American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-8, Issue-5, pp-90-98
www.ajer.org
Research Paper Open Access

A Detection Approach for Finding Rogue Fog Node in Fog Computing Environments

Abdullah Al-Noman Patwary[1], Nishat Hossain[2], Mohammad Aslam Sami[3]
[1](School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China)
[2](School of Computer Science and Engineering, Bangladesh University of Professionals, Dhaka,Bangladesh)
[3](School of Computer Science and Engineering, Jahangirnagar University, Dhaka, Bangladesh)
Corresponding Author: Abdullah Al-Noman Patwary

ABSTRACT :*Recently, the concept of fog computing has attracting much attention due to the huge potential. Fog uses the Internet as a key infrastructure to interconnect numerous geographically diversified end users (IoT devices) with centralized cloud. But at the very early development stage it came up with many challenges. Security is the key challenges in this aspect. One of the most significant and challenging security concerns in fog computing environment is the presence of malicious or rogue node. Without proper detection mechanism it could be difficult to manage fog node in fog. There are renowned techniques for rouge node detection, nevertheless this paper tries to solve the problem from a different perspective. In this paper, we have introduced a statistical based approach to detect a rogue fog node using a Hidden Markov Model (HMM). Our trained HMM can successfully detect the presence of a rogue fog node instantaneously within very short computation time with high accuracy.We have verified our proposed approach using MATLAB simulated environment. Finally, according to the simulation results, our system can perform effectively and efficiently and can successfully identify the presence of rogue fog node in the fog environment.*

Keywords:*fog computing, security issues, rogue fog node, malicious fog node, detection, hidden markov model.*

Date of Submission: 25-04-2019 Date of acceptance: 05-05-2019

I. INTRODUCTION

With the development of computation and communication in recent times, cloud computing significantly changed the landscape of the traditional computing system or information technology world by providing various major benefits to the users. Every secondmore and more devices are connected with the Internet.Therefore, latency sensitive application faces serious problem because of intensive latency of cloud computing. On the other hand, cloud computing is unable to meet the various requirements such as mobility support, location awareness, etc. Therefore, to overcome the traditional or cloud computing problems, a new computing paradigm came up with huge support called fog computing which was proposed in 2012 by Cisco [1].

Fog computing, is a brand new and rising computing technology in the modern computing world. It is a recommended computing paradigm that aims to extend the cloud computing services to the edge of the network. The primary objective of fog computing is to provide cloud services such as storage, networking, computation, etc. on the edge components and reduce the communication overhead on the cloud platform [18]. According to the system architecture of fog computing, it consists of three main components, 1) Central Cloud, 2) Fog nodes, 3) IoT Devices. The fog is an intermediate environment between the cloud and end users residing at the edge of the network to provide various services to close proximity to the edge within a wide range of area. Table.1 represents the various service offered differences between fog and cloud computing system.

On the other hand, with the rapid development of the technology there are many new dimensions has been added to the computing technology world. Internet of Things (IoT) has recognized concern for the years and is enumerated as the future of the Internet. The IoT connects large number of heterogeneous objects, smart systems, and networks all together forming the biggest network worldwide [17]. In the context of IoT, fog computing comes up with several characteristics such as mobility, heterogeneity, and large-scale distribution. Fig.1 represents the basic architecture of fog Computing. Therefore, in the early development stages of fog computing, it faces numerous difficulties and challenges where security and privacy are the main concern [16]. Usually, fog environment is connected with the large-scale heterogeneous IoT devices which are mostly resource-constrained. In that case, end user sends their data stream to the trusted fog nodes, where fog node processed those data stream. If the data stream is heavy, then the fog node used to segment the data stream and distribute it to multiple trusted fog nodes.

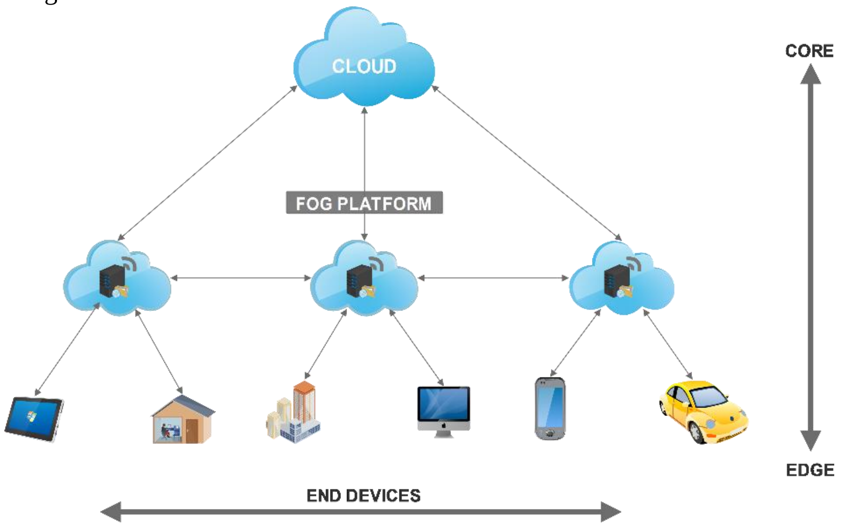


Fig.1. Basic architecture of fog computing

Service	**Fog Computing**	**Cloud Computing**
Control	Distributed	Centralized
Latency	Low	High
Location of service	At the edge of the network	Within the Internet
Mobility	Supported	Limited
Number of users	Billions	Millions
Location awareness	Yes	No
Real-time interactions	Supported	Less supported
Security	Can be defined	Undefined
Vulnerable point	Huge as it is distributed	Less than fog as it is centralized

Table.1. Comparison of Fog and Cloud Computing Concepts

In this regard, if there are any malicious or rogue fog node exists in the fog network it will cause the user's data privacy problem. Therefore, connecting to rogue fog node is highly dangerous, because it could allow attackers to steal user’s sensitive information. If this problem raises extensively, it may occur massive network collusion. According to the above circumstances, we admit that security and privacy issues should be addressed in every layer in designing fog computing system to mitigate the existence of rogue fog node. Therefore, it is essential to secure fog network system and detect suspicious or rogue fog nodes.

In this paper, we will discuss several security and privacy issues in terms of existence of malicious or rogue fog node in fog computing environment. From the existing work of rogue node detection and identification we have found various method and we also identify their limitations and flows in accordance with fog environment. Finally, we will propose our rogue fog node detection scheme in fog computing environment.

This paper is concentrating on presenting a secure and reliable rouge fog node detection technique in the fog computing environment. The principal contribution of this paper can be summarized as follows:

- We propose a secure, and scalable rouge fog node detection technique in terms of fog computing environment using the renowned Hidden Markov Model (HMM).
- We present the details of the overall system including the system architecture, interaction between participants and rouge node detection technique with several phases.
- Our scheme can perform effectively and efficiently within a fog area which can practically detect rouge fog node in fog computing environment.

The rest of this paper is organized as follows: In section II,presents several related works. In section III,presents problem statement and approach. In section IV, we describe our proposed detection technique. In section V, represents our experimental evaluations. In section VI, we discuss our experiment results. In section

VII, we disuses about various challenges and our future work. We have ended up our paper by conclusion in section VIII.

II. RELATED WORKS

After studying and analyzing various relevant literature of fog computing, more comprehensive study of malicious fog node in the system has been carried out. There is not much work has been done in the field of malicious detection or rogue fog node detection in fog computing. Most of the current approaches are for traditional computing or cloud computing environment which is easily compromised by attackers and they already faces other numerous challenges too.

Ma et al.[2], proposed a hybrid framework that can detect the presence of rogue access points in Wi-Fi-based access networks. Their approach protects the networks from rogue access points even if the adversaries use customized equipment.

Stojmenovicet al.[3] have demonstrated a typical man-in-the-middle attack in fog where a legitimate fog node replaces by a fake fog node or compromised fog node. To protecting this challenges, strong data encryption and decryption method consume large amount of resource where most of fog nodes and IoT devices are resource constrained. To mitigate this problem, an intrusion detection method, signature-based detection or behavioral or anomaly-based detection techniques would be a preferable solution.

The authors Han et al.[4] [5], have proposed a measurement-based method which enables a client to avoid connecting rogue access point (AP). Their approach leverages the round-trip time between end users and the Domain Name System (DNS) server to detect rogue AP at the client side.

Sohalet al.[6], proposed a cyber-security framework which can detect and identified malicious edge devices at the edge of the network. Their framework, performs successfully in the real environment. They consider, Hidden Markov model (HMM), IDS and Virtual Honeypot technologies for their framework.

Shivarajet al.[7], proposed to detect rogue access point in wireless network. They used Hidden Markov Model (HMM) to detect the presence of rogue AP in the WLAN. They consider two stages, first stage for training HMM and other stage is for detection based on the trained HMM.

Khan et al.[8], proposed to detect misbehavior's and malicious vehicular node in VANETs. They presented an algorithm called DMN which designated to detect abnormal nodes and it can increase the performance of the network.

Stolfoet al.[9], presented an approach which can detect and mitigate insider data theft attack in cloud. They focused user behavior profiling and decoy technology. By monitoring user data access patterns into the system, if malicious user detected by profiling user behavior then sending the decoy document to that malicious user.

Zaidi et al.[10], presented a data-centric technique to detect rogue node in Vehicular ad hoc networks (VANETs).This approach is based on sending or broadcasting false emergency messages in VANETs. Fault tolerant and resilient against injection of false data also considered.

Shi et al.[11], presented a cloudlet mesh-based security framework which can detection intrusion to distance cloud, securing communication among mobile devices, cloudlet and cloud.

III. PROBLEM STATEMENT AND APPROACH

In this section, we are going to discuss and analyze about the various problem regarding rogue fog node which actually we are going to detect in the environment of fog computing.

What is rogue fog node?: Rogue fog node can be defined in many ways. In fog computing, a rouge fog node is a device which is trying to compromise a legitimate fog node [16]. A rogue fog node is termed as, when a device which is actually compromised by malicious users or intruders and it acts as a legitimate fog node in the fog network and motivate the user to connect to it. It injects false data in the fog network either on purpose with malicious intent or due to faulty devices. Therefore, a rogue fog node is considered as a malicious entity in fog network. The presence of rouge fog node or fake fog node will be a massive threat to user data privacy and security in the fog network. For example, a malicious user compromises a legitimate fog node or in an insider attack, a legitimate fog administrator who willingly or mistakenly introduce a rouge fog node instead of a legitimate fog node.

Why rogue fog node is a problem in fog computing environment?: As fog platform is prone to many security issues, there is a need for concentrating about them deeply. In fog computing environment, in order to provide various services to users, much of the information is gathered into fog nodes. Fog nodes are responsible to process data received from the IoT devices. If the workloads are heavy, then it is divided into several parts and processed it by several fog nodes. If some fog nodes are compounded by a malicious user and a wrong information is spread by exploiting vulnerability in the fog network it is difficult to ensure the integrity of the data. Before the computation begins, fog nodes and fog users must trust each other. Therefore, an authentication technique is required in terms of establishing trusted communication.

How do we identify trusted fog nodes?: Fog node works as a middle-ware which is residing at the edge of the network. It collects or receives different context data from the various IoT devices via sensors or actuators. If the amount of data is heavy, it is then dividing the data into several partition and processed by several fog nodes. Fog users (IoT devices) are mostly resource-constrained, and they outsource their tasks to their trusted fog nodes [13]. If some fog nodes are compromised by the malicious user, it is difficult to ensure the integrity of the data. However, before the computation process begins, the fog nodes and fog users have to trust each other. On the other hand, the fog nodes also need to be trusted by the cloud, as there is no other fog who can manage another fog node because of the distributed nature of fog network system. Initially, an authentication system can build trusted relation between fog and cloud. In order to process a volume of data, fog nodes which is authenticated by the cloud should be only located in the fog environment. Therefore, how to identify the such trusted fog nodes is a significant concern. Among several approaches [14], we should consider in terms of identifying trusted fog nodes in fog computing environment which are as follows:

- To identify trustworthiness of fog nodes on the basis of their trust, we can consider the trust value of the fog node.
- We can also evaluate their trust values utilizing various probability models (Markov) on the basis of their historical behavior.
- Due to the resource-constrained, dynamic nature, latency problem of the fog nodes, it is highly required to design a lightweight solution. If the computation overhead is heavy, then it would be performed in the cloud level.
- By analyzing malicious behavior of fog node and taking proper action against them, we can also identify the trusted fog node.

How rouge fog node manipulate trust establishment among fog nodes?: In fog computing, the fog nodes and fog users communicate with each other by having a high trust value [15]. Fog nodes with high trust values will be selected more times rather than fog nodes with lower trust values. On the other hand, a fog user with high trust value will be accepted more than the fog users with low trust values. Malicious node or rogue node will try to generate different attacks to get higher trust value than they should have. Sometimes a malicious fog node, gives positive recommendations about itself to increase its trust value it’s called self-promotion attack. Sometimes, several malicious nodes together give negative or false recommendations against a good node it’s called bad-mouthing attack. When a malicious node gives positive recommendation to another malicious node to increase the trust value of the malicious node which is called ballot-stuffing attack. sometimes, a malicious node feels that its trust value has dropped, after that it can perform positive service to restore its trust value. Finally, for some situations a fog node can perform positive and negative service simultaneously to avoid being labeled as a malicious or rouge node which is called on-off attack.

IV. OUR PROPOSED TECHNIQUE

In this section, we introduce a technique in order to provide a consistent and rigorous approach to identify vulnerable or malicious fog node in fog computing, which could potentially expose the other fog node or fog user devices and user's sensitive data. Before we describe our proposed technique, we would like to first introduce the renowned Markov process which is used to model the secure or insecure state of a fog node in the fog network.

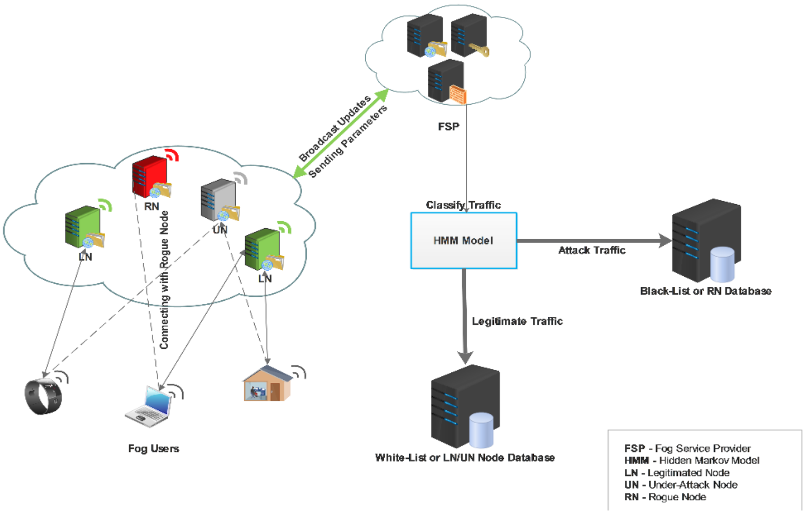


Fig.2. System architecture.

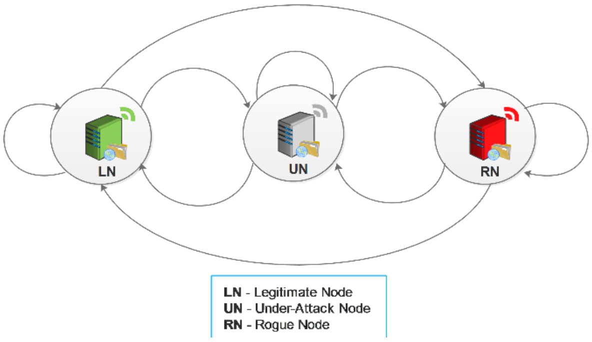


Fig.3. HMM model for the three-security state of fog node.

A. System Architecture

In this sub-section, we are going to describethe overall system architecture and design details with the presence of malicious or rogue fog node in the fog network. Fig.2 represents the system architecture of our proposed system. Our system consists of several fog nodes distributed randomly in an untrusted environment. Each fog node communicates with the neighboring fog nodes within its range. In our scheme, the fog nodes will be categorized into three possible security states,$S = \{LN, UN, RN\}$ where LN = Legitimate Node, UN = Under-attack Node, and RN = Rogue Node. The Fog Service Provider (FSP) will do the capturing and monitoring process according to the state of node and perform the required action after detection of malicious behavior of node.

Legitimate Node (LN): are those fog nodes which are actually use their privileges in the correct manner and never try to manipulate the security of the fog network. This state represent that it is a normal fog node and it behaves normally without doing any malicious activity in the fog network.

Under-attack Node(UN): are those fog nodes which are actually legitimate nodes. But unintentionally or accidentally these nodes turn into malicious nodes but their severity of damages in the network are very low. If the preventive measures against those attacks are not taken properly afterwards it can cause high severity of attacks which can subvert the system.

Rogue Node (RN): In this security state, illegitimate nodes which are prone to attacks. It does intrusive activities in the fog network to compromise the network system. Due to the existence of rogue node in the fog network it will hamper on user’s data privacy or other fog nodes as well.

Fig.3 exhibit the HMM model for the three security states of the fog node. The direction from one node to another node represents the fact that when a fog node is in the state indicated by the source node it can transit to the state indicated by the destination node. Note that the graph is fully connected, which indicates that it is possible to transit from any security state to any other security state. Fig.4 represent the work process of our scheme with our trained HMM model for the detection and identification of rogue fog node in the fog environment.

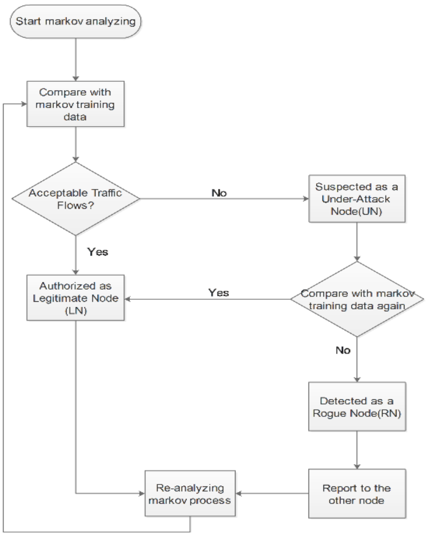

Start markov analyzing
Compare with markov training data
Acceptable Traffic Flows?
No
Suspected as a Under-Attack Node(UN)
Yes
Authorized as Legitimate Node (LN)
Yes
Compare with markov training data again
No
Detected as a Rogue Node(RN)
Re-analyzing markov process
Report to the other node

Fig.4. The work-process of our scheme with trained HMM model

B. Methodology Description

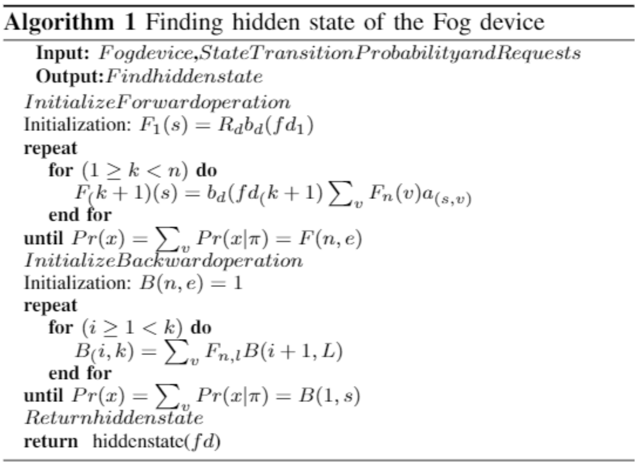
In this section, we are going to present the renowned Markov Models that were used in our rogue fog node detection technique. Markov model predicts the probability of the future outcomes on the basis of present outcomes of system rather than past activities. Hidden Markov Model (HMM) is used to enhance the capability of the classic Markov model [6], [7]. This model is capable to predict the next state of the system with hidden state which was not possible with Markov model. Hidden Markov models are widely used in science, engineering and many other areas (speech recognition, optical character recognition, machine translation, bio-informatics, computer vision, finance and economics, and in social science). Our proposed scheme uses a Hidden Markov Model (HMM) to detect the future behavior of the fog nodes in the fog layer.

The two stage Hidden Markov Model of the proposed scheme can analyze every fog node. Our proposed technique uses a two-stage Markov model for early detection of the rogue fog node in a fog computing environment. On the basis of the previous activities of the fog node, the two-stage Markov model predicts the current state each fog node and also calculates the probability of it being a rogue fog node. The idea of using HMM for rogue fog node detection is for reducing demands on training time and memory resources. In our network model, where the state of the fog node is not observable but the packet traces are the observable parameters that help us to determine the state of the fog node. The packets coming from the fog nodes through the communication medium provide information about the fog node and help us to assume the state of the fog node. Our main goal is to determine what fraction of traffic flows are source of various attacks and for each traffic flow, what is the probability that this particular traffic flow originated from a rogue fog node.

C. Our Solution

In this section, we are going to discuss about the various terminology which is used in our scheme.

1. **Algorithm:** The complete set of parameters of our HMM model and the algorithm are given as follows:



```
Algorithm 1 Finding hidden state of the Fog device
  Input: $Fogdevice,StateTransitionProbabilityandRequests$
  Output: $Findhiddenstate$
$InitializeForwardoperation$
Initialization: $F_1(s) = R_d b_d(fd_1)$
repeat
    for $(1 \geq k < n)$ do
        $F_(k+1)(s) = b_d(fd_(k+1) \sum_v F_n(v) a_{(s,v)}$
    end for
until $Pr(x) = \sum_v Pr(x|\pi) = F(n,e)$
$InitializeBackwardoperation$
Initialization: $B(n,e) = 1$
repeat
    for $(i \geq 1 < k)$ do
        $B_(i,k) = \sum_v F_{n,l} B(i+1,L)$
    end for
until $Pr(x) = \sum_v Pr(x|\pi) = B(1,s)$
$Returnhiddenstate$
return hiddenstate($fd$)
```

Note:F - Forward variable, fd - Fog device, R_d- Probability of d, b_d - Probability emission of d, Pr–Probability,B–Backwardvariable

Our HMM-based detection consists of three phases namely training, monitoring and detection phase. The explanation of each phase are as follows:

2. **Training Phase:**It is the first phase, where the main objective of the training phase is to estimate the parameters. In the training phase, the observation sequence obtained from the various attacks which are transformed into HMM observation sequence, i.e., the HMM model is trained with a normal set of network data. Then, the HMM is inferred from the observation sequence. In the training phase, the observation sequence is first transformed into HMM short sequences, then the HMM is used to calculate the most probable state sequence in order to determine if it is legitimate or rogue. It is also very true that with a larger training set, the detection accuracy of the model will improve. The reason behind larger training data is, the model analyzes more observations or outputs in order to achieve higher likelihood of the security state of the fog node.
3. **Monitoring Phase:**After training the HMM model, the next step is to perform monitoring process of fog node in the fog network. A monitoring point is located at the fog service provider level or cloud broker level capturing traffic flows coming in and going out of the fog network. Each of these fog nodes can be termed as legitimate, under-attack or rogue depending on the traffic generated by them. The traffic was collected from the all nodes in the fog network and an online and offline detection process was carried out

using the trained HMM model. The goal of our model is to report all instances of the presence of rogue fog node in the fog network. By monitoring each legitimate node (LN) activity using the hybrid intrusion detection system deployed within the fog network. After analyzing all fog node activities and when some anomalous behavior of the fog node is detected by it, it generates an attack notification. The attacks have their own unique characteristics which differs from one to another. So, we use the various attacks probabilities as the observation parameter for our HMM model. As mentioned in Table.2, which refers to various probabilities in multiple states in fog node.

4. **Detection Phase:**After training the HMM model, the next step is to perform detection process of rogue fog node. The detection process was carried out by generating packet traces from the fog network. Observation distributions were extracted from the packet traces. For our detection process, the Viterbi algorithm will detect the state of the fog node in the fog network. The output of the detection procedure is a sequence of security states of the fog node corresponding to each packet in the trace file. The first-stage Markov model, predicts the fog node category and the shifting probability of the fog node from the output generated by the IDS. The second-stage Markov model, decides whether to shift the fog node to under-attack node or the rogue node, on the basis of the fog node category and the shifting probability of the fog node.

In the next section we will evaluate the experiment of our detection scheme using HMM model to analyze the performance of the detection process.

V. EXPERIMENTAL EVALUATIONS

In this section, we are going to describe about the experiment of our scheme. To conduct this, we have performed our experiment in MATLAB and JAVA environment in Eclipse IDE. We have used java environment to generate different types of attacks. Table.2, represents the various attack probabilities in multiple states. Various attacks generated are stored in a data file which is imported into Matlab R2016a for Markov model predictions. The Matlab is used for simulating the Hidden Markov Model. Algorithm 1 is implemented in Matlab R2016a for maintaining the transition matrix of each fog device, and on the basis of these matrices, the two-stage Markov model is able to take a decision whether the fog node is to be shifted to the RN state or not. In the graphical representation module, the results of the proposed scheme are displayed in the form of a graph. For the experimental evaluation, two different devices were created which send different kinds of queries to the simulation system. The difference between the two fog devices is the variation in the attack probabilities, as shown in Fig.5. As represented in Fig.5 the first fog device has seven different overall attack probabilities with mean of 0.75, and the second fog device also has seven different overall attack probabilities with mean of 0.67. These overall attack probabilities are generated based on the different queries performed by both devices based on the probability listed in Table.2 This will help the HMM to train effective for different kinds of fog devices.

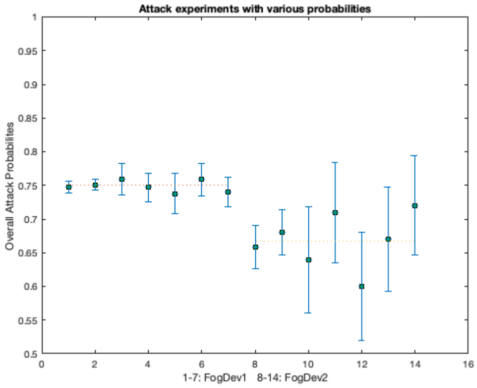


Fig.5. Overall attack probabilities in two Fog devices.

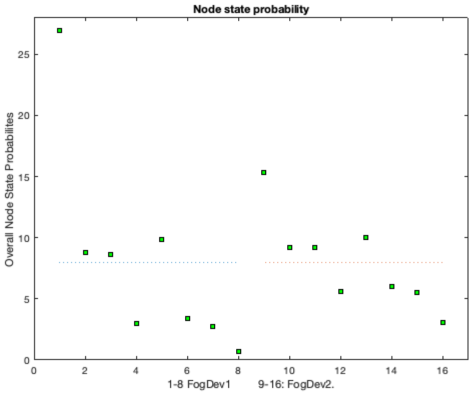


Fig.6. Node state probabilities in two Fog devices.

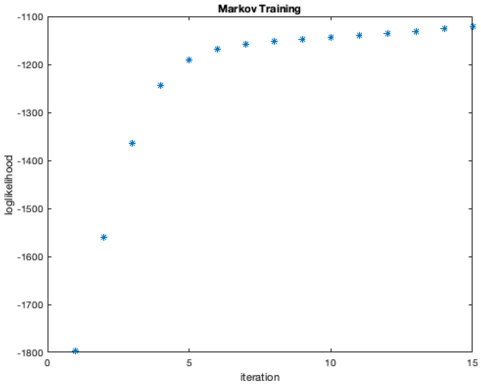


Fig.7. Likelihood of shifting safe state to rouge state.

State	Probabilities	Requests
LN	75%	750
UN	12.5%	125
RN	12.5%	125
LN	50%	500
UN	25%	250
RN	25%	250
LN	25%	250
UN	37.5%	375
RN	37.5%	375

Table.2. Various probabilities in multiple states.

VI. RESULTS AND DISCUSSION

To examine the performance of our proposed rogue fog node detection scheme in the fog network the performance analysis of the proposed scheme are as follows:

Different sets of queries are generated based on the probability listed in Table.2. Two fog devices were selected to perform the experiment, where fog_device1 selected more legitimate queries and fog_device2 selected a greater number of attacks. Selected queries of both fog devices were fed into the HMM toolbox of Matlab where attack probabilities were generated for both nodes for seven iterations. Fog_device1 showed more variation in state probability generation, as shown in Fig.5, because it performed more state on the system. Then the same experiment was conducted with three types of state only, and overall state probabilities were calculated for eight iterationsrespectively as shown in Fig.6. Fog_device1 provided less variation and state probabilities then fog_device2 in both experiments. This is because frequency of state changes queries of fog_device1 is far less than that of fog_device2. As the iterations of state change increase, the likelihood of shifting of legitimate node LNto rogue nodeRN also increases, which is shown in Fig.7.

VII. CHALLENGES AND ROAD MAP FOR FUTURE RESEARCH WORK

Detection of malicious activity and rogue fog node in fog computing environment is challenging anddifficult task. However, in this portion, we are going to present and highlights few significant and considerable issues which make difficulties to identifying the presence of rogue fog nodes in the fog environment which are as follows:

- Complicated and difficult trust management system.
- Insecure authentication and authorization system.
- Dynamic behavior of fog such as creating, deleting, joining, leaving of fog node in the fog layer.
- Intrusion detection on both client and the centralized cloud side in terms of fog computing is challenging.
- There are also challenges such as implementing intrusion detection in large-scale, geo-distributed, high-mobility fog computing system to meet the low-latency requirement.
- When some fog node is compromised, hybrid detection technique is useful to detect malicious code in fog nodes.
- It is required to combined with signature-based detection technique and behavior-based detection technique.
- Dynamic analysis techniques are essential to monitor fog node in real time.
- Typically, the performance overhead of dynamic analysis is high, so lightweight dynamic techniquewould be preferable solution in terms of fog environment.

VIII. CONCLUSION

Fog computing faces numerous security and privacy challenges. Due to the distributed architecture and extensive number of devices connected with it, controlling security and privacy issues is a challenging concern. Rogue fog node is one of the biggest security threats in fog computing environment. In this paper, we have presented a novel approachto effectively and efficiently detect and identified rogue fog node in the fog network. In our scheme, we use Hidden Markov Model (HMM) for predicting of the fog nodes behaviors based on the various attack probabilities. We have simulated our experiment on MATLAB and JAVA Environment. However, the results of the experiment shows that our scheme can successfully identify the presence of rogue fog node and can perform smoothly without generating any false alarm in the fog network. In the future, we intent to explore and design security solutions to tackle the proposed challenges. Moreover, we will study new security and privacy issues in the areas of Cloud-Fog-IoT.

REFERENCES

[1]. Bonomi, Flavio, et al. "Fog computing and its role in the internet of things." Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012.

[2]. Ma, Liran, Amin Y. Teymorian, and Xiuzhen Cheng. "A hybrid rogue access point protection framework for commodity Wi-Fi networks." IEEE INFOCOM 2008-The 27th Conference on Computer Communications. IEEE, 2008.

[3]. Stojmenovic, Ivan, and Sheng Wen. "The fog computing paradigm: Scenarios and security issues." 2014 Federated Conference on Computer Science and Information Systems. IEEE, 2014.

[4]. Han, Hao, et al. "A measurement based rogue ap detection scheme." IEEE INFOCOM 2009. IEEE, 2009.

[5]. Han, Hao, et al. "A timing-based scheme for rogue AP detection." IEEE Transactions on parallel and distributed Systems 22.11 (2011): 1912-1925.

[6]. Sohal, Amandeep Singh, et al. "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments." Computers & Security 74 (2018): 340-354.

[7]. Shivaraj, Gayathri, Min Song, and Sachin Shetty. "Using Hidden Markov Model to detect rogue access points." Security and Communication Networks 3.5 (2010): 394-407.

[8]. Khan, Uzma, Shikha Agrawal, and Sanjay Silakari. "Detection of malicious nodes (DMN) in vehicular ad-hoc networks." Procedia computer science 46 (2015): 965-972.

[9]. Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." 2012 IEEE symposium on security and privacy workshops. IEEE, 2012.

[10]. Zaidi, Kamran, et al. "Data-centric rogue node detection in VANETs." 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2014.

[11]. Shi, Yue, Sampatoor Abhilash, and Kai Hwang. "Cloudlet mesh for securing mobile clouds from intrusions and network attacks." 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. IEEE, 2015.

[12]. Lee, Kanghyo, et al. "On security and privacy issues of fog computing supported Internet of Things environment." 2015 6th International Conference on the Network of the Future (NOF). IEEE, 2015.

[13]. Huang, Hui, et al. "Bitcoin-based fair payments for outsourcing computations of fog devices." Future Generation Computer Systems 78 (2018): 850-858.

[14]. Li, Zhi, et al. "A non-cooperative differential game-based security model in fog computing." China Communications 14.1 (2017): 180-189.

[15]. Guo, Jia, Ray Chen, and Jeffrey JP Tsai. "A survey of trust computation models for service management in internet of things systems." Computer Communications 97 (2017): 1-14.

[16]. Yi, Shanhe, Zhengrui Qin, and Qun Li. "Security and privacy issues of fog computing: A survey." International conference on wireless algorithms, systems, and applications. Springer, Cham, 2015.

[17]. Alrawais, Arwa, et al. "Fog computing for the internet of things: Security and privacy issues." IEEE Internet Computing 21.2 (2017): 34-42.

[18]. Mukherjee, Mithun, et al. "Security and privacy in fog computing: Challenges." IEEE Access 5 (2017): 19293-19304.

Abdullah Al-Noman Patwary, Nishat Hossain, Mohammad Aslam Sami"A Detection Approach for Finding Rogue Fog Node in Fog Computing Environments"American Journal of Engineering Research (AJER), vol.8, no.05, 2019, pp.90-98