ISSN 2347 - 3983

Volume 10. No.3, March 2022

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter041032022.pdf

https://doi.org/10.30534/ijeter/2022/041032022

Investigation on Intrusion Detection Systems (IDSs) in IoT

KarthikKumar Vaigandla[1*], Nilofar Azmi[2], RadhaKrishna Karne[3]

[1,2,3]Dept. of Electronics & Communication Engineering, Balaji Institute of Technology and Science,Telangana,India
[1]vkvaigandla@gmail.com,[2]nilofarazmi484@gmail.com, [3]krk.wgl@gmail.com

Received Date February 06, 2022 Accepted Date : February 28, 2022 Published Date : March 07, 2022

ABSTRACT

In smart environments, comfort and efficiency are important goals in terms of the quality of human life. Recent developments in Internet of Things (IoT) technology have made it possible to design smart environments. IoT-based smart environments are concerned with security and privacy as key issues. Systems based on the IoT pose a security threat to smart environments. In order to prevent IoT-related security attacks which take advantage of some of these security vulnerabilities, intrusion detection systems (IDSs) designed for IoT environments are crucial. Data generated by connected objects in the age of the IoT provides the basis for big data analytics, which could be employed to identify patterns and identifies anomalies in data. In order to detect intrusions, most cyber security systems employ IDSs, which are used by a variety of techniques and architectures. As opposed to signature-based IDS, anomaly-based IDS learns the normal pattern of system behavior and alerts on abnormal events that occur, as opposed to monitoring monitored events against a database of known intrusion experiences. This paper focuses on the IDS implementation on the IoT network. The use of sensor devices to collect data from smart grid environments has led to smart grids becoming the preferred intrusion target due to the IoTs using advanced information technology. Clouds are data storage systems that provide a variety of smart infrastructure services, such as smart homes and smart buildings, over the internet. A deep learning-based intrusion detection system for the Internet of Things requires consideration of key design principles presented in this paper.

Key words: Intrusion Detection System (IDS), Internet of things (IoT), Smart Environments, Anomaly Detection, Machine Learning, Cyber Security, Deep Learning.

I. INTRODUCTION

The number of devices connected to the Internet today worldwide is more than 25 billion [1]–[3]. The IoT is a network of interconnected smart devices, which are integrated into a single network through different services. Smart devices are able to gather sensitive information and operate at high speeds. They are capable of connecting and communicating with each other, and they take decisions based on indicator information [4]. To process information and maintain remote control, IoT environments use cloud services. Data and devices are accessed and controlled by clients via mobile applications or web services. Artificial intelligence algorithms are used to analyze the information extracted from IoT sensors and analyze this data [5]-[6]. 5G must support IoT and machine-to-machine (M2M) communication [7]. Scalability, network management, security, and privacy as well as interoperability and heterogeneity are all issues that must be addressed when implementing IoT [7]. Massive advances in telecommunications networks have led to the emergence of the IoT due to the use of electronic services and applications in everyday life [8]. As a communication paradigm, the IoT describes devices connected to the internet that can sense their environment, exchange data, and connect with each other [9]-[10]. IoT can improve humans' lives, but at the cost of their security [12]. Cybercriminals are becoming increasingly attracted to IoT networks and they are exposed to major risks [47]. 98% of all IoT device traffic is unencrypted, and 41% of attacks take advantage of IoT device vulnerabilities, according to a report by Unit 42 of Palo Alto Networks [13]. Devices that are vulnerable could later be used to launch sophisticated and large-scale attacks by hackers joining an IoT botnet. There are predicted to be one trillion IP addresses or objects linked to the Internet by 2025 through IoT networks [11].

Smart cities, smart homes, and IoT paradigms have recently been used to create smart environments with various applications. By addressing challenges related to the living environment, energy consumption, and industrial needs, smart environments can help humankind live a more productive and comfortable life [14]. The growth of applications and services that are based on IoT across a variety of networks directly correlates with this goal. Smart Cities are based on an IoT system, for example Padova Smart City in Italy [15]. Sensing devices work together in a smart environment to execute tasks. In the evolving smart environment, wireless sensors, wireless communication techniques, and IPv6 are all important components. A smart environment can be a city or a home, a healthcare system, or a service. Smart objects are more effective when they're integrated with IoT systems and smart environments. Denial-of-service (DoS) attacks and distributed denial-of-service attacks are common security threats for IoT systems. An IoT network can be significantly damaged by such an attack, as smart environment applications and IoT services are at risk. Thus, the security of IoTs is becoming a major concern [9]. A security mechanism for detecting intrusions of an IoT system is the intrusion detection system (IDS). A network IDS deployed for the Internet of Things should be capable to analyze packets of data in the IoT network and respond in real time, analyze data packets within the IoT network at different layers and with different protocol stacks, and adapt to different technologies in the IoT environment [11]. A security system that is designed for IoT-based smart environments should deliver fast performance, high-volume data processing, and low processing capability. Consequently, conventional IDSs may not be fully capable of protecting IoT environments. IoT security is a continuous and serious issue. Therefore, it is necessary to develop corresponding mitigation approaches that address the vulnerabilities in IoT systems [16]. Security is maintained by Intrusion Detection Systems (IDS), which detect malicious activities on computers or networks and alert the administrator [17]. Network Intrusion Detection Systems (NIDS) detect intrusions on an entire network, whereas Host-based Intrusion Detection Systems (HIDS) protect a single computer system. Network intrusion detection systems (NIDSs) analyze traffic generated by hosts and devices in a network [18]. Several IDS solutions have been proposed in connection with IoT [19]-[20].

2. INTERNET OF THINGS (IoT)

A recent development in interconnecting devices is IoT [21]. Over the last few years, we've used the Internet more and more in everyday life. Objects are in our modern world capable of gathering, processing, and sending data to other objects, servers, and applications [22]. Engineers, doctors, and safety professionals, among others, use our products to solve problems [21]. Smart objects have already become an integral part of a global networking platform through communication. Wireless sensor networks and nodes form information systems through the IoT technology, allowing people and things to become practically connected [21]. The Internet and social media will be able to communicate freely and effectively. The development of new services and applications is made possible by social media and the internet [21].

2.1 IoT Paradigm

As early as 1999, the Massachusetts Institute of Technology (MIT) created the Auto-ID Center which led to the IoT concept being born. Radio frequency identification (RFID) [23], which is a deterministic process, was first developed by the Auto-ID Center in 2003. The technology behind the IoT depends on this idea [24]. But the IoT is a well-established paradigm, and based on different perspectives, it can be described in different ways. The IoT consists of hardware items and digital information flows that are based on RFID tags, as defined in [25]. Here we will describe various definitions and architectures of IoT provided by various standards and industry organizations. A network of items with sensors connected to the Internet can be defined as a part of the Internet of Things by the Institute of Electrical and Electronics Engineers (IEEE) [24,26]. IoT is defined by the International Telecommunication Union as a network accessible anywhere, anytime, and by anyone, and it has three dimensions [27]. Instead of using the expression "IoT", the European Telecommunications Standards Institute (ETSI) defines machine-to-machine communications (M2M) as an automated system that makes decisions and processes data without direct human intervention [28]. Furthermore, Cisco, a company that works on IoT technologies, has its Internet of Everything (IoE) project. People, data, things, and processes are all part of an IoE network, as described by Cisco. This network creates and moves information and actions [29].

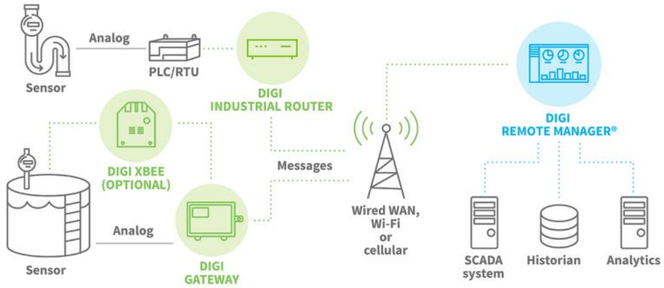

Figure 1: Stages/ Major Components of IoT

2.2 Architecture of IoT

The architecture for the IoT does not have a universal consensus. Research has offered different approaches for IoT architecture [31]. IEEE is developing an architectural framework for the Internet of Things (IEEE P2413). IoT domains and their applications are the subjects of this project [30].

Perception Layer: Sensors in this layer collect information about the surrounding environment and enable the perception layer to gather information. Other smart objects in the environment can be identified by it as well as by sensing some physical parameters [31]. This layer outputs information that is transmitted to the next layer (the network layer) for processing.

Network Layer : Network devices and servers are connected through this layer. Data from sensors is also sent and processed at the network layer. Depending on the physical components and technology of the communication system, this can be a wired or wireless system. This layer outputs information to the next layer (the middleware layer).

Application Layer **:** IoT applications are managed globally by the application layer. Middleware processes information that goes to the application layer. Application-specific services are provided by this layer. Smart homes, smart cities, and smart health are just a few examples of applications for IoT [31].

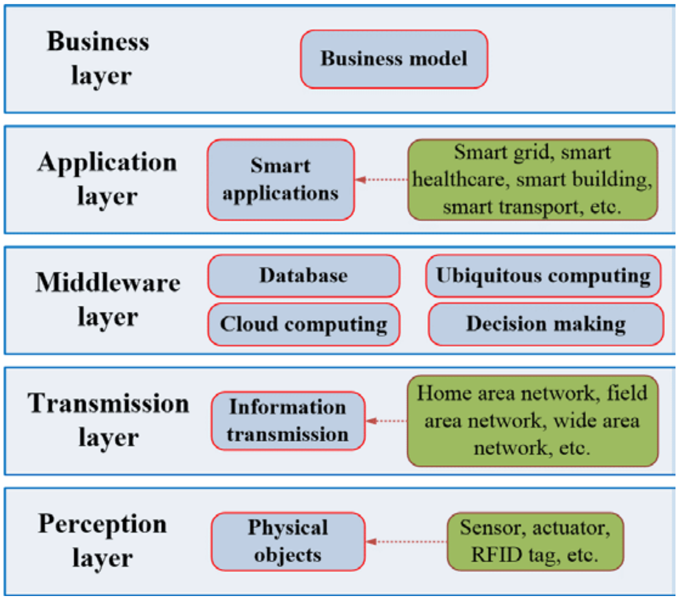

Figure 2a: Five layer IoT Architecture

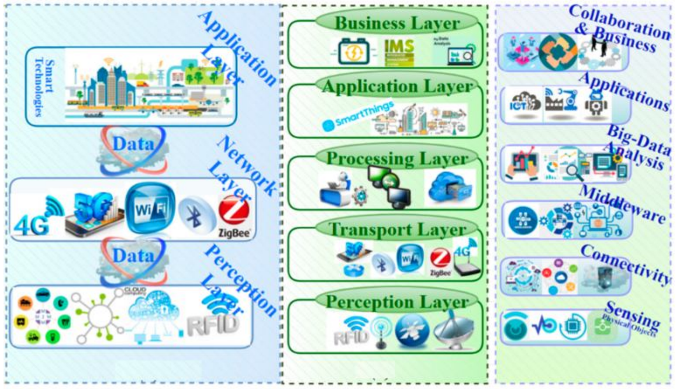

Figure 2b: Three layer, Five layer and Six layer IoT Architecture

Transport Layer **:** Several network protocols, such as wireless, 3G [8], LAN, Bluetooth, RFID, and NFC, are used to transmit sensor data from the perception layer to the processing layer [31].

Processing Layer or Middleware Layer **:** From the transport layer, data is stored, analyzed, and processed by the processing layer. This layer is capable of managing and providing diverse services to the lower layers. Several technologies are utilized, such as databases, cloud computing, and big data processing.

Business Layer **:** In this, applications, income, profit models, user privacy, and business models are managed.

2.3 IoT Smart Environments

Sensing devices are employed in smart environments to improve human comfort and efficiency. The realization of smart objects becomes effective with IoT-based smart environments. Remote monitoring and control are possible when sensors are connected to an IoT network. From 93.5 billion US dollars in 2017 to 225.5 billion US dollars by 2026 [32], Navigant Research estimates the market for smart city services to grow. Whenever people use the term smart, they mean the ability to autonomously obtain and apply knowledge, and when they use the term environment, they mean the environment around them [33]. Smart cities are an example of smart environments. The heart of a smart city is an integrated information center run by an IoT service provider that provides information related to utilities such as power, water, and gas. There are other types of smart environments, such as smart health, smart industry, smart buildings and smart homes [22]. Providing services using smart methods using the information collected by IoT-enabled sensors is the objective of such smart environments. Figure 3 illustrates the architecture of this type of IoT-based smart environment. With IoT-based smart environments, some special characteristics arise, and therefore, specific needs arise when deploying these environments. The ability to collect and process data remotely and to operate smart objects remotely, for example, requires remote monitoring and remote control capabilities [4]. Another important characteristic of such a system is its ability to make decisions. By utilizing data mining and other techniques to extract useful data, smart objects are able to make intelligent decisions without human intervention.

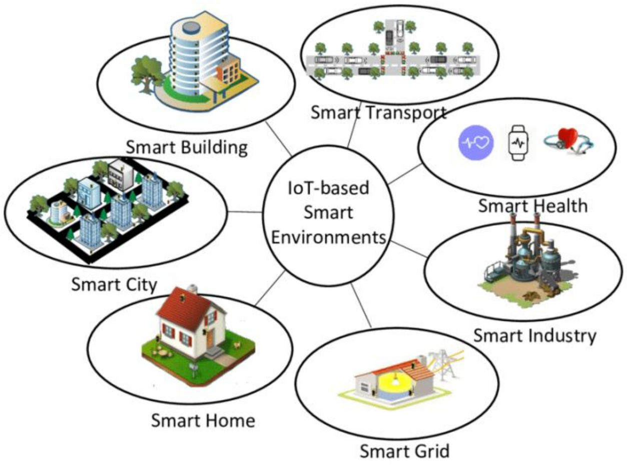

Figure 3: IoT-Based Smart Environments

2.4 IoT Technology for Developing Smart Cities

In order to address traditional public management problems, many national governments are developing information and communication technology (ICT) applications. An effective and modern solution to this problem is the creation of a smart city [15]. The concept of smart cities is an aspect of smart environments. Smart cities have several advantages, including improving public services and reducing public administration costs by converting traditional public services and resources into smart ones [34]. However, smart cities need a powerful software framework to manage and perform public services. Furthermore, the creation of a smart city based on IoT faces many challenges. IoT systems present the greatest challenges due to their novelty, complexity, and technical complexity. In addition, the concept of a smart city is unable to be effectively applied without widely accepted definitions of smart city operations. Smart cities have overcome these barriers successfully in Padova, Italy, an example of a smart city that has been successful. Padova Smart City takes advantage of different types of data and technology in order to develop ICT systems for public administration.

3. INTRUSION DETECTION SYSTEM (IDS)

Defending an information system from unauthorized access is the goal of an IDS. An unauthorized intrusion may compromise the integrity, confidentiality, or availability of information. The goal of an IDS is to find out whether malicious activity is occurring by analyzing network traffic or resource usage and raising an alert if it does. Depending on the strategy used to detect intrusions, the IDSs can be classified into either two main groups. One group uses cross-checking monitored events with a database of intrusion techniques or another group analyzes normal behavior and reports when anomalous events occur [17]. The purpose of an IDS is to monitor traffic data in order to identify and protect an information system against intrusions that could compromise its confidentiality, integrity, and availability [35].

Figure 4: Developing smart cities using IoT Technology

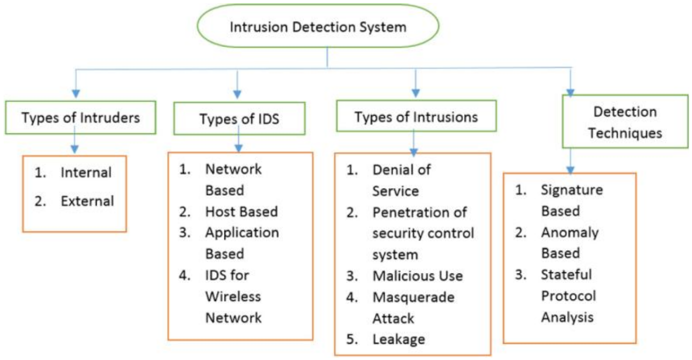

Figure 5: Types of IDS

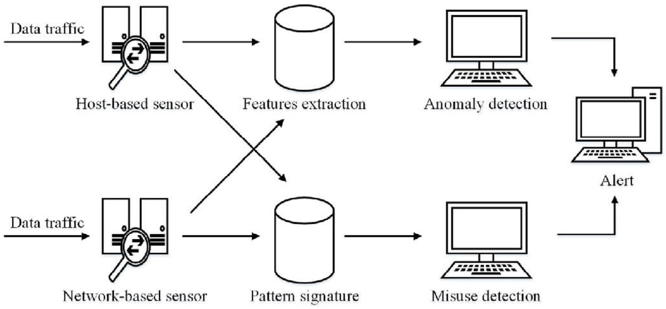

Figure 6: Illustration of the operation of an IDS

Figure 6 represents a schematic illustration of the operation of an IDS. There are three stages in the operation of an IDS. In the first stage (Monitoring Stage), network-based sensors are used to monitor the environment. Feature extraction methods or pattern identification methods are used in the analysis stage, which is the second stage. Anomaly detection and misuse intrusion detection comprise the detection stage. The purpose of an IDS is to capture a copy of information systems' data traffic and to analyze this copy to identify potentially harmful activities [36].

3.1 Signature-based IDS

A signature-based IDS (SIDS) uses a database of old attacks as a basis for detecting new threats. The signatures of the current activities are extracted and compared to the signatures in the database by using matching methods or protocol conformance checks. An alarm is triggered if a match is found. Both online and offline modes are available, where the hosts can be monitored directly and alarms can be generated in real time, as well as looking at system logs. Misuse Detection, and Knowledge-Based Detection, are other terms for this class of IDS [37]. Depending on the number of traffic features to be considered, extraction of traffic signatures may be cumbersome and tedious. Usually, signatures are manually crafted by experts who are intimately familiar with the exploits the system is supposed to detect. As a system for automatically generating malicious traffic signatures proposed in [38]. By extending honeyd [39], they added a subsystem that inspects protocol hierarchy traffic at multiple levels and integrates it with existing IDS. In the early stages of SIDS, single packets were analyzed and matched against a database of rules.

3.2 Anomaly-based IDS

Anomaly-based intrusion detection systems (AIDS) solve the problems of SIDS. A model of the nominal behavior of AIDS is usually built during the training phase. A typical IDS monitors computers and compares them to the nominal one when it is deployed. Whenever there is a significant deviation between the behavior of hosts and the model, an IDS alert may be raised. An AIDS may be capable of capturing zero-day attacks with this strategy, since it does not compare the behavior of current hosts to those in a database. Moreover, an anomaly-based IDS is difficult to exploit because interacting with a target would likely raise an alert, since an attacker can't tell what normal behavior of a host is [40]-[41]. Also, AIDS can provide a system analysis tool in addition to being used for security purposes. An anomaly is reported by the IDS, the difference indicates that something has changed from the baseline conditions, which can indicate both an intrusion as well as a bug in the device's logic. When compared with SIDS, an AIDS has a greater rate of false positives. It is true that an AIDS can raise false alerts if it is not aware that a targeted system can change behavior during operation without any intrusion taking place [17].

3.3 Network Intrusion Detection System (NIDS)

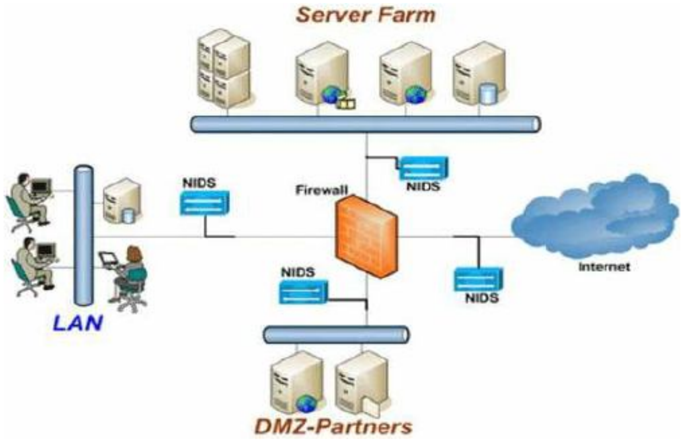

Figure 7: NIDS

The NIDS analyzes all traffic sent by all devices on the network at a planned point in the network. By observing and comparing the traffic flowing over the entire subnet to the known attack collection, it can detect and stop attacks before they occur [42]. The administrator can receive an alert after an attack or abnormal behavior is identified. NIDS can be used on a subnet containing firewalls so you can check if they've been compromised.

3.4 Host Intrusion Detection System (HIDS)

HIDS are deployed on independent hosts or devices. When a HIDS detects suspicious or malicious activity, it will notify the administrator. HIDS monitor only the incoming and outgoing packets from the device. The program compares the current snapshot with the previous one. An alert will be sent to the administrator if the analytical system files have been edited or deleted. Mission critical machines with static layouts can be used as an example of HIDS use. Most HIDS analysis is based on measures in the host environment, such as the log files in a computer system. The HIDS uses these metrics or features to make decisions. Any HIDS is based on the extraction of features from the host environment.

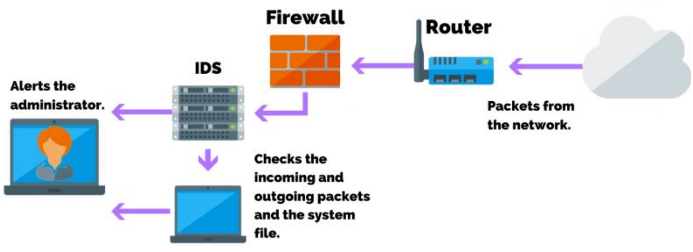
Firewall
Router
IDS
Alerts the administrator.
Packets from the network.
Checks the incoming and outgoing packets and the system file.

Figure 8: HIDS

3.5 Protocol-based Intrusion Detection System (PIDS)

PIDS are systems that run on a server's front end, interpreting and controlling the protocol between a server and a user/device. Monitoring the HTTPS protocol stream regularly and accepting the HTTP protocol is its way of securing the web server. This system would have to reside just before entering its web presentation layer, as HTTPS is un-encrypted, before utilizing HTTPS.

3.6 Application Protocol-based Intrusion Detection System (APIDS)

APIDS resides on a group of servers as a system or agent. By interpreting and monitoring the communication protocols, the intrusions are identified. The middleware would then monitor it while it interacts with the database in the web server using the SQL protocol.

3.7 Hybrid Intrusion Detection System (Hybrid IDS)

Hybrid IDS combine two or more IDS approaches. Hybrid IDS combine host agent and network data to create a comprehensive picture of the network system. In comparison to other IDSs, hybrid IDS is more effective. A good example is Prelude.

4. IDS FOR IoT

An IDS that targets IoT devices may utilize 6LoWPAN, BLE, etc. as the communication technology. It is recommended to deploy this class of IDS on the same network as the device. Based on responses from IoT devices, they typically perform their predictions by leveraging control information, such as checking protocol compliance, that is available from the specific IoT device. IoT-agnostic IDS, are independent of a particular Internet of Things technology. Information from all available technologies can be utilized, such as TCP/IP traffic, no matter what technology is currently used by the device. It can handle traffic generated by heterogeneous devices making use of different communication technologies, which makes this type of IDS suitable for use in an edge environment. The ability to detect low-level attacks generated on a device-level is an advantage of IoT-specific IDS over an IoT-agnostic one. Alternatively, an IDS that is IoT-agnostic can deal with several IoT devices without deploying an additional IDS for each type of communication.

Wi-Fi [7], LoRa [21], ZigBee [23], and Bluetooth [23] have all been proposed as IoT-specific IDSs. They are usually expert systems that capture and analyze the traffic between hosts and ensure that everything complies with the protocol for the specific technology. The physical network layer (PHY), can also be scanned by advanced systems. It is commonly seen that attackers will send bits which do not follow the communication protocol, so that external IDSs are unable to read the data and make the attack hard to detect. IoT security is primarily concerned with issues related to infrastructure and operation, such as routing, topological control, and network maintenance. The Routing Protocol for

Low Power Lossy Network (RPL) [43] provides a new protocol for devices with constrained resources. Destination Oriented Directed Acyclic Graph (DODAG) undergirds the message exchange and enables point-to-point and point-to-multipoint communication between the devices following the protocol. In order to disrupt protocol execution, attackers could create malicious packets. IDSs therefore often concentrate on checking whether the connected devices executed RPL correctly. It is the Rank Attack [44] that is the most prevalent attack, in which a child node advertises a lower rank value than the actual rank. When there are many hops between two nodes, the rank provides the information about which nodes are closer to the parent node, with the rank strictly decreasing from the root to the children. The messages could be routed along loops in a Rank Attack scenario, which fails to select the most optimal path.

While all expert systems are capable of high accuracy and low false positive rates, IoT-specific IDSs are unable to detect zero-day attacks or unusual host behavior. A IDS that doesn't care about the technology for exchanging data between connected devices is called an IoT-agnostic IDS. These IDSs may be applied in IoT gateways, discarding the PHY and MAC layer information, or they may be applied to another sub network, which makes use of TCP/IP traffic features.

5. DEEP LEARNING IDS IN IoT: KEY DESIGN PRINCIPLES

In order to generate effective and efficient algorithms, deep learning-based IDS solutions for IoT need to produce models that perform well. While each model is capable of achieving its goal, some design choices limit their effectiveness. There are some deep learning IDSs in IoT that neglect consideration of the over fitting problem or apply their models to non-balanced datasets, which negatively impacts their accuracy, memory consumption, and computational time. A number of IDSs do not optimize their learning models, while others are evaluated using outdated or irrelevant datasets, which do not represent real-world IoT traffic. These observations lead us to believe that the deep learning-based solution for IoT should be based on the following principles:

Handling Overfitting: The model that's overfitting doesn't generalize well to unseen data, as it achieves a good fit on the training data. Several methods can be used to avoid overfitting in deep learning: a) Regulating the loss function in order to add a cost for large weights; b) Dropout layers do not maintain certain features by setting them to 0. Instead, they randomly remove certain features.

Balancing Dataset: Disproportionate distribution of classes within a dataset can be characterized as data imbalances. An imbalanced dataset will cause a model to become biased, i.e., it will favor the majority classes and misclassify the minority classes. In order to improve the model's performance, the dataset must be balanced.

Feature Engineering: In terms of memory and time consumption, it reduces the cost of deep learning workflows. Moreover, it makes learning more accurate by discarding irrelevant features and applying feature transformations.

Model Optimization: Modelling optimization aims to minimize the difference between predicted and actual outputs, and this is called a loss function. Weights are iteratively adjusted in order to reach this result. The effectiveness of the model will be improved if an optimization algorithm like SGD and Adam is applied.

Testing on IoT Dataset: To get results that reflect real-world IoT traffic, an IDS based on deep learning should be evaluated using an IoT dataset.

6. SECURITY CHALLENGES IN IoT AND IoT IDS

6.1 Security challenges in IoT-based smart environments

IoT security is becoming more and more problematic as the number of services and users in IoT networks increases. Intelligent objects become more efficient when these systems are integrated with smart environments. On the other hand, IoT security vulnerabilities can have massive consequences in fields such as medicine and industry that use smart environments for critical functions. Smart environments based on IoT may be vulnerable to security threats without robust security systems. Information security in IoT systems requires greater research focus to address three important security concepts: confidentiality, integrity, and availability. This call for greater research in IoT systems.

Security issues and complexity and compatibility of IoT environments pose notable obstacles for the creation of smart environments in the real world. The services provided by smart environments can be affected by attacks such as DDoS and DoS on IoT networks. The IoT poses a variety of security challenges from many different perspectives, including vulnerabilities associated with the protocol for IoT communication [45]. In this survey, we looked at IDS systems as part of the Internet of Things paradigm, independent of specific protocols; we therefore focused on the security challenges posed by IoT systems based on the IEEE definition and the general IoT architecture. It is the various layers of IoT that present security challenges in IoT systems. In the physical layer, there are challenges due to physical damage, hardware failures, and power constraints. At the network layer, there can be challenges such as DoS attacks, sniffing, gateway attacks, and unauthorized access. Among the challenges faced at the application layer are malware attacks, application vulnerabilities, and software bugs [46].

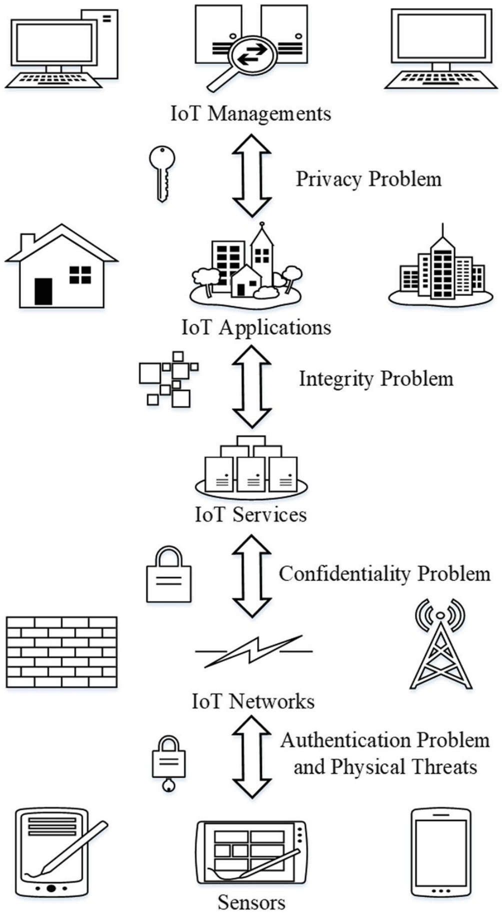

Figure 9: Security issues in the various IoT layers

6.2 Challenges of IoT IDS

Large connected devices are on the rise in the IoT era. In the IoT environment, communications security is a challenge using previously developed IDSs that presents potential research questions for the future. Although a lot of research has been conducted in the area of IDSs, there are still many important issues to be addressed. An IDS must be accurate, capable of detecting a variety of intrusions with fewer false alarms, and have other capabilities.

6.3 Challenges of IoT IDS for Industrial Control Systems (ICS)

Transportation, manufacturing, retailing, and smart city infrastructures have all used industrial IoT systems in the past. In IoT, more and more connected things are being used thanks to advances in wireless communication, smart phones, healthcare, smart grids, household automation, and smart cities. The Cyber Physical System (CPS) is an enhancement of the IoT ecosystem. It integrates a physical sensor and actuator networked with a computer-based control system. ICSs are commonly made up of two components: Supervisory Control and Data Acquisition (SCADA) hardware that gathers information from sensors and controls machines through software; and supervisory communication software that enables humans to manage machines.

The unique architectures of ICSs make them an excellent target for cyber-attacks, as the attackers are currently focusing on them. The first cyber-warfare weapon, Stuxnet attack, is among the most notable attacks against the ICSs in recent years. Stuxnet differed from a typical attacked in that its primary target was most likely the Iranian nuclear program (Nourian & Madnick, 2018). A state-sponsored attack on an ICS could also come from a competitor, an internal attacker with a malicious purpose, or even a hacktivist group. A compromised ICS can have devastating consequences for the economy, public health, and national security. As a result of ICS system problems, dangerous toxic chemicals have been released, causing cascading power outages and explosions. It is essential to use secure ICSs in order to provide reliable performance, safety, and flexibility.

6.4 Challenge of IoT IDS on intrusion evasion detection

Detecting attacks masked by evasion techniques is the main challenge for SIDS and AIDS. As evasion techniques become more sophisticated, IDS can be relied upon to either bring back the original signature of an attack or create new signatures to cover the modifications. Research is still needed to determine whether IDS is robust to various evasion techniques. Regular expressions such as SIDS can detect mutations related to simple mutations such as manipulating spaces, but they are also useless against a number of obfuscation techniques used by hackers to conceal malware, including encryption and packing.

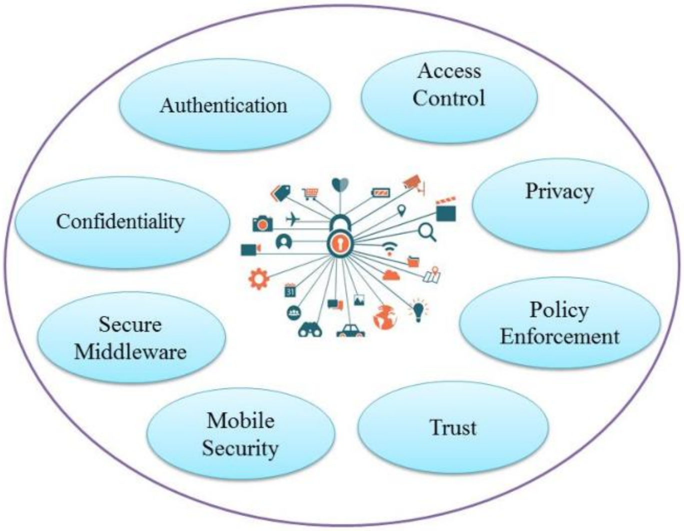

Figure 10: IoT - Security Challenges

7. CONCLUSION

The Internet of Things connects physical objects to the Internet in a variety of application domains, which is essential to the future of technology. There is a growing demand for a secure and lightweight IoT security solution that can be deployed in IoT environments as the number of users, services, and applications of IoT increases. IoT networks are essentially responsible for enabling smart environments; consequently, any flaws in the security of these networks will directly influence the smart environments that they enable. It is extremely important that smart environments be secure. The best solution may be an IDS. We discussed the available IDS for IoT environments in this paper. IDSs for use in smart environments were discussed, including their application to the IoT paradigm. This paper summarized the features of all the IDS methods.

An effective and efficient intrusion detection system for the IoT is identified in this paper using design principles for deep learning. This review may contribute significantly to security researchers by examining the current status of this fascinating and dynamic area of research, facilitating researchers interested in finding novel IDS solutions to address IoT security in the context of communication. Based on the recommendations of this study, future work will examine the design of a high performance hybrid IDS specific to IoT-based smart environments. The IDS design will take account of the security issues related to the IoT enabling technologies and protocols.

REFERENCES

[1] H. Alkahtani, T. H. H. Aldhyani, and M. Al-Yaari, “Adaptive anomaly detection framework model objects in cyberspace,” Applied Bionics and Biomechanics, vol. 6660489, p. 14, 2020.

[2] T. Aldhyani and M. Joshi, “Intelligent time series model to predict bandwidth utilization,” International Journal of Advanced Computer Science and Applications, vol. 14, pp. 130–141, 2017.

[3] M. Tang, M. Alazab, and Y. Luo, “Big data for cybersecurity: vulnerability disclosure trends and dependencies,” Institute of Electrical and Electronics Engineers Transactions on Big Data, vol. 5, no. 3, pp. 317–329, 2019.

[4] Hasan Alkahtani and Theyazn H. H. Aldhyani," Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms," Hindawi, Complexity, Wiley, Volume 2021, Article ID 5579851, 18 pages, https://doi.org/10.1155/2021/5579851

[5] D. Vasan, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin, “MTHAEL: cross-architecture IoT malware detection based on neural network advanced ensemble learning,” Institute of Electrical and Electronics Engineers Transactions on Computers, vol. 69, no. 11, pp. 1654–1667, 2020.

[6] A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti, and M. Alazab, “A comprehensive survey for intelligent spam email detection,” Institute of Electrical and Electronics Engineers Access, vol. 7, pp. 168261–168295, 2019.

[7] Karthik Kumar Vaigandla, Bolla Sandhya Rani, Kallepelli Srikanth, Thippani Mounika, RadhaKrishna Karne, " Millimeter Wave Communications: Propagation Characteristics, Beamforming, Architecture, Standardization, Challenges and Applications," Design Engineering, ISSN: 0011-9342, 2021, Issue: 9 , pp.10144-10169

[8] Karthik Kumar Vaigandla, SandyaRani Bolla , RadhaKrishna Karne, " A Survey on Future Generation Wireless Communications-6G: Requirements, Technologies, Challenges and Applications", International Journal of Advanced Trends in Computer Science and Engineering, Volume 10, No.5, 2021, pp. 3067-3076.

[9] King J, Awad AI (2016) A distributed security mechanism for resource-constrained IoT devices. Informatica (Slovenia) 40(1):133–143

[10] Weber M, Boban M (2016) Security challenges of the internet of things. In: 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, Opatija. pp 638–643

[11] Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, Vienna. pp 84–90

[12] H. Belkhiri, A. Messai, M. Belaoued, and F. Haider, “Security in the internet of things: recent challenges and solutions,” in International Conference on Electrical Engineering and Control Applications, pp. 1133–1145, Constantine, Algeria, 2019.

[13] Palo alto networks, “2020 unit 42 iot threat report,” 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

[14] Kafle VP, Fukushima Y, Harai H (2016) Internet of things standardization in ITU and prospective networking technologies. IEEE Commun Mag 54(9):43–49

[15] Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32

[16] Mohamed Faisal Elrawy, Ali Ismail Awad and Hesham F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," Journal of Cloud Computing:Advances, Systems and Applications, (2018) 7:21, https://doi.org/10.1186/s13677-018-0123-6

[17] Pietro Spadaccino and Francesca Cuomo, "Intrusion Detection Systems for IoT: opportunities and challenges offered by Edge Computing,"2020.

[18] A. Lakhina, M. Crovella, and C. Diot, “Diagnosing network-wide traffic anomalies,” ACM SIGCOMM Computer communication Review, vol. 34, no. 4, p. 219, Oct 2004.

[19] A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Communications Surveys Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[20] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, “A survey of machine and deep learning methods for internet of things (iot) security,” IEEE Communications Surveys Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020.

[21] Karthik Kumar Vaigandla, Radha Krishna Karne , Allanki Sanyasi Rao, "A Study on IoT Technologies, Standards and Protocols," IBM RD's Journal of Management & Research Volume 10, Issue 2, September 2021, pp.7-14, DOI: 10.17697/ibmrd/2021/v10i2/166798

[22] Karthik Kumar Vaigandla, Shivakrishna Telu, Sandeep Manikyala, Bharath Kumar Polasa, Chelpuri Raju, "SMART AND SAFE HOME USING ARDUINO," INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY, Volume 8, Issue 7, 2021,pp.132-138

[23] Karthik Kumar Vaigandla, Dr.N.Venu, " A Survey on Future Generation Wireless Communications - 5G : Multiple Access Techniques, Physical Layer Security, Beamforming Approach", Journal of Information and Computational Science, Volume 11 Issue 9, 2021, pp.449-474.

[24] IEEE The institute, Special Report:The Internet of Things. http://theinstitute.ieee.org/static/special-report-the-internet-of-things. Accessed 8 Jan 2017

[25] Thiesse F, Michahelles F (2006) An overview of EPC technology. Sens Rev 26(2):101–105

[26] Minerva R, Biru A, Rotondi D (2015) Towards a definition of the internet of things (IoT). Technical report, IEEE, Internet of Things [27] SPU (2005) The internet of things executive summary. Technical report, The ITU Strategy & Policy Unit, (SPU)

[28] Krˇco S, Pokri´c B, Carrez F (2014) Designing IoT architecture(s): A european perspective. In: 2014 IEEE World Forum on Internet of Things (WF-IoT). IEEE, Seoul. pp 79–84

[29] Bradley J, Loucks J, Macaulay J, Noronha A (2013) Internet of everything (IoE) value index. Technical report, Cisco.

[30] IEEE (2015) Standards, Internet of Things, IEEE P2413. http://standards. ieee.org/develop/project/2413.html. Accessed 8 Jan 2017

[31] Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Hindawi, Journal of Electrical and Computer Engineering, Volume 2017, Article ID 9324035, 25 pages, https://doi.org/10.1155/2017/9324035

[32] Citron R, Maxwell K, Woods E (2017) Smart city services market. Technical report, Navigant Research.

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

[34] Schaffers H, Komninos N, Pallot M, Trousse B, Nilsson M, Oliveira A (2011) Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. Springer, Berlin.

[35] Ghorbani AA, Lu W, Tavallaee M (2010) Network Intrusion Detection and Prevention, Advances in Information Security, vol. 47. Springer, US

[36] Anwar S, Mohamad Zain J, Zolkipli MF, Inayat Z, Khan S, Anthony B, Chang V (2017) From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. Algorithms 10(2):1–24

[37] A. Khraisat, I. Gondal, and P. Vamplew, An Anomaly Intrusion Detection System Using C5 Decision Tree Classifier. Springer International Publishing, 2018, p. 149–155.

[38] C. Kreibich and J. Crowcroft, “Honeycomb - creating intrusion detection signatures using honeypots,” Computer Communication Review, vol. 34, pp. 51–56, 01 2004.

[39] N. Provos, “A virtual honeypot framework,” in Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13, ser. SSYM’04. USA: USENIX Association, 2004, p. 1.

[40] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” Cybersecurity, vol. 2, no. 1, Jul 2019.

[41] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, “Intrusion detection system: A comprehensive review,” Journal of Network and Computer Applications, vol. 36, no. 1, p. 16–24, Jan 2013.

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

[43] S. Choudhary and N. Kesswani, “A survey,” International Journal of Information Security and Privacy, vol. 13, no. 1, p. 86–105, Jan 2019.

[44] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, “The impact of rank attack on network topology of routing protocol for low-power and lossy networks,” IEEE Sensors Journal, vol. 13, no. 10, p. 3685–3692, Oct 2013.

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

[46] Kumar S, Vealey T, Srivastava H (2016) Security in internet of things: Challenges, solutions and future directions. In: 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa. pp 5772–5781

[47] Abdelouahid Derhab , Arwa Aldweesh , Ahmed Z. Emam ,and Farrukh Aslam Khan, "Intrusion Detection System for Internet of Things Based on Temporal Convolution Neural Network and Efficient Feature Engineering," Hindawi, Wireless Communications and Mobile Computing, Volume 2020, Article ID 6689134, 16 pages, https://doi.org/10.1155/2020/6689134