks are unsuitable for fog computing environment because of the openness of its network [1]. In misuse detection, signature-based scheme is used in which the signature of intrusion is matched with the database of intrusion signatures that has already occurred. This type of detection is meant for known attacks only. While the hybrid IDS combines both host based and network-based approach.

Though many researchers have developed IDS, but are still affected by high rate of false alarms. Another issue with the existing IDS is that unknown attacks are not being detected. This is owing to the rapidly changing network conditions and continuously evolving new security threats. In order to overcome some of these shortcomings, researchers have started focusing on using machine learning techniques for intrusion detection.

4.1 Review of various Machine learning and Deep learning techniques for IDS in fog computing

Fog and Edge computing systems generate large amounts of data from multiple sources, making it challenging to process and analyze the data in real-time. Machine learning (ML) and deep learning-based techniques can help to address this challenge by enabling real-time data analysis and decision-making. Machine learning techniques have been prominently used to efficiently solve various problems relating to IoT [39, 31]. ML is based on the premise that an intelligent machine would be able to learn and adapt from its environment based on its experiences without the need for explicit programming. ML techniques are beneficial for tasks requiring classifications, clustering, decision making, and prediction [65].

One of the key benefits of using machine learning and deep learning-based (DL) techniques in fog and edge computing is their ability to operate in a decentralized environment. ML and DL models can be trained on edge devices and can operate independently of a centralized server, enabling faster decision-making and reduced network traffic. Various researchers have used machine learning algorithms such as decision trees (DT), random forest (RF), support vector machine (SVM), Bayesian network and K means to detect network attacks [35]. The results of their studies shows that these techniques can successfully detect the network attacks of different types with an accuracy varying from 85% to 99%.

Machine learning techniques involves using comprehensive data analysis. The first step comprises of using data pre-processing methods for training data set. This includes feature mapping, that converts categorical variables to numeric features, imputation of missing values, feature normalization and feature selection to obtain the optimized feature set.

Machine learning techniques to detect anomaly can be classified into three approaches as given below:

(i) Supervised learning: It deals with training using well labelled class labels for the traffic arriving regularly from the network. This technique is quite useful in predicting the network traffic with high accuracy. However, it involves lots of computation time in labelling the class.

(ii) Unsupervised learning: In this technique, the data is unlabeled and the model finds the hidden pattern from the given data. Some of the algorithms based on this technique include K-means, K-mediod etc.

(iii) Semi-supervised: It involves supervised and unsupervised learning concepts. The algorithm uses the combination of labelled and unlabeled data sets.

Though machine learning based attack detection mechanisms have been quite successful, but they have less scalability for cyber-attack detection in massively distributed nodes such as fog and IoT [19]. The deep learning techniques exhibit the benefit of automatic hierarchical feature learning from the raw data. Further, deep learning techniques improves the efficiency of multimedia processing for IoT applications since multiple layers extract features instead of traditional complex pre-processing techniques [43].

Fog computing is emerging as one of the prominent areas where the machine learning and deep learning techniques can be applied in detecting the cyber-attacks. The deployment of these techniques on fog nodes is quite useful for IoT applications as the sensitive data analysis can be done close to IoT devices. Further the latency between the data sources and data analysis devices can be reduced. It also minimizes the network bandwidth requirement and requires less data to be sent to the cloud.

In order to defend against the various attacks in a highly dynamic and scalable fog computing environment, various researchers have proposed machine learning and deep learning-based security models. Among the machine learning approaches, most of these studies have used supervised and unsupervised techniques. Table 4 summarizes some of these studies.

Table 4. Summary of Intrusion detection schemes in fog computing.

S.No	Reference	Contribution	Dataset	Classifier	Accuracy
1.	[69]	Proposed a lightweight intrusion detection model based on ConvNeXt-Sf	ToN-IoT and BoT-IoT	CV model ConvNeXt	100
2.	[58]	Proposed a fog computing-based smart farming framework that deploys an IDS at the fog nodes.	CICIDS2017	XGBoost, ET, RF, and DT and K-means.	99.77
3.	[27]	Presented a novel taxonomy of intrusion detection schemes for IoMT.	NA	NA	NA
4.	[57]	Proposed Auto-IF for intrusion detection for fog environment	NSL-KDD	Auto-encoder (AE) and Isolation Forest (IF).	95.4 %
5.	[59]	Proposed a detailed framework of a distributed and robust attack detection for fog computing.	RPL_NIDS-2017, N_BaIoT-2018, UNSW-NB-2015, CICIDS-2017, NSL-KDD.	GRU, LSTM, Bi-LSTM, CNN, CNN-LSTM and DNN.	99.97%
6.	[40]	Proposed a DDoS mitigation framework for IoT using fog computing.	CICDDoS 2019	KNN	99.99
7.	[50]	presented a Anomaly Detection Model (GANBADM) scheme in Fog Environment	NSL-KDD	Genetic Algorithm and Naïve Bayes	99.73
8.	[51]	introduced an Anomaly Behaviour Analysis Methodology to implement an adaptive IDS.	Real time data from test bed	ANN	find
9.	[46]	Proposed ML based IDS system.	KDD’99 cup	K-Means, DT, RF.	93.33%
10	[39]	Proposed random forest based distributed ensemble IDS scheme for	UNSWNB15 and DS2OS	Ensemble technique using KNN, XGBoost and Gaussian naïve Bayes with meta classifier RF.	99.41%
11	[31]	Proposed IDS scheme by combining multiple learners. Also proposed deployment architecture in fog-to-things environment.	NSL-KDD	Ensemble technique comprising of DT and DNN.	85.81%
12	[9]	presented an intrusion detection architecture that operates in the fog computing layer.	NSL-KDD & CICIDS2017	DNN and KNN	99.85%
13	[37]	Presented a lightweight IDS based on a vector space representation using a Multilayer Perceptron (MLP) model.	ADFA-LD and ADFA-WD dataset	Multilayer Perceptron (MLP) model.	94
14	[5]	Proposed an IDS and IPS for Man in the Middle (MitM) attack at the fog layer.			
15	[8]	Proposed a lightweight IDS scheme Sample selected extreme learning machine (SS-ELM).	KDD cup 99	SS-ELM algorithm and ELM algorithm.	99.07%
16	[8]	Analysed and modelled the DDoS attack under the proposed framework of FC-IDS.	NA	Hypergraph clustering algorithm.	NA

17	[54]	Proposed fog computing-based IDS. The proposed model is composed of two phases: in first phase attack detection is carried out at local fog nodes and summarization of IoT system state at cloud server.	NSL-KDD	Online sequential extreme learning machines (OS-ELM).	97.36%
18	[28]	Proposed a new distributed and light weight IDS based on Artificial Immune System (AIS).	KDD cup 99 and ISCX dataset	DBSCAN clustering	98.35
19	[6]	Proposed an intelligent IDS based on multi-layered recurrent neural networks for fog computing security.	NSL-KDD	Recurrent artificial neural network.	92.18
20	[53]	Proposed an anomaly detection system using two-tier classification models.	NSL-KDD	NB and certainty factor voting version of KNN algorithm.	83.24%
21	[48]	Proposed IDS scheme for anomaly detection using ML	UNSWNB15 and KDD99	Decision tree (DT), expectation maximization, clustering, ANN, Naïve Bayes and logistic regression (LR)	Accuracy using DT was 85.56% for UNSWNB15 dataset. ANN provided 97.04 % using KDD99.
22	[20]	Proposed a novel distributed deep learning scheme for cyber-attack detection in fog-to-things computing.	NSL-KDD	Stacked autoencoder for feature extraction and Neural network using 3 layers.	99.2%

From Table 4, it is revealed that most of the researchers using machine learning have used supervised and unsupervised learning techniques. Supervised learning techniques used by researchers included decision tree, Random Forest, logistic regression, KNN, Naïve Bayes etc. Unsupervised learning algorithms included K-Means clustering, hypergraph clustering, DBSCAN clustering technique etc. From the above table, it is also revealed that under unsupervised learning technique, DBSCAN clustering technique achieved higher accuracy. Lately, the detection methods based on ensemble techniques, extreme learning and deep learning approach are emerging as favoured techniques among the researchers. The reason being these techniques have provided higher accuracy compared to other techniques.

Further, most of these models have been deployed either for single tier at the fog layer or two-tier at fog as well as cloud layer. In addition to this, in most studies, NSL-KDD dataset has been used for evaluating the performance. Newer datasets including RPL_NIDS-2017, N_BaIoT-2018, UNSW-NB15, CSE-CIC-IDS2018, TON-IoT, CICIDS2017, DS2OS etc. can be used for IoT environment as it contains various modern IoT based attacks. Thus, there is a need to investigate the studies using newer and latest datasets.

4.2 Review of Machine learning and Deep learning techniques for handling IDS in Edge computing

Various researchers have used machine learning and deep learning algorithms for overcoming the security challenges in edge computing. [29] study showed that edge computing-based framework reduces the network traffic by 80% and running time by 69%. According to [33], edge computing has become the appropriate place for deploying machine learning models. [21] suggested that edge computing could be used to extract features and reduce the number of features to be sent to the cloud. [10] analyzed the various security threats to edge computing and proposed solutions for several data analytics. Author advocated for various machine learning techniques for edge computing that includes multi-layer perceptron, random forest, support vector machine etc.

Deep learning techniques are also quite suitable for edge computing. Various researchers have supported deep learning models for edge computing [2, 49, 62]. A typical deep learning-based model has many different levels in the learning network. The parts of the learning layers can be offloaded in the edge and reduced intermediate data can be transferred to the centralized server [22]. In order to defend against the various attacks in edge computing environment, various researchers have proposed security models. The existing literature is classified by highlighting the contribution, dataset, technique used, application area, types of attacks and accuracy for the different security models. Table 5 summarizes some of these studies.

Table 5. Summary of security issues in edge computing using ML and DLM techniques.

Reference	Contribution	Dataset	Technique	Tech type	Result
[2]	Proposed a model for the classification of ransomware in edge computing devices.	RISS (Resilient Information Security System)	Deep neural network algorithm using auto-encoder.	DL using MATLAB	99.7% of true positive rate.
[29]	Proposed smart home architecture based on edge computing.	NA	RBF function and SVM.	ML	99.87% to 92.12%.
[18]	Developed deep hierarchical network by cascading two types of networks	CICIDS2017	Deep hierarchical network	DL	90%
[38]	Proposed distributed attack detection scheme.	CTU	Extreme Learning Machine	ML	Accuracy varying from 99% to 74% .
[62]	Proposed Edge-Detect model to enable DDoS detection on edge devices.	UNSW2015	Developed deep learning model by stacking the FAST cells.	DL	99%

[70]	Anomaly detection	NA	SVM	ML	90%
[60]	Anomaly detection	NA	Federated learning		95-98%
[20]	Distributed attack detection	NA	Deep learning approach	DL	92%
[44]	Designed a lightweight privacy preserving medical diagnosis mechanism on edge called LPME.	Heart disease and thyroid disease dataset	XGBoost framework.	ML	Accuracy of 80.4% over heart disease dataset and 89.3% over thyroid disease dataset.
[55]	Presented a new method in which the data processing is divided between the edge and fog nodes. Used active learning on edge devices and federated learning on fog nodes	MNIST	Convolution neural network	DL	
[42]	Developed a light weight machine learning based IDS model namely IMPACT.	AWID	Deep feature learning with gradient-based linear SVM.	DL	Accuracy of 98.22%; detection rate of 97.64% and 1.2%false alarm rate.

5. RESEARCH CHALLENGES AND OPEN ISSUES

Designing and implementing intrusion detection system based on machine learning and deep learning for fog and edge computing is emerging as a research topic of immense interest among the academia and industry. Fog computing as a new paradigm has many characteristics that are different from cloud computing. It presents several challenges in security aspects as the security solution devised for cloud computing cannot be applied directly. Though various researchers [57, 58] have proposed security models and developed authorization techniques for fog as well as edge computing, there are various aspects that are still unaddressed or partially addressed. From the detailed review of the literature, some of the open research challenges and research issues relating to fog as well as edge computing are highlighted and possible solutions are proposed.

5.1 Research Challenge 1: Developing a generalized model

In IoT applications, cyber-physical systems are involved, thus monitoring and ensuring security has become a critical issue. Intrusion detection is still an open and challenging task because of the dynamic, distributed and heterogeneous nature of IoT devices. IoT devices have limited resources in terms of power consumption, memory and processing capabilities.

5.2 Proposed Solution

There is a need to design and develop a generalized model for detecting various types of attacks. The model should be fast, based on less resource intensive algorithm and accurate. In fog as well as edge computing, most of the nodes are widely distributed, heterogeneous and vulnerable to invasion by malicious attackers. Further, these nodes have limited resources for data computation and storage, thus there is a need for developing light weight real time IDS that would enable swift action to be taken when intrusion is detected.

5.3 Research Challenge 2: Developing a decentralized architecture

Most of the existing research on intrusion detection make use of the centralized architecture, where in the detection model have been deployed at the cloud layer. Such models have been found to have low accuracy and high false alarm rate.

5.4 Proposed Solution

There is a need to develop a lightweight IDS model that is distributed and covers three layered IoT structure that includes cloud, fog and edge. Thus, a distributed architecture is preferred for fog computing in order to better detect and prevent malicious attacks.

5.5 Research Challenge 3: Developing a standardized security framework

The complex and distributed nature of fog and edge computing systems make them vulnerable to a wide range of security threats.

5.6 Proposed solution

There is a need for developing a standardized security framework for fog and edge computing system. Without a standardized security framework, it is difficult to ensure that all components of the system are adequately protected and that security policies and mechanisms are consistent across the system.

5.7. Research Challenge 4: Improving the learning accuracy of machine learning and deep learning techniques

Various studies have focused on using machine learning based solutions for detection of network attacks. Some of these approaches overcome the security challenges but yielded low accuracy. Majority of these solutions are based on single learners and are directly affected by the limitations of individual learning algorithm.

5.8 Proposed solution

Ensemble technique comprising of various base learners can be used in order to enhance the accuracy of detection. Investigating more diverse base learners and various combination methods can be undertaken to improve better these results. In addition to this, further enhancements of these machine learning algorithms is required to get higher accuracy and faster computation time to efficiently detect various kinds of attacks. Further, in case of deep learning techniques, there is need to explore other neural networks based deep learning algorithms for improving the performance. In the context of edge computing, more advanced learning techniques like autoencoder can be deployed on edge servers and the performance of different techniques can be compared. Further, a new training method for autoencoder based on de-noising autoencoder and dropout training method can be used to significantly improve learning accuracy when conducting the classification. More research is required when edge learning framework is implemented for a large-scale distributed network, consisting of hundreds of edge devices.

5.9 Research Challenge 5: Security issues in distributed learning strategies

Machine Learning and deep learning-based techniques have the potential to significantly improve the security of Fog and Edge computing systems by enabling real-time data analysis and decision-making. However, there are also challenges associated with using machine Learning and deep learning-based techniques in fog and edge computing, including limited computational resources, limited storage capacity, and limited bandwidth.

5.10 Proposed solution

To overcome these challenges, more research is required in implementing new techniques for efficient model training and deployment. Researchers need to explore further active learning and federated learning techniques in distributed architecture consisting of fog and edge nodes. Such a study would enhance the understanding of security issues when large number of edge nodes are considered. Using such techniques, processing of data can be divided between the edge nodes and fog nodes in order to reduce communication overheads and latency. By implementing these techniques, the data sample to train the model and also cost can be reduced. However, security aspects need to be further explored in such settings.

5.11 Research Challenge 6: Developing model for real time applications

Most of the research in intrusion detection for fog and edge computing has focused on using publicly available datasets. Further, in some studies obsolete datasets are being used which do no not cover the latest attacks in IoT environments.

5.12 Proposed solution

There is a need to investigate the studies using newer and latest datasets as highlighted in this study. Further, there is a need to develop machine learning and deep learning-based models for intrusion detection using real time data and using latest datasets.

5.13. Research Challenge 7: Automating the feature engineering

Feature engineering process used in machine learning is manual and is not effective in detecting newer attacks.

5.14 Proposed solution

There is a need for automating the feature engineering and simplifying the training procedure. In this regard, Stacked Auto Encoder (SAE) has been successfully used in research relating to edge computing for extracting abstract features automatically. There is a need to explore other techniques that involve automatic feature extraction that can further improve accuracy and detect unknown attacks in fog and edge computing.

5.15 Research Challenge 8: Explainable AI solution for security

Machine learning and deep learning-based techniques are often seen as "black boxes," making it difficult to understand how they make decisions. Future research could explore the use of explainable AI techniques to provide more transparency and accountability in security applications.

6. CONCLUSIONS

Internet of Things (IoT) is emerging as new computing paradigm that is exhibiting enormous growth with the development of wireless communication technologies. The unprecedented growth of IoT devices has led to rapid increase in the generated data and computational load. One of the solutions to handle this huge volume of workload is cloud computing. However, the cloud only model is unsuitable for IoT applications as it suffers from network congestion, high latency and bandwidth bottlenecks. By selectively moving the computation and storage towards the network, edge and fog computing provides an effective solution for overcoming these issues. The new paradigm of fog and edge computing can optimize the cloud computing system by performing data processing at the edge and fog layers. However, these are vulnerable to various security attacks that needs serious attention.

Machine learning and deep learning techniques have been widely adopted in various fields. It has high potential for fog and edge computing in addressing the security issues. The present work reviews various machine learning and deep learning techniques that have been used for detecting abnormalities and attacks and dives into security issues concerning fog and edge computing. In addition to this, various research challenges and their solutions have been proposed which require further investigation.

REFERENCES

1. Abdulkareem, K.H., Mohammed, M.A., Gunasekaran, S.S., Al-Mhiquani, M.N., Mutlag, A.A., Mostafa, S.A., Ali, N.S. and Ibrahim, D.A. (2019). A review of fog computing and machine learning: concepts, applications, challenges and open issues. IEEE Access, 7, pp-153123-153140.
2. Abdulsalam Yáu, G., Job, G. K., Waziri, S.M., Jaafar, B., SabonGari, N.A., Yakubu, I.Z. (2019). Deep learning for detecting ransomware in edge computing devices based on Autoencoder classifier. In proceedings of 4th International Conference on Electrical, Electronics, Communication, Computer technologies and Optimization techniques (ICEECCOT), pp.240-243.
3. Agoni, A. E., Dlodlo, M. (2018). IP spoofing detection for preventing DDoS attack in fog computing. In 6th Global Wireless Summit (GWS-2018), pp.43-46.
4. Alharbi, S., Rodriguez, P., Maharaja, R., Iyer, P., Subaschandrabose, N. and Ye, Z. (2017). Secure the internet of things with challenge response authentication in fog computing. In proceedings 36th IEEE International Performance Computing and Communications Conference (IPCCC), pp.1-2.
5. Aliyu, F., Sheltami, T. and Shakshuki, E.M. (2018). A detection and prevention technique for man in middle attack in fog computing. Procedia Computer Science,141, pp. 24-31.
6. Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., Razaque, A. (2019). Deep recurrent neural network for IoT intrusion detection system. Simulation Modelling and Practice Theory, pp. 101-105.
7. Alrawais, A., Alhothaily, A., Hu, C., X. Cheng, X. (2017). Fog computing for the internet of things: security and privacy issues. IEEE Internet Computing, 21(2), pp.34–42.
8. An, X., Zhou, X., Lü, X., Lin, F., Yang, L. (2018). Sample selected Extreme learning machine-based intrusion detection in fog computing and MEC. Wireless Communication and Mobile Computing, 43, pp.1-11.
9. Antonio de Souza, C., Westphall, C.B., Machado, R.B., Loffi, L., Westphall, C. M., G. A. Geronimo, G.A. (2022). Intrusion detection and prevention in fog based IoT environments: A systematic literature review. Computer Networks, 214, pp.109154.
10. Anusuya, R., Karthika Renuka, D., Ashok Kumar, L., (2021, April). Review on challenges of secure data analytics in Edge computing. In 2021 International Conference on Computer Communication and Informatics (ICCCI).
11. Anwar, S., Zain, J.M., Zolkipli, M.F., Inayat, Z., Khan, S., Anthony, B., Chang, V. (2017). From intrusion detection to an intrusion response system: fundamentals, requirements and future directions. In Algorithms, 10(39), pp.1-24.
12. Ayoubi, S., Limam, N., Salahuddin, M.A., Shahriar, N., Boutaba, R., Estrada-Solano, F., Caicedo, O.M. (2018). Machine learning for cognitive network management. IEEE Communications Magazine, 56, pp. 158-165.
13. Bierzynski, K., Escobar, A., and Eberl, M. (2017). Cloud, fog and edge: Cooperation for the future? In 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), pp. 62-67.
14. Chiang, M., Ha, S., Chih-Lin, I., Risso, F. and Zhang, T. (2017). Fog Computing and Networking: Part 1 (Guest editorial). IEEE Communications Magazine. 55(4), pp.16-17, 2017.
15. Cimpanu, C. (2016). You can now rent a Mirai botnet of 400,000 bots," http://www.bleepingcomputer.com/news/security/ you-can-now-rent-a-mirai-botnet-of-400-000-bots/, 24 Nov. 2016.
16. Dastjerdi, A.V., Buyya, R. (2016). Fog computing: helping the internet of things realize its potential. Computers, 49(8), pp.112–116.
17. Deepali and Bhushan, K. (2017, May). DDoS attack defense framework for cloud using fog computing. In 2nd IEEE International conference on recent trends in Electronics Information and Communication Technology, pp-534-538.
18. Ding, Y., Shi, Y., Wang, A., Zhang, X., Wang, Z. and G. Zhang, G. (2019). Adaptive chosen plain text collision attack on masked AES in edge computing, 7, pp.63217-63229.
19. Diro, A. A. and Chilamkurti, N. (2018, Sept.). Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications. In IEEE Communications Magazine, 56(9), pp. 124-130.
20. Diro, A. A., Chilamkurti, N. (2017). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, pp.1-12.
21. Fadlullah, Z.M., Tang, F., Mao, B., Kato, N., Akashi, O., Inoue, T. (2017). State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems. IEEE Communications Surveys & Tutorials, 19, pp. 2432-2455.

22. Gao, T., Li, Y., Guo, N. and You, I. (2018). An anonymous access authentication scheme for vehicular ad hoc networks under edge computing. International Journal of Distributed Sensor Networks, 14(2), pp. 15501477-18756581.
23. Gu, K., Wu, N., Yin, B., Jia, W. (2019). Secure data query framework for cloud and fog computing. IEEE Transactions on Network and Service Management, pp.1-14.
24. Guo, Y., Zhang, Z. and Guo, Y. (2020). Fog centric authenticated key agreement scheme without trusted parties. IEEE Systems Journal, 34, pp. 1-10.
25. Gupta, B.B. and Badve, O.P. (2016). Taxonomy of DoS and DDoS attacks and desirable defence mechanism in a Cloud computing environment. Neural Computing and Applications, pp. 1-28. Springer 2016.
26. He, Q., Wang, C., Cui, G., Li, B., Zhou, R., Zhou, Q., Xiang, Y. (2022). A game theoretical approach for mitigating edge DDoS attack. IEEE Transactions on Dependable and secure Computing, 1, pp.1-16.
27. Hernandez-Jaimes, M.L., Martinez-Cruz, A., Ramírez-Gutiérrez, K.A., Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. Internet of Things, 23, pp.1-33.
28. Hosseinpour, F., Plosila, J., Tenhunen, H. (2016, Dec.). An Approach for Smart Management of Big Data in the Fog Computing Context. In 2016 IEEE International Conference on Cloud Computing Technology and Science. pp. 468-471.
29. Hou, S., Huang, X. (2019). Use of machine learning in detecting network security of edge computing system. In proceedings of 4th IEEE International conference on Big Data Analytics, pp.1-6.
30. Ibrahim, M. (2016). Octopus: An Edge-Fog Mutual Authentication Scheme. Journal of Network Security, 18(6), pp. 1089-1101.
31. Illy, P., Kaddoum, G., Moreira, C.M., Kaur, K., S. Garg, S. (2019, April). Securing Fog to Things environment using Intrusion Detection system based on Ensemble learning. In proceedings of IEEE Wireless Communications and Networking Conference, pp.1-7, Marrakesh, Morocco.
32. Inayat, Z., Gani, A., Anuar, N.B., Anwar, S., Khan, M.K. (2017). Cloud based intrusion detection and response system: open issues and solutions. Arabic Journal of Science and Engineering, 7, pp. 1-25.
33. Janakiram, M. (2020). How AI Accelerators are changing the face of edge computing. Available from: https://www.forbes.com/sites/janakirammsv/2019/07/15/how-aiaccelerators- are-changing-the-face-of-edge-computing/#4afed777674f, last accessed March 2020.
34. Kafle, V.P., Fukushima, Y., Harai, H. (2016). Internet of things standardization in ITU and prospective networking technologies. IEEE Communications Magazine, 54(9), pp.43–49.
35. KarsligÐ¸ M.E., Yavuz, A.G., GÃijvensan, M.A., Hanifi, K. and Bank, H. (2017, May). Network intrusion detection using machine learning anomaly detection algorithms. In 25th Signal Processing and Communications, Applications Conference (SIU), pp. 1–4.
36. Khan, S., Parkinson, S. and Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing, 6, p. 19, 2017.
37. Khater, B.S., Wahab, A.W.B.A, Idris, M.Y.I.B., Hussain, M.A., Ibrahim, A.A. (2019). A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing. Applied Sciences, 9(1).
38. Kozik, R., Choraś, M., Ficco, M., Palmieri, F. (2018). A scalable distributed machine learning approach for attack detection in edge computing environment. Journal of Parallel Distributed Computing, 15, pp.1-34.
39. Kumar, P., Gupta, G.P. and Tripathi, R. (2020). A distributed ensemble design-based intrusion system using fog computing to protect the internet of things networks. Journal of Ambient Intelligence and Humanized Computing (Springer).
40. Lawal, K.N., Olaniyi, T.K., Gibson, R.M. (2021). Fog computing infrastructure simulation toolset review for energy estimation, planning and scalability. International Journal of Sustainable Energy Development, pg. 1-10.
41. Lee, H., Ryu, J., Lee, Y., Won, D. (2021). Security analysis of blockchain based user authentication for smart grid edge computing infrastructure. pp. 1-4.
42. Lee, S.J., Yoo, P.D., Asyhani, A. T., Jhi, Y., Chermak, L., Yeun, C. Y., Taha, K. (2020). IMPACT : Impersonation attack detection via edge computing using deep autoencoder and feature abstraction, 8, pp.65520-65529.
43. Liu, C., Cao, Y., Luo, Y., Chen, G., Vokkarane, V., Yunsheng, M., Chen, S., Hou, P. (2017). A New Deep Learning-Based Food Recognition System for Dietary Assessment on an Edge Computing Service Infrastructure. IEEE Transactions on Services Computing, 11(2), pp.249-261.
44. Ma, Z., Ma, J., Miao, Y., Liu, X., Choo, K.R., Yang, R., Wang, X. (2022). Lightweight privacy preserving medical diagnosis in edge computing. IEEE Transactions on Services Computing, 15(3), pp.1606-1618.

45. Mach, P., and Becvar, Z. (2017, 3rd Quart.). Mobile edge computing: A survey on architecture and computation offloading. IEEE Communication Surveys and Tutorials, 19(3), pp. 1628–1656.
46. Maharani, M.P., Daely, P.T., Lee, J.M. and D. Kim, D. (2020). Attack detection in fog layer for IIoT based on machine learning approach, ICTC 2020, pp.1880-1882.
47. Mell, P., Grance, T. (2018) SP 800-145. The NIST Definition of cloud computing. | CSRC (online) Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800- 145/final, accessed 11 Dec 2018.
48. Moustafa, N., Slay, J. (2016). The evaluation of network anomaly detection systems: statistical analysis of the UNSW-NB15 data set and the comparison with the kDD99 data set. Information Security Journal: A Glob Perspective, 25(1), pp.18–31.
49. Niu, Y., Zhang, J., Wang, A., Chen, C. (2019). An Efficient Collision Power Attack on AES Encryption in Edge Computing. IEEE Access, 7, pg-18734-18748.
50. Onah, J., Abdulhamid, S., Misra, S., Sharma, M., Rana, N. and J. Oluranti, J. (2020). Genetic Search Wrapper-Based Naïve Bayes Anomaly Detection Model for Fog Computing Environment. Advances in Intelligent Systems and Computing, 1351, pg. 1371-1382.
51. Pacheco, J., Benitez, V.H., Felix-Herran, L. C., Satam, P. (2020). Artificial neural networks-based intrusion detection system for internet of things fog nodes. IEEE Access, 8. pg-73907-73918.
52. Pahl, M.O., Aubet, F.X. (2018a). All eyes on you: distributed multidimensional IoT micro service anomaly detection. IEEE Xplore, pp 72–80.
53. Pajouh, H.H., Dastghaibyfard, G., Hashemi, S. (2015). Two tier network anomaly detection model: a machine learning approach. Journal of Intelligent Information systems, pp. 1-14.
54. Prabavathy, S., Sundarakantham, K., Shalinie, S.M. (2018). Design of cognitive fog computing for intrusion detection in internet of things. Journal of Communications and Networks, 20(3), pp.291–298.
55. Qian, J., Gochhayat, S.P., Hansen, L.K. (2019, Oct). Distributed active learning strategies on edge computing. In sixth IEEE International Conference on Cyber Security and Cloud Computing.pp.221-226.
56. Rahman, A., Hassanain, E. and M. S. Hossain, M.S. (2017). Towards a secure mobile edge computing framework for Hajj. IEEE Access, 5, pp. 11768-11781.
57. Sadaf, K., and Sultana, J. (2020). Intrusion Detection Based on Autoencoder and Isolation Forest in Fog Computing. IEEE Access, 8, pg-167059-167068.
58. Sajid, J., Hayawi, K., Malik, A.W., Anwar, Z. (2023). A Fog computing framework for intrusion detection of energy-based attacks on UAV assisted smart farming. Applied Science, 13(6), pp.1-23.
59. Samy, A., Yu, H. and Zhang, H. (2020). Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning. IEEE Access, 8, pg-74571-74585.
60. Schneible, J., Lu, A. (2017). Anomaly detection on the edge. In: MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), pp 678–682.
61. Shanshan, T., Waqas, M., Rehman, S.U., Aamir, M., Rehman, O.U., Jianbiao, Z., C. Chang, C. (2016). Security in fog computing: a novel technique to tackle an impersonation attack. 4, pp.1-9.
62. Singh, J., Bello, Y., Hussein, A.R., Erbad, A., Mohamed, A. (2021). Hierarchical security paradigm for IoT multi access edge computing. IEEE Internet of Things Journal, 8 (7), pp.5794-5805.
63. Sun X., and Ansari, N. (2016). EdgeIoT: Mobile edge computing for the internet of things. IEEE Communications Magazine, 54(12), pp.22–29, 2016.
64. Swarna Priya, R.M., Maddikunta, P.K., Parimala, M., Koppu, S., Reddy, T., Chowdhary, C.L., Alazab, M. (2020), An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. Computer Communications, 160, pp.139–149.
65. Wang, J., Jiang, C., Zhang, H., Ren, Y., Chen, K., Hanzo, L. (2020a). Thirty years of machine learning: the road to pareto- optimal wireless networks. IEEE Communications Surveys and Tutorials, pp.1–1.
66. Wang, M., Cui, Y., Wang, X., Xiao, S. and Jiang, J. (2018). Machine learning for networking: Workflow, Advances and Opportunities. IEEE Network, 32, pp. 92-99.
67. Zhang, C., Patras, P. and Haddadi, H. (2019). Deep Learning in Mobile and Wireless Networking: A Survey. In IEEE Communications Surveys & Tutorials, pp.2224-2287.
68. Zhang, H., Hao, J., Li, X. (2020). A method for deploying distributed denial of service attack defense strategies on edge servers using reinforcement learning. IEEE Access, 04, pp.1-10.
69. Zhang, J., Zhao, Y., Wu, J. and Chen, B. (2018). LPDA-EC: A Lightweight Privacy-Preserving Data Aggregation Scheme for Edge Computing. In 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor System (MASS), pp. 98-106.
70. Zissis, D. (2017). Intelligent security on the edge of the cloud. In International conference on Engineering, Technology and Innovation, IEEE, Funchal, pp. 1066–1070.