Survey: Intrusion Detection for IoT

B R Chandavarkar, Joshitha Reddy D., Surla Lakshmi Poojitha, and Reshma Tresa Antony

1 Introduction

The Internet of Things (IoT) is a network of interconnected devices that can be remotely monitored and controlled [1]. Smart TVs, smart phones, and other gadgets are few examples. The primary goal of IoT is to make people's lives more comfortable and productive. On the other hand, these IoT devices are vulnerable to a variety of security threats. Denial of service (DoS), routing attacks, and man in the middle attacks are prominent among the others. These attacks have a negative impact on IoT services and smart environments. As a result, it is our primary concern to protect IoT systems, which is why IDS comes into the picture [2].

An Intrusion Detection System (IDS) is a technology which aims to detect actions that attempt to gain unauthorised access to a computer system. These attacks are also referred to as intrusions. That is why the term IDS was coined. According to M. F. Elrawy et al. [2], IDS for IoT can review data packets in real time and respond appropriately by examining them and notifying system authorities whenever a security breach is detected. This Intrusion Detection System (IDS) was designed to detect security threats to IoT services and will work in difficult conditions while also providing a quick response if any abnormal behaviour is detected, which is quite impressive. Given the significant advancements in IDS for IoT, this chapter presents a survey on Intrusion Detection for IoT, with the primary goal of deciphering the IDS categorisation taxonomy for IoT and determining which type of Intrusion Detection System is more appropriate for a given assault in a specific situation.

The rest of this chapter is structured as follows. Section 2 delves deeper into the Internet of Things (IoT) and its security challenges. Section 3 discusses the

B. R. Chandavarkar · Joshitha Reddy D. · S. L. Poojitha (✉) · R. T. Antony
National Institute of Technology Karnataka Surathkal, Computer Science & Engineering, Mangalore, Karnataka, India

R. Misra et al. (eds.), *Advances in Data Science and Artificial Intelligence*,
Springer Proceedings in Mathematics & Statistics 403,
https://doi.org/10.1007/978-3-031-16178-0_26

various kinds of IDS. Section 4 discusses the categorisation of IDS based on their deployment strategy and detection techniques used. Section 5 discusses the potential security threats in IoT. Section 6 examines suitable IDS in general for a specific attack, which is the survey's most important contribution. Lastly, some concluding remarks are made in Sect. 7.

2 Internet of Things (IoT)

IoT is a system of interconnected devices that allows smooth exchange of information between physical devices. These devices can be healthcare gadgets, vehicles, industrial products, wearable items, city infrastructures, and even everyday household items like kitchen appliances, baby alarms, temperature sensors, and smart TVs as shown in Fig. 1. To monitor such devices, there is no need to be in close proximity of them. This field has advanced as a result of the convergence of various technologies, including pervasive computing, inexpensive sensors, and machine learning.

IoT has evolved as one of the most critical technologies in the recent years. We can now link common objects to the Internet via embedded technology, allowing us to establish seamless communication between people, processes, and things. Items can share and gather data with very less human contact because of cheaper computers and advanced technologies like the cloud and big data analytics. Every interaction in today's super-connected environment can be noted and changed because of digital systems. IoT helps the digital and physical worlds that complement one other [3, 4].

2.1 Security Challenges of IoT

Security of IoT systems has become a hypercritical issue, because of the ever-expanding number of utilities and operators of these utilities in IoT networks. Smart devices are more efficacious when IoT peripherals and smartly set-up surroundings are combined. While diversity can provide users with a large number of devices to choose from, it is also one of the reasons for the IoT's fragmentation and many of its security concerns. Compatibility concerns have arisen as a result of the absence of industry foresight and standardisation, further complicating the security issue. Because of the portability of devices, there is a larger risk of attacks infecting several networks. The consequences of IoT security flaws are extremely unfavourable in indispensable fields such as health and industry [5].

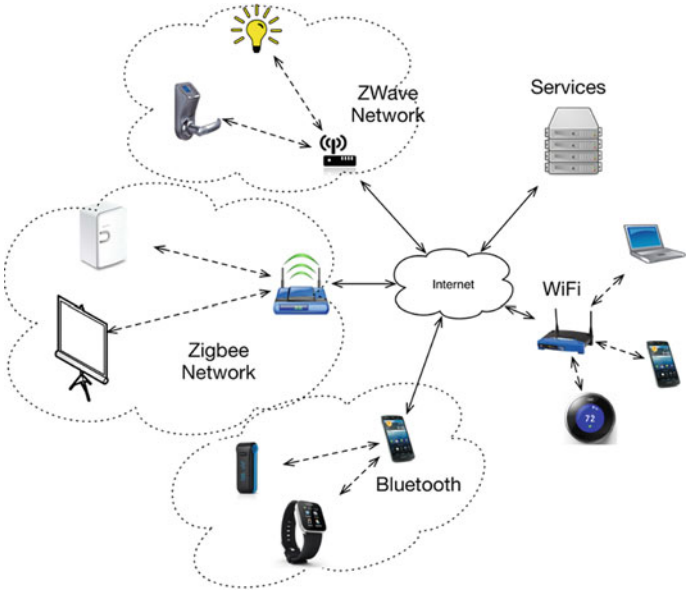

Fig. 1 Internet of Things

Factors Affecting IoT Security

Vulnerabilities The reason IoT devices are defenceless is because of the fact that the algorithmic capacity necessary for security is absent. The budget for finding and checking safe firmware is quite insufficient and this is another contributing factor to the extensive susceptibilities. The funds are decided based on the device prices and development cycles. As illustrated by Ripple20 and URGENT/11, vulnerable standard components harm millions of devices. Liabilities in web applications and related software for IoT devices, in addition to the devices themselves, could be the reason for a system whose integrity has been adversely impacted. Malicious software users are like hawks, always in search for new vulnerabilities, and are well-versed in previous ones.

Malware Despite the fact that most IoT devices have very less computer capacity, malware can still affect them. Impostors have made great use of this tactic in recent years. IoT botnet malware is both, a versatile and a profitable option for cybercriminals which makes it one of the most common types of malware. Cryptocurrency mining malware and ransomware are two other types of malware.

Escalated Cyberattacks Distributed denial-of-service (DDoS) attacks usually involve damaged devices. Using hijacked devices as an attack base is a way to infect new machines as well and hide malevolent activities or as an access point into a communal network for lateral mobility. Businesses are a more common target, but surprisingly there are quite a lot of attacks on smart homes as well.

Information Threat and Unknown Exposure Data leaks are the biggest threats in anything that involves the Internet. Connected gadgets are no exception to this. Without the user's knowledge, important data might be retained and used in these devices.

Device Mismanagement What further fuels these threats is security breaches, poor passwords, and just overall device mishandling. Also, not all users will be aware of the security measures that need to be taken and so the service providers and manufacturers will need to help their clients improve their security [5].

Emerging Security Issues

Due to a lack of foresight on the part of the industry, there was insufficient time to build tactics and countermeasures against common dangers in the emerging IoT ecosystems. To anticipate emerging issues, IoT security research must be done on a regular basis. Below are some of the new issues that need to be kept an eye on [5].

Complex Environments Complex IoT environments are characterised as a linked network of at least ten IoT devices. Because of its intricate web of interconnected processes, such an ecosystem is nearly impossible to manage and govern. In such a setting, an unnoticed misconfiguration can have disastrous effects, putting the physical security of the home at danger.

Prevalence of Remote Work Arrangements The Covid-19 pandemic shattered many aspirations. It ushered in large-scale work-from-home (WHF) arrangements for businesses all over the world, as well as a greater reliance on home networks. Many WHF users benefited from IoT devices. These changes have emphasised the need for IoT security approaches to be re-examined.

5G Connectivity There is a lot of excitement and expectation surrounding the move to 5G. It is a development that will help other technologies advance as well. The current focus of 5G research is on how it will influence companies and how they can properly use it.

3 Intrusion Detection System (IDS)

An IDS is a device that looks at incoming and outgoing network traffic for any signs of strange activity or security breaches. IDS solutions work by alerting the user to any activity that could affect the user's network.

3.1 Types of IDS

Network-Based IDS

NIDS are network devices that are set up at a predetermined location to examine traffic from all devices on the network [6]. Whenever strange behaviour is noticed by the IDS, the administrator is notified. NIDSs are either physical devices or software-based devices. They are linked to several network media such as Ethernet, FDDI, etc. There are two network interfaces available. The promiscuous interface is used for listening to the network conversations, and the other interface is used for control and reporting. When a network interface is set to promiscuous mode, all packets, including those not intended for the network interface card's MAC address, are delivered to the kernel for processing.

As the count of Internet nodes has increased dramatically in recent years, NIDSs have become a vital component of network security management. It can cause high-speed network traffic overflow, signature creation lag time, encoding, and scaling problems.

Signature-Based IDS

It uses a list of known threats and associated indicators of compromise (IOCs) that has already been encoded into the system. As packets move through the network, a SIDS cross checks the packets with a database of known IOCs or attack signatures, flagging any unusual behaviour.

An example of SIDS is SNORT. There are five components in the system: Packet Decoder, Preprocessor, Detection Engine, Logging and alerting system, and output modules [7]. The packet decoder gathers packets from various network ports and forwards them to the preprocessor. The preprocessor modifies the packets before sending it to the detection system. Another function of the preprocessor is defragmentation of the packets. The detection system mainly works to find out if there is an intrusion activity based on the rules defined by SNORT. In the logging and alerting system component, based on the detection engine's results, a packet is either used to generate an alert or the activity is logged. The output module saves the results of the previous component.

Signature classifications are based on previously identified intrusive behaviour. As a result, the user may quickly analyse the signature database and decide which kind of intrusive behaviour the abuse detection system is set to alert on [8]. When you install the Misuse Detection System, it immediately starts protecting your network. There are minimal false positives as long as assaults are accurately described in advance. When an alert raises, the user can immediately associate it with a specific type of network activity. For these reasons, SIDS is a worthwhile IDS.

But one of the biggest issue of SIDS is managing the traffic as each packet is compared with every single signature in the database. Therefore, it is a time-consuming process. The database has to be frequently updated to make sure all possible attack signatures have been tracked. Another problem is that the database will be very environment-specific. This is because the attack information is dependent on OS version and application.

Anomaly-Based IDS

An AIDS uses machine learning to train the detection system to recognise a normalised baseline rather than seeking for recognised threats. Rather than looking for known IOCs, AIDS simply detects any unusual behaviour and sends out alerts [9].

The different types of anomaly-based IDS are host-based anomaly and network-based anomaly. The calculation of host-based anomalies dealt with operating system call traces. The incursions take the form of anomalous subsequences of the traces (collective anomalies). Malicious programming, unlawful activity, and policy abuse are among the consequences. The data are ordered, and the alphabet is made up of specific system functions like open, close, and create. Some network type anomalies are UDP flood, ICMP flood, etc.

A UDP flood attack is a type of DoS attack. It involves sending a huge number of UDP packets to a remote host's random ports. As a result, the remote system will look for a programme that is listening on this port. The host will respond with an ICMP "Destination Unreachable" message if no application is listening on the port [10]. As a result, the affected system will be forced to send a huge number of ICMP packets in response to a high number of UDP packets, eventually rendering it unreachable by other clients. The system will go down if sufficient UDP packets reach the victim's ports. To detect a UDP flooding assault, the amount of the traffic (flow) and the count of packets (packet count) in incoming traffic must be used.

ICMP flood is a simple sort of attack in which the attacker sends a huge number of ICMP Echo Request (ping) packets of various sizes to the target host. The Ping-of-Death (PoD) assault was succeeded by ICMP flooding. PoD attempts to send an extra-large ping packet to the target in the hopes of crashing the system due to its inability to handle large ping packets [10]. Ping flood takes the attack to a new level by flooding the victim with a massive amount of ping traffic. The attacker expects that the victim will be too preoccupied with responding to ICMP Echo Reply packets, using both outgoing and incoming server bandwidth.

Distributed-Based IDS

DIDS is made up of numerous IDSs scattered over a broad network that connect one another or with a central server for better network monitoring, scenario analysis, and real-time assault data. The DIDS architecture combines centralised data analysis

with distributed monitoring and data minimisation. This is a one-of-a-kind approach among current Intrusion Detection systems. There is a DIDS Director. A single Host Monitor exists for each host along with single LAN Monitor [11]. The Host and LAN Monitors are mainly in charge of gathering evidence of unauthorised or questionable behaviour, while the DIDS Director is in charge of aggregating and evaluating it.

Host-Based IDS

Only the device's incoming and outgoing packets are monitored by a HIDS [12], which alerts the administrator if possible fraudulent behaviour is detected. HIDSs, unlike NIDSs, have easy accessibility to data and system activities targeted by these attacks, and thus they are aware of the potential consequences.

An attacker may tamper with a host-based IDS, which is a worry. The IDS cannot be trusted if an attacker gets control of a system. As a result, unique anti-tampering protection for the IDS should be built into the host. There are a few issues with HIDS. First, a large amount of resources is utilised. This in turn affects the system's performance. Also, the detection of the attack will not happen until it has reached the host. Usually, host-based and network-based IDSs are used together.

4 IDS for IoT

This section will discuss the different classifications of IDS for IoT based on placement strategies and detection methods as illustrated in the flowchart below (Fig. 2).

4.1 Placement Strategies

Before diving into placement strategies, it is critical to understand the structure of IoT and its components. According to B. B. Zarpelão et al. [13], the architecture

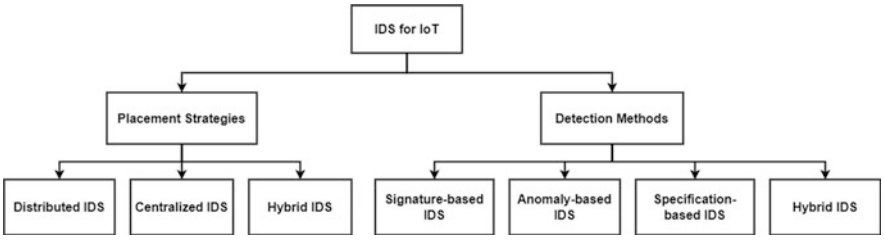

Fig. 2 IDS classification for IoT

is primarily made up of three domains: physical, network, and application. The physical level is made up of devices that perceive and connect with our surroundings, forming an LLN. The primary goal of the network domain, i.e., the second domain, is to bring together traditional network technologies and protocols for data transmission. The interfaces that allow users to interact with items in the physical domain are included in the application domain. Placement strategies deal about the location of IDSs in the IoT network. Three different placement options for IDSs are described in the subsections below.

Distributed IDS Placement

Le et al. [14] state IDSs are installed in every node of the LLN in this distributed placement technique. The nodes are in charge of keeping an eye on their neighbours. These nodes are categorised as leader, affiliated nodes forming a hierarchy within them. They can alter their roles depending on the type of attack. In this process, each node keeps track of a higher level node by calculating its inward and outward amount of data which moves across a network. So, whenever a security threat is identified by the IDS, it alerts all the other nodes to isolate the attacker. According to A. Khraisat et al. [6], this distributed IDS is very effective in detecting DOS assaults for high-speed networks.

Centralised IDS Placement

In this strategy, IDS is placed in a centralised component. Raza et al. [15] say that a central console is in charge of all IDS actions. All of the data gathered by LLN nodes are transmitted to the Internet and would pass through the border router. As a result, an IDS installed here can examine all the data flowing between the architecture components. In comparison to a distributed system, the cost of maintenance and administration is reduced. And Liu et al. [16] indicated that, most importantly, it is unable to detect harmful events occurring in multiple locations at the same time.

Hybrid IDS Placement

It is a hybrid of both distributed and centralised placement strategies, as the name implies. It combines centralised and distributed placement approaches to maximise their benefits while minimising their drawbacks. Lee et al. [17] proposed that the network is divided into clusters or regions using this hybrid placement method, with only the cluster's main node hosting an IDS instance (only selected nodes that are effective will be used for hosting). This node is in charge of monitoring the other nodes in the cluster. Cluster members should provide relevant data about themselves and their neighbours to the cluster leader. This technique is constructed with more resources than the previous placement strategies. Thanigaivelan et al. [16] proposed

a hybrid deployment model for IDS placement in both network nodes and border routers. It differs from the previous one because of its central component. The border router's IDS modules handle tasks that necessitate more resource capacity, whereas standard node IDS modules are frequently lightweight. Both of these methods have a number of advantages over other methods of placement.

4.2 Detection Methods

Depending on the sort of detection method utilised in the system, Intrusion Detection techniques are divided into distinct categories. This chapter will go through them briefly in the subsections that follow.

Signature-Based Approach

This approach detects the assaults by comparing the system behaviour with the predefined attack signatures in the database. As stated by Kasinathan et al. [18], it functions by using a pre-programmed list of threats and IOCs. File passwords, fraudulent URLs, and the content of subject line headings of emails are all the instances of IOCs. A signature-based IDS compares packets as they pass through the network to a list of known IOCs or threat patterns to detect any unusual behaviour. System raises an alert whenever if an activity matches with the predefined attack signatures or saved IOCs. Study [13] states that these kinds of IDS are highly good at spotting known threats. But the disadvantage is that, since there are no known matching signatures for all assaults, this technique is incapable of detecting new attacks or versions of current ones, which is one of the most serious flaws of this IDS.

Anomaly-Based Approach

As stated by Mitchell et al. [19], anomaly-based approach has a normal behaviour which is already prewritten and it detects any illegal activity whenever the divergence of the system behaviour from the normal one exceeds a limit. This method works well for detecting new assaults, especially those involving resource exploitation. usually, ML algorithms are used to generate the normal behaviour. From source [8], basically, any activity which does not coincide with the normal behaviour is identified as an illegitimate action. Also, Study [2] states that the disadvantage of this approach is that many non-malicious actions will be identified as attacks simply because they are out of the usual. Hence, the heightened possibility of false alarms with anomaly-based intrusion detection necessitates more resources and time to evaluate all possible threat alarms.

Specification-Based Approach

A specification is a set of rules and criteria that govern how network components should behave. Study [13] proposes that when network activity deviates from specification definitions, specification-based techniques detect intrusions. As a result, it serves the same function as anomaly-based detection in terms of detecting deviations from the norm. But, there is a key difference between the two methods: in specification-based approach, we will have to manually state the rules and criterion of each specification unlike the anomaly approaches. These manually created requirements are utilised to characterise legitimate software behaviours in this method. Study [20] says this technique does not raise false alarms when unexpected (but legitimate) software actions are encountered because it is based on legitimate activities. As a result, it has a lower false positive rate than an anomaly-based IDS. It also has the ability to detect previously unknown assaults because it detects attacks as deviations from legitimate behaviour. As a consequence, it has a lesser probability of false detection compared to anomaly-based intrusion detection system. It can also identify previously undiscovered attacks since it recognises attacks as aberrations from normal behaviour.

Hybrid Approach

There have been significant developments in this hybrid intrusion detection system, which combines the attributes of all detection techniques to optimise their benefits while minimising their shortcomings. INTI, proposed by Cervantes et al. [21], is a promising and efficient hybrid IDS method for detecting sinkhole attacks, combines an anomaly-based methodology for analysing the packet traffic between nodes with specification-based approaches for extracting two forms of node evaluation: reputation and trust. Numerous studies show that INTI exceeds other methods in terms of system performance in combating sinkhole attacks.

5 Security Threats

The impact of IoT security threats could be a serious challenge in IoT implementation. Cybercriminals can use security flaws in IoT infrastructure to launch sophisticated cyber-attacks. Most users are unaware of the security threats, and hence do not have the means to prevent them. A few of the threats are:

5.1 Botnets

A botnet basically tries to gain remote access to a user's computer and spread malware [22]. Botnets are used by attackers to steal private data to initiate cyber

assaults such as DDoS and phishing. The Mirai botnet is one such botnet that affects IoT systems. A total of 2.5 million devices, including photocopiers, modems, and webcams, were impacted. This botnet was also used by intruders to perform widespread denial of service attacks against various IoT devices. Following the effect of Mirai, a number of cybercriminals have created a number of complex IoT botnets. These botnets are capable of launching sophisticated cyber-attacks on IoT devices that are vulnerable.

5.2 Denial of Service (DoS)

The main purpose of this assault is to slow down the server. It attempts to do so by sending multiple requests and causing an overflow in the victim's system [23]. A denial-of-service attack, for example, will prohibit a travel agency from accepting requests for new ticket reservations, vehicle condition inquiries, and booking cancellations. In such instances, people may opt to travel with alternative agency. The attacker effectively harmed the company's reputation in this manner.

5.3 Man in the Middle (MITM)

In this form of assault, a hacker tries to intercept the messages between two communicating systems. They hack into the communication channel between the two and hence get in the "middle" of them [24]. Attackers seize control and send fake messages to systems that are a part of the communication channel. Such attacks can be used to compromise IoT devices like smart refrigerators and self-driving cars.

MITM may be used by intruders to capture communications between several IoT devices, ending in major failure. Smart home accessories such as fans, for example, can be turned on and off by an attacker via MITM. Attacks on IoT devices, such as industrial equipment and medical devices, might have severe repercussions.

5.4 Identity and Data Theft

Attackers may now use IoT devices such as smart wristbands and smart home appliances to get more information on a range of people and businesses. Intruders can utilise this data to commit more intricate and thorough identity theft [25].

Cybercriminals, for instance, can gain access to a company's corporate network by exploiting a flaw in an IoT sensor. As a result, attackers have access to critical data from multiple organisational structures.

5.5 Social Engineering

Social engineering is used by attackers to induce individuals to divulge personal information such as passwords and bank account details. Cybercriminals may also utilise social engineering to get access to a system and discreetly install malicious software. Typically, social engineering assaults are carried out through the use of phishing emails, in which an attacker must create convincing emails in order to manipulate others [26]. In the case of IoT devices, however, social engineering assaults may be easier to carry out.

In order to give customers with a personalised experience, IoT devices, especially wearables, collect massive quantities of personally identifiable information (PII). Users' personal information is also used by such gadgets to provide user-friendly services, such as ordering things online using voice control. However, attackers can access PII to obtain sensitive information such as bank account numbers, purchasing history, and home location. This information might be used by a cybercriminal to execute a sophisticated social engineering attack against a person, his family, and friends via vulnerable IoT networks [26]. In this approach, IoT security concerns such as social engineering might be used to get unauthorised access to user data.

5.6 Routing Attacks

Routers play an important role in communication networks by allowing data transfer. Router attacks can take advantage of protocol weaknesses, incompatibilities in router architecture, and inadequate authentication. There are two sorts of attacks that can occur: distributed denial of service and brute force attacks [27]. While an attack is taking place, it has an effect on the system operations and corporate operations.

There are different types of routing attacks such as sinkhole attack, selective forwarding attack, etc. Sinkhole attacks are the most damaging routing assaults in the IoT context, among others [21]. It generates network traffic and dissipates network communication. It made use of a variety of routing metrics. Fake link quality, shortest path, and other criteria are used. Sinkhole attacks generate fictitious data and send routing requests to nearby nodes. The nodes were compromised as a result of this assault.

6 Analysis of Suitable IDS

In the previous sections, the different types of detection methods and the placement strategies that are used in IDS were discussed. Along with that the characteristics of various security threats were seen. Based on the assessment of these, the following observations have been made.

Table 1 Summary of appropriate IDS types for various IoT attacks

S. No	Security attack	Placement strategy	Detection technique
1	Botnet attacks	Distributed-based	Specification-based
2	DoS attacks	Distributed-based	–
3	Man in the middle	Centralised	Anomaly-based
4	Sinkhole attacks	Distributed, centralised	Hybrid
5	Wormhole attacks	Distributed	–

It was found that botnets that launch Distributed Denial-of-Service [DDoS] attacks, which are triggered by internet traffic overflow, can be better spotted using Distributed IDS as this type of IDS identifies attacks based on inbound and outgoing traffic. Furthermore, because signature-based approaches cannot detect new threats and anomaly-based approaches have a high false positive rate, a specification-based approach could be employed as a detection technique here. Also, because DoS assaults have many of the same traits, these strategies are a better fit for them too. As man-in-the-middle (MITM) attacks are known to use any available technique suitable to the attacker to intercept, decrypt and exploit user's resources, anomaly-based stimulative IDS can better identify these type of attacks since they have the ability to detect out-of-the-ordinary patterns and are better at detecting resource exploitation attempts. Moreover, since this attack has no precise requirements, a centralised IDS as a placement strategy could be used as it would be less expensive than a distributed-based approach.

And as mentioned in Sect. 5.6, among the many routing attacks that exist, sinkhole attack is one. It is one of the deadliest attacks as it may act as a catalyst for other attacks. For such an attack, hybrid detection methods are more suitable. INTI [28] is a very efficient hybrid-based IDS that is used for sinkhole attacks. Wormhole attack is another routing attack. In this case, the node is targeted from many directions, making it difficult to pinpoint the location of the intruder. For this reason, a distributed IDS is suitable for this type of attack. These are summarised in Table 1.

7 Conclusion and Future Work

IoT has exalted expectations due to its ability to transform physical items from many application areas into Internet hosts. Intruders, on the other hand, may make use of the IoT's enormous potential by considering it a new means to endanger the privacy and security of users. Thus, IoT security solutions should be developed and IDS is one of the most important security technologies for IoT. Through careful survey, this chapter has managed to review current classifications and existing methodologies, with the help of which the most appropriate IDS for a particular attack on IoT is proposed.

Future research could concentrate on the following topics: (1) investigating more about the strengths and weaknesses of various detection methods and placement strategies, (2) developing IDS for social engineering threats, (3) addressing more IoT technologies, (4) investigating about ANN based IDS systems for Routing attacks [28], and (5) improving alert traffic and management security.

References

1. A. A. Ansam Khraisat, A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00077-7#Sec59, [Accessed: 18-01-2022] (2021).
2. H. F. A. H. Mohamed Faisal Elrawy, Ali Ismail Awad, Intrusion detection systems for IoT-based smart environments: a survey, https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-018-0123-6, [Accessed: 18-01-2022] (2018).
3. Internet of Things, https://en.wikipedia.org/wiki/Internet_of_things, [Accessed: 09-02-2022] (2022).
4. What is IoT?, https://www.oracle.com/in/internet-of-things/what-is-iot/, [Accessed: 09-02-2022] (2022).
5. IoT Security Issues, Threats, and Defenses, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses, [Accessed: 09-02-2022] (2021).
6. Intrusion detection system (IDS): What it is; its types, https://www.geeksforgeeks.org/intrusion-detection-system-ids/, [Accessed: 19-01-2022] (2022).
7. Sagar N. Shah* Ms. Purnima Singh M.E. (Computer Science & Engineering), Assistant Professor, Computer Science & Engineering, Parul Institute of Engineering & Technology, Parul Institute of Engineering & Technology, Vadodara, Gujarat, India Vadodara, Gujarat, India, Signature-Based Network Intrusion Detection System Using SNORT And WINPCAP, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 10, December- 2012 ISSN: 2278-0181 (2012).
8. Intrusion Detection System (IDS): Signature-based vs. Anomaly-based, https://www.n-able.com/blog/intrusion-detection-system, [Accessed: 19-01-2022] (2021).
9. S. A. Tamara Saad Mohamed, IoT-Based Intrusion Detection Systems: A Review, https://www.tandfonline.com/doi/abs/10.1080/23080477.2021.1972914?journalCode=tsma20, [Accessed: 18-01-2022] (2021).
10. Vasima Khan (Computer Science & Engineering), All Saint Inst. of Tech, Bhopal, M. P., India; Anomaly based Intrusion Detection and Prevention System, International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March - 2013 ISSN: 2278-0181 (2013).
11. StevenR. Snapp,StephenE. Snaha- HaystackLaboratories,Inc. DanielM. Teal,TimGrance-UnitedStatesAir ForceCryptologicSupportCenter, The DIDS (DistributedIntrusion Detection-System) Prototype, Summer'92USENIX- JuneE-June12, lgg - SanAntonio,TX (1992).
12. K. Letou, D. Devi, Y. Jayanta, Host-based intrusion detection and prevention system (hidps) (05 2013). https://doi.org/10.5120/12136-8419.
13. Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de Alvarenga, 2018. A survey of intrusion detection in Internet of Things, http://www.ttcenter.ir/ArticleFiles/ENARTICLE/10201021.pdf, [Accessed: 18-01-2022] (2018).
14. Intrusion Detection in IoT, https://securityboulevard.com/2021/12/intrusion-detection-in-iot/, [Accessed: 18-01-2022] (2021).

15. Raza, S., Wallgren, L., Voigt, T., 2013. SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw. 11 (8), 2661–2674. (2013).
16. Liu, C., Yang, J., Zhang, Y., Chen, R., Zeng, J., 2011. Research on immunity-based intrusion detection technology for the Internet of Things. In: Natural Computation (ICNC), 2011 Proceedings of the Seventh International Conference on, Vol. 1, pp.212–216 (2011).
17. Lee, I., Lee, K., 2015. The internet of things (IoT): applications, investments, and challenges for enterprises. Bus. Horiz. 58 (4), 431–440 (2015).
18. Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C., Spirito, M.A. 2013b. DEMO: an IDS framework for internet of things empowered by 6LoWPAN. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13, ACM, New York, NY, USA, pp. 1337–1340 (2013).
19. Mitchell, R., Chen, I.-R., 2014. A survey of intrusion detection techniques for cyberphysical systems. ACM Comput. Surv. (CSUR) 46 (4), 55. (2014).
20. Le, A., Loo, J., Luo, Y., Lasebae, A., 2011. Specification-based IDS for securing RPL from topology attacks, In: Wireless Days (WD), 2011 IFIP, pp. 1–3 (2011).
21. Cervantes, C., Poplade, D., Nogueira, M., Santos, A., 2015. Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606–611 (2015).
22. Hemanth, Jude, Xing, Ying, Shu Hui, Zhao Hao, Li Dannong, Guo Li, 2021, 2021/04/15, Survey on Botnet Detection Techniques: Classification, Methods, and Evaluation 6640499 2021 https://doi.org/10.1155/2021/6640499, Mathematical Problems in Engineering Hindawi (2021).
23. Kasinathan, P., Pastrone, C., Spirito, M., Vinkovits, M., 2013a. Denial-of-service detection in 6LoWPAN based Internet of Things. In: Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE Proceedings of the 9th International Conference on, pp. 600–607. (2013).
24. Farouq Aliyu, Tarek Sheltami, Ashraf Mahmoud, Louai Al-Awami, Ansar Yasar, "Detecting Man-in-the-Middle Attack in Fog Computing for Social Media" Vol.69, No.1, 2021, pp.1159-1181 (2021).
25. E. Aïmeur, D. Schönfeld, The ultimate invasion of privacy: Identity theft (2011). https://doi.org/10.1109/PST.2011.5971959.
26. C. Bhusal, Systematic review on social engineering: Hacking by manipulating humans. journal of information security (2021).
27. Cervantes, Christian; Poplade, Diego; Nogueira, Michele; Santos, Aldri (2015). [IEEE 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM) - Ottawa, ON, Canada (2015.5.11-2015.5.15)] 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM) - Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. (), 606–611. https://doi.org/10.1109/INM.2015.7140344 (2015).
28. S. V. V. Sharma, Aiemla: artificial intelligence enabled machine learning approach for routing attacks on internet of things. (2021). https://doi.org/10.1007/s11227-021-03833-1.