International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 794-799 www.ijaem.net ISSN: 2395-5252

A Review on Machine Learning Based Security Measures for Massive IoT Networks

Ishika Shrivastava[1], Prof.ReenaKarandikar[2]
Department of CSE, SDBCT, Indore[1,2]

Date of Submission: 20-07-2023 Date of Acceptance: 31-07-2023

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 architectureis 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

II. NETWORK LEVEL SECURITY

Network and cyber security techniques and methodologies have been developed and utilized for some time. Not only are IoT systems vulnerable to most if not all of the existing manner of threats, but also that they pose new security concerns due to several factors. Here, we briefly

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 794-799 www.ijaem.net ISSN: 2395-5252

summarize three main challenges for IoT systems: Limited Device Capability: IoT devices and systems have entered areas that have traditionally been the domain of physical control devices. Such devices are often required to be simple and efficient for dedicated functionalities [4].

As a result, they are designed/equipped/deployed with limited computing and networking capability. Converting these to IoT systems requires significant thought, planning and design, but the rush to market can short circuit this process and imposes severe security risks to the systems.

• Gigantic Scale and Volume: The sheer scale of IoT deployments creates very tempting attack targets for cyber criminals. Discovering and exploiting vulnerability can quickly create a massive army of attackers with which to perpetrate further attacks.

• Vulnerable Environments: IoT devices tend to be placed in unprotected environments easier for attacks to access, comparing to firewall-protected networks. Perhaps most concerning is that low-cost devices are less likely to be patched and maintained in the same manner as traditional physical devices might be, creating an economic disincentive to maintain the software that operates IoT devices. In light of these concerns, considerable thought and effort has been expended to better understand and define the challenges posed by this emerging paradigm, with the hopes that these efforts will result in a more standardized way of considering and addressing the issues that are presented by IoT 5]. The IoT security model is depicted in figure 2.

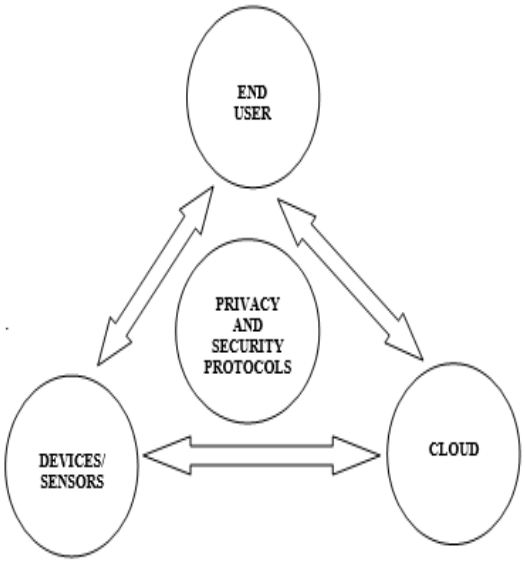

Fig.2 The IoT Security Model

This laudable goal may prove to be challenging given the wide variety of IoT-enabled devices and systems that continue to proliferate rapidly. This challenge is exacerbated by our increased reliance upon these IoT systems and the threats posed by the aforementioned factors. Given this, it is clear that security deployment for IoT must be given careful consideration**.** As discussed earlier, the main challenge faced by the IoT gateway is the decision regarding the authentication of IoTDs and the elated computational complexity. One of the most effective approaches is adding digital fingerprints to the data stream to be transmitted so as to secure the transmission and subsequently use some framework to authenticate the data for [6]:

1) Non-compromise on security
2) Compromised security.

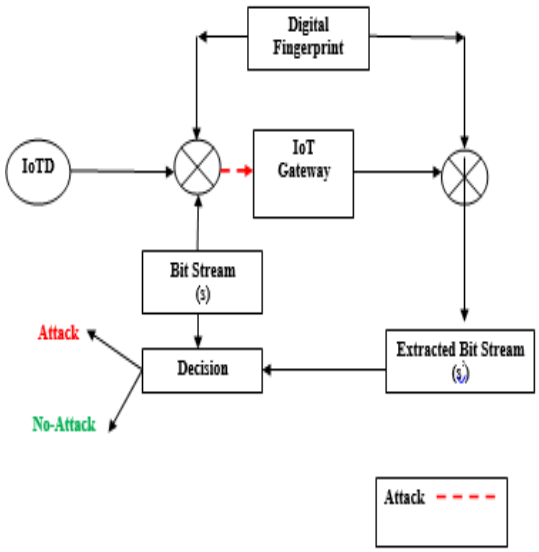

Fig.3 Security Framework for Massive IoT Systems

Let there be 'N' IoTDs which are connected to the gateway 'G'.

Let an $IOTD_i$ generate a bit stream y_i at a given time 't' with a sampling frequency f_i.

This data stream then reaches the gateway 'G' which estimating the status of the IOTDs and controlling them.

The attacker typically records the samples of the IOTDs and tries to manipulate the data to generate a stream y_i'

The responsibility of the gateway 'G' is to compare both y_i and y_i' and take the informed decision based on the comparison. The decision becomes non-trivial with the following constraints [7]:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 794-799 www.ijaem.net ISSN: 2395-5252

1) Extremely large number of IOTDs transmitting simultaneously,
2) Changes in stochastic parameters of the bit stream while travelling from the IOTD to the gateway due to channel effects.
3) Resemblance of y_i and y_i'.
4) Constraints of computational power and latency.

Let the embedded (watermarked) IOTD data stream be given by:

$$\mathbf{w_i(t) = y_i(t) + \beta_i b p_i(t) \forall t = 1 \ldots . n_i}$$

Here,
$w_i(t)$ is the embedded data stream
p_i is a pseudo-noise or pseudo-noise sequence taking values of +1 or -1 for IOTDi

$$\boldsymbol{\beta_i = \frac{\text{Power (PN Data Stream)}}{\text{Power (Original Data Stream)}}}$$

b is the hidden bit stream in the embedded bit stream which can take values of +1 or -1
n_i is the number of samples or frame length of the original bit stream used to hide a single bit.
The IOT Gateway correlates the embedded bit from IOTDi and the PN Sequence to extract the watermarked bit. Mathematically, the gateway computes:

$$\mathbf{\widehat{b_i} = \frac{\langle w_i, p_i \rangle n_i}{\beta_i n_i}}$$

$$\mathbf{\widehat{b_i} = \frac{\langle y_i, p_i \rangle n_i}{\beta_i n_i} + \frac{\beta_i b_i \langle p_i, p_i \rangle n_i}{\beta_i n_i}}$$

Above expressions can be simplified to obtain:

$$\mathbf{\widehat{b_i} = \widehat{y_i} + b_i}$$

Two conditions can exist on evaluation of $\widehat{b_i}$, which are:

{
If $(\widehat{b_i} > 0)$
Extracted bit = 1
elseif $(\widehat{b_i} < 0)$
Extracted bit = - 1
}

Here,
$\langle w_i, p_i \rangle n_i$ denotes the inner product of n_i samples (time metric) of w_i and p_i
$p_i(t)$ and $y_i(t)$ represent independent stochastic variables at time 't'

In case, based on the computation of the stochastic parameters, the gateway computes the received bit stream to be $\widehat{y_i(t)}$ in place of $y_i(t)$, it will trigger an alarm indicating a possible attack. The use of an appropriate machine learning algorithm is mandatory for the purpose. The basic categories of machine leanring are depicetd in figure below.

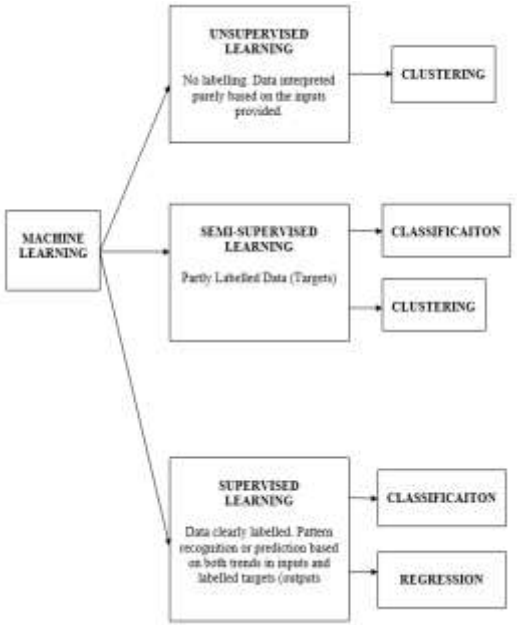

Fig.4 Classes of Machine Learning

A supervised machine learning model is needed in this case for the detection of potential attacks on the IoT gateway based on the stochastic features of the data stream.

III. 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 QoEis 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] proposedanalyzes 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

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 794-799 www.ijaem.net ISSN: 2395-5252

LF Bittencourtet 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. Authorsanalyze 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.

IV. PERFORMACNE METRICS

The performance evaluation metrics for the system which can be computed are:

1) Bit Error Rate
2) Iterations to convergence for the machine learning model
3) Accuracy of machine learning model

For the data transmission to be reliable, the number of bit errors should be as low as possible. The bit error rate of any transmission system is given by [13]:

$$\mathbf{BER} = \frac{\mathbf{No.\ of\ erroneous\ bits}}{\mathbf{No.\ of\ received\ bits}}$$

The BER scenario can be visualized from two aspects:

1) From the Gateways' point of view
2) From the attackers point of view

It is desirable to achieve as low BER as possible for the gateway and as high BER for the attacker. This combinedly can be modelled as [14]:

For the Gateway,

$$\mathbf{P_e = Pr\{\widehat{b_i} = 0, for\ b_i = 1\} \leq P}$$

Here,

Pr denotes probability

$\widehat{b_i}$ is the estimated bit

b_i is the actual bit transmitted

P is a desired low probability

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 2018.

[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 2019

[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

[13] S. Sathyadevan, Vejesh V, R. Doss and L. Pan, "Portguard - an authentication tool for securing ports in an IoT gateway," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 624-629.

[14] PSF Sheron, KP Sridhar, S Baskar, "A decentralized scalable security framework for end to end authentication of future IoT communication", Special Issue on Cross layer innovations in Internet of Things and Advanced Microprocessor Optimization methods for the Internet of Things, Wiley Online Library, vol. 31, no. 12, pp.1-12.

[15] J. Eriksson, E. Ollila and V. Koivunen, "Essential Statistics and Tools for Complex Random Variables," in IEEE Transactions on Signal Processing, vol. 58, no. 10, pp. 5400-5408, Oct. 2010.