International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 02 | February - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

A Review on Intrusion Detection in IoT Networks: Existing Challenges

Pritibala Mali[1], Prof. Pankaj Raghuwanshi[2]

ABSTRACT: Advancements in computer networks has led to the inter-connectivity of different types of smart devices over the internet. Such a diversified connected network is often termed as internet of things or IoT. Off late, an ancillary of the IoT framework called the fogging or fog computing has gained tremendous prominence. . Fog computing decentralizes the infrastructure without depending on centralizing it, such as with cloud computing. Fog computing is a paradigm proposed that integrates the IoT and the cloud concept to support user mobility, low latency, and location awareness. Due to the de-centralized nature of the Fog architecture, the sharing of data among different smart devices is susceptible to security threats. In this paper, a comprehensive review on fog computing and the allied performance metrics such as coverage, error rate and throughput have been discussed. Moreover, a channel load sensing techniques utilizing the channel state information (CSI) has also been proposed with the aim to enhance the throughput and error rate of the system.

Keywords: Internet of Things (IoT), Fog Computing, End Device, Error Rate, Throughput, Channel State Information.

I. INTRODUCTION

Fog computing, also known as edge computing deploys data centres to the edges of the network, and it offers location awareness, low latency, and improves quality of service (QoS) for near real-time applications. Typical examples include transportation, industrial automation, agriculture, and other smart city applications [2]. Fog computing can be thought of as a subset of internet of things (IoT). The IoT architecture is depicted in the figure below.

Fig.1 The IoT Architecture

Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. Some applications of IoT are:

- Smart Cities.
- Healthcare
- Transportation
- Traffic Control
- Manufacturing
- Large Scale Automation
- Big Data Applications etc.

Fog infrastructure supports heterogeneous devices, such as end devices, edge devices, access points, and switches. Fog servers are considered to be micro data centres by inheriting cloud services at the network edges. Fog computing facilitates the operation of compute, storage, and networking services between end devices and cloud computing data centres

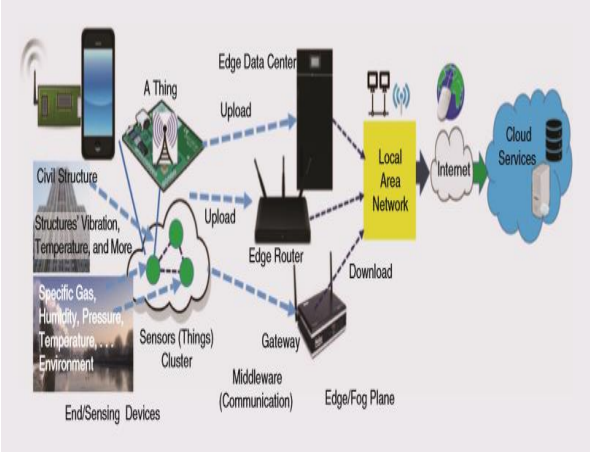

Fig.2 The Network Cross Layer in IoT

The data centres are positioned for near real-time applications, big data analytics, and distributed data collection, and they offer advantages in various applications in smart cities. Fog computing is deployed to overcome latency issues. However, fog computing completely ignores the cloud because of the limited sources at the fog server and always relies on the cloud for complex processing. Many research issues relating to fog computing are emerging because of its ubiquitous connectivity and heterogeneous organization. In the fog computing paradigm, the key issues are the requirements and the deployment of the fog computing environment. This is because the devices that exist in fog environments are heterogeneous. The fog computing architecture can be further divided into three layers which are:

1) Sensing Layer
2) Middleware
3) Fog Server.

The attributes of the different layers is explained subsequently.

Sensing Layer: The sensing layer is the bottommost layer in the three-layered architecture. The physical layer and datalink layer of communications stack together to form the sensing layer which is made up of numerous sensing technologies, such as radio-frequency identification tags, wireless sensor networks (WSNs), and near-field communications (NFCs) etc. The following is a list of functions performed in the sensing layer:

1) uniquely identify physical objects as a part of the IoT to collect data on these object
2) convert the sensed data to digital signals
3) send data collected from the surrounding objects to upper layers for network transmission and processing.

Middleware: The network and transport layers together form the middleware of the fog hierarchy. The data received from the bottom layer are processed at the middleware and transmitted to the fog server for further evaluation. Abundant data are processed using network technologies, such as local area networks, wireless/wired networks, and transmission medium, such as Wi-Fi, Bluetooth, and Zigbee. The following functions are performed in the middleware:

1) Sensing layer information is processed with network support.
2) Processed sensing data are received and transmitted to the upper layer.
3) Secure data transmission assigns Internet Protocol version 6 addressing to the physical objects.

Fog Server: The fog server layer can be further divided into application and business aspects. This layer acts as a front end to users. Its main function is to facilitate the management of different applications. IoT application deployment platforms are used to differentiate between various applications, such as transportation, health, and banking. The business sublayer manages the end data and its security.

II. RELATED WORK

This section discusses the previous work in the domain along with the salient features.

G. Sun et al. in [1] proposed a technique for smart vehicles to partake in data crowd sensing while maintaining security and privacy, which includes privacy preservation, data aggregation, and traceability in a proposed data collection approach based on a heterogeneous two-tier fog architecture. These are three properties that prior attempts cannot all achieve. Moreover, a new scheme for trust authority (TA) security queries in fog computing to obtain outsourced encrypted map lists (MPLs) of the

participants to achieve online traceability and identity retrieval for malicious participants is proposed in our study, which can reduce the storage burden of TA. Finally, the simulation results demonstrate the efficiency of our approach both in computation and communication

R.Mahmud et al. in [2] roposed a quality of experience (QoE) -aware application placement policy that prioritizes different application placement requests according to user expectations and calculates the capabilities of Fog instances considering their current status. In Fog computing environment, it also facilitates placement of applications to suitable Fog instances so that user QoE is maximized in respect of utility access, resource consumption and service delivery. The proposed policy is evaluated by simulating a Fog environment using iFogSim. Experimental results indicate that the policy significantly improves data processing time, network congestion, resource affordability and service quality.

Y.Zhou et al. in [3] proposed analyzes the heterogeneity of FogMNW with both advanced communication techniques and fog computing. Then a heterogeneous communication and hierarchical fog computing network architecture is proposed. With both communication and computing resources, Fog-MNW is enabled to achieve much higher capacity than conventional communication networks. This has been well demonstrated by the coded multicast scheme. Furthermore, a systematic management of communication and computing resources is necessary for Fog-MNW. By exploiting the communication load diversity in N cells, a communication load aware CLA scheme can achieve much higher computing resource efficiency than comparing schemes.

T.Wang et al. in [4] proposed a fog computing model and extend the Hungarian algorithm to manage the coupling resource which can get smaller delay to realize effective and sustainable services. The fog computing layer acts as a buffer and controller between CPS layer and cloud layer which can handle malicious attacks to build highly sustainable systems. Experimental results and theoretical analysis show that the method can reduce the coupling computing and increase the resource utilization to make systems more effectively.

A. Rahmani et al. in [5] proposed to use the concept of Fog Computing in Healthcare IoT systems by forming a Geo-distributed intermediary layer of intelligence between sensor nodes and Cloud. By taking responsibility for handling some burdens of the sensor network and a remote healthcare centre, the Fog-assisted system architecture can cope with many challenges in ubiquitous healthcare systems such as mobility, energy efficiency, scalability, and reliability issues. A successful implementation of Smart e-Health Gateways can enable massive deployment of ubiquitous health monitoring systems especially in clinical environments.

M.Azaam et al. in [6] presented the idea of industrial internet of things (IIoT). IIoT refers to making industrial processes and entities part of the Internet. Restricting the definition of IIoT to manufacturing yields another subset of IoT, known as Industry 4.0. IIoT and Industry 4.0, will consist of sensor networks, actuators, robots, machines, appliances, business processes, and personnel. Hence, a lot of data of diverse nature would be generated. The industrial process requires most of the tasks to be performed locally because of delay and security requirements and structured data to be communicated over the Internet to web services and the cloud. To achieve this task, middleware support is required between the industrial environment and the cloud/web services. In this context, fog is a potential middleware that can be very useful for different industrial scenarios.

S. Bitam et al. in [7] proposed bio-inspired optimization approach called Bees Life Algorithm (BLA) aimed at addressing the job scheduling problem in the fog computing environment. The proposed approach is based on the optimized distribution of a set of tasks among all the fog computing nodes. The objective is to find an optimal trade-off between CPU execution time and allocated memory required by fog computing services established by mobile users. The empirical performance evaluation results demonstrate that the proposal outperforms the traditional particle swarm optimization and genetic algorithm in terms of CPU execution time and allocated memory.

D. Puthal et al. in [8] showed that Load balancing is the process of redistributing the work load among

Edge Data Centres (EDCs) to improve both resource utilization and job response time. Load balancing also avoids a situation where some EDCs are heavily loaded while others are in idle state or doing little data processing. In such scenarios, load balancing between the EDCs plays a vital role for user response and real-time event detection. As the EDCs are deployed in an unattended environment, secure authentication of EDCs is an important issue to address before performing load balancing. This article proposes a novel load balancing technique to authenticate the EDCs and find less loaded EDCs for task allocation. The proposed load balancing technique is more efficient than other existing approaches in finding less loaded EDCs for task allocation. The proposed approach not only improves efficiency of load balancing; it also strengthens the security by authenticating the destination EDCs

LF Bittencourt et al. in [1] showed that the distributed capacity provided by Fog computing allows execution and storage to be performed at different locations. The combination of distributed capacity, the range and types of user applications, and the mobility of smart devices require resource management and scheduling strategies that takes into account these factors altogether. Authors analyze the scheduling problem in Fog computing, focusing on how user mobility can influence application performance and how three different scheduling policies, namely concurrent, FCFS, and delay-priority, can be used to improve execution based on application characteristics.

L.Liu et al. in [10] proposed the use of queuing theory to bring a thorough study on the energy consumption, execution delay, and payment cost of offloading processes in a fog computing system. Specifically, three queuing models are applied, respectively, to the mobile (MD), fog, and cloud centres, and the data rate and power consumption of the wireless link are explicitly considered. Based on the theoretical analysis, a multi-objective optimization problem is formulated with a joint objective to minimize the energy consumption, execution delay, and payment cost by finding the optimal offloading probability and transmit power for each MD. Thus it is explained in the paper that the performance metrics for the design of an effective fog architecture should include energy consumption, latency and error rate.

III. PROBLEMS IDENTIFIED IN PREVIOUSLY EXISTING TECHNIQUES

The following challenges have been identified in regards to the implementation of fog computing architectures.

High Bit Error Rate:

The computation of the bit error rate (BER) of the system is done on the basis of the condition of mismatch among the bits which are transmitted and the bits which are received. Mathematically, a bit error occurs if the following condition holds true:

$$b_{Tx} \cong b_{Rx}$$

Here,

b_{Tx} is the transmitted bit

b_{Rx} is the received bit

For a stream of bits, the total BER is computed as:

$$BER = \sum_{i=1}^{i=n} b_i^{Tx} \cong b_i^{Rx}$$

Here,

I is the bit index

n is the total number of bits transmitted

the bit error may arise in 2 cases, either a zero is received as one or a one is received as zero. Both cases may result in an error. The comparator is responsible for the decision of 0 or 1 depending on the threshold set for the decision for 1/0 bit reception at the receiving end.

Outage Probability

In case the system is affected by interference as well as noise effects, then a term called SINR is computed which is the signal to interference plus noise ratio (SINR). For a system with clustered wave reception, there must exist a threshold Vk above which the signal quality must hover so as to receive satisfactory quality. The mathematical expression for the outage

probability in terms of the CCDF is given by the following expression:

$$\text{Prob}(\text{SIR}_k \geq \text{SINR}) = \exp\{-K_k \sum_{j\epsilon\phi} \sigma_{kj}\lambda_j\}$$

Te outage in terms of absolute parameters $q(\lambda)$ is given by[1]:

$$q(\lambda) = \exp\left\{-\frac{2\pi^2}{\sin\left(\frac{2\pi}{\eta}\right)} R_k^2 \text{SINR}_k^{2/\eta}\lambda\right\}$$

Here,

$K_k = C_k R_k^2 \text{SNR}_k^{2/\eta}$ is a constant depending on system and channel parameters

SINR represents the signal to noise plus interference ratio

R is the distance

λ_j is the device density

σ_{kj} is the shadowing factor

$q(\lambda)$ is the absolute outage in terms of node density

The CCDF function can be defined as the complementary cumulative distribution function and mathematically governed as:

$$CCDF(x) = 1 - CDF(x)$$

Here,

CCDF represents complementary cumulative distribution function

CDF represents cumulative distribution function

x is the random variable

Network Delay or Latency

The network delay is often computed w.r.t. the distance from the sink. In case the node is far away from the sink, its chances for a long distance transmission reduces, hence it would transmit to a nearby node, thereby reducing the energy consumption. This would in-turn increase the residual energy of the nodes.

Thus as the distance from sink increases, the energy consumption decreases and the residual energy increases. Thus,

$$E_C = f(d_{sink})$$

$$E_{Residual} = f(d_{sink})$$

Thus two important considerations have been seen which are conserving the energy of the system so as to increase the network lifetime and moreover increasing the efficacy with which the packets are transmitted and received by the transmitting end and the receiving end. This would in turn increase the latency performance of the system by reducing the delay of the system. The formulations above give the relation among various variables for the computation of the same.

Reduced Throughput

The throughput of the system is defined as:

$$Throughput = \frac{Data\ Size}{Time}$$

Throughput is critically important for high speed fog computing networks since the throughput decides how fast data exchange takes place in the network. Often, the reason for degraded or reduced throughput is the unavailability of free spectrum in the network or jammed data packets.

IV. CHANNEL LOAD SENSING AND CHANNEL STATE INFORMATION

The most effective and simple technique to sense the channel loading and channel state information is energy sensing.

Energy Sensing

This technique is used for the energy detection mechanism and senses the energy of the channel at any given point of time. The hypothesis that governs this technique is the following:

$$h(t) = k(t); ideal\ no\ attack\ condition$$
$$h(t) = k(t) + j(t);\ atatck\ present$$

The chances for a false alarm occur when there is attack present but the CSI suggest that a possible attacking adversary is absent or vice versa. The methodology for channel load sensing (CLS) and

obtaining channel state information (CSI) is depicted in the figure below:

Fig.3 Methodology for Channel Load Sensing

Effect of Noise on Probability of False Alarm (Security Threat)

The chances of false alarm increase when there is actual addition of noise in the desired spectrum. It is noteworthy that such noise effects may lead to a false interpretation that there is jamming noise being injected in the signal spectrum and it is the act of eavesdropping by the adversary. This however is not true and leads to misleading and inaccurate results. The effect can be summarized as follows:

Let the threshold for jamming to be present by 'T'

If $h(t) > T; attack\ presnet$

However,

If $h(t) + n(t) > T$ holds true;

Then there is a clear chance of false alarm often computed as the probability of false alarm of security threat.

Practical fog environments would change over time. The frequency response no longer remains a function of frequency alone but becomes a function of time as well. Such a frequency response d designated as:

$$H = g(f, t)$$

Here,

g is a function

H is the channel condition

f is the frequency

t is the time

If one takes snippets of the frequency response of the channel over time, one gets a temporal sample. It is clear that the frequency response changes over time. Thus in case the channel is estimated using channel sounding every $\mathbf{T_{rep}}$

where $\mathbf{T_{rep}}$ is the repletion interval for taking samples of the channel frequency response by the channel sounder, it will obtain different values for a practical wireless channel. Thus, the Channel State Information (CSI) would change over time.

Nonetheless, assuming availability of **CSI** for the wireless channel for every $\mathbf{T_{rep}}$, the frequency selective nature results in some sub-carriers getting suppressed and causing degraded BER at the receiving end which is a direct consequence of low Signal to Noise Ratio (SNR).

Mitigating Challenges in Utilizing CSI

Consider a bandwidth B which is double sided bandwidth available for data stransfer. Typically, we employ symbol time $T = \frac{1}{B}$, in bandwidth B, one symbol is transmitted every T sec. Therefore,

$$\text{symbol rate} = \frac{1}{1/B} = B$$

Therefore transmission of signal s(t) is roughly expressed as:

$$\begin{aligned} s(t) &= X(k) \quad kT \le t \le (k+1)T \\ X(0) &\quad 0 \le t \le T \\ X(1) &\quad T \le t \le 2T \\ X(2) &\quad 2T \le t \le 3T \end{aligned}$$

Thus the fog environment has to be sensed and the information updated as per the equation:

$$H(f,t) = \sum_{i=1}^{n} H(t - iT_{rep})$$

Here,

H (f,t) is the temporal CSI

T_{rep} is the time after which the channel needs to be sensed to obtain fog CSI.

CONCLUSION: It can be concluded from the previous discussions that fog computing is the future interface between edge devices and the cloud working for smart automation and massive IoT systems. This paper presents the current status of fog computing research regarding its architecture security threats, existing solutions to those threats, and the open research challenges. The fog system holds the potential to make better decisions and automatically improve the service experience in the future. Constantly evolving technology and security mechanisms with various protocols are used to keep the IoT secure, which is a priority for constrained IoT, Cloud and Fog networks. It is expected that this paper presents headway into future research in the domain of fog computing.

References

[1] G Sun, S Sun, J Sun, H Yu, X Du, M Guizani "Security and privacy preservation in fog-based crowd sensing on the internet of vehicles", Journal of Network and Computer Applications, Vol-34, pp:89-99, Elsevier 2021

[2] R Mahmud, SN Srirama, K Ramamohanarao, "Quality of Experience (QoE)-aware placement of applications in Fog computing environments", Journal of Distributed and Parallel Computing, Vol-132, pp:190-203, Elsevier 2020

[3] Y Zhou, L Tian, L Liu, Y Qi, "Fog computing enabled future mobile communication networks: A convergence of communication and computing", IEEE Communications Magazine, Vol-57, Issue-5, pp_20-27, IEEE, 2019

[4] T Wang, Y Liang, W Jia, M Arif, A Liu, M Xie, "Coupling resource management based on fog computing in smart city systems", Journal of Network and Computer Applications, Vol-135, pp:10-19, Elsevier 2019.

[5] AM Rahmani, TN Gia, B Negash, A Anzanpour, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach", Future Generation Computer Systems, Vol-78, Issue-2, pp: 641-658

[6] M Aazam, S Zeadally, KA Harras, "Deploying fog computing in industrial internet of things and industry 4.0", Vol-14, Issue-10, pp:4674-4682, IEEE Transactions on Industrial Informatics.

[7] S Bitam, S Zeadally, A Mellouk, "Fog computing job scheduling optimization based on bees swarm", Vol-12, Issue-4, pp: 373-197, Journal of Enterprise Information Systems, Taylor and Francis 2018

[8] D Puthal, MS Obaidat, P Nanda, "Secure and sustainable load balancing of edge data centers in fog computing", IEEE Communications Magazine, Vol-56 , Issue: 5, pp: 60-65, IEEE 2018

[9] LF Bittencourt, J Diaz-Montes, R Buyya, "Mobility-aware application scheduling in fog computing", IEEE Cloud Computing, Vol-4, Issue-2, IEEE 2017

[10] L Liu, Z Chang, X Guo, S Mao "Multi-objective optimization for computation offloading in fog computing", IEEE Internet of Things Journal, Vol-5, Issue- 1, IEEE 2017

[11] AV Dastjerdi, R Buyya, "Fog computing: Helping the Internet of Things realize its potential", IEEE Computer Society, Vol-49, Issue-8, pp:12-16, IEEE 2016

[12] R Deng, R Lu, C Lai, TH Luan, "Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption", IEEE Internet of Things Journal, Vol-3, Issue-6,pp: 1171-1181