Cyber Security Framework for Detecting Malicious Devices in Fog Computing and (IoT) Environments: Challenges and Open Issues

Muhammad Isah Lamir [1], Abdulsalam Yau Gital[2], Fatima Umar Zambuk[3], Danlami Muhammad[4], Emmanuel Ramson Nannin[5], Mustapha Abdulrahman Lawal[6] & Ismail Zahraddeen Yakubu[7]

[1, 2, 3, 4, 5 ,6] *Department of Mathematical Science, Abubakar Tafawa Balewa University, Bauchi, Nigeria*
[7] *Department of Information Technology, SRM Institute of Science and Technology, Chennai, India*

ABSTRACT

One of the greatest challenges for the creation of fog or edge paradigms ecosystem is security stressed in strong terms that, there are several reasons for this. First, at the core of edge paradigm, there are several enabling technologies such as wireless networks, distributed and peer-to-peer systems, and virtualization platforms. It is then necessary not only to protect all these building blocks, but also to coordinate the diverse security mechanisms. This is by itself a complex issue, as we need to create a unified and transversal view of all the security mechanisms that allows their integration and interoperability. Therefore, there is immediate requirement of a proactive and predictive cybersecurity measure for protecting the edge services from malicious edge devices. Proactive prediction of malicious edge device attacks on the system will result in better and secure deployment of fog or edge layer in IoT environment. Therefore, the main purpose of this study to investigate the existing cybersecurity frameworks and identify their weaknesses for improvement.

Keyword Edge Computing, Fog Computing, Cloud Computing, Intrusion Detection, Cyber Attacks and Denial of Service

1. INTRODUCTION

The technological improvements in personal gadgets and wearable computing devices are permitting a new stream of real-time and ubiquitous applications, such as augmented reality, cognitive assistance, traffic monitoring, vehicular tracking, and interactive video streaming [1, 2]. It can be gleaned from prior studies of [3-6], such real time applications require real-time response, which is one of the major constraints in the cloud computing platform owing to the delays from distant cloud data centers. Although cloud computing provides many benefits, the latency sensitive and data intensive IoT applications appear to be a challenge for current cloud computing paradigm.

The needs for real-time response and ever-increasing data demands novel solutions[7]. In order to address this issue, unique computing paradigms were introduced to bridge the existing gap between the cloud and data generating devices that enable applications generate and process data on real time basis for real time decisions making. Fog and Edge computing are emerging as viable solutions to these challenges, offering real-time response and near to end cloud services. The term fog computing technologies is used to encompass different emerging technologies situated at the edge of the network to provide computational and storage resources to deliver real time communication with minimum latency [8, 9].[10] argued that fog computing augments cloud computing by bringing networking and computational resources on fog devices near to the end users. A fog device can be a router, gateway, switch, or a base station, that provides an entry point into the service provider’s core network.

Mobile Edge Computing equally brings computation and storage capacity of traditional core network within the range of the radio of access network. In this new architecture, traditional base station not only perform traffic control, but also deploy less resourceful edge server/cloud to provide context-aware services towards mobile subscribers within the close proximity. The primary objective of Mobile Edge Computing is to provide application and services with less latency and minimum bandwidth [11-13].

One of the greatest challenges for the creation of fog or edge paradigms ecosystem is security [14], [4, 15]. [12, 16] stressed in strong terms that, there are several reasons for this. First, at the core of edge paradigm, there are several enabling technologies such as wireless networks, distributed and peer-to-peer systems, and virtualization platforms. It is then necessary not only to protect all these building blocks, but also to coordinate the diverse security mechanisms. This is by itself a complex issue, as we need to create a unified and transversal view of all the security mechanisms that allows their integration and interoperability. According to [17] edge devices that are controlled by the users are also important elements of the whole ecosystem. They not only consume services, but also can become active participants that provide data and participate in the distributed infrastructure at various levels. However, there will be also rogue users that might try to disrupt the services in one way or another[17].

Any fog or edge device that is controlled by an adversary can be reprogrammed to distribute fake information when queried (e.g. users providing fake data to crowd-sourcing services)[18]. Note that an edge device might also provide bogus values due to an anomaly in their sensors or internal systems. In a survey conducted by (S. Furnell, 2004) stated that system security administrators are more aware and concerned about the outside attacks that most of the insider attacks go undetected. [15] further affirmed that, edge computing environment is a multitenant architecture and that resources are shared among different applications, it is very difficult to identify the insider attacker. Similarly, Rigorousness of insider attack in edge computing environment is also very high because applications using real-time data are of high importance[9]. Therefore, there is immediate requirement of a proactive and predictive cybersecurity measure for protecting the edge services from malicious edge devices. Proactive prediction of malicious edge device attacks on the system will result in better and secure deployment of fog or edge layer in IoT environment.

A Markov process is a particular case of stochastic process [19], where the state at every time belongs to a finite set, the evolution occurs in a discrete time and the probability distribution of a state at a given time is explicitly dependent only on the last states and not on all the others[20]. A Markov chain is a first-order Markov process for which the probability distribution of a state at a given time is explicitly dependent only on the previous state and not on all the others [21]. In other words, the probability of the next (future) state is directly dependent only on the present state and the preceding (past) states are irrelevant once the present state is given. More specifically there is a finite set of possible states, and the transitions among them are governed by a set of conditional probabilities of the next state given the present one, called transition probabilities. The transition probabilities are implicitly (unless declared otherwise) independent of the time and then one speaks of homogeneous, or stationary, Markov chains. A Hidden Markov Model is a generalization of a Markov chain, in which each “internal” state is not directly observable (hence the term hidden) but produces “emits” an observable random output “external” state, also called “emission”, according to a given stationary probability law [22].

Mobile Edge Computing is an emerging technology that provides cloud and IT services within the close proximity of mobile subscribers. Traditional telecom network operators perform traffic control flow (forwarding and filtering of packets), but in Mobile Edge Computing, cloud servers are also deployed in each base station [23]. Therefore, network operator has a great responsibility in serving mobile subscribers. Mobile Edge Computing platform reduces network latency by enabling computation and storage capacity at the network. It also enables application developers and content providers to serve context-aware services (such as collaborative computing) by using real time radio access network information. Mobile and Internet of Things devices perform computation offloading for compute intensive applications, such as image processing, mobile gaming, to leverage the Mobile Edge Computing services. Therefore, in other terms, Mobile Edge Computing is a model for enabling business oriented, cloud computing platform within the radio access network at the close proximity of mobile subscribers to serve delay sensitive, context aware applications[24].

Therefore, it is then necessary not only to protect all these building blocks, but also to coordinate the diverse security mechanisms. This is by itself a complex issue, as we need to create a unified and transversal view of all the security mechanisms that allows their integration and interoperability. Therefore, there is immediate requirement of a proactive and predictive cybersecurity measure for protecting the edge services from malicious edge devices. Proactive prediction of malicious edge device attacks on the system will result in better and secure deployment of fog or edge layer in IoT environment. Therefore, the main purpose of this study is to investigate the existing cybersecurity frameworks and identify their weaknesses for improvement. The remainder of this paper is organized as follows: section 2 presents the literature review, section discuss the challenges identified and final section concludes the research.

2. LITERATURE REVIEW

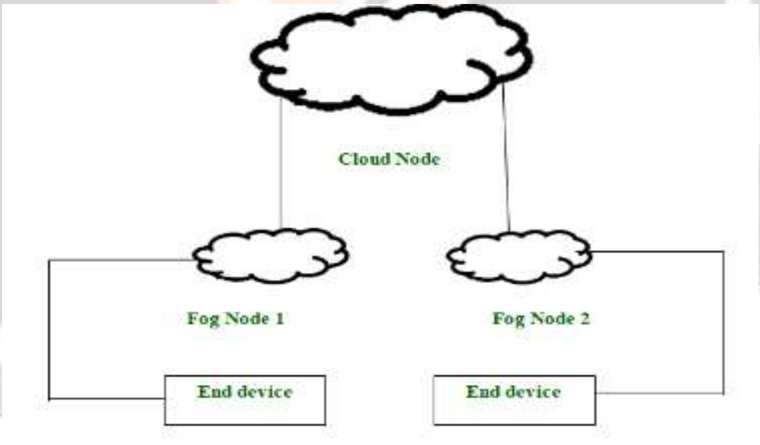
This section gives a review of related work done by some researchers on different security mechanisms that can be applied to create cyber security frameworks that can be designed and deployed to address security challenges associated with Fog Computing and Internet of Things environments.

2.1 Contrasting Cloud Computing and Fog Computing

The term fog computing was coined by Cisco in January 2014. This was because fog is referred to as clouds that are close to the ground in the same way fog computing was related to the nodes which are present near the nodes somewhere in between the host and the cloud. It was intended to bring the computational capabilities of the system close to the host machine. After this gained a little popularity, IBM, in 2015, coined a similar term called "Edge Computing" [14]. Fog Computing is the term coined by Cisco that refers to extending cloud computing to an edge of the enterprise's network. Thus, it is also known as Edge Computing or Fogging. It facilitates the operation of computing, storage, and networking services between end devices and computing data centers. The for-computing architecture is depicted in Fig. 1. The devices comprising the fog infrastructure are known as fog nodes.

In fog computing, all the storage capabilities, computation capabilities, data along with the applications are placed between the cloud and the physical host. All these functionalities are placed more towards the host. This makes processing faster as it is done almost at the place where data is created. It improves the efficiency of the system and is also used to ensure increased security[25]. Numerous benefits of fog compute are highlighted among others, they include:

i. This approach reduces the amount of data that needs to be sent to the cloud.
ii. Since the distance to be traveled by the data is reduced, it results in saving network bandwidth.
iii. Reduces the response time of the system.
iv. It improves the overall security of the system as the data resides close to the host.
v. It provides better privacy as industries can perform analysis on their data locally.



The fog-computing architecture is depicted in Fig. 1

The cloud and fog computing paradigms are compared and contrasted in the table 1 below:

Table I: Differences and similarities of cloud and fog computing Paradigms Source: [6]

Cloud Computing	**Fog Computing**
Centralized architecture	Decentralized architecture
Average scalability	High scalability
High latency	Low latency
Service access (through core)	Service access (at the edge)
Service availability (high)	Service availability (high)
Explicit mobility (not possible)	Explicit mobility (possible)

Despite all the numerous benefits, fog computing is not free from certain drawbacks which if not carefully understood and considered may refute the operational benefits of fog computing: Fog computing adds more complexity into a network, and invariably increases certain amount of overhead commercially, a greater number of points of failure is equally introduced through the implementation of fog computing technology and large volumes of data are presently being distributed to more users to optimize the concept of the cloud. Organizations and data processing centers need to device a medium to effectively deliver contents to end users through a more centralized distributed platform. The idea behind the concept of fog computing is to distribute data to move it geographically closer to the end users' data generating devices by bridging the existing gap between the cloud and cloud users in order to remove latency and numerous hops, and support mobile computing, real time data generation and processing as well as data streaming [6]. The differences and similarities between the fog and the cloud computing paradigms are as summarized in Table 1 above.

2.2 Related Work on Fog Computing Security Mechanism

In this section after studying some relevant literatures of edge computing, more comprehensive studies of insider user attacks on fog computing platforms were undertaken. According to [26], fog computing, as an extension to cloud computing has addressed some pressing issues identified with the cloud computing by providing additional features, such as low latency, mobility support, location awareness. Its unique features have also opened a way toward security challenges, which need to be focused for making it bug-free for the users. They put forward that, dealing with the physical objects involved in the IoT network and the connected devices, data collection and keeping it secure is an issue that is noteworthy.

In a survey conducted by [27], the authors opined that, the data surge expected by the massive adoption of IoT solutions, coupled with the demand and desire for better network performance needed by modern end-user applications, underscore how the classic network Cloud model is not capable to efficiently respond to the new growing needs. The Cloud computing paradigm provides a scalable infrastructure that relieves end users from the expenses of designing, purchasing and maintaining computing and storage resources. Notwithstanding the obvious advantages, this model is not appropriate for latency sensitive applications, that requires geographical proximity with the service provider to effectively meet their delay requirements. To address this major challenge, Cisco researchers defined a new network architecture, termed Fog Computing, that extends the Cloud computing model to the edge of the network, paving ways for new variety of applications and services, such as real-time video stream processing, gaming and augmented reality, and. This new computing model provides storage and computational capabilities geographically closer to data generating digital devices of the end users. The most important among the characteristics of Fog Computing include: low latency and location awareness, supports real-time applications, heterogeneity, widespread geographical distribution handling of a huge number of nodes, supports mobile end-devices and wireless access.

The term fog computing was coined by [28] in a paper published by Cisco. The basic architecture of fog computing was critically explained and how it extends the cloud computing paradigm to location geographically closer to end users. The paper equally explained relationship of cloud computing with the Internet of Things. The term Fog computing is used to simply imply extension of cloud computing to the edge of an enterprise's network. It can be perceived both in large cloud systems and in big data structures; this is apparent in the growing complexity in accessing information objectively [29]. The computation, storage and networking services operations between end devices and cloud-computing data centers are greatly facilitated by the fog computing. While edge computing typically refers to the point or location where computations are initiated, fog computing on the other hand, connotes distribution of the communication, computation as well as storage resources and services relatively on or close to data generating devices and systems within the control of end users. Fog computing significantly complements IoT operations and most of the devices on the network are connected to each other. The features of fog computing include: edge location, location awareness and low latency. Others include large number of nodes, real-time interaction, large-scale sensor networks, support for mobility and predominance of wireless access [30]. However, it is equally opined that rather than solving a problem, utilizing Fog Computing when there is no real use case can be a burden [31]. To that end, there are ways in which fog computing can be absolutely applicable so as to enjoy the benefits of fog-computing technology. Bringing data close to the users' data generating devices, improving data processing and delivery efficiency, reduces network congestion, support for mobility and the IoT, boasts some impressive scaling abilities and possible integration with the cloud and other services [6].

In 2014, [29] analysed the major scenarios and security challenges that fog computing paradigm is likely to face and also studied the real-time application of fog in smart grid and traffic situations. The relationship of mobile cloud computing and fog computing was analysed in an extensive study conducted by [32]. He also stressed that fog computing is the perfect solution for running latency sensitive applications from mobile to cloud computing architecture. System analysts are aware of "insider" threat on the edge, for or cloud system for a while now. Many studies surveyed the definitions, causes and effects of a malicious insider user. Though research on insider user devices and security of edge computing is still in its nascent stage[4].

Similarly, [33] tried to bridge the gap between natural language description of any malicious insider user and his/her technical activities. They use semantic ontology approach to detect the malicious insider user from large pool of users. The ontology is developed to create a bridge between natural language descriptions of potential indicators of malicious insider activity on case data as well as the operational data that contain the technical and behavioral observables associated with malicious insider activity. Their insider threats indicator provides a mechanism that allows sensitive information to be concealed while maintaining sufficient descriptive ability to effectively communicate behaviors and actions of interest across organizations. Their work laid a foundation for more effective fusion of traditionally disparate data sources by introducing the application of ontology as an analysis hub that combines operational and human resources data.

Still in 2014, [15] proposed a framework which uses user's current behavior, his/her past behavior and his/her community behavior to detect anomaly in any user activity. This system removes false anomaly detection and helps to improve performance of the system.

Moreso, [3] affirmed that Mobile Device Clouds (MDC) are becoming a concrete reality owing to the qualitative quantitative and upgrades on mobile devices such as tablets and smartphones. This evolution renders mobile devices capable of initiating classic and complex cyberattacks especially when they coordinate together and form a distributed mobile botnet which is termed as "MobiBots". The authors first introduced the concept of MobiBots and asserted that MobiBots infect a large number of mobile devices and schedule targeted attacks by leveraging Device-to-Device (D2D) short range wireless communications. The MobiBots Formation, challenges and limitations were discussed and then made case for MobiBots utilization. The authors argued that MobiBots use device to device communication which renders mobile devices vulnerable to fast and hardly detectable propagation within MobiBots. The impact of the large-scale infection and coordination of mobile devices via short range wireless technologies in attacks against other mobile devices that come within proximity was also investigated. Their results have shown that the infection rate takes only few hours and this time can drop considerably if more sinks are used. Propagation waiting time, however, requires longer period of time and the existence of more sinks is mandatory to achieve successive results within couple of hours. The authors also investigated the impact of existing trust-based prevention techniques on MDC performance and the results confirmed that deploying prevention techniques over MDC can be capital intensive. While we have looked into making efficient malicious attacks within MDC, in the future, we plan to implement a prevention algorithm. Such preventive algorithm will hinder mobile infection by leveraging different trust levels to enforce confidence values to a given application. We will also propose a fully distributed preliminary detection algorithm for MobiBots that identifies and stops short range botnet infection

In 2015, [34] analyzed pattern key strokes of all the users for effective profiling of insider user. Based on the profile output, effective security mechanism can be imposed hence preventing insider user attack.

In 2015, [35] conducted a research for mitigating insider user attacks in their work they proposed a hybrid approach for preventing insider user attack in cloud by using multiple technologies. They used selective encryption for data encryption, neural network to create profile of users and decoy technology for concealing sensitive information.

In the year 2015, [36] came up with an attribute-based authentication framework for authorization in peer-to-peer networks. In their work they proposed an authorization framework with AC (Attribute Certificates) to aiming at efficient and effective allocation of privileges without involving any third party.

Additionally, [3] in their work titled: Friend or Foe? Detecting and Isolating Malicious Nodes in Mobile Edge Computing Platforms opined that, with the current trends in the field of computing, mobile devices are now evolving into highly capable computing platforms that read, sense, generate, store and execute complex tasks is greatly transforming them into attractive mechanisms for edge computational micro-cloud settings. However, due the fact that, there is hardly any solution, be it science, technology or engineering is without shortcoming or limitation, such solutions are creating novel security challenges due to the ever-increasing demands for more seamless computational cyber foraging that influences exploding propagation of mobile devices. A major area of utmost concern is that, security challenges emanating from these trends, are growing at a rate exceeding the evolution of security solutions. The researchers anticipated challenging future security attacks resulting from the adoption of collaborative mobile edge cloud computing platforms, such as Femto Clouds and MDCs despite all prior contributions proffered as solutions to the identified challenges. Their work asserted that, in typical botnet attacks, "vertical communication" between a botmaster and infected bots, enables attacks that originate from outside the network referred to as outside attacks. This assertion further unequivocally supports the findings of the great works of [37-40] respectively.

According the researches above, intrusion detection systems typically examine network traffic to spot anomalies. Whereas, honeypots are deployed to attract and detect attackers as much earlier established in the work of [41] and [42] respectively. They equally established that firewalls are deployed at the periphery of networks to filter undesired traffic. However, based on their analysis of different security mechanisms available as at the time of their work, these traditional security measures (IDSs, Honeypot and Firewalls) are not as effective in protecting networks from insider attacks such as MobiBots, a mobile-to-mobile distributed botnet as established by [43] due to the fact that, these mechanisms are designed to detect and address vertically propagated attacks (outside attacks or intrusions), but not horizontally propagated attacks (insider attacks). The researchers further justified that, this shortcoming is due to the mobility of bots and the distributed coordination that takes place in MobiBot attacks. In contrast to classical network attacks, these attacks are difficult to detect because MobiBots adopt "horizontal communication" that leverages frequent contacts amongst entities capable of exchanging data/code. In addition, this architecture does not provide any pre-established command and control channels (C&C) between bots and their botmaster. As a result, such mobile device infections will invariably sidestep classical security measures, ultimately enabling more sophisticated and dangerous attacks from within the network.

Furthermore, [44] In their attempt to address the aforementioned implications identified with the traditional security mechanisms criticized, they considered an environment in which computational offloading is performed among a set of mobile devices and proposed a novel mechanism codenamed HoneyBot, which is a defense technique for device-to-device (d2d) malicious communication. While classical honeypots are designed to isolate Distributed Denial of Service (DDoS) attacks, HoneyBot nodes detect, track, and isolate such attacks. They proposed and investigated detection and tracking algorithms that leverage insecure d2d infected communication channels to accurately and efficiently identify suspect malicious nodes and isolate them.

Similarly, [45] designed a lightweight and secure data access control based on Ciphertext-Policy Attribute-Based Encryption algorithm (SL-CP-ABE), the scheme provides secure data access control in mobile cloud computing.

In a survey conducted by [17] they opined that it is possible to reuse or adapt various security mechanisms that were specifically designed for one edge paradigm to the other contemporary computing paradigms.

In 2016, [46] proposed a handover authentication for heterogeneous mobile cloud networks, this allows mobile device users to migrate from one geographical location to another with intractability. The proposed system uses elliptic curve algorithm cryptography on identity authentication to keep client's identity and location, authentication hidden during authentication process.

According to prior research works of [47] it was put forward that, the combination between anomaly and signature-based detection techniques (termed as hybrid intrusion detection system) incurs high detection and low false positive rates. However, deployment of an anomaly detection over IoT devices that are generally resource-constraints invariably generates high energy consumption due to the computational cost leading to a rapid decrease of the network lifetime. This was further reaffirmed in the work of [47] and stressed the need for researchers to look towards the direction of developing lightweight intrusion detection systems that can be deployed on such resource constraints IoT devices for enhanced security.

Years later [47] argued that, resources' constrained tiny sensors and devices in the Internet of Things (IoT) could be connected to unreliable and untrusted networks. Nevertheless, securing IoT technology is obligatory, due to the relevant and sensitive data handled by such devices. The researchers gleaned that Intrusion Detection System (IDS) is the most efficient technique to detect the attackers with a high accuracy when cryptography is broken. This can successfully be achieved by hybridizing anomaly and signature detection, which are high detection and low false positive rates, in order to take the strengths of both and eliminate their weaknesses respectively. To achieve a high detection rate according to the researchers, the anomaly detection technique relies on a learning algorithm to model the normal behaviour of a node and when a new attack pattern (often known as signature) is detected, it will be modelled with a set of rules. This latter is used by the signature detection technique for attack confirmation. They however, argued that, the deployment of anomaly detection on resource constraints IoT devices could generate a high-energy consumption, specifically when this technique is activated all the time.

To this regard, [48] proposed a lightweight anomaly detection technique based on game theory concept. With the help of Nash equilibrium, the researchers predicted the equilibrium state that allows the IDS agent to enable its anomaly detection technique to detect new attack's signature. They analysed the performance and demonstrated the viability of their proposed approach under WSN, using TOSSIM simulator. According to their simulation results, they proved that the proposed lightweight anomaly detection approach requires a low energy consumption to achieve a high security level, i.e. high detection and low false positive rates. This is unlike the current anomaly detection techniques that require a high energy to exhibit a high detection rate since these detection techniques are activated at each node in a permanent fashion (i.e. does not switch to idle time). They further recommended future direction to embed their proposed lightweight anomaly detection technique unto a large-scale IoT devices to improve the accuracy detection, energy consumption and network delay.

Furthermore, [49] proposed a cross domain dynamic anonymous Authenticated group key management system with symptom-matching (CD-AGKMS) in e-health social systems enabling different patients establish sessions securely without interference. [50] proposed a handover authentication for mobile wireless Network (MWN) and presented a protocol using the Identity based public key cryptography with high level of security.

Also, [51] proposed a hybrid filtrations recommendation system based on privacy preserving in edge computing (HFRS-PP) which can prevent users' private information from leaking through the merits of edge computing processing and also ensure real time, accuracy and stability of the query results. They proposed a privacy-preserving recommendation algorithm to obtain users desired results through hybrid filtration.

Additionally, [11] in their research work titled: Identification of malicious edge devices in fog computing environments, proposed in their article titled a framework using three different mechanisms, a Markov model, an intrusion detection system (IDS), and a virtual honeypot device (VHD) to identify malicious edge devices in a fog computing environment. The framework works by categorizing edge devices effectively into four different levels, store and maintain a log repository of all identified malicious devices, which assists the system to defend itself from any unknown attacks in the future. The proposed model is tested in a simulated environment, and results indicate the effectiveness of the system. The proposed model is successful in identifying the malicious device as well as reducing the false IDS alarm rate. They provided illustration of DDoS attack strategies that sufficiently covers all of the phases involved in DDoS attacks. Presented also defense technique that effectively addresses DDoS attacks for both important prevention and mitigation techniques. Their work equally included recent attack types as well as research works on DDoS defense, presenting the current state of the art of DDoS research. The proposed model is tested in a simulated environment, and results indicate the effectiveness of the system. The proposed model is successful in identifying the malicious device as well as reducing the false IDS alarm rate. Furthermore, they were able to outline certain critical challenges identified with the current research and future research directions with justifications, that are all complete agreement with the directions recommended by the work of (Rajinder, *et. al* 2018).

Recently, [52] in their work titled: A Cybersecurity Framework to Identify Malicious Edge Device in Fog Computing and Cloud-of-Things Environments, proposed a cybersecurity framework encompassing three novel mechanisms: Hidden Markov Model (HMM), Intrusion Detection System (IDS) and Virtual Honeypot Device (VHD), just as in the work of Sandhu, R., et. al. (2017) to identify malicious edge device in fog computing environment. A two-stage Hidden Markov Model is used to effectively categorize edge devices in four different levels: Legitimate Device (LD), Sensitive Device (SD), Under-attack Device (UD) and Hacked Device (HD). VHD is designed to store and maintain log repository of all identified malicious devices which in turn assist the system to defend itself from any unknown attacks in the future. The proposed cybersecurity framework is tested with real attacks in virtual environment created using Openstacks and Microsoft Azure in contrast to the work Amandeep, *et. al*. (2017). The proposed framework, according their expectation, should be able to handle all issues of edge device attacks and also be capable of reverting back LD from the VHD. They succeeded in presenting the functionality comparison of the proposed framework with other insider security frameworks in tabular form to validate their proposed framework. Their framework equally reaffirmed that with the IoT and fog computing coming into the market, detection of malicious edge devices and IoT devices is one of the key challenges in their successful adoption. From their framework, it can be inferred that, the key point of the proposed security framework is the effective classification of edge devices based on the frequency and severity of attacks. Whereas, the VHD is a novel concept proposed in their research work, to provide a hacked device with the decoy of a real environment and make the system more adaptive. The VHD will provide attack log files and paths so that similar kinds of attacks can be prevented in the future. Simulated evaluation and experimental results suggest the applicability of the proposed framework in a fog computing environment. They finally recommended for future work to look into the designing of an effective framework for the VHD to deal with the transferred HD on it. Suggesting that, different Markov models can be designed for the VHD to deal with hacked devices more effectively.

Similarly, [53] presented a survey on edge computing-based designs for IoT security, Digital Communications and Networks Pervasive IoT applications enabled them to perceived, analyzed, controlled, and optimized the traditional physical systems. It was established in their survey that, security breaches in many IoT applications indicate that IoT applications may put the physical systems at risk. Severe resource constraints and insufficient security design are two major causes of many security problems in IoT applications. As an extension of the Cloud, the emerging edge computing with rich resources provides us a new venue to design and deploy novel security solutions for IoT applications. Although there are some research efforts in this research direction, edge-based security designs for IoT applications are still in its infancy. There review is aimed at presenting a comprehensive survey of existing IoT security solutions at the edge layer as well as to inspire more edge-based IoT security designs. The first presented an edge-centric IoT architecture. They extensively reviewed edge-based IoT security research efforts in the context of security architecture designs, firewalls, intrusion detection systems, authentication and authorization protocols, and privacy-preserving mechanisms. Finally, proposed insight of future research directions and open research issues. They finally established that, in recent years, the challenge of securing IoT systems has sparked tremendous research interests. Yet it remains a significant challenge. Emerging edge computing has resulted in many novel edge-based securities designs for IoT security. According to their findings, the existing solutions so far, cover the most important topics in IoT security, including comprehensive security architecture, firewalls, intrusion detection systems, authentication and authorization mechanisms, as well as privacy-preserving designs. Furthermore, the researchers have identified a set of challenges in the field and outlined a list of research directions as: They observed that the research in this direction is still in its early age. There are still many challenging issues to be addressed. Outlined a set of open research issues that include securing the edge layer, dealing with untrusted edge layer, data quality for security, distributed and cross-domain machine learning algorithms for IoT security, safety simulation and response mechanisms, lightweight protocols for end device-edge communications, as well as secure operating systems and lightweight virtual machines.

More recently, [54] in their survey on intrusion detection at the edge of a network established that Fog Computing, that consists of moving the computation services geographically close to where computing is needed. This architectural shift moves security and privacy issues from the Cloud to the different layers of the Fog architecture. In this scenario, IDSs are still necessary, but they need to be contextualized in the new architecture. Indeed, while on the one hand Fog computing provides intrinsic benefits (e.g., low latency), on the other hand, it introduces new design challenges. Since the Fog computing network architecture brings the typical services offered by Cloud computing closer to the end-user, most of its security and privacy issues are inherited from the Cloud itself. These problems include, but not limited to, Distributed Denial of Service (DDoS) attacks, Man in the Middle (MitM) attacks, rogue gateway attacks, privacy leakage, privilege escalation attacks, service manipulation attacks, and injection of information. However, although the problems are the same in Fog computing, they should be contextualized in the new physical and logical elements of the Fog computing network architecture.

Moreover, [2] in their work titled: Security and Privacy Issues in Cloud, Fog and Edge Computing confirmed that Internet of Things (IoT) is an ever-growing field. Increase in data and data generating devices invariably necessitated the move from traditional computing techniques to new powerful techniques. Fog and edge computing have started replacing traditional cloud computing for the computation of data from IoT devices. However, with a myriad of data coming shortly soon, there is strong likelihood to discover new computation techniques, but keeping in mind the security and privacy of the user data first before anything else. They opined that, in the near future, fog and edge computing paradigms should take over all other traditional cloud computing as much as possible. They equally recommended that more research works should be geared towards concepts and techniques to reduce the latency and the bandwidth requirement even further without compromising with the security of the system and that system should work autonomously after setting it up initially with all the requirements.

Similarly, in the novel work of [55] which by standard is one of the state of the arts surveys titled: Security challenges in fog-computing environment: a systematic appraisal of current developments, discussed in details various techniques, with most popular security protection and the taxonomy created, based on the security mechanisms found in the fog-computing related literatures. The trend of publication and the future trend of publication are also discussed. They affirmed that, Decoy technique is quite effective in addressing authentication and account hijacking, Markov's model is effective in prediction for detection of malicious edge devices in fog-computing environment, whereas, block chain technique addresses authentication problem and also reduces delay time, while DDoS can effectively be managed by situational awareness mechanism combined with trust management services The trend of publication with respect to the authors, the range of time, and the most recent publications were equally presented. The paper clearly and sufficiently presented a systematic review on security challenges in fog computing. The review discussed and summarized various techniques applied to solve the security problems within the fog-computing environment alongside their major drawbacks. The study established that, most of the security techniques that were applied by various researchers are somewhat, not dynamic and robust enough to completely address all the fog security problems. In addition, they review confirmed further that, most of the research in this regard did not follow interdisciplinary approach to arrive at major findings. Rather, the studies mostly focused on particular paradigm. MitM attack, DOS, and identity authentication still constitute major challenges that needed researchers' attention for better solutions. Their review work succeeded in presenting comprehensive analysis of the problems and major research findings. This covers problem addressed, major findings, parameters used, and the limitations of the various techniques employed.

Despite data set availability constituting a major challenge in their research survey, due to the fact that most of the authors did not disclose the data set or parameters used for the research. From their tables of analysis, it can clearly be established that most of the techniques utilised so far could not address all threats noticeable in fog platform. Some security problems were partially addressed, while others were constrained due to the limitations of the proposed techniques. Their work figured out certain challenges that are yet to be resolved in fog computing model and recommended areas of future research as per as fog or edged computing is concerned.

Similarly, [56] both opined that, fog computing is an evolving area of interest in computing that require novel solution concepts from researchers. To this effect, a number of serious research works are currently ongoing to unravel more other benefits of the model that can be tapped for optimal utilization of either fog or edge computing platforms. They identified three (3) basic area of challenges that are yet to be resolved in the fog computing paradigms, despite researchers' attempt in this direction, and these are: Man-in-the-Middle (MitM) Attack, Distributed Denial of Service (DDoS) and Identity Authentication respectively.

Moreover, in the work of [57] titled: Intrusion Detection at the Network Edge: Solutions, Limitations and Future Directions established that, since the Fog computing network paradigm migrates the typical services offered by cloud computing locations geographically closer to the end-user, most of its security and privacy issues are invariably inherited from the cloud itself. These problems include, but not limited to, Distributed Denial of Service (DDoS) attacks, Man in the Middle (MitM) attacks, Rogue Gateway Attacks, Privacy Leakage, Privilege Escalation Attacks, Service Manipulation Attacks and Injection of Information. They further stressed that, however, although the problems are the same in Fog computing as in the cloud, the mother architecture, they should be contextualized in the new physical and logical elements of the Fog or edge computing network platforms. According to them also, several systems such as Cloud, SCADA and Smart Grid rely on IDSs as the first line of defense against malicious attacks such as DDoS, Insider, Man in the Middle and scanning attacks respectively. For this reason and more, after the introduction of the Fog and edge computing network platforms, a new line of research started studying the adoption of such IDSs for such security breaches within these network platforms. Since the viability of such IDSs is strongly determined by the tiers in which it is deployed, to amplify the level of security mechanism of such IDSs, they should be deployed on every tier of the architecture in order to obtain a secure system with minimal security threats. However, they confirmed in their study that, this choice brings new challenges onboard that need to be addressed.

In this regard, **[58]** established that novel solutions were proposed and designed by researchers and implemented to address the security challenges so far identified with the fog, edge of IoT environments They were however, unanimous in justifiably buttressing that, most of the solutions did not focus on solving other important challenges, such as the development of lightweight IDSs able to work within resource-constrained devices, the false-alarm control, the reduction of false positive/negative number, Port Scanning and the DDoS attack protection. Furthermore, [58] categorically stated that Tier 1 of either fog or edge computing platforms typically comprises of resource-constrained devices, with a limited amount of energy, storage as well as computational capability. These restrictions make the deployment of IDSs solutions within this tier quite challenging.

In the work of [59] it was established that, due the ever-growing need of end users to offload data to the MEC server under privacy and security protection to avoid outflow of certain sensitive data and information is an urgent challenge to be addressed by novel and emerging researchers in the field of computing. Furthermore, there study reveals that surroundings with extremely variable network edges also produces susceptibility in the network that can be compromised. Therefore, demands of privacy protection platforms to process edge data comes into focus.

More recently, [60] affirmed that SaaS as one of the service models of the cloud computing models have been exploding in popularity owing to ease of deployment, utilization as well as maintenance, with in turn raises the issue of security of such applications. To this effect, cyber security expert teams are battling to keep pace with emerging list of applications utilized within their domains as with the processes of tracking the data and information the applications generate, process and store. Attackers have been taking advantage of these vulnerability and visibility gaps to launch attacks that are detrimental to the safety and privacy of SaaS applications on regular basis. This necessitates the urgent need for researchers to employ anomaly detection techniques to detect, track and respond to such attacks. The summary of related work by title, method, problem and solution concept is presented in Table 2.

Table 2: Summary of Cybersecurity models against the insider attack

S/N	Authors/Year	Title of Research	Proposed Technique	Solution	Problem	Proposed Solution
01	[33]	An ontology for insider threat indicators development and applications	They used semantic ontology approach to detect the malicious insider user from large pool of users.	The framework is found to be effective for workflow-based analysis and incident escalation process	The evaluation of specific instances of indicators requires expert analysis and investigation to remove false positives,	Provide enhanced support for behavioral components of potential indicators of malicious insider activity
02	[61]	Xen-based virtual honeypot system for smart device	Proposed a lightweight Xen-based virtual honeynet to capture intruder behavior and malicious data for smart devices	The framework is effective in detecting a highly controllable attack or decoy for the security analysis of a network	Even though the honeypot is hidden, it is implemented as static which implies that, over time, it is likely that the position of the VHD may be identified and thus, be bye passed by the attackers	Consider the deployment of a Virtual Honeypot whose position changes dynamically from one point to another in order to avoid to continuously elude attacks
03	[62]	Intrusion Detection and Prevention System for Cloud Simulation Environment using Hidden Markov Model and MD5	proposed new security architecture for cloud computing platform to secure communication system and hiding information from others by authentication using shared secret key MD5 and provides security using Hidden Markov Model	The framework was effective in providing authentication from unauthorized user and security for authorized users who store their data in Cloud Data center and some authorized users that try to misuse secure data	HMM cannot capture long-distance relationship interaction and therefore, the proposed framework may not be efficient for such interactions	Although the intrusion detection using HMM provides efficient results but further enhancements can be done to make effective for long-distance relationship interaction in the cloud computing when the data is stored in the data centers
04	[15]	Detecting insider threat based on document access behavior analysis	They proposed a framework which uses user's current behavior, his/her past behavior and his/her community behavior to detect anomaly in any user activity.	According to their experimental test results, the proposed model successfully detects anomaly access to files in the internal systems	The framework is designed to only to detect intrusion based on anomaly neglected other two (2) major forms of intrusions i.e. Misuse-based and Network-based Intrusions	The limitation of this framework can be enhanced by deploying a hybrid Intrusion Detection System that is capable of detecting more than one form of intrusion into a system

					respectively	
04	[63]	Quantitative prediction of the effect of genetic variation using hidden Markov models	They proposed a quantitative prediction method, HMM variation (HMMvar), to predict the effect of genetic variation, both indels and SNPs, using hidden Markov models	Results show that HMMvar achieved good performance in identifying deleterious or neutral variants for different datasets, and effectively predicts protein functional effects of both single and multiple mutations	HMMvar designed cannot capture long-distance relationship interaction and therefore, the proposed framework may not be efficient for such interactions	Consider other forms of sequential supervised machine learning algorithms that can capture long-distance relationship interactions, such as MEHMM, Input/Output HMM etc.
	[35]	Automatic and Scalable Fault Detection for Mobile Applications				
05	[34]	Analyzing user behavior using keystroke dynamics to protect cloud from malicious insiders	The proposed approach uses SVM to design a host-based user profiling technique where a key stroke and a retraining mechanism for analyzing user behavior and as the imposter patterns are absent at the time of registration in order to detect and mitigate insider attacks	The proposed work shows better results in mitigating the insider threat in the presence of a masquerader and as well as provides authentication to user considering non static biometrics and thus, suitable for the cloud environment	The proposed system considered only non-static biometrics and uses Support Vector machine (SVM) which is a binary classifier and therefore, not suitable for static biometrics and situations that require multi-class classification	The efficiency of the proposed approach can be enhanced by integrating it with the other behavioral techniques like search and command sequence analysis that can learn from both static and non-static biometrics and multi-class classifiers
06	[35]	A hybrid protocol to secure the cloud from insider threats	They proposed a hybrid approach for preventing insider attack in cloud by using multiple technologies i.e. selective encryption for data encryption, neural network to create profile of users and decoy technology for concealing	The proposed framework effectively combats the insider threat resulting into an unprecedented level of security for sensitive data/information in cloud environment	Cryptography algorithms generally increase the information density of data blocks and consequently handicap the existing lifetime enhancement	Consider other security mechanisms that do not increase information density that improves on the existing shorter lifetime and security enhancement solutions

			sensitive information		solutions	
07	[64]	Online Risk Assessment and Prediction Models for Autonomic Cloud Intrusion Prevention Systems	Proposed framework integrated Early Warnings about future ongoing attacks, Autonomic Prevention Actions and Risk Measure to their Autonomic Cloud Intrusion Detection Framework (ACIDF) for Risk Assessments While HMM is deployed for potential Attacks Prediction in Cloud Computing environment	The practical implementation of both the prediction and risk models proved promising results. The proposed prediction model has successfully fired the early warning alerts before the launching of the LLDDoS1.0 attack by 39 minutes and 37 seconds and by 64 minutes and 42 seconds before the detection phase starts.	HMM is generally requires very large training sample which is very difficult in case of attack prediction because of the few attack tracks available in the available datasets. Also, the controller decision making does not effectively consider goals of attacks and the possible spread of the intrusion	The major drawback of the model can be addressed by modifying the HMM to build a Variable Order Markov Mode (VMM) which can model sequential data of considerable complexity that can be computed independently for each attack, whereas, the controller decision making could be further enhanced through both the detection and prediction outcomes to consider the goals of the attack and the possible spread of intrusion
08	[65]	Detection of Distributed Denial of Service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems	Proposed a DDoS detection and mitigation system using hybrid Neuro-Fuzzy systems which is Adaptive and Incremental Learning Classifier, Less Computational complexity, and accurate decision making from uncertain information.	Results showed that, NFBoost classification algorithm results in high detection accuracy that outperforms the other existing Neural Networks algorithms and provides an efficient False-Positive reduction	Accommodate several types of inputs including vague, distorted or imprecise data and needs to be reprogram in case the feedback sensor stops working	Consider other Machine Learning Algorithms that do not accommodate vague, distorted or imprecise data and do not require reprogram in case the feedback sensor stops working
09	[66]	A Fast Algorithm for HMM Training using Game Theory for Phoneme Recognition	Proposed a game-theoretic approach for Hidden Markov Model training was used which is superior in terms of time-complexity over Baum-Welch algorithm is introduced.	Results show that the proposed algorithm converges faster than Baum-Welch algorithm and the accuracy of recognition using the proposed training algorithm is comparable with that of the Baum-Welch algorithm	HMMs lack the ability to capture long-distance relationship interaction and therefore, the proposed framework may not be efficient for such interactions	Consider other forms of sequential supervised machine learning algorithms that are suitable to capture long-distance relationship interactions, such as MEHMM, Input/Output HMM etc.

10	[3]	Friend or Foe? Detecting and Isolating Malicious Nodes in Mobile Edge Computing Platforms	Proposed HoneyBots, a novel defense technique for malicious device to device (d2d) communication. It consists of detecting, tracking, and isolating malicious activity in a d2d disconnected opportunistic network such as MobiBots	The proposed model was found to be successful in detecting, tracking, and isolating malicious activity in a d2d disconnected opportunistic network such as MobiBots	The proposed solution however, is identified with False Alarm Rate which may render the framework inefficient	Integration with a suitable sequential machine Learning model that can be able to predict and classify devices based on certain attributes to address False Alarm Rate
11	[67]	HMM-based Intrusion Detection System for Software Defined Networking	Proposed HMM based Intrusion detection system integrated with a Network Intrusion Detection Systems (NIDS) that can work very well with SDN networks for overall security of a network by analyzing the network as a whole and making choices to defend the network based on data from the entire network.	The proposed system improves, greatly the efficiency of security applications as the security filters, monitoring systems and the application adapts to the increase in the number of networking devices	The proposed system only considered NIDS neglecting other forms of system intrusions which invariably makes them go undetected	the efficacy of this system can be improved by streamlining the training sets used. By constantly updating the model with data of different network attacks and consider integrating the system with a Hybrid Intrusion Detection System.
12	[68]	A New Take on Detecting Insider Threats: Exploring the use of Hidden Markov Models	The researchers used Hidden Markov Models to learn a user's normal behavior in order to identify deviations from it, which may be indicative of a threat (or at least behavior worth following-up).	Their results show that the proposed approach is indeed successful at detecting insider threats, and in particular is able to accurately learn a user's behaviour and provide a useful approach in addressing this part of the insider-threat challenges	HMMs lack the ability to capture long-distance relationship interaction and therefore, the proposed framework may not be efficient for such interactions	Consider replacing the HMM with a more complex model such in order to learn a richer representation of a user's behaviour using longer term dependencies in order make a more informed decision about the current action a user might take.
13	[69]	Forecasting distributed denial of service attack using Hidden Markov Model	Proposed a HMM based method for forecasting DDoS attacks using the inherent characteristic features of DDoS to determine the observable states of the system. Kullback-	The performance of the proposed method was empirically measured using the DARPA 2000 data set. The framework was	HMMs lack the ability to capture long-distance relationship interaction and therefore, the proposed framework	Consider other forms of sequential supervised machine learning algorithms that are suitable to capture long-distance relationship interactions, such as MEHMM,

			Leibler divergence algorithm was employed to avoid intractable computations, in order to reduce the number of observable states to three.	effective in using features of the DDoS attack as observable states of an HMM to successfully predict attack in a network	may not be efficient for such interactions	Input/Output HMM etc.
14	[70]	Distributed Network Intrusion Detection System: An Artificial Immune System Approach	Proposed a framework for a distributed network intrusion detection system (dNIDS) based on the artificial immune system concept	The framework was effective in distributing NIDS among connected network segments, to identify potential threats individually and enables sharing of identified threat vectors between the communicating distributed NIDSs	The proposed system only considered NIDS neglecting other forms of system intrusions which invariably makes them go undetected	Consider expanding on this area further by implementing a fully distributed NIDS that that uses both the Self-Nonself model and algorithms for other forms of Intrusions detection to facilitate intercommunication
15	[71]	Intrusion Detection Using Secured and Efficient Data Mining	Proposed an Intruder detection system using Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features.	The proposed system was effective in detecting and mitigating device intrusion and DoS type of attacks based on the results obtained	The framework takes time to analyze network traffic in order to identify and detect intrusion when large volume of dataset is used	This framework can further be enhanced extending it in order to Reduce the processing time when large amount of dataset is provided.
16	[22]	Hidden Markov models for advanced persistent threats	They describe a Stochastic model for the evolution of an Advanced Persistent Threat (APT) based on hidden Markov models (HMM) and is accompanied by a score.	The approach effectively validates whether the evolution of the partially reconstructed attack campaigns are indeed consistent with the evolution of an APT. it is thus, suitable in taking into account the inevitable presence of undetected	HMMvar designed cannot capture long-distance relationship interaction and therefore, the proposed framework may not be efficient for such interactions	Consider other forms of sequential supervised machine learning algorithms that can capture long-distance relationship interactions, such as MEHMM, Input/Output HMM etc.

				attacks in the attack campaigns.		
17	[72]	Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems	Modelled a threads detection system that incorporates a novel real-time threat detector with an adaptive risk assessment methodology to ensure unabridged threat mitigation during the deployment of devices using Cumulative Distribution Functions (CDFs) to model normal device behavior	The framework was successful by dynamically detecting and assessing risk, subsequently taking automated mitigative actions when the risk is elevated to ensure safety, security, and privacy in the presence of unknown security threats, devices with reduced false-positive rate	The probabilistic threat detector (CDF) is used to assess and manage the system's risk, which results in a precise real-time update of the current system risk Thus, may not cope with long-distance relationship interaction	Consider replacing the CDF with a more complex model such in order to learn a richer representation of a user's behaviour using longer term dependencies in order make a more informed decision about the current action a user might take.
18	Sandhu et al 2017	Identification of malicious edge devices in fog computing environments.	They proposed a security framework using three technologies: Markov Model, Intrusion Detection System (IDS) and Virtual Honeypot Device (VHD) to identify malicious edge device in fog computing environment	The proposed model is tested in a simulated environment, and results obtained indicate the effectiveness of the system. The proposed model is successful in identifying the malicious device as well as reducing the false IDS alarm rate	The proposed solution however, did not consider DDoS attacks and as well attacked device recovery which may invariably render the framework inefficient	Consider improving the VHD with a suitable DDoS prevention & mitigation mechanism and tracking heuristics & algorithms to be able to prevent & mitigate DDoS attacks as well as detects, tracks, isolates & blocks attack paths to recover attacked devices
19	[52]	A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments.	Proposed a Cybersecurity Framework which uses three technologies: Markov Model, Intrusion Detection System (IDS) and Virtual Honeypot Device (VHD) to identify malicious edge device in fog computing environment.	Proposed cybersecurity framework is tested with real attacks in virtual environment created using Openstack and Microsoft Azure. Results indicated that proposed cybersecurity framework is successful in identifying the malicious device as well as	The proposed solution neglects DDoS prevention & mitigation mechanisms and as well, attacked device recovery which may invariably render the framework inefficient	Consider integration with Large Scale Ethical Hacking or improve on the VHD with a suitable DDoS prevention & mitigation mechanism and tracking heuristics & algorithms to be able to prevent & mitigate DDoS attacks as well as detects, tracks, isolates & blocks attack paths to recover attacked

				reducing the false IDS alarm rate.		devices
20	[73]	A Hybrid-Optimizer-Enhanced Neural Network Method for the Security Vulnerability Study of Multiplexer Arbiter PUFs	Proposed a Multiplexer based PUF (MPUF) in order to improve upon the reliability while maintaining a similar resistance to Machine Learning (ML) attacks on Internet of Things (IoT) Environment to enhance the predictive power of NN as PUF attack methods	Experimental results have shown that the proposed solution converges faster than a traditional NN with a single optimizer on attacking MPUFs, and requires less training data as compared with a recent NN-based attack study of MPUFs.	The proposed solution ignored DDoS attacks which is one of the major challenges in the IoT environments and Attacked Device Recovery	The proposed solution can be enhanced by integration with DDoS prevention & mitigation mechanisms such as Classical Honeypot as well as Tracking Heuristics & Algorithms

From the above table, it can be deduced that, a lot of security frameworks to protect systems from unauthenticated and unauthorised device (also known as outsider and insider) attacks respectively have been proposed by researchers and explored by IT organisations. However, most of the solutions did not focus on solving other important challenges, such as the false-alarm rate, the DDoS attack, attacked devices recovery and development of lightweight IDSs able to work within resource-constrained devices [12]. For instance, a cyber-security framework proposed by [3]was found to be successful in detecting, tracking and isolating malicious insider attacks, and as well isolating Distributed Denial of Service (DDoS) attacks, but failed to address dynamically preventing & mitigating DDoS, false alarm rate and create a log repository of all identified malicious devices which assists the system to defend itself from any unknown attacks in the future which may likely render the security frame work ineffective. Another framework by both [11] and [52] proposed another model using three distinctive technologies that were tested in different platforms and found to be successful in identifying malicious device as well as reducing false IDS alarm rate, but could not prevent & mitigate DDoS, effectively deal with malicious edge devices sent to VHD for recovery back to their initial states or isolate Distributed Denial of Service (DDoS). Similarly, [74] proposed a Lightweight Perceptron-based Intrusion Detection System for Fog Computing. The model proposed can be deployed favorably on any of the three tiers of the fog or edge computing architecture, but failed to assist the system defend its self from unknown potential future attacks, reduce false alarm rate or recover hacked devices from attacks.

Having carefully reviewed some related literature of cyber security frameworks up to this stage, we proposed an improved cyber security frame work that addresses unauthorized attacks detects, tracks and isolates attacks, dynamically prevents & mitigates Distributed Denial of Service (DDoS) and recovers attacked devices back to their initial states system to complement the models of [3] and as presented in the table 2 below:

Table 2: Comparison of the proposed solution with the existing based solutions

	Challenges				**Deployment**	
S/N	**Year**	**DDoS**	**FA**	**DR**	**Static**	**Dynamic**
01	2015	√	X	√	√	X
02	2017	X	√	X	X	√
03	2018	X	√	X	X	√
04	2021	√	√	√	X	√

3. DISCUSSIONS CHALLENGES AND OPEN OPPORTUNITIES

From the foregoing, it can justifiably be deduced that, despite the efforts explicitly put forward by researchers towards addressing challenges identified with the fog or edge computing models, much is equally desired due to the fact that, there are still key security issues that are yet to be effectively addressed. Thus, signifies the urgent need for researchers to propose in earnest, improved cyber security frameworks capable of mitigating such uncovered challenges in order to make these computing models secure for both the end users and service providers. Based on the review of related literature to this stage, the challenges that are yet to be addressed include the followings: -

1. Man-in the-middle (MitM) Attack: This remains a problem that is yet to be resolved in fog and edge computing platforms. Fog or edge devices within the environment are usually out of surveillance, such that attackers can easily interject and reply the communication. Encryption and decryption method is not suitable to counter the MitM attacks because of high consumption of battery power especially in mobile phones that use high speed data transmission channels. Though the previous research shows that it consumes small amount of network resources, the threats very are difficult to be addressed.
2. Distributed Denial of Service (DDoS): DDoS is a type of network attack that blocks the legitimate users to have access to fog, edge or cloud resources. Intrusion detection is the usual recommended method for detecting and mitigating this challenge. However, in fog environment, there is no known solution available that can handle DDOS issues effectively at present.
3. Identity Authentication: There are many authentication schemes that have been proposed and developed for internet services, e.g., fingerprint, face recognition, and facial (Irish) recognition. IoT devices mobility is a necessary factor to be considered, because user of fog computing may move from one coverage area to another. Each of the nodes authenticates the users when accessing services. However, when the users increase in number, the latency may not be supported in real time. Even though cooperative authentication schemes are used to reduce authentication overhead, it is therefore, necessary to design and implement authentication schemes that effectively support Fog nodes to confirm users' identifications before offering services.
4. Port Scanning: A port scanning is a method for determining which ports on a network are open. As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home. ... It is also valuable for testing network security and the strength of the system's firewall. A port scanner sends a network request to connect to a specific TCP or UDP port on a computer and records the response.

4. CONCLUSIONS

The main purpose of this study to investigate the existing cybersecurity frameworks and identify their weaknesses for improvement. From the survey, it can justifiably conclude that, despite the efforts explicitly put forward by researchers towards addressing challenges identified with the fog or edge computing models, much is equally desired due to the fact that, there are still key security issues that are yet to be effectively addressed. Thus, signifies the urgent need for researchers to propose in earnest, improved cyber security frameworks capable of mitigating such uncovered challenges in order to make these computing models secure for both the end users and service providers.

5. ACKNOWLEDGEMENT

We wish to thank our research supervisors Ass. Prof. A.Y Gital, Dr. Fatima Umar Zambuk and Dr. K. I. Musa for their immense contribution and academic guidance towards the success of this research work.

6. REFERENCES

1. Chen, Z., et al. *Early implementation experience with wearable cognitive assistance applications*. in *Proceedings of the 2015 workshop on Wearable Systems and Applications*. 2015.
2. Parikh, S., et al., *Security and privacy issues in cloud, fog and edge computing.* Procedia Computer Science, 2019. **160**: p. 734-739.
3. Mtibaa, A., K. Harras, and H. Alnuweiri. *Friend or foe? Detecting and isolating malicious nodes in mobile edge computing platforms*. in *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*. 2015. IEEE.

4. Amandeep, T.S. and Y. Kumar, *Data Transmission in Clouds Using Heed and Energy-Efficient Routing Algorithm.* Cognitive Informatics and Soft Computing: Proceeding of CISC 2021: p. 27.
5. Anoop, S. and J. Singh, *Multi-user energy efficient secured framework with dynamic resource allocation policy for mobile edge network computing.* Journal of Ambient Intelligence and Humanized Computing, 2021. **12**(7): p. 7317-7332.
6. Yakubu, J., et al., *Security challenges in fog-computing environment: a systematic appraisal of current developments.* Journal of Reliable Intelligent Environments, 2019. **5**(4): p. 209-233.
7. Eid, M.A., et al., *LAMAIDS: A Lightweight Adaptive Mobile Agent-based Intrusion Detection System.* Int. J. Netw. Secur., 2008. **6**(2): p. 145-157.
8. Arya, D. and M. Dave. *Security-based service broker policy for FOG computing environment*. in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 2017. IEEE.
9. Bilal, K., et al., *Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers.* Computer Networks, 2018. **130**: p. 94-120.
10. Krishnaveni, B., et al., *SECURED AND EFFICIENT CLOUD COMPUTING FRAMEWORK FOR MOBILE.* 2019.
11. Sandhu, R., A.S. Sohal, and S.K. Sood, *Identification of malicious edge devices in fog computing environments.* Information Security Journal: A Global Perspective, 2017. **26**(5): p. 213-228.
12. Raponi, S., M. Caprolu, and R. Di Pietro. *Intrusion detection at the network edge: Solutions, limitations, and future directions*. in *International Conference on Edge Computing*. 2019. Springer.
13. Mao, Y., et al., *A survey on mobile edge computing: The communication perspective.* IEEE communications surveys & tutorials, 2017. **19**(4): p. 2322-2358.
14. Vaquero, L.M. and L. Rodero-Merino, *Finding your way in the fog: Towards a comprehensive definition of fog computing.* ACM SIGCOMM computer communication Review, 2014. **44**(5): p. 27-32.
15. Zhang, R., et al. *Detecting insider threat based on document access behavior analysis*. in *Asia-Pacific Web Conference*. 2014. Springer.
16. Sa’ad, S., et al., *An enhanced discrete symbiotic organism search algorithm for optimal task scheduling in the cloud.* Algorithms, 2021. **14**(7): p. 200.
17. Roman, R., J. Lopez, and M. Mambo, *Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges.* Future Generation Computer Systems, 2018. **78**: p. 680-698.
18. Patel, A., et al., *An intrusion detection and prevention system in cloud computing: A systematic review.* Journal of network and computer applications, 2013. **36**(1): p. 25-41.
19. D’Orazio, C.J., K.-K.R. Choo, and L.T. Yang, *Data exfiltration from Internet of Things devices: iOS devices as case studies.* IEEE Internet of Things Journal, 2016. **4**(2): p. 524-535.
20. Abraham, S. and S. Nair, *Cyber security analytics: a stochastic model for security quantification using absorbing markov chains.* Journal of Communications, 2014. **9**(12): p. 899-907.
21. Lee, L.M. and A.P. Liu, *A microfluidic pipette array for mechanophenotyping of cancer cells and mechanical gating of mechanosensitive channels.* Lab on a Chip, 2015. **15**(1): p. 264-273.
22. Brogi, G., *Real-time detection of Advanced Persistent Threats using Information Flow Tracking and Hidden Markov Models*. 2018, Conservatoire national des arts et metiers-CNAM.
23. Tanaka, H., et al., *Multi-access edge computing: A survey.* Journal of Information Processing, 2018. **26**: p. 87-97.
24. Pan, Z., S. Hariri, and J. Pacheco, *Context aware intrusion detection for building automation systems.* Computers & Security, 2019. **85**: p. 181-201.
25. Bittencourt, L.F., et al. *Towards virtual machine migration in fog computing*. in *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*. 2015. IEEE.
26. Zahra, S., et al., *Fog computing over IoT: A secure deployment and formal verification.* IEEE Access, 2017. **5**: p. 27132-27144.
27. Raj, M., et al., *A survey on the role of Internet of Things for adopting and promoting Agriculture 4.0.* Journal of Network and Computer Applications, 2021. **187**: p. 103107.
28. Bonomi, F., et al. *Fog computing and its role in the internet of things*. in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. 2012.
29. Stojmenovic, I. and S. Wen. *The fog computing paradigm: Scenarios and security issues*. in *2014 federated conference on computer science and information systems*. 2014. IEEE.
30. Wang, Y., T. Uehara, and R. Sasaki. *Fog computing: Issues and challenges in security and forensics*. in *2015 IEEE 39th annual computer software and applications conference*. 2015. IEEE.

31. Madni, S.H.H., et al., *Multi-objective-oriented cuckoo search optimization-based resource scheduling algorithm for clouds.* Arabian Journal for Science and Engineering, 2019. **44**(4): p. 3585-3602.
32. Luan, T.H., et al., *Fog computing: Focusing on mobile users at the edge.* arXiv preprint arXiv:1502.01815, 2015.
33. Costa, D., et al., *An ontology for insider threat indicators development and applications. Pittsburgh*. 2014, PA: Carnegie-Mellon University Software Engineering Institute.
34. Bondada, M.B. and S.M.S. Bhanu. *Analyzing user behavior using keystroke dynamics to protect cloud from malicious insiders*. in *2014 IEEE international conference on cloud computing in emerging markets (CCEM)*. 2014. IEEE.
35. Sriram, M., et al. *A hybrid protocol to secure the cloud from insider threats*. in *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*. 2014. IEEE.
36. Touceda, D.S., et al., *Attribute-based authorization for structured Peer-to-Peer (P2P) networks.* Computer Standards & Interfaces, 2015. **42**: p. 71-83.
37. Choi, H., H. Lee, and H. Kim. *BotGAD: detecting botnets by capturing group activities in network traffic*. in *Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE*. 2009.
38. Traynor, P., et al. *On cellular botnets: measuring the impact of malicious devices on a cellular network core*. in *Proceedings of the 16th ACM conference on Computer and communications security*. 2009.
39. Vural, I. and H.S. Venter. *Using network forensics and artificial intelligence techniques to detect Bot-nets on an organizational network*. in *2010 Seventh International Conference on Information Technology: New Generations*. 2010. IEEE.
40. Eslahi, M., R. Salleh, and N.B. Anuar. *MoBots: A new generation of botnets on mobile devices and networks*. in *2012 International Symposium on Computer Applications and Industrial Electronics (ISCAIE)*. 2012. IEEE.
41. Levine, J., et al. *The use of honeynets to detect exploited systems across large enterprise networks*. in *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.* 2003. IEEE.
42. Spitzner, L., *Honeypots: tracking hackers*. Vol. 1. 2003: Addison-Wesley Reading.
43. Mtibaa, A., K.A. Harras, and H. Alnuweiri. *Malicious attacks in Mobile Device Clouds: A data driven risk assessment*. in *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*. 2014. IEEE.
44. Cavilla, H.A.L., *Flexible Computing with Virtual Machines*. 2009: University of Toronto (Canada).
45. Jin, Y., et al. *A secure and lightweight data access control scheme for mobile cloud computing*. in *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*. 2015. IEEE.
46. Yang, X., X. Huang, and J.K. Liu, *Efficient handover authentication with user anonymity and untraceability for mobile cloud computing.* Future Generation Computer Systems, 2016. **62**: p. 190-195.
47. Sedjelmaci, H., S.M. Senouci, and T. Taleb, *An accurate security game for low-resource IoT devices.* IEEE Transactions on Vehicular Technology, 2017. **66**(10): p. 9381-9393.
48. Sedjelmaci, H., S.M. Senouci, and M. Al-Bahri. *A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology*. in *2016 IEEE international conference on communications (ICC)*. 2016. IEEE.
49. Yang, Y., et al., *Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system.* Future Generation Computer Systems, 2018. **84**: p. 160-176.
50. He, D., et al., *Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation.* Science China Information Sciences, 2017. **60**(5): p. 1-17.
51. Ni, L., et al., *Hybrid filtrations recommendation system based on privacy preserving in edge computing.* Procedia Computer Science, 2018. **129**: p. 407-409.
52. Sohal, A.S., et al., *A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments.* Computers & Security, 2018. **74**: p. 340-354.
53. Sha, K., et al., *A survey of edge computing-based designs for IoT security.* Digital Communications and Networks, 2020. **6**(2): p. 195-202.
54. Della Valle, E., et al., *Worksite energy cost assessment in non-surgical versus surgical medical residency programs.* The International Journal of Occupational and Environmental Medicine, 2019. **10**(4): p. 216.
55. Yakubu, J., et al., *Security challenges in fog-computing environment: a systematic appraisal of current developments.* Journal of Reliable Intelligent Environments, 2019. **5**: p. 209-233.

56. Arya, D. and M. Dave. *Priority based service broker policy for fog computing environment*. in *Advanced Informatics for Computing Research: First International Conference, ICAICR 2017, Jalandhar, India, March 17–18, 2017, Revised Selected Papers*. 2017. Springer.

57. Raponi, S., M. Caprolu, and R. Di Pietro. *Intrusion detection at the network edge: Solutions, limitations, and future directions*. in *Edge Computing–EDGE 2019: Third International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings 3*. 2019. Springer.

58. Caprolu, M., et al. *Edge computing perspectives: architectures, technologies, and open security issues*. in *2019 IEEE International Conference on Edge Computing (EDGE)*. 2019. IEEE.

59. Nischitha, G., et al. *A CNN Based Anomaly Detection System for Real Time Fog Based Application*. in *2021 Asian Conference on Innovation in Technology (ASIANCON)*. 2021. IEEE.

60. Ahmed, M.I., *A Novel Framework to Secure Schema for Data Warehouse in Cloud Computing (Force Encryption Schema Solution)*. 2021, Middle East University.

61. Zhang, W., H. He, and T.-h. Kim, *Xen-based virtual honeypot system for smart device.* Multimedia Tools and Applications, 2015. **74**(19): p. 8541-8558.

62. Banafar, H. and S. Sharma, *Intrusion detection and prevention system for cloud simulation environment using Hidden Markov Model and MD5.* International Journal of Computer Applications, 2014. **90**(19).

63. Liu, M., L.T. Watson, and L. Zhang, *Quantitative prediction of the effect of genetic variation using hidden Markov models.* BMC bioinformatics, 2014. **15**(1): p. 1-10.

64. Kholidy, H.A., et al. *Online risk assessment and prediction models for Autonomic Cloud Intrusion srevention systems*. in *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*. 2014. IEEE.

65. Kumar, P.A.R. and S. Selvakumar, *Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems.* Computer Communications, 2013. **36**(3): p. 303-319.

66. Rekha, J.U., K.S. Chatrapati, and A.V. Babu, *Automatic Speech Segmentation and Recognition using Class-Specific Features.* International Journal of Computer Applications, 2015. **113**(17).

67. Hurley, T., J.E. Perdomo, and A. Perez-Pons. *HMM-based intrusion detection system for software defined networking*. in *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*. 2016. IEEE.

68. Rashid, T., I. Agrafiotis, and J.R. Nurse. *A new take on detecting insider threats: exploring the use of hidden markov models*. in *Proceedings of the 8th ACM CCS International workshop on managing insider security threats*. 2016.

69. Afolorunso, A., et al., *FORECASTING DISTRIBUTED DENIAL OF SERVICE ATTACK USING HIDDEN MARKOV MODEL.* LAUTECH Journal of Engineering and Technology, 2015. **10**(1): p. 41-54.

70. Igbe, O., I. Darwish, and T. Saadawi. *Distributed network intrusion detection systems: An artificial immune system approach*. in *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. 2016. IEEE.

71. Borkar, G.M., et al., *A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept.* Sustainable Computing: Informatics and Systems, 2019. **23**: p. 120-135.

72. Rao, A., et al., *Probabilistic threat detection for risk management in cyber-physical medical systems.* IEEE Software, 2017. **35**(1): p. 38-43.

73. Mursi, K.T., B. Thapaliya, and Y. Zhuang. *A hybrid-optimizer-enhanced neural network method for the security vulnerability study of multiplexer arbiter pufs*. in *Journal of Physics: Conference Series*. 2021. IOP Publishing.

74. Sudqi Khater, B., et al., *A lightweight perceptron-based intrusion detection system for fog computing.* applied sciences, 2019. **9**(1): p. 178.