International Journal of Computer Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 10, Issue 2, Jul–Dec 2021; 17–26

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

INTRUSION DETECTION ON INTERNET OF THINGS: A DESCRIPTIVE REVIEW

Pranavi Patel & Mala Mehta

Research Scholar, Department of Information and Technology, Sardar Vallabhbhai Patel Institute of Technology, Gujarat Technological University, India

ABSTRACT

With the growing usage in the field of IoT (Internet of Things), cyber threats and malicious activities are also at their peak. Widening in the utilization of the Internet of Things (IoT) has raised awareness of security and has become a major concern of many IoT users. For the smooth working of IoT networks, it is essential to protect devices from malicious activities. For security purposes, an advanced Intrusion Detection System (IDS) is required. In this paper, we discussed approaches of IDS and different datasets. Later on, IDS types on the basis of application are discussed with their limitations. For future assessment, current challenges faced by IDS of IoT are discussed. An ID plays a pivotal role in IoT by discovering and repealing malicious activity for lag-free service networks.

KEYWORDS: *Intrusion Detection System (IDS), Internet of Things (IoT), Smart Devices, and Malicious Activities*

Article History

Received: *16 Dec 2021* **|** ***Revised:*** *17 Dec 2021* **|** ***Accepted:*** *21 Dec 2021*

INTRODUCTION

Internet of Things (IoT) is an automation-related field, it majorly runs without human interactions. It is a group of connected devices like sensors, actuators, CCTV, and other devices (smart devices) which are used in industrial applications, smart homes, smart cities, and other IoT applications. The vital part of any system is to provide undisrupted service ensuring a high level of security by maintaining Integrity, confidentiality, and availability [1].

IoT devices are connected through wireless or wired systems as they contain many devices in the same network. Third-party usage of devices makes them vulnerable to an attacker. IoT mainly contains two types of application methods, Centralized IoT and Distributed IoT. In centralized IoT, all the devices are controlled from one device, while distributed IoT operates at each node individually. However, both systems are vulnerable to unauthorized access by intruders. To prevent the network from the malicious activity, an Intrusion detection system is installed on the system which monitors traffic and filters the packages called a firewall [2]. Intrusion Detection Systems are implemented for abnormal behaviour and troubleshoot online threats, malware attacks, and kinds of intrusions to safeguard single devices/networks. fig1. refers to the procedural IDS on IoT networks. which starts with a knowledge-based dataset. training procedures take place in order to obtain efficiency during testing time. If Detection systems refer to any abnormal behaviours in Packets it sends them to the Intrusion prevention Model (IPS), which generate alarm and also drop the packages. In recent years many researchers do not use standard benchmarked datasets. Instead, they prefer data traffic packers of the live systems in order to have the latest traffic patterns.

In this paper, Sec 2. provides works of literature we studied, onwards in Sec 3. includes approaches of IDS in IoT. In Sec 4. different Datasets are listed in brief. Moreover, Sec 5. shows types of IDS in IoT. Sec 6. describes challenges recent IDS systems are facing. To sum up Sec 7. and Sec 8. has conclusion and bibliographies likewise.

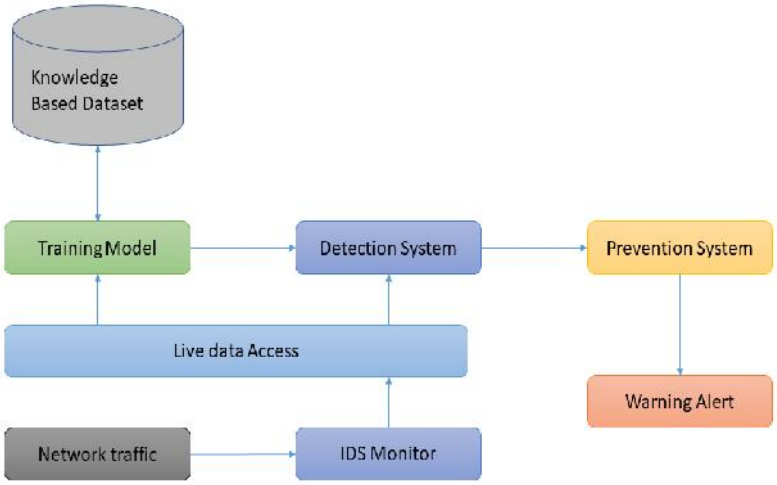

Figure 1: IDS Working on IoT.

LITERATURE REVIEW

Intrusion Detection System (IDS) in IoT decodes every packet transmitting and verifies if it is free of malicious activity anomalous behaviour for smooth smart device interactions. The researchers implemented an alert system in sound, whenever suspicious activity takes place. They used a deep learning algorithm to implement a system, in order to verify system performance they used the KDD Cup 99 dataset. Implementation was divided into two categories Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), with batch processing computation they achieved 91.4% accuracy. Researchers found issues in the privacy of IoT networks [3]. To overcome this problem advanced authenticated technologies are required.

The researchers in [4] designed a mutual authentication scheme that analyzes outdoor and indoor resilience. A proposed method is efficient in detecting Relay attacks, Men In The Middle (MITM) attacks and quality attacks. They concluded that sophisticated protocols on integrity enable better security on IoT networks.

The proposed research in [5] uses a machine learning approach Bayesian Network which is a probabilistic graphical model for representing knowledge about an uncertain domain where each node corresponds to a random variable and each edge represents conditional probability corresponding to a random variable. The method uses a query-based intrusion detection system, which requires improvements in the authentication of IDS in Signature-Based Detection (SBD).

[6 - 7] Studied mobile ad-hoc network-based smart IDS to monitor security as they used Artificial Neural Network (ANN). They indicated the importance of classification in Intrusion Detection (IDS). The developed models are effective in detecting Boat, rare attacks, DoS, and probing.

Wifi-enabled IoT smart devices of smart homes are used to design IDS. Researchers developed Received Signal Strength Indicator (RSSI) dependent on an identification router that analyzes and visualizes whole-home security. The final results show astounding accuracy in detection rate [8].

The authors of this paper Implemented IDS in edge routed systems which include DoS attack analysis, edge network intrusion detection, and edge node cloud security and related systems. SDMMF single-layered Min-max fair allocation scheme is utilized. In this study, multi-layer resource allocation is stated effectively [9-10].

Analysts of [11] identified Intrusions in a real-time environment and Network Functional Virtualization (NFV) which is a new working standard. They highlighted imbalance classification using Supervised Machine Learning (SML) algorithms. In more environments changing, cloud models require more security protocols.

The proposed model in [12] deals with challenges in intrusion detection systems in terms of computation efficiency and time, privacy conservative authentication, and power utilization. Additionally, deep information gathering research overlap issues are discussed.

APPROACHES OF IDS ON IOT

IDS approaches on IoT are three first is centralized IDS, Distributed IDS and Hybrid IDS. IDS are selected on the basis of IoT's application.

Centralized IDS

Centralized IDS (CIDS) is interdependent on traffic patterns and smart devices. This system contains logs of all IoT devices in the network and all transmission among all packages. CIDS is cost-effective to implement as it is installed on one main device that regulates all the smart devices [13]. CIDS are efficient in sensor networks due to the centralised control system. The main components of CIDS are data collection and central analyzer for performance analysis. Distributed data are collected throughout all connections that are correlated. CIDS has a less complex architecture compared to Distributed IDS (DIDS). Although, one system failure can lead to compromise of all connected device connections in IoT. As figure 2. shows local agents of IDS are part of the main IDS(Global Detection logic).

The whole system is maintained and updated through a centralized unit that regulates the system logs and keeps track of all records. As all the procedures of IDS appear in IDS agents to Central IDS agents it is more time consuming than DIDSs.

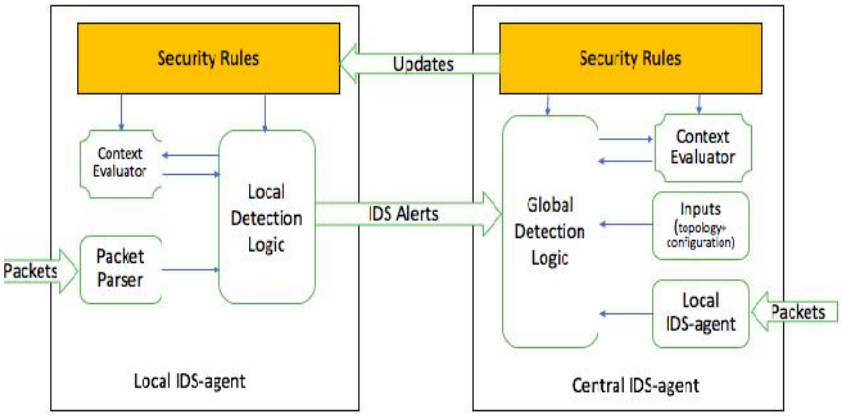

Figure 2: Central Ids Architecture [14].

Distributed IDS

DIDS is divided into every single node with separate monitoring among all smart devices for detecting malicious activity and abandons it from affecting nodes. Possibly in some cases, intruders gain success to exploit one node, hence in those cases compromise of one node did not lead to whole network compromise. Hence, it is safer than CIDS in a practical approach. Still, it contains complex and hazardous configurations in the implementation. Additionally, as it should be installed on each node of the IoT network might increase the prices of development. However, it provides better scalability throughout the system. Also, less detection time is required to check transmitting packages. Fig 3. refers to the architecture of smart home smart devices regulations.

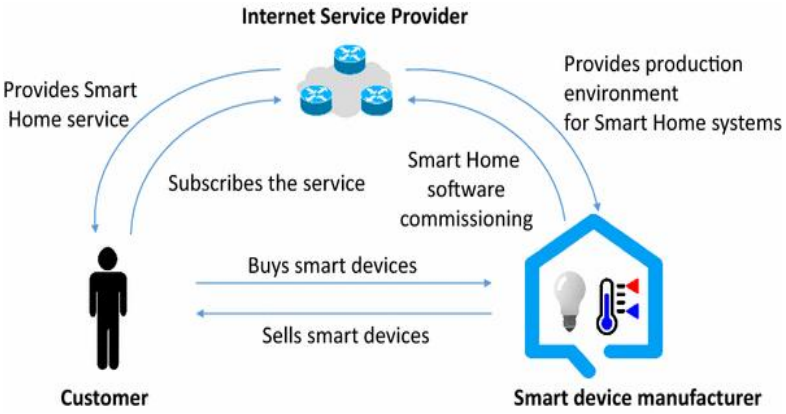

Figure 3: Distributed IDS in Smart Homes [15].

Hybrid IDS

For maximising safety and reducing the cost-effectiveness with compatible computation timing of IDS. The above two approaches CIDS and DIDS are used in the combined manner for many systems. Recent IoT systems are majorly working on HIDS according to the risk factors of smart devices. HIDS is the most effective proven approach as it contains cost management, detection time reduction than CIDS and also it is less complex than DIDS. figure 4. refers to the Advantages of HIDS.

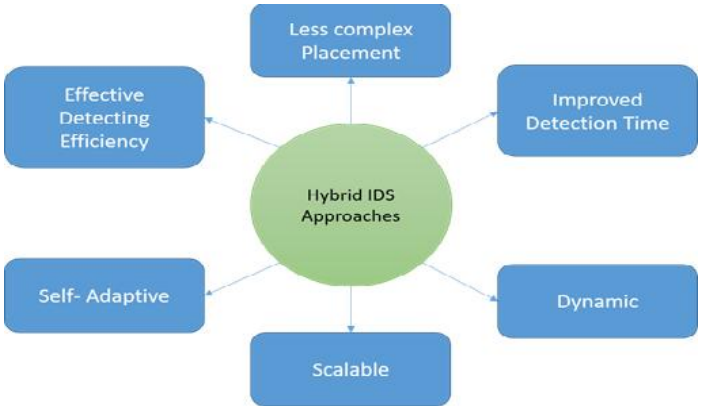

Figure 4: Merits of Hybrid IDS Approach.

DATASETS

Recently, many datasets have started to be generated from the regular traffic of server requests, although the standard datasets with respect to anomaly and misuse are discussed in this paper. the benchmark datasets which are used for IDS standards since 1999 [16].

KDDCup99

KDDCup99 is an updated version of DARPA dataset which was the first benchmark dataset for intrusion detection. The Mining Audit Data of Model Automated for ID (MADMAID) framework was utilized for feature extraction in raw TCP dump data. The detailed datasets are enlisted in Table 1. A dataset is captured with 41 features and 5 classes. These features are divided into basics, content and Time-based traffic features [17]. The basic feature does not use payloads; instead it is extracted from TCP segments and UDP datagram. Basic features contain only headers files of normal classes, while content features have a full payload of TCP/IP. Content feature specifically used to identify 'R2L' and 'U2R' types of attacks [18]. Time-based features are narrow bandwidth of two seconds from 'same host' and 'same service' connections. Connection-based and host-based traffic are featured in a time-based feature- extractions. KDDCup99 training set has 494,021 connections likewise testing contains 311,029 network connections [19].

Table 1: KDD Cup 99 and NSL-KDD's Comparisons

Connections	Explanation	KDDCup99 Training	KDDCup99 Testing	NSL-KDD Training	NSL-KDD Testing
Normal	Usual connections	97,278	60,593	67,343	9,710
DoS	Network jamming attacks	391,458	229,853	45,927	7,458
Probe	Configuration information gathering attacks	4,107	4,166	11,656	2,422
R2L	Illegal access from a remote computer	1,126	16,189	995	2,887
U2R	Being a root user gaining super-user access	52	228	52	67
Total	-	**494,021**	**311,029**	**125,973**	**22,544**

CAIDA

This dataset was developed from Denial of Service (DoS) and Distributed Denial of Service(DDoS) intrusions from regular traffic traces in 2007. Attacks of DDos and DoS are made for service disruption as the router has limited request handling capacity, they try to exceed the capacity to disrupt the service. This dataset does not have a variety of intrusions, hence solely it is not an ideal dataset to evaluate models of robust IDS [21]. Additionally, it does not have a whole traffic feature, a partial feature makes it difficult to distinguish between malicious behaviour or normal behaviour in IoT.

UNSW-NB15

The Cyber Security research team of Cyber range lab in Australia used IXIA PerfectStorm tool to collect traffic data and named UNSW-NB15. The classification of this dataset is Normal and other 9 types of malicious traffic. In this scientists have exceeded target classes to avoid model bias towards normal traffic. More number records are included in the 42 features and different measures added are flow, Basic, Content, Time, and generalization. TCP dump tool used for capturing network packet traces and contained 100GBs data and divided into 100 MB using the same tool. The final connection and malicious connections are shown in table 2.

CICIDS2017

Recently, many researchers started to use this data set due to the latest benchmarked dataset for their IDS models. CICIDS2017 dataset contains benign and most up-to-date common attacks, which resembles the true real-world data. It also includes the results of a network traffic analysis using CiCFlow Meter with labelled flow based on the timestamp,

source, destination IPs, source and destination ports, protocols, and attack. Table 3. shows CICIDS2017 detailed connections.

Table 2: Training and Testing UNSW-NB15 Dataset

Connections	Trining	Testing
Normal	56,000	37,000
Intrusions	37,500	8,519
Total	**93,500**	**28,481**

TYPES OF INTRUSION DETECTION ON IOT

Network Oriented Intrusion Detection

Network Oriented Intrusion Detection (NOID) is evolved in network nodes for detecting and regulating traffic. The working of NOID is checking for malicious activities and whenever it is detected, it directly sends an alert to the administration. In simple methodology how a firewall blocks suspicious applications in our personal computer the same way, the NOID works at traffic diversion nodes. And every node of traffic contains NOID for safe IoT working.

Host Oriented Intrusion Detection

The host here is considered as a singular device of an IoT network. That makes Host Oriented Intrusion Detection (HOID) devices with their private firewalls distinguished from centralised IDS. HOID takes records and checks of secure management of the device it is oriented to. In some malicious activity related to a single host becomes an open door to intruders to exploit the whole system as IoT all devices are co-connected throughout the network. Attacks like Worms are required to be initiated in only one system and globally it spreads through the whole system. Additionally, it does not require any human interaction once it is installed it goes multiplied by itself. HOID not only monitors online traffic it also monitors system cells, the current procedure, file updations, background procedure, and application logs. It also changes command lines if anonymous behaviours are detected in the system or IoT device.

Table 3 Training and Testing CICIDS2017 Dataset

Connections	Explanation	Training	Testing
Normal	Usual connections	56,000	37,000
Fuzzers	Spams, HTML files penetration and port scans relevant attacks	18,184	6,062
Analysis	Port scan, HTML relevant attacks	2,000	677
Backdoors	Evading from background security	1,746	583
DoS	Network jamming Attacks	12,264	4,089
Exploits	Security hole observation for future exploits	33,393	11,132
Generic	Block-cipher relevant attacks	40,000	18,871
Reconnaissance	Vulnerability Gathering	10,491	3,496
Shellcode	Section of a program used for exploitation	1,133	378
Worms	Auto-mutiliable virus	130	44
Total		**93,500**	**28,481**

Protocol Oriented Intrusion Detection

This type of Intrusion detection is inbuilt in front-end servers for saving server systems from being compromised and avoids disruption of service. Protocol Oriented Intrusion Detection (POID) is crucial for checking protocol interruptions

between requested devices and servers. POID mostly checks the regulations of HTTP protocols. Major applications of the POID are related to web servers of IoT.

Application Oriented Intrusion Detection

Application Oriented Intrusion Detection (AOID) is also called Cloud Oriented Intrusion Detection (COIS). The AOID are multiple servers configured for the detection method that monitors all logs of the cloud-based system [22]. Whenever malicious activity is being noted in servers it blocks specific servers and sends a notification to the administrator of the system. As cloud computing is an inevitable part of IoT, AOID is a necessity of multi configured servers for smooth IoT running.

Perimeter Oriented Intrusion Detection

A Perimeter Oriented Intrusion Detection (POID) located on the main server comes with electronic or fiber optics devices like the digital perimeter. Which is sensible towards detecting disturbances. Whenever it senses some malicious attempt on the system it triggers an alert alarm. POID is also being considered as the first line of defence methodology throughout servers. Moreover, it is simply installed in devices without any critical procedures.

Hybrid Oriented Intrusion Detection

As IoT is not limited to only devices and servers that created requirements of robust Intrusion Detection. Combining types of detection methodologies provides a solution to security over multiple devices at the same time. However, Hybrid Oriented Intrusion Detection is not in the application for real-time intrusion detection.

CHALLENGES

Advanced IDS requires an understanding of current approaches of IoT, IDS and their united architecture. To enhance the robustness of IDS, the current system's challenges are a must to overcome. We classified challenges into three categories: Multi-Layer attacks, Device protection and Data Collection.

Multi-layer Attacks

In layer attack, it consists of four types of attack: Perception, Network, Support and Application. Due to the advancement of detection methodologies, singular layer corresponding attacks are majorly blocked by IDS and IPS. To have advancement in malicious activities hackers started using multi-layer attacks to have success in breaching nodes. The major research only focuses on single-layer detections.

Device Protection

To safeguard networks in IoT devices, it requires all the devices protected from attackers. Sometimes the credentials information violations result through people in the network in order to gain some financial or other sums in exchange. This is a serious matter that smart devices of IoT are handling.

Data Collection

All the research experimentation appears on the data available through specific networks and datasets. As emerging technologies new benchmarked datasets are required for experimentation. Also taking traffic packets from a singular kind of device does not contain all area traffic patterns. Hence data gathering is a critical area for researchers.

CONCLUSIONS

From individuals to huge organizations, all use services of IoT and expect to have a secure allocation of their information. As there is increasing malicious activity even though network detection methodologies are also improving simultaneously. In this paper, we started with a basic architecture of IoT approaches which are Centralized, Distributed and Hybrid. Also, hybrid architecture has more merits over both singular methods. Then we discussed literature studies. Onwards, benchmarked datasets and we enlisted recent types of IDS on IoT. Issues that are faced by current IDS in IoT are also listed. Nowadays Intrusion detection systems are efficient in dealing with known attacks still, unknown attacks is a complicated procedure as limited data sources for experimentations.

Conflicts of Interest

The authors have no conflicts of interest to declare.

REFERENCES

1. *Sheikh Tahir Bakhsh, Saleh Alghamdi, Rayan A Alsemmeari and Syed Raheel Hassan, An adaptive intrusion detection and prevention system for Internet of Things SAGE open access journal in Soft Computing in Intrusion Detection System, published Volume : 15 Issue : 11 published Year 2019*
2. *Akhil Krishna, Dhanya Sarah Jacob, Ashik Lal M A, Hari M and Athul Joe Mathewkutty Research on Intrusion Detection & Prevention model Using Deep Learning, International Conference on Electronics and Sustainable Communication Systems (ICESC), ISBN: 978-1- 7281-4108-4 published Year 2020*
3. *Amir Ali and Muhammad Murtaza Yousaf, Research entitled Novel three- tier Intrusion Detection and Prevention System in Software Defined Network, in IEEE Open-Access Volume : 8, ISSN: 2169-3536, published Year 2020.*
4. *Zhigang Huang ; Lei Zhang ; Xinyu Meng ; Kim-Kwang Raymond Choo, Key-Free Authentication Protocol Against Subverted Indoor Smart Devices for Smart Home, IEEE Internet of Things journal, Volume: 7, Issue: 2, ISSN: 2327-4662, published Year 2019.*
5. *Rafał Kozik & Michałl Choras, Machine Learning Techniques for Cyber Attacks Detection, Advances in Intelligent Systems and Computing book series Springer International Published Volume: 233, ISBN: 978-3-319-01621-4, published Year 2014.*
6. *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.*
7. *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.*
8. *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.*

9. *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, published Year 2018.*
10. *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.*
11. *PrakashDuraisamy, XiaohuiYuan, ElSaba,A. and Sumithra Palanisamy, Contrast enhancement and assessment of OCT images, Proceedings of International Conference on Informatics, Electronics & Vision (ICIEV), pp.91-95, publish year 2012*
12. *Bayu Adhi Tama a, Sunghoon Lim b, Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation, Computer Science Review, published year 2020*
13. *Fauzi Hidoussi, Homero Toral-Cruz, Djallel Eddine Boubiche, Kamaljit Lacktaria, Albena Mihovska and Miroslav Voznak, Centralized IDS Based on Misuse Detection for Cluster- based Wireless Sensors Networks, published year 2015*
14. *Ansam Khraisat and Ammar Alazab, A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, SpringerOpen, published year 2021*
15. *Lyes Bayou, Assessment and enforcement of wireless sensor network-based SCADA system security, ReserchGate, published year 2018*
16. *Mariusz Gajewski, Jordi Mongay Batalla, George Mastorakis and Constanding X. Mavromoustakis. A distributed IDS Architecture for smart home systems, published year 2017*
17. *R. Vinayakkumar, Mamoun Alazab, K.P. Soman, Prabharan Poornachndran, Ameer Al-nemrat and Sitalakshmi Venkatraman, Deep Learning Approach for Intelligent Intrusion Detection System, IEEEAcess, published 2019*
18. *Y. LeCun, Y. Bengio, and G. Hinton, ‘‘Deep learning,’’ Nature, vol. 521, no. 7553, p. 436, 2015.*
19. *M. Alazab et al., ‘‘A hybrid wrapper-filter approach for Malware detection,’’ J. Netw., vol. 9, no. 11, pp. 2878–2891, 2014.*
20. *Creech G, Hu J (2014b) A semantic approach to host-based intrusion detection systems using contiguous and Discontiguous system call patterns. IEEE Trans Comput 63(4):807–819*
21. *P. Hick, E. Aben, K. Claffy, and J. Polterock, "the CAIDA DDoS attack 2007 dataset," ed, 2007*
22. *T Karthick Krishnan, S Sridevi, G Bindu, R Anandan, Comparison and detail study of attacks and detection methods for wireless sensors networks, published year 2018*

AUTHOR PROFILE

Pranavi Patel Holding B.E. in Computer Engineering. Currently pursuing M.E. in System and Network Security from Gujrat Technological University.

Mala Mehta PhD. pursuing from SVIT, Along with an Assistant Professor at the same institute.