A Study on Intrusion Detection System of Smart Embedded - IoT Environment

[1]Mr.Suresh.B, [2]Dr.M.Venkatachalam, [3]Dr.M.Saroja

[1]Research Scholar, [2]Associate Professor & Head, [3]Associate Professor
[1,2,3]Department of Electronics, Erode Arts and Science College, Erode, Tamil Nadu, India.
[1]Assistant Professor, Department of ECS, VLB Janakiammal College of Arts and Science.

***Abstract*: Internet of Things [IoT] is a rapid technology after mobile communication networks. IoT enables the user with smart applications by connecting the number of devices and sensors. The IoT infrastructure is larger than the conventional network and the security challenges are more in the integrated smart environment. Whenever, the services and applications are notified in embedded IoT smart environment, the raising security issues are to be addressed in a correct manner. The security of IoT systems is a serious issue due to the increasing numbers of services and users in IoT networks. So, the impacts of IoT security problems are very critical issues in industry. This paper deals the security for integrated IoT Smart Services Environment which could resolve the security problems in order to performance metrics.**

***Index Terms:* IoT, Smart environment, Security issues , Sensors**

I. Introduction

Embedded based Smart environments consist of sensors that work together to execute various operations. Wireless sensors, wireless communication techniques, and IPv6 assist in the expansion of smart environments. Such environments are wide ranging, from smart homes to smart healthcare and smart services. The integration of IoT systems and smart environments makes smart objects more effective. The IoT systems are affected by various security attacks, such as denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks. Such attacks can damage to the IoT services and smart environment applications in an embedded IoT network[10]. Hence, securing IoT systems has become a major concern that has been achieved by Intrusion detection system (IDS).

The implementation of IDS depends on the environment. A host-based intrusion detection system (HIDS) is designed to be implemented on a single system and to protect that system from intrusions or malicious attacks that will harm its operating system or data [1]. A HIDS generally depends on metrics in the host environment, such as the log files in a computer system [2]. A network-based intrusion detection system (NIDS) sniffs network traffic packets to detect intrusions and malicious attacks [2]. A NIDS can be either a software based system or a hardware-based system.

II. Literature STUDIES

Researchers study the security challenges of the IoT from many different points of view, one of which is the security vulnerability of IoT communication protocols [3]. This survey focuses on IDSs for the IoT paradigm, independent of any specific protocol; thus, this study focuses on the security challenges facing IoT systems on the basis of the IEEE definition and the general IoT architecture. According to Liu X et al, [4], the security-related problems of any IoT system can be categorized into four types: authentication and physical threats, confidentiality risks, data integrity issues and privacy problems.

In 2013, Ganapathy et al. [5] presented a survey on intelligent techniques for feature selection and classification-based intrusion detection in networks. This survey considered fuzzy techniques, neural networks, genetic algorithms, neuro-genetic algorithms, particle swarm intelligence and rough sets for Internet security protection and QoS enhancement.

In 2014, Mitchell and Chen [6] surveyed 60 papers on IDSs designed for wireless environments. Their survey revealed the strengths and weaknesses of IDS techniques for wireless local area networks (WLANs), wireless mesh networks (WMNs), wireless personal area networks (WPANs), wireless sensor networks (WSNs), cyber-physical systems (CPSs), ad hoc networks and mobile telephony.

In [7], Yung et al. concluded certain IDS approaches which are an essential network structure that belongs to IoT. By examining and evaluating attack techniques and detection, this work evaluated prevailing GIDP, CRADS and other intrusion detection structures for MANET.

Ahmed et al. [8] state that “The term smart refers to the ability to autonomously obtain and apply knowledge, and the term environment refers to the surroundings”. A smart city is one type of smart environment. The core element of a smart city is an integrated information center operated by the IoT service provider, which provides information on services such as electricity, water, and gas.

III. ANALYSIS OF PERFORMANCE METRICS

The Smart embedded IoT environment security performance of IDS and its Simulation to be carried out in MATLAB 2018, for classification of IDS modelling. The measurement of the performance is with IDS datasheet [9]. Precision, Recall and F1-score are the accountable performance metrics in this simulation method. It provides simulation over real time IoT data transmission. F1-score, recall and precision were evaluated as in Table I and Figure 1.

Table I: Performance metrics

Class	Precision	Recall	F1-score
0	98	94	81
1	85	96	92
Total	92	95	87

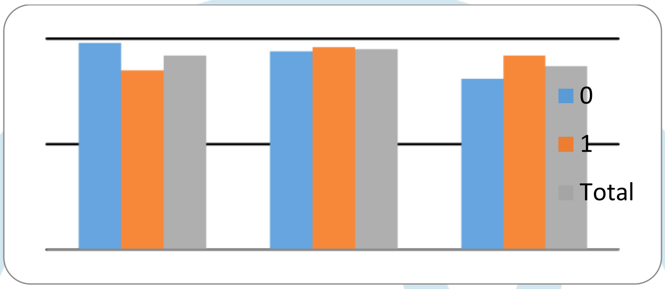

Fig.1. Performance metrics

CONCLUSION

The security attacks of Embedded- IoT Environment has prevented by IDS. Here, the performance of IDS to be carried out with the help of IDS data sheet and MATLAB Simulation. In addition, the IDS will be implemented on programmable reconfigurable hardware devices, such as FPGAs, to facilitate adaptation to IoT-based smart environments. In Future the IoT traffic distribution among the embedded network, Precision, Accuracy concepts have to analyse.

REFERENCES

[1]. Creech G, Hu J (2014) A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns. IEEE Trans Computer 63(4):807– 819

[2]. Kumar S, Gautam, Om H (2016) Computational neural network regression model for host based intrusion detection system. Perspect Sci 8:93–95

[3] . Granjal J, Monteiro E, SáSilva J (2015) Security for the internet of things: A survey of existing protocols and open research issues. IEEE Commun Surv Tutor 17(3):1294–1312

[4]. Liu X, Zhao M, Li S, Zhang F, Trappe W (2017) A security framework for the internet of things in the future internet architecture. Future Internet 9(3)

[5]. Ganapathy S, Kulothungan K, Muthurajkumar S, Vijayalakshmi M, Yogesh P, Kannan A (2013) Intelligent feature selection and classification techniques for intrusion detection in networks: a survey. EURASIP J Wireless Communication Networks 2013(1):1–16

[6]. Mitchell R, Chen I-R (2014) A survey of intrusion detection in wireless network applications. Comput Commun 42:1–23

[7]. YH Yang, HZ Huang, QN Shen, et al., Research on intrusion detection based on incremental GHSOM. Chin. J. Comput.. 37(5), 1216–1224, 2014.

[8]. Ahmed E, Yaqoob I, Gani A, Imran M, Guizani M (2016) Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wirel Commun 23(5):10–16

[9] Moustafa, N., Slay, J.: UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: 2015 Military Communications and Information Systems Conference (MilCIS). IEEE, 2015.

[10] Pacheco, J., Hariri, S.: IoT security framework for smart cyber infrastructures. In: 1st International Workshops on Foundations and Applications of Self Systems, 2016.