Rakhi,, 2022, 10:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

# Survey on IoT Network Security Challenges and Techniques of Detection

**M.Tech. Scholar Rakhi, Asst. Prof. Sumit Sharma**
Dept. of CSE
Vaishnavi Institute of Technology, Bhopal, MP

**Abstract-Technology improve life of human at every stage but small network increase this comfort by various appliance. Network appliance mostly depends on IoT 9Internet of Things), hence intruders always take advantage of such weak network. This paper has survey on different requirement of IoT network and its importance in human life. Types of attack were also discuss in the paper with its attack pattern. In order to protect from such attacks network uses intrusion detection system for the safe communication of devices. Basic architecture of the IDS were elaborate in paper with its types. This paper cover different techniques proposed by scholars in field of IoT network intrusion detection system. Some of primary evaluation parameters were also discuss in the paper.**

**Keywords- Deep Learning, Intrusion Detection, Feature Optimization, Soft Computing.**

## I. INTRODUCTION

IoT [1] is an emerging Internet-based computing model that provides tenants with seemingly "unlimited" IT services, thereby freeing them from complex underlying hardware, software, and protocol stacks. Although "open for all service" is the essence of cloud computing, it does not necessarily comprise useless information. Tenants can use cloud services for efficient computing.

However, they can also abuse the cloud environment and attack the network. For example, a malicious tenant may reside in a virtual machine (VM), successfully intrude into other VMs in the cloud, and use the puppet machines to spread malicious software, or launch distributed denial of service (DDoS) attack, and so on. In fact, tenant behavior will generate massive network traffic in the cloud environment, mainly including "north-south" and "east-west" traffic. The "north-south" traffic mainly refers to the traffic of tenants accessing

One of the primary concerns in the cloud is the ability to maintain data protection and trust management between multi-cloud service providers [5]. Cloud systems are public, distributed and decentralised, and this potentially leads to challenges of trust as different components are controlled by different parties. Cloud providers are usually reluctant to share data or report intrusion events due to concerns about data confidentiality and privacy [3], [6]. It is quite difficult to measure the level of reputation among untrusted participants.

A collaborative IDS (CIDS) would be a protection layer to detect insider and outsider attacks, which denotes the development of distributed intrusion detection engines across network nodes of cloud systems [4]. It should be scalable and cost-effective to inspect various cloud nodes for discovering new cyber attacks. Intrusion Detection Systems (IDS) are used to detect attacks. Intrusion detection methods are classified into two groups as anomaly detection and misuse detection according to their detection technique [7], [8]. Misuse detection methods use patterns of attacks to identify the intrusions.

International Journal of Science, Engineering and Technology

An Open Access Journal

Anomaly detection methods use attack-free network traffic patterns to identify the attack.

## II.TYPES OF ATTACK

### 1.Insider attack

Sometimes people having the authorization to use the cloud service, though choose to gone through the insider way. This mainly done with the intention of using the unauthorized privileges and revealing the information to other clients or in market. An insider attack has been planned mostly by the employees of the competitors or the cloud administrator in the domain client company having right to access those. They also had hand in modifying the company's information and documents. The best-known example to clear about this insider attack is the Amazon Elastic Compute Cloud (EC2) – an internal attack of DoS.

### 2.Malware injection attack

In this attack, the attacker has the motive of not only accessing the information but also get control over it of the client data. For this attacker creates its own service implementation module for setting it into a client cloud system. For this uses SaaS/PaaS method or the virtual machine instance into the IaaS solution. To result in a performing malicious activity, attacker if gets succeed in his work of cloud fouling, the cloud will automatically accept and sends the hacker module information to the user. Due to which the begins of malicious activities performing by the attacker.

Types of attacks under this category:

**Cross site scripting attack**: XSS uses the HTML for the attack in which malicious code is injected into the data by using the Flash, JavaScript or others.

**SQL injection attack:**In this attack the attacker uses the input field of the database of the user. The most common example for such types of attacks are the attack occurred on the Sony play station in the year 2008 website.

**Command injection attack:** the name of this attack is given as per its role, because it injects the command and those commands are run according to the runtime environment or may create shell.

### 3. Abuse and Nefarious use of cloud services

The main difference in this attack than the insider is the attackers background, otherwise all is in common. In the insider attack the attacker is the authorised user of the data while in this attacker is the hacker which attacks the less secured database or poor clouds. As due to this no need of using expensive DoS and did brute forced attacks on the target.

### 4. Denial of service attack

This type of attacksis mainly done by the flooded networks having many packets like TCP, UDP, ICMP or their combinations.due to the risk of the intruder attack on the distributed services of the computer, some of them are not even available to the authorised users also. As this attack overloads all the systems, due to which legal users are unable to used them.These types of attacksprove very dangerous for the single cloud data and servers as many users depends on that cloud distributed network.

### 5. Side channel attack

This type of attack done with the cryptographic algorithm of the system. For this they used the special VMM service which is virtual machine manger which guides the user attack for the creation of virtualization layer. They placed a physical virtual machine on the targeted system, while VMM helps other users and supervises known as hypervisor.

### 6. User to root attack

In this attack, the attacker uses the sniffing password for the authentication of the targeted user's system. So, by combining traditional various methods for the raising of the privileges to the super user access acceptance. An example of such escalation technique is the smashing stack, in which a packet of the set-UID- root program that corrupts the address space, so that returning information from the instruction to subshell space.

### 7. A remote to Local attack

In this attacker takes the advantages of the targeted user local privileges. This attack is also known as remote to user attack. In this attacker sends packets to the user host and close the exposures of the access of asxlock, guest, xnsnoop, phf and sendmail.

**8. Scanning Attacks** A scanning attack [27] is an attack that attempts to send packets of information to a network system to gather information about the topology. It involves looking for ports which are either open or closed, what type of traffic is

International Journal of Science, Engineering and Technology

An Open Access Journal

permitted and not permitted, which hosts are active or even the type of hardware running on different devices. For instance, a type of attack that finds weak points in a network is Blind SQL injection attacks. A Blind SQL injection attack is an attempt to ask a database questions that make it respond by a Boolean value to find vulnerabilities. These types of attacks often attempt to find open ports to be exploited by injecting malicious code or malware.

**9. Asymmetric Routing** When packets take a specific route to the destination, and a different route back to the source, this behaviour is called asymmetric routing [27]. This behaviour is normal in general, but it is unwanted. The reason behind that is adversaries can benefit from asymmetric routing by sending malicious data through particular parts of the network to bypass security systems, depending on firewalls configuration. If the network is allowed to perform asymmetric routing, then it is exposed to attacks such as SYN flood attacks. An SYN flood attack is an attack that attempts to open many connections without closing them (half-open attack), which leads to a total consumption of system or server resources so that it becomes unresponsive. This attack is a DDoS attack type, and one reason to deactivate asymmetric routing in the network.

**10. Buffer Overflow** Attacks Buffer overflow [27] attacks attempt to replace normal data with malicious data in penetrated memory parts, such that a malicious code gets executed later on. In generic terms, a buffer overflow attack writes more data in the memory's buffer than it can handle; performing this action results in making the data overflow into the neighbouring memory.

## III.IDS Architecture and types

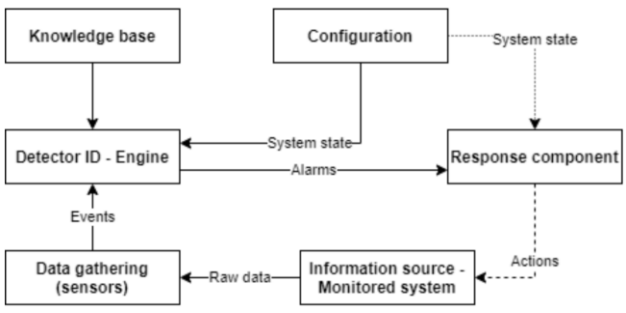


Fig. 1: A simplified IDS architecture.

In Intrusion Detection Systems, there are a diversity of techniques to gather data [7], but in general, as shown in Figure 1.2, IDSs consist of the following:

- Data gathering (sensors) is device that is responsible for gathering information from the system.
- Detector ID - Engine analyzes the data collected from the sensors to identify any attacks.
- Knowledge base (database) is the component where the IDS contains information about traffic collected by the sensors. Security professionals usually provide such information.
- The state of the Intrusion Detection System is revealed by the configuration device.
- When an attack or intrusion is discovered, the response component is in charge of taking action. There are two types of responses: passive and active.

## IV.TYPES OF INTRUSION DETECTION SYSTEM

Without taking into account any hybrid or distributed combinations, there are two types of intrusion detection systems; host based intrusion detection systems (HIDS) and network based intrusion detection systems (NIDS). For completeness of this research, we also take into account additional log sources that can be analysed. For example, one might use firewall logs as alternative source to verify intrusions on the network boundary. This is relevant in the cloud setting as CSPs might provision certain infrastructural, activity, diagnostic or application logs. HIDS and NIDS are usually interleaved. HIDS catches intrusions the NIDS misses out on and vice versa.

**Host Based Intrusion Detection** As the name indicates, HIDS monitors a host. In general, it accomplishes this by monitoring a list of objects (e.g., the files from the file system). HIDS then checks logs and activity occurring on these objects for unwanted modifications, memory and data integrity, system calls and more.

**Network Based Intrusion Detection** A NIDS on the other hand, monitors packets that flow through the network, checking them for malicious content or policy violations [1]. The detection unit is usually placed as test access point (TAP) or switch port analyzer (SPAN) on a switch that mirrors the data elsewhere. Traditionally, there are two placement options for a NIDS sensor.

International Journal of Science, Engineering and Technology

An Open Access Journal

Firstly, there is an inline option, which is a device that is placed on the network route. Consequently, the NIDS can actually stop packets from reaching their destination, possibly turning the intrusion detection system in an intrusion prevention system. However, this requires the packet analysis to happen inside this inline NIDS device, which introduces additional latency.

Secondly, there is out of band NIDS, which sits outside the network. Instead out of band uses copies of the data. The copies are usually provided via a mirroring port on a switch or TAP. Out of band introduces little to no extra latency, which is desirable, especially in networks under heavy loads. On the downside, out of band looks at copies, so the data is no longer real time.

## V.RELATED WORK

Xiu Kan et. al. in [9] proposed a novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network (APSO-CNN). In particular, the PSO algorithm with change of inertia weight is used to adaptively optimize the structure parameters of one-dimensional CNN. The cross-entropy loss function value of the validation set, which is obtained from the first training of CNN, is taken as the fitness value of PSO. Especially, we define a new evaluation method that considers both the prediction probability assigned to each category and prediction label to compare the proposed APSO-CNN algorithm with CNN set parameters manually (R-CNN).

M Islabudeen et. al. in [10] work on mobile ad-hoc network based smart IDS is evaluated for MANER-Security. They have utilized artificial neural network (ANN) for data packets classification. They stated that classification plays a major criteria in intrusion detection. Boat classifier is developed here. The system is efficient in rare attacks, Dos and probing problems are discussed [11].

Yue Jin et. al. in [12] works on home level intrusion detection system, using Wifi-Enabled IOT devices. They implemented a RSSI (Received signal strength indicator) based identification router that incorporate with a detection algorithm and visualize the whole home security through IOT. The idea of IOT security with RSSI gives apt results for them, that they concluded proposed design optimizes accurate detection.

Fuhong Lin et. al. in [13] proposed study and implementation on IDS in edge routed networks that blend with Dos attack analysis, edge network intrusion detection, edge node cloud security etc., SDMMF single-layered Min-max fair allocation scheme is used. The concluded paper states that they have given efficient solution for multi-layer resource allocation problem [14].

J. Liu. Et. al. in [15] proposed a particle swarm optimization-based gradient descent (PSO-LightGBM) for the intrusion detection. In this method, PSO-LightGBM is used to extract the features of the data and inputs it into one-class SVM (OCSVM) to discover and identify malicious data. The UNSW-NB15 dataset is applied to verify the intrusion detection model.

E. Anthi et. al. in [16] proposed a three layer intrusion detection system (IDS) that uses a supervised approach to detect a range of popular network based cyber-attacks on IoT networks. The system consists of three main functions: 1) classify the type and profile the normal behavior of each IoT device connected to the network; 2) identifies malicious packets on the network when an attack is occurring; and 3) classifies the type of the attack that has been deployed. The system is evaluated within a smart home testbed consisting of eight popular commercially available devices. The effectiveness of the proposed IDS architecture is evaluated by deploying 12 attacks from 4 main network based attack categories, such as denial of service (DoS), man-in-the-middle (MITM)/spoofing, reconnaissance, and replay.

In [17] author proposed an efcient AI-based mechanism for intrusion detection systems (IDS) in IoT systems. We leverage the advancements of deep learnings and metaheuristics (MH) algorithms that approved their efciency in solving complex engineering problems.We propose a feature extraction method using the convolutional neural networks (CNNs) to extract relevant features. Also, we develop a new feature selection method using a new variant of the transient search optimization (TSO) algorithm, called TSODE, using the operators of differential evolution (DE) algorithm. The proposed TSODE uses the DE to improve the process

International Journal of Science, Engineering and Technology

An Open Access Journal

of balancing between exploitation and exploration phases.

## VI.EVALUATION PARAMETER

**1.Evaluation parameters**

In order to evaluate results there are many parameter such as accuracy, precision, recall, F-score, etc. Obtaining values can be put in the mention parameter formula to get results.

$$\text{Precision} = \frac{\text{True\_Positive}}{\text{True\_Positive} + \text{False\_Positive}}$$

$$\text{Recall} = \frac{\text{True\_Positive}}{\text{True\_Positive} + \text{False\_Negative}} \quad (6)$$

$$F\_Score = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

$$Accuracy = \frac{Correct\_Classification}{Correct\_Classification + Incorrect\_Classification}$$

## VII.CONCLUSIONS

This paper has elaborates various authors work with techniques used by them for the development of intrusion detection system. Paper has brief different attack found by the scholars with its pattern. It was desired by the system to develop a model that can detect the attack with high accuracy as most of system have high false alarm. Feature set is also a great issue n this type of work as different set of information increases the confusion in the decision model, hence it is highly desired to reduces the feature for the training and testing of the model.

## REFERENCES

1. M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, ``Deep recurrent neural network for IoT intrusion detection system,'' Simul. Model. Pract. Theory, vol. 101, May 2020, Art. no. 102031.
2. C. G. C. Index, "Forecast and Methodology, 2016–2021 White Paper," 2018.
3. ] N. Moustafa, G. Creech, E. Sitnikova, and M. Keshk, ''Collaborative anomaly detection framework for handling big data of cloud computing,'' in Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), Nov. 2017.
4. N. Moustaf and J. Slay, ''Creating novel features to anomaly network detection using DARPA-2009 data set,'' in Proc. 4th Eur. Conf. Cyber Warfare Secur. Academic Conf. Limited, 2015, pp. 204–212.
5. W. Li, W. Meng, L.-F. Kwok, and H. H. S. Ip, ''Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model,'' J. Netw. Comput. Appl., vol. 77, pp. 135–145, Jan. 2017.
6. M. Keshk, N. Moustafa, E. Sitnikova, and B. Turnbull, ''Privacypreserving big data analytics for cyber-physical systems,'' Wireless Netw., vol. 24, pp. 1–9, Dec. 2018.
7. B. B. Zarpelao, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, ¯ ''A survey of intrusion detection in Internet of Things,'' J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017.
8. O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, ''An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks,'' Expert Syst. Appl., vol. 29, no. 4, pp. 713–722, Nov. 2005.
9. Xiu Kan, Yixuan Fan, Zhijun Fang, Le Cao, Neal N. Xiong, Dan Yang, Xuan Li. "A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network". Information Sciences, Volume 568,2021.
10. M Islabudeen and MK Kavitha Devi A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad-hoc Networks Against Security Attacks, Wireless Personal Communications Springer International published Year 2020.
11. Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac and Parvez Faruki, Network Intrusion Detection for IoT Security Based on Learning Techniques, in IEEE Communication Surveys, Volume: 21, Issue: 3, ISSN: 1553-877X, Published Year 2019.

International Journal of Science, Engineering and Technology

An Open Access Journal

12. Yue Jin, Zengshan Tian, Mu Zhou, Ze Li and Zhenyuan Zhang. A Whole-Home Level Intrusion Detection System using WiFi-enabled IoT International Wireless Communications & Mobile Computing Conference (IWCMC), ISSN: 2376-6506, Published Year 2018.
13. Fuhong Lin, Yutong Zhou, Xingsuo An, Ilsun You, Fair Resource Allocation in an Intrusion Detection System: Ensuring the Security of Internet of Things Devices, IEEE conference on Consumer electronics Computing Magazine, Volume: 7, Issue: 6, ISSN: 2162-2248, publishedYear 2018.
14. Mohammad Saeid Mahdavinejad, Mohammadreza Rezvan, Mohammadamin Barekatain Peyman Adibi, Payam Barnaghi, Amit P Sheth Machine learning for internet of things data analysis: a survey Digital Communications and Networks Science Direct, Volume:4, Issue 3, Pages: 161- 175, published Year 2018.
15. J. Liu, D. Yang, M. Lian and M. Li, "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," in *IEEE Access*, vol. 9, pp. 38254-38268, 2021.
16. E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042-9053, Oct. 2019.
17. A. Fatani, M. Abd Elaziz, A. Dahou, M. A. A. Al-Qaness and S. Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," in IEEE Access, vol. 9, pp. 123448-123464, 2021
18. Jang, J.-S.R. (1993). "ANFIS: adaptive-network-based fuzzy inference system". IEEE Transactions on Systems, Man and Cybernetics. 23 (3): 665–685.
19. Abraham, A. (2005), "Adaptation of Fuzzy Inference System Using Neural Learning", in Nedjah, Nadia; de Macedo Mourelle, Luiza (eds.), Fuzzy Systems Engineering: Theory and Practice, Studies in Fuzziness and Soft Computing, 181, Germany: Springer Verlag
20. Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020.
21. Kaiyuan Jiang , Wenya Wang , Aili Wang , And Haibin Wu. "Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network" IEEE, 2020.