THINK INDIA JOURNAL

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

Issues and Challenges In IDS In Smart Environment of Iot

Ashish Kumar[1], Chavi Kapoor[2], Rahul Saha[3]

[1,2,3] Lovely Faculty of Technology and Sciences

Lovely Professional University, Punjab, India

[1]ashish.11801008@lpu.in, [2]ch.kapoor01@gmail.com, [3]rahul.18818@lpu.co.in

Abstract

The purpose of IoT is to improve the efficiency of the work done by a human in every aspect of life either home, city, hospital, agriculture. So, along with high-efficiency security is also a major area of concern. An analysis of the data which flows over the smart environment may contain malicious data which can be more harmful. So, finding these types of data introduced IDS in the IoT network. In this paper, there is an analysis of some of the IDS technique which is already used in IoT smart environment. Some of the technique are lightweight which matches the requirement of IoT. Finally, at last, some of the open research problems are discussed in the paper.

Keywords: Internet of things (IoT), Intrusion detection system (IDS), CIA, HIDS, NIDS.

1. INTRODUCTION:

The Internet of Thing is the network where all the heterogenous and homogenous devices connected and form a smart environment. The smart environment like smart cities, smart hospitals, smart homes and many more. Devices in smart cities such as street cameras, traffic signals, street light and many more, similarly in smart hospital devices such as a smart wheelchair, call points and many more, and in smart homes devices such as washing machines, air conditioners, fan, led bulb and many more. Using all the devices together smart environment is formed. In IoT network end node devices such sensors, RFID tags collect, analysis and transfer the data over the network [1]. These end node devices work at the back end for each device which is used for the IoT network. The exchange of data can be by using ZigBee, Bluetooth, router or any other medium. But while exchanging data over the network maintaining security is a major factor. While creating a network device can be registered, authenticated, verified, but how to monitor the data when actual communication will take place. IoT network is the network which communicates over wireless sensor network and when the data travel in the wireless network there could be many attacks can happen in the network like DoS attack, Man In the middle attack (MiM) and many new or old types of attacks. And as per the survey by the end of 2025, there may be more than 73 billion connected devices in an IoT network [2]. So how to manage security for such a huge network.

An intrusion detection system (IDS) is the security technique which is used for the detection and prevention of intrusion, intrusion such as attacks, malicious code, infected file [3]. It works mainly on the network layer of IoT. It analyses any type of intrusion it will be informed to the admin and prevent with that intrusion. There are criteria that IDS which are designed for IoT are it should work with less processing capacity but the quick response, high data volume. Therefore, in standard IDS all the condition is not fulfilled in IoT smart environment due to its requirement of high processing capacity.

Architecture of IoT:

The typical architecture means that how data will be transfer over the network of IoT i.e., form end node device to the user interface and vice versa. So, it follows three-layer architecture.

1. *Application layer* [4]: It is the topmost layer of the IoT architecture, its layer provides the anthropomorphize based services according to user pertinent needs. Its major responsibility

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

is to receive data from the network layer and fulfil the gap between the user interface and application of IoT.

2. *Network layer* [4]: It is the middle layer of the IoT architecture, this layer main responsibility is to form secure communication between application and end node device and secure the data over the network. It also ensures the unique routing and addressing of the innumerable devices in a single cooperative network.
3. *Perception layer* [4]: This layer is the lowest in the architecture of the IoT. The main responsibility of this layer is that it connects all the end node devices either sensor or the mobile or any other type of the devices and transfer the data in digital setup.

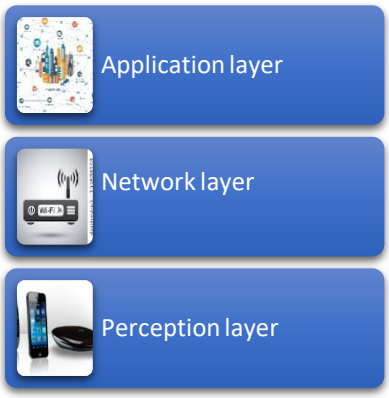

Figure 1: Architecture of IoT

Further in this paper section 2 objective of security, section 3, some brief about IDS, section 4 IDS in IoT network in section 5 literature review, Open research problem in section 6 and lastly in section 7 conclusion of the paper.

2. OBJECTIVE OF SECURITY

Whenever any network is formed it must the CIA security traid model, it is a prominent model for the evolution of the security mechanisms, executes the security by making use of the three major areas which are always considered these are Confidentiality, Integrity, and Availability this is the CIA security traid model, as illustrated in the figure 2.

1. *Confidentiality:* It is the capability to give trust to the user that "data is protected" and about the privacy of the impervious or sensible information. The main reason is to secure the network from unauthorized access. To provide confidentiality to the network there is various encryption bases authentication technique.
2. *Integrity*: It is the ability to provide trust that data over the network is unchangeable form unauthorized persons by the mean of criminal causes.
3. *Availability:* It is the ability that ensures that the entire device in the network should remain online and available. There are many protocols which provide availability such as firewall intrusion detection system, redundancy methods.

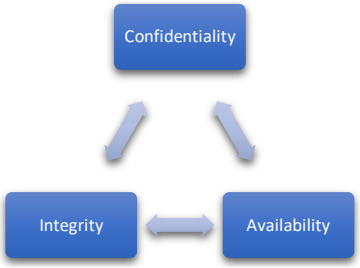

Figure 2: CIA model

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

3. INTRUSION DETECTION SYSTEM

Intrusion detection system or IDS helps to discover and analyse the user's data, network traffic. It analyses the traffic and data over the network and finds the security vulnerabilities in time to time manner [5, 6]. It helps to protect the CIA traid model over any type of data and network [7]. The process of IDS is majorly splitted into three areas, the first area is observing the traffic over the network, the next area is the analysing phases and the last is the detection if any malicious or threat is found by the IDS, there can be an additional phases where IDS along with detection, it also prevent from that type of threat if the solution is already available with IDS. And send the log file of every phase either monitoring, analysing, detection or prevention to the administrator.

Classification of IDS is depending as per the requirement either it is used for a single system or it is used for the whole network. For a single system, host-based IDS (HIDS) [8] is required and when the number of systems is increased or the whole network is monitored network-based IDS (NIDS) [8] came into existence. HIDS and NIDS working are explained in the figure 3 and 4.

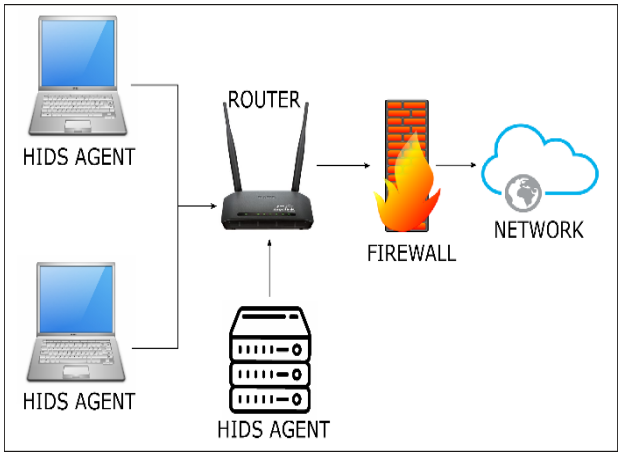

Figure 3: HIDS

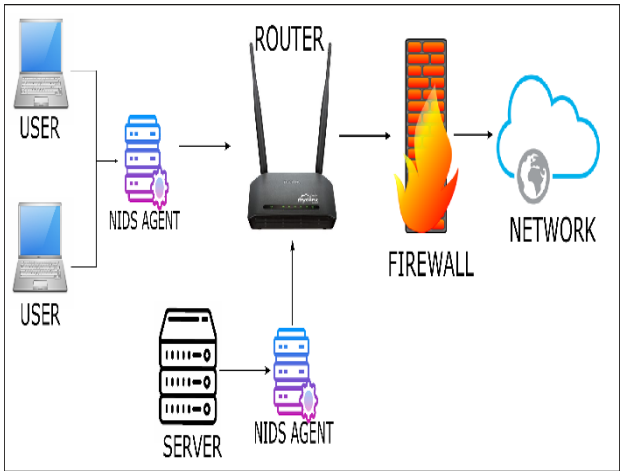

Figure 4: NIDS

4. IDS IN IoT NETWORK

In the network of IoT either it can be smart cities, hospitals, homes, etc., IDS is executed in the network layer of IoT architecture. It is done because it can monitor the data flow in the network either it is coming from the application layer or it is going to the application layer. In the network layer, the data are being analysed in real-time. There is a requirement that all the processing i.e., monitoring, analyses or detection should work with low processing ability with fast responses along

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

with large data processing. These requirements of IoT in IDS separate the general IDS which are used in a conventional network. The basic workflow of IDS in the IoT network is shown in figure 5.

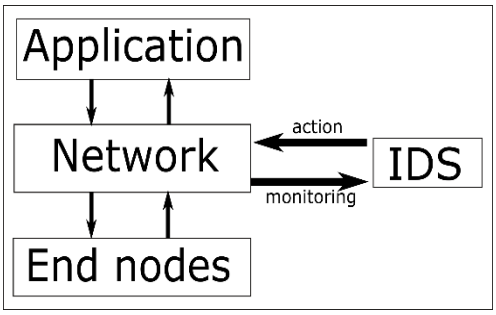

Figure 5: IDS in IoT

Basically, IDS is splitted in two types host-based IDS and network-based IDS.

i. **Host based Intrusion detection System (HIDS):** HIDS or Host based Intrusion detection system is IDS that provides security for internal computer system along with network packets on its network interface. HIDS has capacity to monitor the dynamic behaviour of the computer system. It can detect which program have access to what resources. For instance, suddenly word-processor start modifying the password database files.
ii. **Network based Intrusion detection System (NIDS):** NIDS or network-based intrusion detection system is the system which help to detect all the activity related to hacking on the network such as any types of attacks like DoS attacks, MiM attack or any other type of attacks. It helps in detection of incoming, outgoing or local traffic.

5. REVIEW LITERATURE

Many works have been done in for making IDS for IoT in smart environment. In the work done by Mohan et al. proposed a host-based IDS (HIDS) [9]. It works on signature and rule-based detection techniques. It works with the combination of traditional signature-based and SNORT rule-based IDS [10, 11]. A machine learning (ML) approach is proposed by Arrignton et al. [12], it is also a HIDS. The ML is build on the idea of an artificial immune system. It provides highly efficient monitoring and able to cancel the noise in the environment.

Deng et al. [13] propose a lightweight network-based IDS (NIDS) which works on fuzzy c-means clustering and PCA algorithm [14]. In this approach, both machine learning and data mining concept are merge. Its main feature is that it has improved the detection capability with low FRP. Another lightweight NIDS is proposed by Abhishek et al. [15], it depends on the packet dropping probability. It works on the statistical model for the detection of any malicious activity. The major feature of this IDS is that it works in real-time. It doesn't require any training dataset. There is a drawback that it only detects downlink packet but if the packet is uplink it will not detect. Oh et al. [16], suggested another lightweight pattern matching IDS, it replaces the traditional IDS.

Another lightweight IDS is proposed in [17], it is host based IDS and working with resources constraint devices. As many of the devices which are used in IoT network are having very less resources. Author targeted DDoS type attack with this IDS. For classification it uses machine learning based support vector machine (SVM). In the work proposed by Peisong et al., in [18], clam deep belief Network (DBN) for IDS. It basically works on unsupervised data. Its main advantage is that it creates specific structure for specific attack. It requires small training set and provide more classification accuracy. Another protocol was suggested by EAnthi et al. [19]. It is network-based detection system which is working in two phases. In first phase where testbed is built for IoT network and in second phase various attacks are scanned over the network. It helps in finding the

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

abnormality in the network. IDS is IoT. Shreenivas et al., propose an IDS for IoT [20]. The major aim of this work is to be upgrading the security inside 6LowPAN systems, the author broadens SVELTE with an interruption recognition module which uses the ETX (Expected Transmissions) metric. In RPL, ETX is a connection unwavering quality measurement and observing the ETX worth can keep a gate-crashed from effectively captivating 6LoWPAN hubs in malignant exercises. They likewise propose geographic insights to recognize pernicious hubs that direct attacks against ETX-based systems.Midi et al. proposed an IDS for IoT called Knowledge-driven Adaptable Lightweight Intrusion Detection System (Kalis) [21]. The author utilizes an incorporated position technique on which Kalis can be sent on outskirt switch or as independent apparatus on isolated, outer gadget. The hybrid method of detection is depending on the way that Kalis is a self-adjusting, information driven IDS for IoT frameworks running diverse correspondence conventions. Kalis self-governing gathers information about the highlights of the checked system and elements and use such information to powerfully arrange the best arrangement of recognition strategies.

A comparison of different intrusion detection systems is shown in table 1, where the category is based on the type of IDS i.e., HIDS or NIDS and the feature of the protocol and the limitation in the protocol.

Table 1: Comparison of different IDS protocol in IoT

Protocols	Type	Features	Drawbacks
Mohan et al. [9]	HIDS	Rule based and signature model	More resources and privacy issues
Arrignton et al. [12]	HIDS	Machine learning and cancelation of noise	Not worked on real world data
Deng et al. [13]	NIDS	ML and Data mining, light weight, detection with low FRP	Security issue with heterogeneous device
Abhishek et al. [15]	NIDS	Statically model, no training dataset	Unable to detect uplink packet
Oh et al.[16]	NIDS	Light weight, patter matching.	With limited memory lead to performance degradation
SU Jam et al. [17]	HIDS	Light weight, Supervised machine learning based SVM,	Limited only to DoS attack, Unable to handle high traffic.
Peisong et at. [18]	NIDS	Unsupervised data set, high classification accuracy	Other parameters in DBN is not optimized.
EAnthi et al. [19]	NIDS	Work on two phases, it uses ML for distinguish the data from each phase.	Less attacks are taken in consideration.
Shreenivas et al. [20]	NIDS	Improve security of 6LoWPAN.	Unable to handle from some attacks like routing attacks
Midi et al., [21]	NIDS	Lightweight IDS, it uses ML concepts	More improvement is to be done for detection more attack.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

6. OPEN RESEARCH PROBLEM

As most of the IDS in current time is work on the traditional IDS to maintain the performance of the system, but the requirement of the IDS is not matching with IoT. As in every IoT network, the device which we are using is having very little memory and the processing speed is very less. So, with these issues, many other challenges are being faced by IoT as it has a dynamic nature.

Traffic characterization: As the flow of data is from the same as well as a different type of devices in the network, so the data is more complicated and so traffic characterization is very much important.

Traffic filtration: IDS provides whitelist as well as a blacklist after filtration but it difficult in IoT network because there aremany devices is connected on the network, IDS provides the filtration but failed to generate the full list.

7. CONCLUSION

As IoT is the emerging technology and with a rise in the number of devices connected in the network, the security of data that flows over the network should be in danger. Various steps had already been taken such as providing secure authentication protocol, but it fails to monitor every data which flows over the network. Monitoring the data firewall are installed. Again, it cannot provide full security as false positive will increase. So, IDS came into existence. And it has solved many problems like detection and prevention of malicious activity, but at a high cost. It required high computation speed, large memory. But end nodes used in IoT networks have very less processing speed, less memory. So, the solution to this problem is to use lightweight IDS in IoT which can be compatible with IoT network. Some work is done which introduced lightweight version of IDS, but they are capable with single attack detection and handling. So, taking the requirements into consideration IDS should be developed in such a way which can be used in any type of IoT network either in Smart homes, or Smart grid.

REFERENCES:

[1] https://www.lifewire.com/introduction-to-the-internet-of-things-817766

[2] https://www.newgenapps.com/blog/iot-statistics-internet-of-things-future-research-data

[3] Gendreau, A. A., & Moorman, M. “Survey of intrusion detection systems towards an end to end secure internet of things”. *IEEE 4th international conference on future internet of things and cloud (FiCloud)* (pp. 84-90). IEEE, 2016.

[4] Frustaci, M., Pace, P., Aloi, G., &Fortino, G. “Evaluating critical security issues of the IoT world: present and future challenges.” *IEEE Internet of Things Journal*, *5*(4), 2483-2495,2018.

[5] Scarfone, K., & Mell, P. “*Guide to intrusion detection and prevention systems (idps)*”(No. NIST Special Publication (SP) 800-94 Rev. 1 (Draft)). National Institute of Standards and Technology,2012.

[6] Elrawy, M. F., Awad, A. I., & Hamed, H. F, “Intrusion detection systems for IoT-based smart environments: a survey”. *Journal of Cloud Computing*, *7*(1), 21.,2018.

[7] Ghorbani, A. A., Lu, W., &Tavallaee, M.” *Network intrusion detection and prevention: concepts and techniques”* (Vol. 47). Springer Science & Business Media,2009.

[8] Gautam, S. K., & Om, H.“Computational neural network regression model for Host based Intrusion Detection System”. *Perspectives in Science*, *8*, 93-95,2016.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[9] Danda, J. M. R., &Hota, C. "Attack identification framework for IoT devices. In *Information Systems Design and Intelligent Applications"* (pp. 505-513). Springer, New Delhi,2016.

[10] Olanrewaju, R. F., Khan, B. U. I., Najeeb, A. R., Zahir, K. N., & Hussain, S. "Snort-based smart and swift intrusion detection system". *Indian Journal of Science and Technology*, *8*(1), 1-9,2018.

[11] Karen Scarfone and Peter Mell, "Manual for Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology, Special Publication 800-94, Feb. 2007.

[12] Arrington, B., Barnett, L., Rufus, R., & Esterline, A. "Behavioralmodeling intrusion detection system (bmids) using internet of things (iot) behavior-based anomaly detection via immunity-inspired algorithms." *25th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-6). IEEE, (2016, August).

[13] Deng, L., Li, D., Yao, X., Cox, D., & Wang, H. "Mobile network intrusion detection for IoT system based on transfer learning algorithm." *Cluster Computing*, 1-16,2018.

[14] Heba, F. E., Darwish, A., Hassanien, A. E., & Abraham, A. "Principle components analysis and support vector machine based intrusion detection system." *10th international conference on intelligent systems design and applications* (pp. 363-367). IEEE.,2010.

[15] Abhishek, N. V., Lim, T. J., Sikdar, B., & Tandon, A. "An intrusion detection system for detecting compromised gateways in clustered iot networks." *IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)* (pp. 1-6). IEEE, (2018, May).

[16] Oh, D., Kim, D., & Ro, W. "A malicious pattern detection engine for embedded security systems in the Internet of Things." *Sensors*, *14*(12), 24188-24211,2014.

[17] Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I. "Toward a Lightweight Intrusion Detection System for the Internet of Things." *IEEE Access*, *7*, 42450-42471,2019.