International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 02, February-2023

An Improved Security Framework For Cyber Malicious Device Detection In Fog Environments

Lamir Isah Muhammad
Department of Mathematical Science
Abubakar Tafawa Balewa University Bauchi,
Nigeria

Fatima Umar Zambuk
Department of Mathematical Science
Abubakar Tafawa Balewa University Bauchi,
Nigeria

Danlami Muhammad
Department of Mathematical Science
Abubakar Tafawa Balewa University Bauchi,
Nigeria

Fatima Shittu
Department of Mathematical Science
Abubakar Tafawa Balewa University Bauchi,
Nigeria

Abdulsalam Ya'u Gital
Department of Mathematical Science
Abubakar Tafawa Balewa University Bauchi,
Nigeria

Kabiru Musa Ibrahim
Department of Mathematical Science
Abubakar Tafawa Balewa University Bauchi,
Nigeria

Mustapha Abdulrahman Lawal
Department of Information Technology
SRM Institute of Science and Tech 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 is to come up with a framework that can improve existing cyber-security models via, first, investigating the existing cybersecurity frameworks and identify their weaknesses for improvement. Secondly, design an effective cyber-security framework that tracks and isolates unauthenticated device attacks and finally evaluate and validate the proposed framework. Experimental results have demonstrated the suitability of the proposed approach in detecting malicious activities in Fog and IoT environment.**

Keywords*— *Hidden Markov Model, Vertibi, HoneyPots, Intrusion Detection, Cyber Attacks and Denial of Service.

I. 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 need 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.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 02, February-2023

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, based on the literature, 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 come up with a framework that can improve existing cyber-security models via, first, investigating the existing cybersecurity frameworks and identify their weaknesses for improvement. Secondly, design an effective cyber-security framework that tracks and isolates unauthenticated device attacks and finally evaluate and validate the proposed framework.

II. LITERATURE REVIEW

The ever increasing demands of data expected by the huge adoption of IoT solutions, and as well coupled with the need for more efficient and effective network performance desired by modern end-user applications, clearly stress how the definitive network Cloud model lacks the ability to efficiently respond to the new and emerging demands and needed [12]. The Cloud model that is centrally deployed but on global scale, provides a scalable infrastructure that relieves users from the costs of designing, purchasing, and maintaining computing and storage resources. However, despite the numerous advantages, this model is not suitable for latency

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 02, February-2023

sensitive applications, that require geographical proximity with the service providers in order to meet their delay requirements[25].

To address this challenge, Cisco researchers deduced and introduced a new network architecture platform, referred to as Fog Computing, that extends the Cloud computing paradigm to the edge of the network, enabling a new variety of applications and services, such as gaming, augmented reality, and real-time video stream processing [26]. Due to this type of architecture, it will automatically improve the quality of service as it will result in reduction of delay while transmitting of data from source to destination This new paradigm provides computational and storage capabilities physically and geographically closer to end users' data generating devices. Among the characteristics of Fog Computing, the most important are: low latency and location awareness; handling of a huge number of nodes; heterogeneity; widespread geographical distribution and most importantly, support for mobile end-devices; support for real-time applications; as well as wireless access.

This technology enables the execution of the data at the edge of the network. Fog computing is rather a perfect complement of many applications and services to eliminate the inadequacies of the cloud. The technology is conceptualized, designed and built upon distributed computing paradigms, such as content delivery networks, that eventually permits the delivery of more complex services, using cloud technologies. Nevertheless, the distinguishing features of fog computing as against the cloud are in proximity to the end user, since they offer processing powers, data storage, and provision of application services to the client.

HMM is a technique is used to learn Markovian processes, those whose probability of being at a given state α at time t depends on being observed at α and the probability of reaching α from another state at t - 1. This means that HMM cannot predict values based on historical data. This inconvenience can be overcome by using a n-order Markov model, but the computational cost may be very high [27].

[11] in their research work proposed 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.

[17] 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[28].

[29] proposed 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 [28] 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 [4]. The proposed framework, according to 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.

However, 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.

[30] surveyed 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

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 02, February-2023

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, they presented 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 the findings in [19], 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.

[31] survey on intrusion detection at the edge of a network and established that Fog Computing 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.

III. RESEARCH FRAMEWORK

This research proposed an improve cyber security system. The framework also introduces the Hidden Markov Models (HMM), IDS and Virtual Honeypot Device (VHD) which is an attempt that greatly improves the work. The framework for the proposed study is depicted in Fig. 1

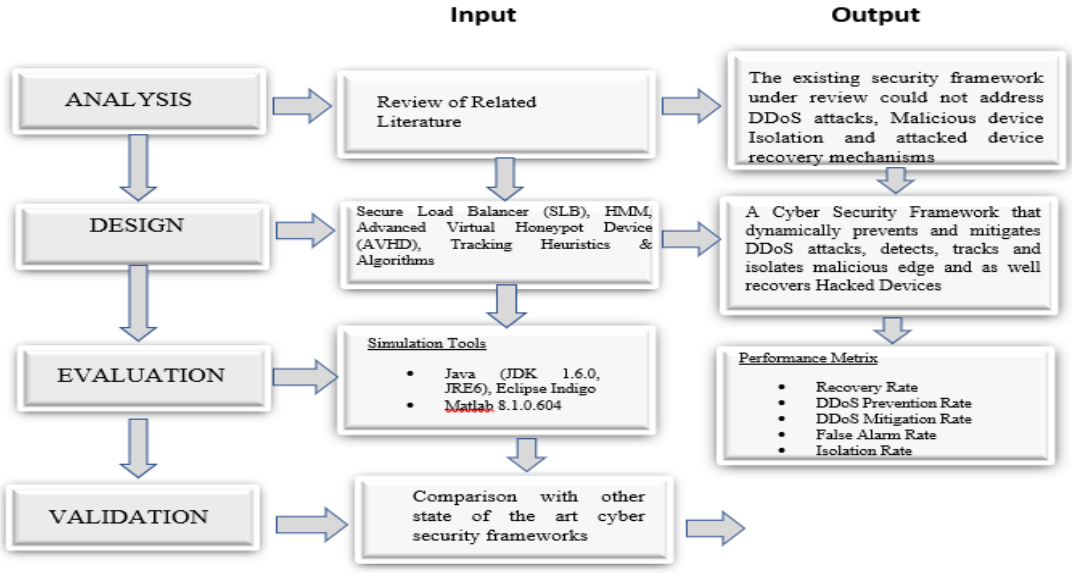

Fig. 1 proposed research framework

There is currently a number of Open Source-based tools that can be used to stress testing of web servers or web services. To test the proposed framework, an Apache based web service has been used because it is easy to create vast number of attacks to be performed on any web service. Also, using different URL and port number the size of total attacks can also be increased drastically so that overall system can be tested exhaustively. The synthetic load and attack generator uses the Pytbull which is a python based flexible IDS/IPS testing framework shipped with more than 300 tests, grouped in 9 modules, covering a large scope of attacks (client-Side Attacks, test Rules, bad Traffic, fragmented Packets, multiple Failed Logins, evasion Techniques, shell Codes, Denial of Service, Pcap Replay, and Internet Protocol Spooling Attack). These requests generated by pytbull can be easily mixed with genuine requests so to test the system with distinction of attacks from the genuine requests. Fig. 2 shows the different requests generated by the load generator.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 02, February-2023

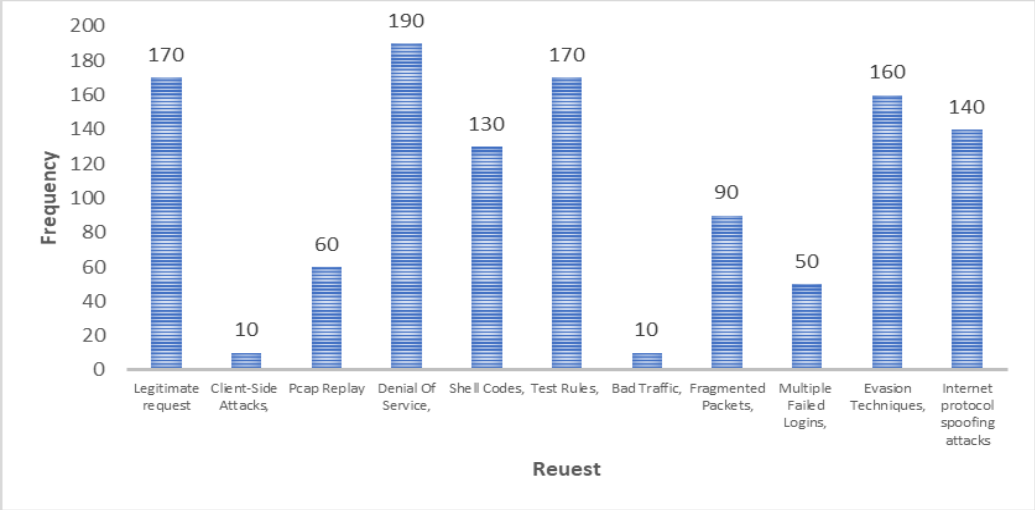

Fig. 2 Number of Request and Attack probability

The total requests generated by the pytbull is emulated on 4 Virtual Machines. This module differentiates the attacks on the basis of the probabilities assigned to them. User requests and attacks generated are stored in a data file which is imported into MATLAB for Markov model predictions. The MATLAB environment is used for simulating the Markov model. Algorithm 1 is implemented in MATLAB for maintaining the transition matrix of each edge device, and on the basis of these matrices, the two-stage Markov model is able to take a decision whether the edge device is to be shifted to the VHD or not. In the graphical representation module, the results of the proposed framework are displayed in the form of a graph.

Algorithm.1 Honey Bot (Hb) Tracking

```
Require: ACTORS = Infected, Cured, Hb
While 1 Do
If Hb receive_msg (j, msg, I, TCP/UDP, PORT) Then
If j == infected, Then
Intrusion detection (i, TCP|UDP,PORT,node)
save (i, TCP|UDP, PORT)
end if
if j == cured then
if msg == purge msg then
suspect ← DeQueue(PATH)
wiat to pronouce(suspect, TTT)
for all binPATH do
if b == suspect then
kill (wait to pronouce(suspect, TTT))
end if
b ← cured
end for
end if
end if
end if
if Hb in contact with j then
if j == infected then
patch (j, i, TCP|UDP, PORT)
cure (j, i, TCP|UDP, PORT)
end (j, purge msg (k, TTT))
j ← cured
end if
if j == cured then
end (j, purge msg (k, TTT))
end if
end if
end while
```

A. *Experimental setup*

The Mendel HMM toolbox of MATLAB is used for simulation of the two stage Markov model The synthetic requests generated by the synthetic load and attack generator module are saved in the data file of our experiment. Hidden Markov models should be trained before they can be used to predict the attack probabilities of edge devices. So, the generated synthetic data file is used by the Mendel HMM toolbox in MATLAB (Models, 2005) to train the hidden Markov model and generate attack probabilities.

For the experimental evaluation, two different devices were created which send different kinds of queries to the simulation system. The difference between the two edge devices is the variation in the attack probabilities, as shown in Fig. 3 Where edge_device1 selected more legitimate queries and edge_device2 selected a greater number of attacks. Selected queries of both edge devices were fed into the HMM toolbox of MATLAB where attack probabilities were generated for both devices for fifteen iterations. as shown in Fig. 3. Edge_device1 showed more variation in attack probability generation, because it performed more attacks on the system.

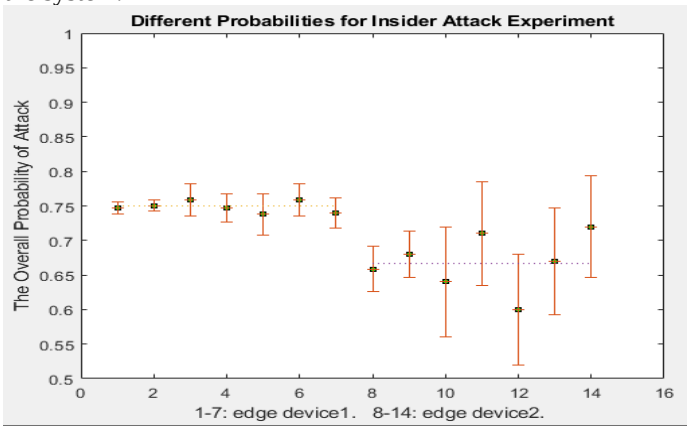

Fig. 3 Overall attack probabilities for both edge devices.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 02, February-2023

IV. RESULT

The key point of the research is the effective classification of edge devices based on the frequency and severity of attacks as shown in Fig. 10 The IVHD is a novel concept proposed in this research to provide a hacked device with the illusion of a real environment and make the system more adaptive to False Alarm Rate, DDoS Detection Rate, Recovery Rate, DDoS Mitigation Rate and Isolation Rate.

In order to evaluate and validate the proposed framework. First, we compare the number of attacks detected by the IDS and the proposed framework with the actual number of attacks on the system. As the IDS treats everything apart from legitimate requests as attack, it generated a very large number of attacks. These attacks, when fed into the trained Markov model calculated the attack probabilities, which removed many false alarms generated by the IDS as shown in Table 1. If we subtract total IDS requests from total Markov model detected attacks, we get the false alarms from the IDS, which are shown in table 2.

TABLE 2 TOTAL NUMBER OF FALSE ALARMS OF IDS DETECTED BY THE SYSTEM

S/No	Number of False Alarm Detected	Times (Min)
1	800	5
2	2000	10
3	2700	15
4	4000	20
5	5000	25
6	5200	30
7	5250	35
8	5432	40

Clearly, from Table 2. the number of false alarms detected increases with increasing time. This result is graphically depicted in Fig. 4

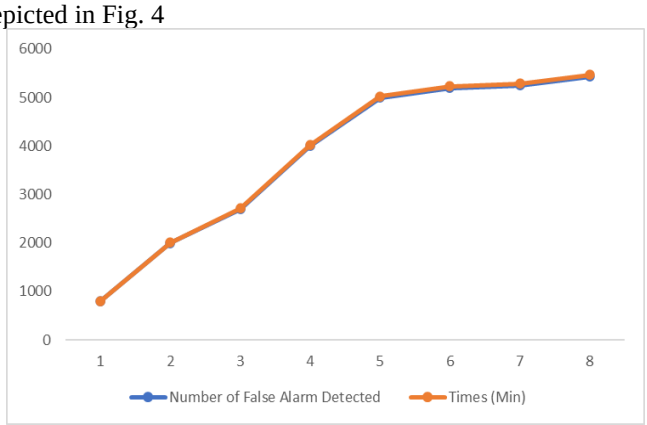

Fig. 4 Total number of false alarms of IDS detected by system

Fig. 4 clearly proves the accuracy of the proposed framework, because actual attacks and Markov model attacks are almost the same throughout the experiment. For the isolation phase which consists of accurately localizing the malicious device inside or outside the network simulation bed. Indeed, localization represents an important step towards isolating malicious nodes. We vary the number of Honeypots deployed in the experiment. We assume that there is only 1 attacker node in each experiment. We repeat the experiment 10 times. In each run, we randomly place the attacker node. We therefore measure the isolation accuracy as the number of times we efficiently locate the attacker in the 10 considered runs. Table 2 Shows the number of times an attack is fully detected and isolated for 10 runs.

TABLE 2 NUMBER OF IVHD AND ISOLATED ATTACKS FOR 10 RUNS

Number of Runs	No of Honey Pot	Percentage of Attack Isolated (%)
1	2	60
2	4	63
3	6	68
4	8	70
5	10	79
6	12	82
7	14	85
8	16	91
9	18	96
10	20	99

Finally, the calculated attack probabilities for both edge devices when multiple types of attack are used is depicted in Fig. 5.

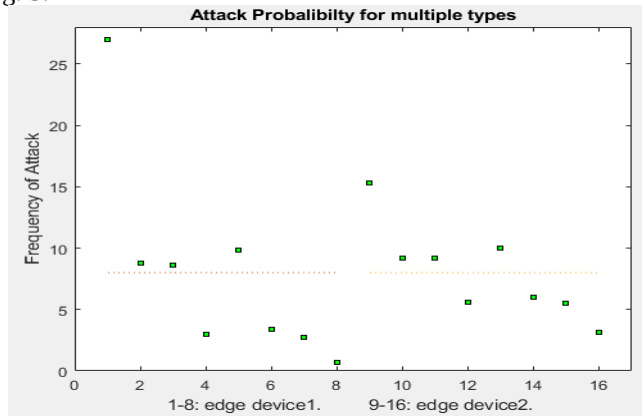

Fig. 5 attack probabilities for both edge devices when multiple types of attack are used.

As represented in Fig.8 depict the calculated attack probabilities for both edge devices when multiple types of attack are used from Mendels HMM tool box. The first edge device has eight (8) different attack probabilities with mean of 0.39, and the second edge device also has eight (8) different overall attack probabilities with mean of 0.4. Edge_device1 provided less variation and attack probabilities than edge_device2. This is because frequency of attack queries of edge_device1 is far less than that of edge_device2. The likelihood of shifting of LD to IVHD based on iteration of attacks performed is computed as shown in

V. CONCLUSION AND FUTURE WORK

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. However, 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

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 02, February-2023

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 is to come up with a framework that can improve existing cyber-security models via, first, investigating the existing cybersecurity frameworks and identify their weaknesses for improvement. Secondly, design an effective cyber-security framework that tracks and isolates unauthenticated device attacks and finally evaluate and validate the proposed framework. Experimental results have demonstrated the suitability of the proposed approach in detecting malicious activities in Fog and IoT environment.

In the future, we will extend by developing a cyber security framework that dynamically prevents and mitigates DDoS attacks, detects, tracks and isolates malicious edge and as well recovers Hacked Devices. The performance matrix will include recovery rate, DDoS prevention rate, DDoS mitigation rate, false alarm rate and isolation rate

ACKNOWLEDGEMENT

We wish to thank research our 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.

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] Saad, M., *Fog computing and its role in the internet of things: Concept, security and privacy issues.* International Journal of Computer Applications, 2018. **180**(32): p. 7-9.
[26] 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.
[27] 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).
[28] Mishra, A. and N. Gupta. *Analysis of cloud computing vulnerability against DDoS*. in *2019 international conference on innovative sustainable computational technologies (CISCT)*. 2019. IEEE.
[29] 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.
[30] Sha, K., et al., *A survey of edge computing-based designs for IoT security.* Digital Communications and Networks, 2020. **6**(2): p. 195-202.
[31] Song, J., J. Wang, and Y.B. Moon. *Blockchain Applications of Manufacturing Systems: A Survey*. in *ASME International Mechanical Engineering Congress and Exposition*. 2021. American Society of Mechanical Engineers.