Journal of Industrial Information Technology and Application *ISSN(Online): 2586-0852*
Vol.7 No.4

Intrusion detection and prevention in Cloud using Edge intelligence

N.G.S.Parameswaran[1,*)] and Dr.M.Sumathi[2)]
[1)]Department of Computer Applications, VHNSN College, Virudhunagar, Tamilnadu, India
[2)]Department of Computer Science, Sri Meenakshi Govt. Arts College for Women, Madurai, Tamilnadu, India

Abstract. Cloud computing is a booming technology used by IT organizations since it provides all types of services based on pay per use model. Security and privacy is the major concern of clouds. IoT devices are resource constrained devices, and are unable of securing and defending themselves, and can be fluently negotiated and compromised. Thus, it is important to take up proper schemes for authentication and control access to assure the overall security for IoT devices, their communications, and their data. Accessing the IoT devices using cloud is increasing. Also the authentication scheme must be reliable, scalable, and secure against known attacks and threats. Cloud and IoT need to follow stringent security mechanisms to detect its anomalies. Intrusion detection system (IDS) is used to analyse the intruder attack on the cloud. We emphasise the use of anomaly based intrusion detection techniques to prevent the intruder attack. Edge intelligence is the combination of AI and Edge Computing; it enables deployment of machine learning algorithms to the edge devices where the data is generated. It has the potential of providing artificial intelligence to any person and every organization at any place.

Keywords. IoT, Authentication, Cloud, Security, IDS, Edge Intelligence, Edge Computing

1. Introduction

Authentication is the process of certifying an identity by which a set of given credentials are checked against stored data in a database or authentication server [1]. The various threats to cloud are by attacks such as Denial of Service, Distributed Denial of Service, network sniffing, cross-site scripting, IP spoofing, man-in-the-middle attack

* Corresponding author: parameswar2003@gmail.com
Received: Oct 27, 2023; Accepted: Nov 28, 2023; Published: Dec 31, 2023

etc. A traditional way to protect a network device is by assigning it a unique name and password [4]. In this work we discuss about the Intruder attack on cloud network. This attack compromises the Confidentiality, Integrity and Availability of the system. The intruder tries to gain access of the resources which he is not intended to use.

There are many types of Intrusion Detection System as shown in Figure 1.

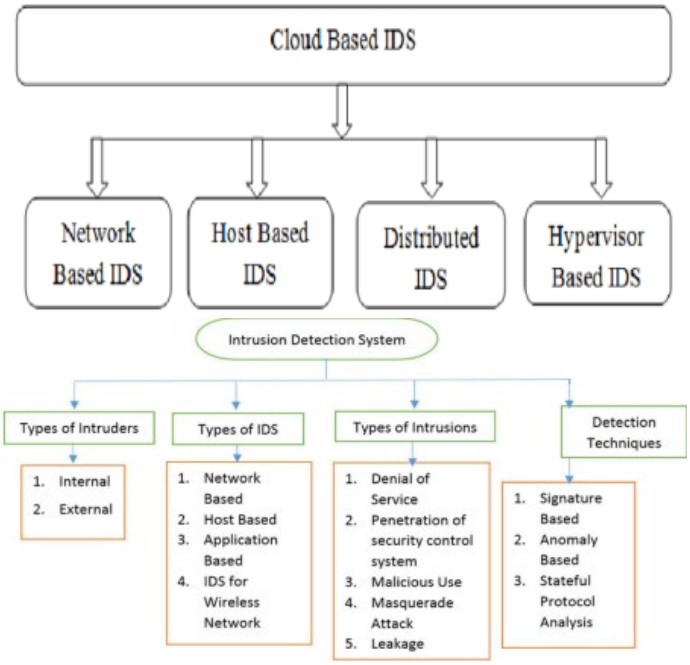

Figure 1. Types of IDS

Edge intelligence along with cloud computing provides lot of benefits including low latency, context awareness, energy efficiency, privacy protection, reduced bandwidth consumption etc [7][8]. Edge computing is the concept of capturing, storing, processing, and analyzing data closer to the location where it is needed to improve response times and save bandwidth. Hence, edge computing is a distributed computing framework that brings applications closer to data sources such as IoT devices, local end devices, or edge servers [3]. Edge computing complements and extends the cloud.

2. Survey

The work of Subburaj.V and Chitra K launches PSO to detect vulnerabilities in mobile sensor, which can be used for detecting anomalies in IoT devices [2]. Gateway verification, generated fitness ratio and node dynamism fight against the attack.

The work of Mehmood, Yasir, et al describes all the features of the available cloud based Intrusion Detection System. It describes the type, positioning, attacks covered, limitations and challenges of the Intrusion Detection Systems [6].

3. Types of intruder attacks

A. Insider attack

The attackers may be the authorised users who intent to misuse the privileges that are allocated or not allocated to them. The attackers may reveal the secrets of the cloud to the opponents or the competitors [6].

B. Attack on hypervisor

The attackers compromise the hypervisor and take control over the virtual machines. The attackers aim at accessing the hypervisor or virtual machines by exploiting the vulnerabilities in the hypervisor or virtual machines.

C. Denial of service attack

The attackers send large number of packets to the available virtual machines and making them unavailable to the legitimate users. Since huge number of request arrives the virtual machines are allocated to handle the request. Availability of the systems becomes the target of this attack.

4. Proposed system

In the earlier work Anomaly detection was done for the IoT devices, the virtual instances and the authentication data. Anomaly detection also eradicates the attacks against the devices and instances. The work used the MDGAN anomaly detection algorithm to eradicate the systems that fail authentication. MDGAN algorithm works with an offline data set [5]. The edge computing devices are capable of processing real time data with the deep learning algorithms and artificial intelligence.

Deep learning gives the ability to identify patterns and detect anomalies in the data sensed by the edge device. Edge computing devices and services act as local data processing and storage source of these systems. It can act as an edge gateway capable of processing data from an edge device and transferring the relevant data back through the cloud.

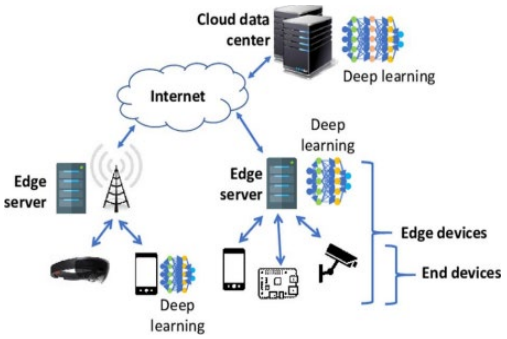

Figure 2. Deep learning in Edge devices

When the intruder tries to gain access over the IoT devices the user credentials are checked. If their intruder has fake credentials the intruder is denied access to the IoT devices and the attack is stopped.

When an inside attacker tries to misuse his privileges to gain access over the cloud resources the user credentials are checked. The resources allocated to the insider can be accessed. The resources beyond the insiders' scope cannot be accessed. When the insider tries to access the devices beyond his scope the insider fails the anomaly detection of authentication data. When the authentication fails the insider is stopped from accessing the cloud resources.

5. Results and discussions

The objective of MDGAN is to improve efficiencies by avoid anomaly detections. It is done by comparing the datasets with different parameter to increase the identification ration in terms of anomaly detections.

The parameter used here are Area Under Receiver Curve (AUC), Precision recall (PR) and Equal Error Rate (EER) respectively. Table 1 to Table 3 displays the various comparison measures based on warm up ratio.

Table 1. COMPARISON BASED ON AUC

Dataset	No Warm Up	One Epoch Warm Up	Three Epochs Warm Up	Six Epochs Warm Up
NSL-KDD	0	0.3%	0.3%	0.3%*
Pendigit	14.2%*	12.6%*	12.5%*	3.9%
Video injection	-0.01%*	-0.01%*	0	-0.22%
Annthyroid	-2.4%	2.3%	4.1%*	4.2%*
Forest cover	44.8%*	25.2%*	25.6%	12.3%

Table 2. COMPARISON BASED ON PR

Dataset	No Warm Up	One Epoch Warm Up	Three Epochs Warm Up	Six Epochs Warm Up
NSL-KDD	0	0.3%	0.3%	0.3%*
Pendigit	14.2%*	12.6%*	12.5%*	3.9%
Video injection	-0.01%*	-0.01%*	0	-0.22%
Annthyroid	-2.4%	2.3%	4.1%*	4.2%*
Forest cover	44.8%*	25.2%*	25.6%	12.3%

Table 3. COMPARISON BASED ON ERR

Dataset	No Warm Up	One Epoch Warm Up	Three Epochs Warm Up	Six Epochs Warm Up
NSL-KDD	0	-2.5%	-3.9%*	-5.3%*
Pendigit	-20.6%*	-12.8%	15.7%*	8.6%
Video injection	1.1%	7.7%*	4.1%*	3.3%*
Annthyroid	6.2%*	5.7%	8.1%*	7.5%*
Forest cover	-15.9%*	-10.8%*	-5.8%	-4.3%

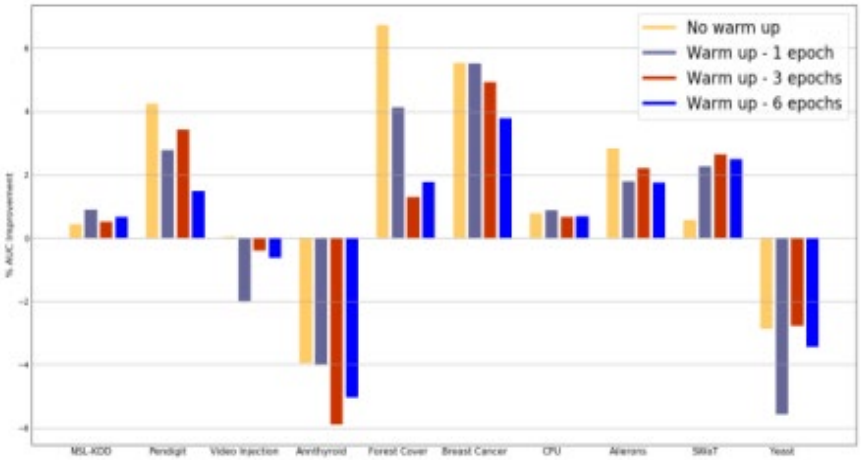

Figure 3. AUC performance at different Warn up to boost accuracy ratio to eradicate error rate

6. Conclusion

Cloud computing faces lot of issues related to security and privacy. Intruder attack is the major concern that affects the availability and trustworthiness of the cloud. Anomaly based intrusion detection system helps in identifying the intruder attack. The

PSO and Anomaly Detection algorithm helps in preventing the intruder attack and other unknown attacks that happens in the cloud environment. In the future work more attacks to the cloud environment can be identified and solved using the PSO and Anomaly Detection techniques.

References

[1] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann,"A review on authentication methods," vol. 7, pp. 95–107, 06 2013.

[2] Subburaj V and Chitra K, "Mobile Node Dynamism using Particle Swarm Optimization to fight against Vulnerability Exploitations", International Journal of Computer Applications (0975 – 8887), Volume 41– No.13, March 2012

[3] Kaur, Kamaljit, and Gaurav Raj. "Comparative analysis of Black Hole attack over Cloud Network using AODV and DSDV." Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology. 2012.

[4] Divyasree, I. R., K. Selvamani, and H. Riasudheen. "Detection of Colluded Black-hole and Grey-hole attacks in Cloud Computing." CoRR (2020).

[5] Parameswaran, N.G.S and M.Sumathi. "Anomaly detection using PSO in cloud integrated IoT devices using MDGAN", International Journal of Aquatic Science, Volume 12, Issue 03, 2021.

[6] Mehmood, Yasir, et al. "Intrusion detection system in cloud computing: Challenges and opportunities." 2013 2nd National Conference on Information Assurance (NCIA). IEEE, 2013.

[7] An, Yufei, et al. "Edge intelligence (EI)-enabled HTTP anomaly detection framework for the Internet of Things (IoT)." IEEE Internet of Things Journal 8.5 (2020): 3554-3566.

[8] Liu, Yaqiong, et al. "Toward edge intelligence: Multiaccess edge computing for 5G and Internet of Things." IEEE Internet of Things Journal 7.8 (2020): 6722-6747