

Review Article


A Security Based Perspective of Internet of Things

Shivlal Mewada^{1*}, Meghna Chandel², Pradeep Sharma³

¹Department of Computer Science, Govt. College Makdone, Ujjain – India

²Department of Computer Science, SGISTS, Indore – India

³Department of Computer Science, Govt. Holkar Science College, Indore - India

*Corresponding Author: 

Received: 12/Feb/2025, Accepted: 28/Mar/2025, Published: 30/Apr/2025. | DOI: <https://doi.org/10.26438/ijsrnsc.v13i2.275>



Copyright © 2025 by author(s). This is an Open Access article distributed under the terms of the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited & its authors credited.

Abstract- Information technology is offering many technologies to all of us and among such systems and technologies IoT, Big Data, Cloud Computing etc. are considered as important and vital. The advancement and escalated growth of the Internet of Things (IoT) has started to reform and reshape our lives by different sorts. The deployment of a large number of objects adhered to the internet has unlocked the vision of developing Digital Society and simply smart world around us, thereby paving a road towards automation and humongous data generation and collection. This intelligent Internet systems supported by the automation and continuous explosion of information to the digital world provides a healthy ground to the adversaries to perform numerous IT based Services and making our lives easy and it also helps in adhering cyber systems and information enriched society. The Security related aspects are important in emerging systems and here IoT based systems play a perfect role. Timely detection and prevention of such threats are pre-requisites to prevent serious consequences. Here in this work the survey conducted provides a brief insight into the technology with core attention to various attacks and anomalies including their detection based on the intelligent intrusion detection system(IDS). Further here comprehensive look-presented which provides an in-depth analysis as well as assessment of diverse machine learning and deep learning-based network intrusion detection system (NIDS). Moreover in this work aspects of healthcare in IoT is presented. This study also deals about the architecture, security, and privacy issues including their utilizations of learning paradigms in this sector. The research assessment here finally concluded by the listing of the results derived from the knowledge sources and literature. The paper also discusses numerous research challenges to allow further rectifications in the approaches to deal with unusual complications.

Keywords- Internet of Things(IoT), Cloud Computing, Machine learning, Deep learning, Intrusion Detection System, Wireless Sensor Network, Information Assurance.

1. Introduction

The rapid escalation in numerous technological aspects of wireless sensor networks (WSN), mobile communication, radio-frequency identification (RFID), and various lightweight protocols have endorsed the concept of the Internet of Things. The core conviction of IoT revolves around the dynamic interconnection of billions of different units or entities in an ecosystem driving either in a wired or a wireless fashion via the assistance of intelligent sensors, actuators, and other components. These components mesh with each other to yield the state of things and thus, providing extensive benefits and comforts to humans. Numbers stipulate that the IoT market has reached a mark of approximately 200

billion in 2020, starting with just 2 billion in 2006 [1]. The result of this automation has manifested the presence of smarter and intelligent objects, thus paving a way in all spheres: smart cities, healthcare, finance, manufacturing, academia, etc. The application of IoT with percentage implementation in diverse fields is depicted in Figure 1. IoT is, therefore, an amalgamation of diverse technologies at various layers coming up together to bestow the best of ubiquitous and pervasive computing to provide numerous benefits in different application areas.

Smart services have become an integral part of today's lifestyle. For example, disabled people could manage things with IoT assistance, specially-abled children could interact

using the Autism Glass, and remote health tracking aids in curing. Moreover, IoT sensors working with warning system alerts about environmental disasters. A lot many use-cases show the usefulness of IoT in managing natural resources too. With smart grids and smart meters, the daily power-consumption could be optimized and the supply-demand ratio could be efficiently maintained to meet the growing demands. Likewise, intelligent transportation systems provide valuable insights into different services. For example, on the basis of

real-time traffic conditions traffic signals consequentially set their timer to avoid traffic congestion and thus, environmental pollution. With smart agriculture, the crop yield could be predicted, fertilizers needed, disease-prone crop areas could be identified and isolated. Alongside these services, it brings deep-rooted security challenges as these IoT nodes are flooded to market with inherent vulnerabilities.

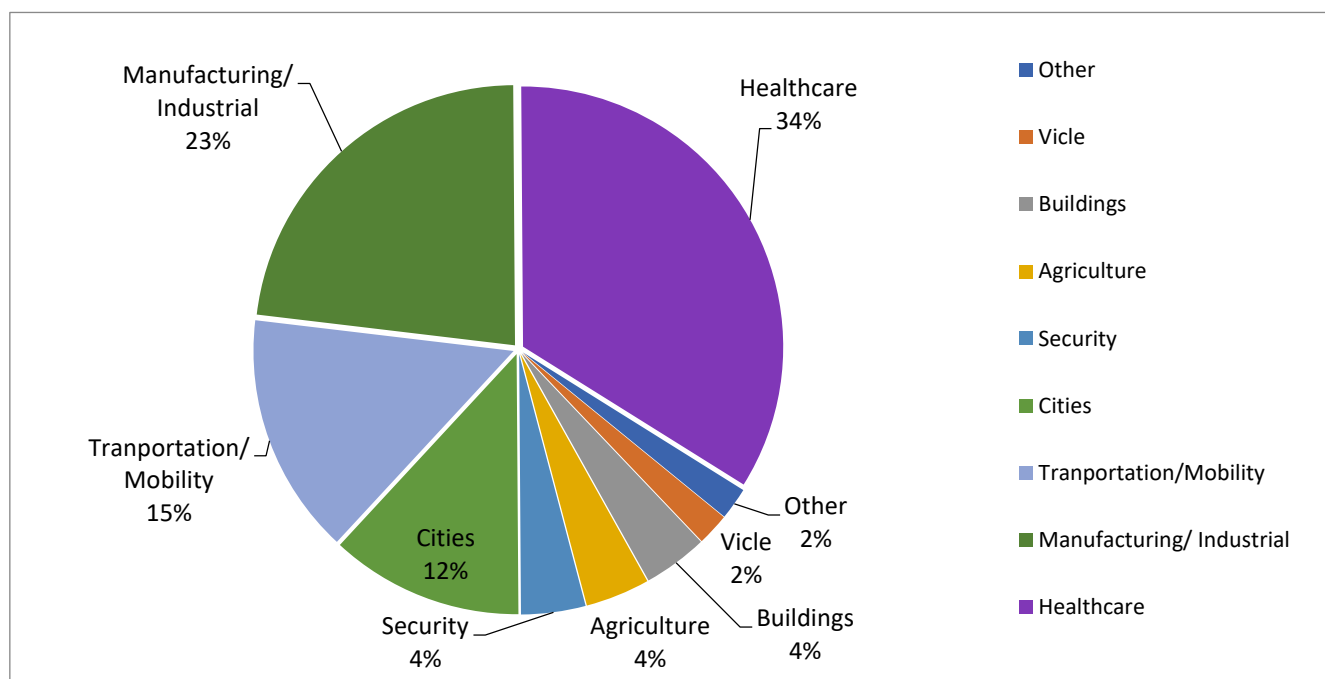


Figure 1: Applications of IoT in Different Sectors

The exponential growth and integration of IoT with other technologies have provided a bigger attack surface to play with. Moreover, it's challenging to maintain the security requirements of an IoT system due to the very nature of IoT nodes in terms of scarce resources and unattended environment. Employing existing security mechanisms such as encryption, authentication, and access control is also not a feasible solution for systems with a large no. of connected devices entertaining inherent vulnerabilities. Also, the end-users and developers are ignorant about the security risks complimenting the extensive smart applications. Their negligence could be apprehended from the IoT based cyber-attacks on Iran Nuclear System, German steel mill, Saudi Arabia oil plant, Dyn service provider, Hajime botnet, baby monitors, and security cameras. Furthermore, this negligence in securing IoT devices has been proven to be life-threatening. For example, the reconfiguration of the devices implanted in the human body compromised sensors in self-driving cars, and the ones used in mining activities. Now, these cyber-attacks like Stuxnet turned out to be another way of declining the economy of the developed

countries[energies]. Thus, the security challenges being an integral part of these useful IoT services must not be overlooked and should be handled at priority.

The learning methods are the appropriate tools for differentiating the 'usual' and 'unusual' behavior of IoT components and the way they interact with each other to provide services. The input to different components of an IoT system is analyzed to find the regular patterns of interaction, so as to recognize the malicious behavior in a system in the early stages. With learning methods (machine learning and deep learning) nascent zero-day attacks could also be predicted, as these are generally the mutations of foregoing attacks. Moreover, the unique features of deep learning such as automatic feature extraction, compression competencies, etc., make it more feasible for resource-constrained IoT systems. The wide acceptance of deep learning is all due to its ability to self-learning, faster processing, and accuracy. Consequently, IoT systems must have a transition from merely facilitating secure communication amongst devices to security-based intelligence enabled by DL/ML methods for effective and secure systems.

1.1 Scope of the survey

IoT plays a significant role in our lives by enabling the digitization of the physical world around us. A large number of surveys have been conducted to review and analyze the multiple IoT facets. Table 1 surmises the relative comparison of the proposed work with the considered state-of-the-art works. However, the study conducted in this paper provides a detailed, in-depth review of those facets/dimensions in an appropriate order. An exhaustive analysis of various research surveys is compiled together to convey an overall assessment, which has not taken place in the past. For example, Neshenko *et al.*[1] provides a unique taxonomy of numerous attacks and vulnerabilities occurring in IoT devices along with methodologies and security capabilities to counter those flaws. In addition, architectural vulnerabilities occurring in each respective layer are also represented diagrammatically. Furthermore, an appropriate assessment is provided in multiple sections to deliver the essence of the problems occurring due to the coupled nature of IoT devices. Also, Butunet *et al.*[2] has shed light on the integration of WSN with IoT and laid stress on the possible attack avenues available generated.

Divyakmika *et al.*[3] analyzed the application of ML in IoT security by proposing two-tier NIDS. The approach is based on TCP/IP data packet features obtained from NSL-KDD DATASET. It clustered the data into two (normal and new patterns). The classification was done using KNN, MLP, and reinforcement learning. A similar approach is presented by Pajouh *et al.*[4] to develop an intrusion detection model by collaborating Naïve Bayes and KNN. The challenge of upgrading the mechanism to extend the model to the higher layers is also highlighted. To overcome the problem of availability of the dataset Canedo *et al.*[5] constructed a testbed to monitor the application of artificial neural networks in attack detection in the IoT sites. However, to generate better analysis, an upgraded testbed with a large number of sensors and devices is required. To construct a real-world attack scenario, Anthi *et al.*[6] have proposed novel real-time IDS named pulse, which deploys supervised ML for the identification of maleficent activities like scanning, probing, and other elementary forms of DOS attacks. An IoT smart home testbed was created that comprised of a range of commercially relevant and representative IoT hardware. Such devices included a TP-Link NC200 IP camera, the Hive, which was connected to two sensors; a motion sensor and a window/door sensor, a TP-Link Smart Plug, an Apple TV, an HP wireless printer, and an Amazon echo. Ten-fold cross-validation was performed in which the Naïve Bayes technique gave the most promising results. The main drawback was the employment of a limited number of attacks. Further, Hasan *et al.*[7] compared and contrasted the application of multiple

ML algorithms in a real-time virtual IoT scenario to further substantiate the research.

Contemporary improvisation includes the application of deep models in IoT. Rahul *et al.*[8] analyzed the application of various deep models to detect multiple network attacks. KDD cup 99 was used for the purpose of training the network. However, a lack of real-time IoT datasets and evaluation of deeper networks still posed a challenge. To overcome this Roopak *et al.*[9] explored the capabilities of the deeper networks by training models like 1D-CNN, RNN, LSTM, and a hybrid model of CNN+LSTM on the CICIDS2017 dataset. Furthermore, from the considered start-of-the-art we have found that only a few works have explicitly focused on both machine learning and deep learning-based solutions for securing IoT in an elaborated manner. Thus, in this manuscript, we aimed the same. The inherent vulnerabilities in IoT devices and IoT environments (communication protocols) have also been explored as being the root cause of these emerging attacks in smart applications.

1.2 Contributions

The key contributions of this paper areas follows:

- A taxonomy that focuses on attacks, vulnerabilities, and anomalies in IoT has been given.
- The benefits of the growing usage of machine learning and deep learning techniques for securing IoT are highlighted. And a critical analysis of different learning techniques has also been presented.
- A case study on the usage of IoT and learning methods in Smart Healthcare has been presented.
- Finally, research challenges and future recommendations for the end-users have been given to ensure secure IoT infrastructure.

1.3 Methods and materials

The methodical approach has been adopted to conduct this study in a proper way with the goal of providing in-depth analysis of different learning methods used to secure the IoT system in one way or the other, as security in IoT questions its sustenance. The related research articles, blogs, use-cases, tutorial papers, reports, and white papers have been discovered to conduct this review. The quality checks are applied to the extracted data to get the reliable material for the proposed survey. The ones from the SCI journals and with a good number of citations are commonly chosen. This work primarily focused on the state-of-the-art research on IoT attacks, threats, anomalies, vulnerabilities, and learning-based approaches to handle them in general and with respect to smart healthcare specifically. Also, to emphasize the

current research challenges, open issues, and future scope related to the same. The peer-reviewed and high-quality database journals and reputed conferences like *IEEEExplore*, *Springer*, *Mdpi*, *Wiley*, *ACM*, *Elsevier*, and *Google Scholar*, are investigated to get the relevant research articles. For searching, the vital keywords like IoT, security, attacks,

vulnerabilities, threats, machine learning, deep learning, smart healthcare, etc., have been benefitted. The authors have analyzed and discussed the significance of related works in the field explored in the proposed survey.

Table 1: A relative comparison of the proposed work with state-of-the-art works.

Author(s)	Year	Discussion	Challenge(s)	1	2	3	4	5
Divyatmikaet al.	2016	Analyzed the application of machine learning in intrusion detection.	The analysis is required for the implementation of the approach at the application layer.	✓	✓	×	×	✓
J. Canedoet al.	2016	Focussed on the application of ANN to detect anomalies in the edge devices.	Generating data entries by creating a testbed with more devices and sensors.	×	×	×	×	✓
Alaba et al.	2017	Discussed multiple security scenarios, and possible countermeasures.	To develop lightweight authentication schemes for IoT environments.	✓	×	✓	×	×
E. Anthiet al.	2018	Discussed the application of a novel IDS model named pulse for the identification of Dos attacks.	No clustering of similar devices, limited attacks covered.	×	×	✓	×	✓
Rahul et al.	2018	Discussed the application of deep models as IDS to detect attacks of varying complexity.	Lack of real-time IoT dataset, evaluation of deeper networks.	✓	✓	✓	×	×
A Diroet al.	2018	Provides a comparison of machine learning and deep learning models for attack detection.	Testing of the mentioned technique on a different dataset.	✓	✓	✓	×	×
I.Butunet al.	2019	Analyzed the application of WSN in IoT. In addition, an in-depth review of various attacks constituting WSN in IoT.	A better Approach/ standard for the routing, trust management, and schemes for data collection for the multiple IoT layers.	×	×	✓	×	×
N.Neshenkoet al.	2019	Provides a detailed analysis of IoT along with its various facets. Also, a taxonomy constituting various attacks,vulnerabilities, and methodologies to monitor them are also discussed.	More detailed investigation to provide prompt remediation for detecting malicious IoT devices.	×	×	✓	✓	×
Pajouhet al.	2019	Focussed on the application of machine learning techniques (Naïve Bayes and K nearest neighbor) to detect malicious activities.	To perform anomaly and intrusion detection at the application and support layer, considering different protocols of the network layer.	✓	✓	✓	×	✓
M Hasan et al.	2019	Provides a detailed framework for attack and anomaly detection in IoT using machine learning.	More robust algorithms are required; more inspection is required for framework creation; more attention is required for real-time detection.	✓	✓	✓	×	✓
M Roopaket al.	2019	Focussed on the detection of DDoS attacks using deep models along with numerous other challenges in their application.	Lack of Deep learning models that can work with highly unbalanced datasets.	✓	✓	×	×	×
Anand et al.	2020	IoT vulnerabilities and their assessment techniques, with a case study on Sustainable Smart Agriculture.	Lack of intelligent vulnerability assessment technique.	✓	×	✓	✓	✓
Yazdinejadet al.	2020	Applying blockchain in IoT for secure data transmission and access control.	Comparative analysis with other such architectures.	×	×	✓	✓	×
The Proposed one	2021	Machine learning and deep learning-based IoT security mechanisms with comparative analysis.	Hybrid learning-based techniques will be explored.	✓	✓	✓	✓	✓

Note: 1, Architecture; 2, Dataset; 3, Attacks; 4, Vulnerabilities; 5, Machine learning based IoT

1.4 Organization

In Section 1 we present an introduction to IoT and its services, several security issues and attacks, and how ML/DL methods can be the conceivable solution. Section 2 provides a general perspective to the technology and its applications followed by background information, which prominently includes its prime driving technologies, architectural view, and protocol suite. Section 3 introduces security-related concepts by highlighting imminent attacks, anomalies, and vulnerabilities in this area with a brief introduction to the IDS mechanism. The next section presents ML and DL based IDS solutions to deal with the security intricacies mentioned in the previous section, followed by a case study to understand the practical implementation of IoT in the healthcare sector along with research challenges, open issues, and future scope.

2. Background and preliminaries

This section focuses on the background and importance of security in IoT. This section is bifurcated into three subsections. Firstly, we cover IoT driving technologies which include RFID, sensors, wireless sensor networks, communication, cloud computing, and embedded systems. Secondly, we briefly discuss the IoT ecosystem, followed by the IoT architecture with protocol suite in the subsequent subsection

2.1 IoT Driving Technologies

IoT systems consist of various technological/functional components to lubricate the task of sensing, identification, communication, analysis, and management. Colakovic *et al.* [4] have detailed the vision towards IoT along with various technologies used at different levels. Besides, the survey conducted in [1][5] also introduces these technologies.

- *RFID (radio-frequency identification) Technology*: It is a technology used for the identification of a person or any other object by exercising the wireless radio frequency technology in the network. It utilizes the labels/tags on the objects for identification. It is a combination of e-labels, an integrated circuit for processing information by modulating and demodulating the signals along with a reader-writer system [6]. Jia *et al.* [7] have presented detailed interpretation and applications of RFID in IoT.
- *Sensor Technology*: It is responsible for interacting with the physical environment and subsequently detecting, observing, storing, and providing the necessary information by converting it into a human-readable form. The primary purpose is to interpret the real world conditions by monitoring the documentation collected in the form of sound, light, humidity, pressure, and many other values for analysis of various surrounding

scenarios [8]. These, therefore, bridge the gap between the physical and the digital world.

- *Wireless Sensor Network Technology*: It is an integration of numerous self-configurable devices with embedded sensors for scanning and documenting the conditions of the physical environment and subsequently forwarding them to the appropriate sink node for analysis [9]. Actuators can also be a part of WSN in certain conditions; hence they are often referred to as wireless sensor and actuator networks. The various applications of WSN include weather monitoring systems in which nodes collect temperature, humidity, and other data, soil moisture monitoring system, health monitoring system, etc.
- *Network Communication Technology*: For the communication between various sensor technologies, numerous short-distance communication strategies are available like Bluetooth, RFID, Zigbee, Wifi. Each one has its pros and cons, and further subsequent selection depends on the application scenario.
- *Embedded System Technology*: These are a blend of numerous peripheral hardware (Sensors, Actuators) combined with software running or embedded OS (Real-time operating system) to accomplish some specific tasks. Principal components include microcontrollers, memory, network units, etc. running on an embedded operating system such as (RTOS) with critical features like real-time computing, low maintenance, and low power consumption [10].
- *Cloud Computing*: It is an essential IoT component provisioning the users with processing and storage capabilities on demand. It is used as a powerful tool in IoT to handle the big-data and, in turn, rendering intelligent monitoring and decision making in various applications, thus turning them smart. The prime benefits are elasticity, agility with less deployment time [11].

2.2 IoT Ecosystem

The technologies mentioned above provide a hazy overview of the IoT. To get a crisp and unclouded perspective, understanding IoT architecture is extremely vital before proceeding into the intricate details of the various facets of it. It is hugely challenging to standardize one architecture for IoT due to its inability to capture a particular image characterizing it due to vast expansion and variation in this sector. There are miscellaneous three, four, five, and seven-layer architecture, which are accepted by various professionals to have a visual sculpture of this technology. Table 2 describes some of the prominent IoT architectures. Figure 3 Depicts the general three-layer architecture [12][13] with its extension into five layers [14][15].

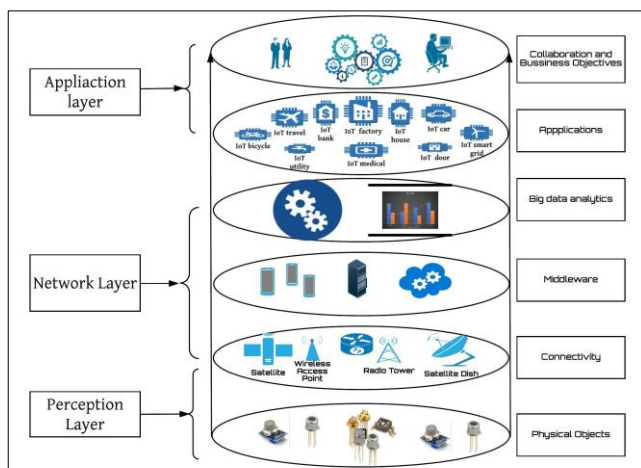
Figure 2: Basic IoT Architecture.

Table2: Prominent IoT architectures.

Author	Description
Bauer <i>et al.</i> [16]	IoT-A. An amalgamation of different IoT perspectives.
Atzori <i>et al.</i> [17]	The author has presented a SocialIoT-architecture based on the integration of IoT with the social networking concept.
Qin <i>et al.</i> [18]	The author presents SDN-based architecture for provisioning IoT with better quality-of-service, deployment, scalability, and context awareness.
Li <i>et al.</i> [19]	Mobility first mainly addresses the challenges concerning the usage of mobile phones as gateways and dealing with the security aspect of sensor data.
Singh <i>et al.</i> [20]	JDL(joint director of labs) based model for IoT architecture with the combination of semantic layer.
Cecchinel <i>et al.</i> [21]	Software architecture for collection of sensor-based data with cloud-based storage(sensor, sensor board, bridges, middleware)
Kraijak <i>et al.</i> [22]	5-layer architecture(perception, network, middleware, application, business)
Ray <i>et al.</i> [23]	It describes major IoT functional elements with multiple IoT architectures in different application areas.

2.3 The Prominent IoT layers

The two most prevalent architectures IoT-A (internet of things-Architecture) and IIRA (industrial internet reference architecture) synchronized with the IoT community and incorporating multiple views are given in [24]. In concern to IoT, many different wired and wireless protocols are introduced despite the similarity towards the general TCP/IP stack, primarily because of the differences in the characteristics of IoT devices with regard to memory and computational power. Priyadarshi *et al.*[25] and Sahrawi *et al.*[26] provides a detailed analysis of various IoT protocols. The prominent IoT layers with working protocols are briefly described subsequently.



Perception Layer: It is also referred to as the physical layer in IoT. It is an amalgamation of a wide variety of sensors, actuators, and devices mainly for the purpose of data accumulation from the surroundings [27]. The primary objective is to acquire all the essential insights for more in-depth analysis in the succeeding. The connected objects should not only establish communication with their respective gateways but also must be able to recognize and talk to each other to merge in real-time to leverage the benefits of the technology. Lightweight M2M(machine to machine) has become a standard for low memory, lightweight devices that typically find an application in IoT[28].

Network Layer: The main goal of the network layer is to establish communication amongst smart devices via the assistance of appropriate IoT protocols. The prime purpose is to transfer data to proper edge infrastructures or cloud-based platforms through intermediaries like gateways or any other data collection systems. Another important aspect here is security. Appropriate security tools like NIDS or any other form of encryption can be applied to reduce the risks of threats and attacks.

Support Layer: It consists of cloud-based applications with prime tasks of storing, processing, and analyzing the data. It is mainly referred to as the brain in the IoT body. The main challenges faced here are restricted access and slow data transfer rate, which ultimately leads to late response. These challenges necessitate the need for appropriate edge analytics for quicker replies[28].

Application Layer(AL): AL is responsible for the dispatching of the required services to the end-users via the assistance of appropriate audio and video interfaces.

The application layer is responsible for providing services and determines a set of protocols for message passing at the application level

3. IoT Security Landscape

Security is a crucial zone of this technology, as recent trends and surveys have captured numerous changes in this sector, which in turn, indicates the evolution of the attacking mechanism leading to the generation of several zero-day attacks[29]. This behavior is mainly because most vendors are only concerned about dealing with some aspects of the IoT ecosystem. Those involve mostly providing new functionality to get their products into the market and thereby ignoring the privacy and security risks associated, thus making them easy targets of the hackers. The past few years have already recorded some damaging effects of lack of security in IoT in the form of attacks like Mirai botnet attack, Bashlite attack, and many more. Attackers are not only inaugurating

numerous scanning, probing, and flooding attacks but are also escalating malware in the form of worms, viruses, and spams to exploit the weaknesses of the existing software, thereby causing severe damage to the sensitive information of the users. Therefore proper detection and prevention of such threats are very vital. IDS provides a platform to deal with

such issues. Table 3 and Table 4 provides a brief insight into various such attacks and anomalies at different IoT levels and layers[30][31][32]. Adversaries primarily try to detour the security framework with subsequent launching of zero-day attacks, which in turn reduce the network throughput and produces huge discomforts to the legitimate users.

Table3: Attacks in IoT.

Nature of attack	Description	Classification
Active attacks	These are performed mainly to carry out malicious acts against the system, thus affecting or disrupting the services for legitimate users. They hamper both confidentiality and integrity of the system.	Dos(denial-of-service),DDOS(distributed denial of service), MITH(man-in-the-middle), Interruption, Alteration[33].
Passive attacks	These are performed mainly for gathering useful information without getting sensed, i.e., they do not disturb the communication.	Monitoring, Traffic Analysis, Eavesdropping, Node destruction/malfunction[34].
Physical layer attacks	These attacks try to tamper and exploit the devices making them the most vulnerable terminal of IoT.	Node tampering, Jamming, Replication[35].
Datalink layer attacks	These undertake the advantage of mac schemes to launch different attacks.	Collision, Dos, ARP spoofing, unfairness.
Network layer attacks	These attacks try to disrupt the communication between the source and the destination by playing with the packets.	Dos, Routing Attack, Sybil Attack, blackhole, spoofing, alteration.
Privacy threats	The capabilities of IoT allows it to launch acute attacks targetting the privacy of users.	Identification, profiling, tracking, linkage, inventory[15].
Software-based attacks	These attacks make use of third party software to gain access to the system and cause destruction.	Virus, Trojan horse, Worms.
Side-channel attacks	These are hardware-based attack that uncovers the secret information like cryptographic keys to exploit the device.	Timing Analysis, Power Analysis.
Botnet attacks	These are a collection of infected devices(zombies) like printers, cameras, sensors, and similar smart devices, which launch large-scale DDOS attacks to compromise other intelligent devices. The principal components are command and control servers, along with the bots.	Mirai, Hydra, Bashlite, lua-bot, Aidra[36].
Protocol-based attacks	The attacks work against the connectivity protocols of IoT.	RFID-based(replay, tracking, killing tag) Bluetooth based (bluesnarfing, bluejacking, Dos), Zigbee Based(sniffing, replay, ZED sabotage attack)[37].

Table4: Anomalies in IoT.

Type	Description
Point Anomaly	It is the most basic type of anomaly. One data point is abnormal in comparison to the rest of the data points.
Contextual Anomaly	It is a sophisticated type anomaly type where a data point is considered unusual in a specific context. E.g., if any system accesses services at a particular time and if there is a sudden change in the background, i.e., time changes, it is considered abnormal.
Collective anomaly	Data points are anomalous w.r.t to the whole dataset or the entire services but not by themselves individually.

3.1 IoT Security Analysis

The listing of various attacks and anomalies prescribes the difficulties in the construction of a secure smart network. The prime goal is to safeguard the security requirements (integrity, confidentiality, availability) of the legitimate users. Figure 3 depicts the various security requirements to be considered in the security perspective of IoT. Various researchers have carried out a rigorous survey to list down all possible attacks, their nature, challenges, and countermeasures to deal with them.

Sadique *et al.* [38] have highlighted the critical future security challenges in IoT and open issues w.r.t the various IoT layers. Also, Riahi *et al.* [39] have presented a roadmap to IoT security by representing a systemic approach to it by discussing its every aspect, beginning from persons/nodes to the ecosystem to managing privacy, trust, responsibility in the technology via the assistance of a smart manufacturing case study. Mardiana Binti *et al.* [40] have discussed all recent trends in IoT security from 2016 to 2018. Also, a layer-wise security approach in IoT with all possible attacks, tools, and simulators are discussed.

Gudtmenko *et al.* [41] present a list of various critical challenges in IoT, required to be addressed to maintain security in this area. Whitter *et al.* [42] have presented a research paper that primarily focuses on the various historical attacks and malevolent activities that happened against the IoT networks. Also, the solutions to deal with them and possible areas for future developments are mentioned.

Benzarti *et al.* [43] have presented a taxonomy of attacks against IoT by categorizing them into six classes based on architecture, attributes of security (integrity, authentication, confidentiality), communication disturbance, faulty or corrupted packets, channel, device functionalities. Also, the solutions to various existing attacks in different IoT applications like smart grid, smart home, VANET (vehicular ad-hoc networks) are discussed. Also, the survey conducted in [44][45][46] provides different IoT attack taxonomies and countermeasures to deal with it.

3.2 IoT Vulnerabilities

Vulnerabilities, in general, refer to the weaknesses of a system that can be overburdened by the adversaries to perform unintended activities. In IoT, hackers can exploit the integrity, confidentiality, availability of services to legitimate users by taking advantage of such teething problems. Therefore an understanding of such delicacy in the system becomes mandatory before the development of appropriate defense mechanisms. The authors have presented a multidimensional view of the IoT vulnerabilities with a detailed explanation of their effects on the diverse security paradigms [47]. OWASP (Open web application security project) has also listed the top ten IoT vulnerabilities [48].

Figure 4 explains the prime categorization of various IoT vulnerabilities.

- **Device Security:** This aspect of security surface primarily includes physical damage to the IoT devices mainly caused by unauthorized access to them. The foremost reason is that these devices are in open territory, thus wholly left at the disposal of nature and adversaries. Therefore, they can be easily get damaged, or hackers can clone the firmware to produce their malicious counterpart and can also manipulate the data. Typical examples include the cloning of radio frequency signals in electric cars to unlock them or gaining access to the controller area network bus of the vehicle to execute any damaging activity. In the medical field, attackers can gain control over external devices like insulin pumps or cardiovascular objects to play with the health of people [49].
- **Insecure Booting:** Lack of proper verification before the implementation of the device refers to insecure booting. This aspect is an essential requirement in terms of maintaining security because it provides a comfortable surface for attackers to launch their malicious activities by injecting the devices before their launch [50].
- **Network-Based Vulnerabilities:** These typically target the connectivity of IoT devices, thus making them susceptible to a large number of attacks. These typically include the insecure services within the devices themselves, lack of proper authentication and encryption, i.e., using default or weak passwords, and deploying encryption techniques that do not match the standards of lightweight cryptography in IoT, thereby hampering the security. Research work related to authentication and encryption is provided in [51][52] and [53][54][55] respectively.

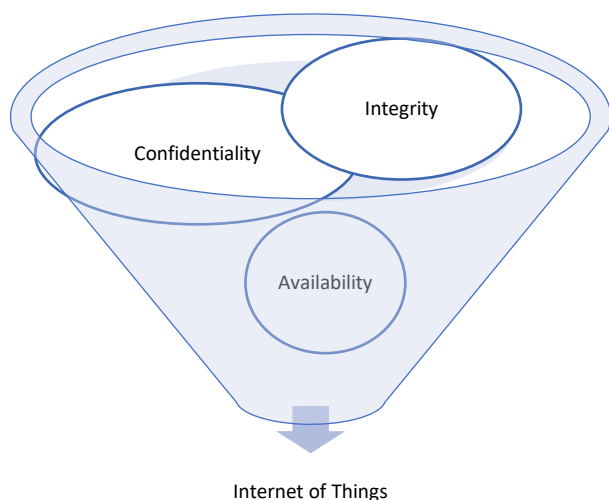


Figure 3: Security Requirement in IoT based Systems.

- **Open Ports:** The presence of open ports is a significant threat to the IoT devices because they can expose the existence of smart devices in the surroundings, thus providing a platform to adversaries to conduct mischievous activities. Sivanathan *et al.*[56] have explained the use of SYN and TCP scans to discover IoT devices at the disposal of open ports. Further, Markowsky *et al.*[57] have described the usage of dark web SHODAN [58], Masscan, and NMAP to find and connect to vulnerable devices in the network.
- **Software-Based Vulnerabilities:** These typically include the usage of readily available, guessable, and default passwords, also in addition to this, not performing suitable software updates/patch updates or using deprecated or outdated software libraries or components. All these factors together increase the vulnerability of the entire system [59] explains the attacks launched due to firmware modification. Further, deliberately following weak programming practices, i.e., launching firmware with well-known vulnerabilities, aids hackers to perform their dark activities.
- **Insufficient Privacy:** This means compromising user's personnel information without seeking their permission because of current default settings that often restricts users from altering the configurations.
- **Insufficient Audit Mechanism:** Lack of sufficient logging mechanism lead to such vulnerabilities. The research survey in [60][61] provides some insights towards audit mechanisms in IoT. Figure 5 depicts the most vulnerable IoT devices by 2020.

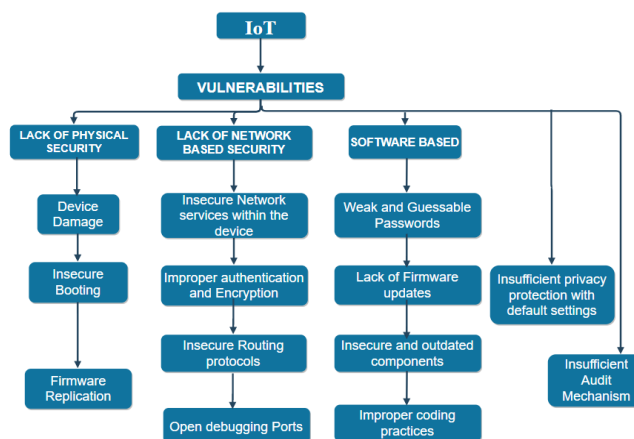


Figure 4: Vulnerabilities in IoT.

The devices, mainly security cameras, virtual assistants, smart TVs, and smart lights, have proved to be the most vulnerable towards the adversaries. These devices can be easily hijacked to perform both active and passive attacks. In the case of security cameras, mainly, the fault lies at the purchase corner of these. Buying cheap models can open doors for hackers. Similarly, in the case of home assistants, eavesdropping may be a carrier of your activities to the adversary. Also, remote access to various devices can be undertaken to perform all kinds of mischief[62].

3.3 Intrusion Detection System

Several countermeasures are proposed to deal with the wide variety of attack scenarios in IoT. These vary from better authentication, device identification to introducing lightweight encryption to several others like adding risk assessment models, and intrusion detection at higher layers of IoT. In this survey, we have particularly narrowed our research to IDS based attack and anomaly detection. It is defined as an appropriate ensemble of various tools, techniques, and methods required to detect unintentional activities of the hackers.

Figure 5 provides a view of the multiple properties of IDS like its occurrence, placement, recognition strategy, and usage frequency, the knowledge of which is essential for its proper implementation to achieve the desired results. The properties are described in terms of whether they are host-based or network-based, i.e., deals with attacks and anomalies launched against the entire network by analyzing all the incoming packets in the system. Snort, Suricata, Zeek are some of the examples of NIDS, or they can be hybrid, i.e., composed of both HIDS and NIDS. It is referred to as the network monitoring stage of IDS, which is followed by analysis. Finally, the detection stage, which is again categorized into misuse based, anomaly-based, or can be policy-based [63][64]. There are several IDS techniques based on data mining, ML, statistical model, payload model, rule-based, but due to the massive data generation in IoT, ML can be thought of as a suitable paradigm to provide

intelligence in this area. It can leverage the vast data generated by IoT devices for training to create patterns and behavior to make appropriate predictions and assessments. Thus IDS based on ML-based learning approaches can prove to be an excellent tool for attack detection in a smart IoT environment.

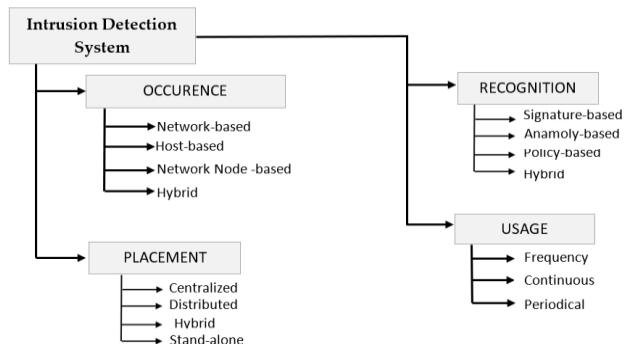


Figure 5: Intrusion Detection System.

4. Learning -based solutions for Securing IoT

The vulnerabilities, attacks, and anomalies mentioned in the previous section have already focused on the broad range of concerns popped-up due to the expansion of IoT. Also, the advances in big data and computing power have further surfaced the platform for carrying out unintentional activities by the adversaries. However, ML-based specialists identify learning approaches as a productive tool to deal with IoT based security issues, thereby leading to the amalgamation of ML and DL approaches with IDS technology. Figure 6 depicts a classification of existing learning techniques. In this section, we will mainly focus on various learning approaches, their types, and multiple solutions for IoT security based on these approaches. Existing methods can be classified based on the mode and the approach used. Figure 8 provides a visual sculpture of these.

- **Based on the mode-** There are two modes: offline and online. In offline mode, the input is processed in batches and is known as lambda learning, whereas in online mode, the data is processed piece by piece serially and is known as kappa learning.
- **Based on the approach-** There are three approaches: supervised, unsupervised, and reinforcement.

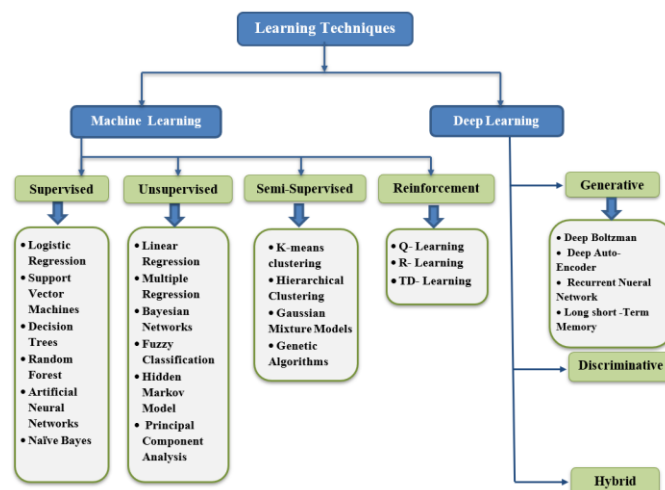


Figure 6: Various Learning approaches.

Supervised Learning: It is a procedure of learning the functionality from the training dataset. The prime goal is the estimation of the mapping function to predict the correct output labels for the prescribed new data. Based on the essence of target labels, it can be classified into classification and regression. The technique is enormously useful in fault detection and misuse based intrusion detection, quality of service, event detection, etc. The prime prerequisite in implementing supervised ML algorithms in IoT is the availability of the dataset with signatures for known attacks for the learning purpose. There are various supervised learning approaches like Knn[65], Decision tree[66], SVM[67], Naïve Bayes[68], ANN[69] utilized for attack detection in IoT. Despite high detection statistics, lack of detection of different attack footprints, more resource consumption limits their usage in the era of numerous Zero-Day attacks.

Unsupervised Learning: It is very useful in modeling the elementary or the concealed structure of the data due to the non-availability of the labeled dataset. The unavailability of the labeled dataset differentiates it from the supervised approach, thus promotes a comprehensive evaluation of the data. It is majorly bifurcated into three sections, namely clustering[70], dimensionality reduction[71], and density estimation. Hence, these approaches are instrumental in detecting outliers and novel anomalies. Also, Dimensionality reduction techniques like PCA helps in eliminating the features which have no contribution to class separability.

Reinforcement Learning: The technique is concerned with the application of appropriate actions taken by the software agents in an environment to maximize the cumulative reward. More generally, it can be a catchphrase as learning from the environment. Two principal methods of reinforcement learning include policy search and value function approximation. The primary classification includes Q-learning, TD-learning, and R-learning. The mentioned ML classification techniques with their pros and cons indicate that there is no particular algorithm that is applicable in all the

situations. Also, the increase in the number of IoT devices and the continuous evolution of zero-day attacks have urged the researchers to come up with Ensemble, hybrid, and other fused models to overcome the pros and cons of individual classifiers. Figure 7 depicts various learning models of machine learning.

4.1 ML-Based solutions for IoT security

Arthur Samuel coined the term "Machine Learning" in 1959 and defined it as "a field of study that gives computers the ability to learn without being explicitly programmed [57]. It is used to comprehend a model defining the particular behavior or characteristic and then subsequently utilizing it to predict the traits in seen or unseen instances. The flexibility, adaptability, and low CPU load of ML algorithms can help us build numerous analytical models with better accuracy and reduced false alarm rates for attack and anomaly detection. Further, understanding of various ML approaches is a prerequisite to understanding their suitability towards various attacks and anomalies. Table 5 summarizes the different machine learning-based solutions to secure IoT systems against the growing attacks.

Anthi *et al.*[72] have proposed novel real-time IDS named pulse, which deploys supervised ML for the identification of maleficent activities like scanning, probing, and other elementary forms of DOS attacks. An IoT smart home testbed was created that comprised of a range of commercially relevant and representative IoT hardware. Such devices included a TP-Link NC200 IP camera, the Hive, which was connected to two sensors; a motion sensor and a window/door sensor, a TP-Link Smart Plug, an Apple TV, an HP wireless printer, and an Amazon echo. Additionally, on the same network, there were connected two traditional IT devices. One of them consistently recorded the network traffic and saved the log files for executing the model on a realistic IoT environment for four consecutive days. After which ten-fold cross-validation was performed in which the Naïve Bayes technique gave the most promising results.

Divyakhmika *et al.*[73] have proposed a two-tier NIDS using machine learning techniques. The approach is based on TCP/IP data packet features obtained from NSL-KDD DATASET. The research commenced by preprocessing the data in wekas. The preprocessing was followed by the construction of an autonomous model based on hierarchical agglomerative clustering. It clustered the data into two(normal and new patterns). After this, the data were classified using KNN, MLP, and reinforcement learning. A similar approach is presented by Pajouh *et al.*[74]. They have introduced a state-of-the-art technique for subsequent detection and classification of malignant activities like the user to root and remote to local attacks by acquainting the

readers with TDTC(two-layer dimension reduction and two-tier classification module) model. As the name indicates, there is an employment of two-dimensionality reduction and two classifiers on the NSL-KDD dataset. Both PCA and LDA are employed to reduce the computational complexity, then succeeding forward by the application of Naïve Bayes and CF-KNN along with the KD tree to present a more efficient classification.

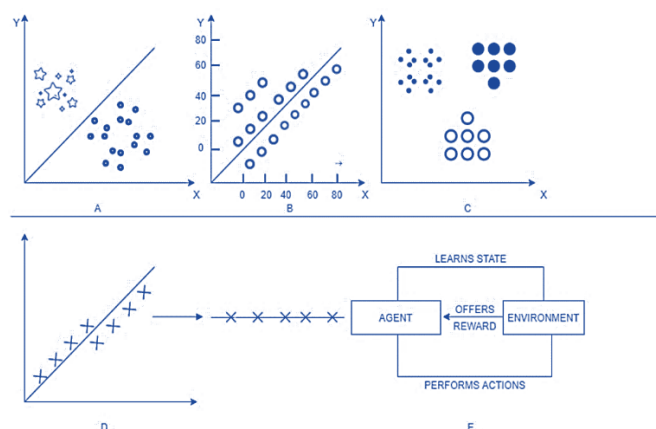


Figure 7: A. classification B. Regression C. clustering D. Dimensionality reduction E. Reinforcement.

Shahid *et al.*[75] have presented a smart home monitoring system to generate legitimate traffic data. Data generation is followed by implementing classification algorithms for device recognition to ensure proper. The malicious traffic can be created offline by deliberately attacking the device or by using IoT honey-pots. Six machine learning algorithms were deployed, followed by a comparison of their accuracies in which Random Forest outperformed by achieving an accuracy rate of 99.9%. Srinivasan *et al.*[76] have leveraged the power of machine learning techniques like random forest, support vector machine, MLP(multilayer perceptron) to ease the recognition and localization of link faults in the highly sophisticated network like IoT. A three-stage passive approach using the machine layer technique was adopted by experimenting with a mininet platform with two small networks and one inter route network.

Moustafa *et al.*[77] have proposed an Adaboost ensemble model using three techniques of machine learning, i.e., Decision tree, Naïve Bayes, ANN, to detect malevolent activities, particularly attacks in the network by using features of DNS, HTTP protocols in TCP/IP models. It is a three-step framework initialized by feature extraction by using Tcpdump, Bro-ids, and other extractor module followed by generation of data-sources from UNSW-NB15 and NIFS dataset and simulated IoT traffic. In this paper, Canedo *et al.*[78] have conducted suitable experimentation to generate their own synthetic data to inspect and carefully scrutinize the usage of ANN(Artificial neural networks) in IoT gateway

devices present in the transport layer to work at the security aspects of the technique. Ioannou *et al.*[79] presented an ML approach known as a support vector machine for the detection of malicious activities within the IoT network. A key feature of their work was the use of actual IoT traffic with specific network layer attacks such as blackhole, selective forward, etc. conducted by them.

Zhao *et al.*[80] have proposed a novel framework for real-time intrusion detection for numerous attacks and other suspicious activities occurring at the network layer using online machine learning. The structure consists of a dimensionality reduction approach, i.e., PCA followed by classifiers, KNN (K nearest neighbor), and softmax regression, which were applied and compared against each other using a benchmark KDD cup 99 data set. Both ML classifiers evinced

similar accuracy level, but softmax regression came up with more excellent time performance

Prabavathy *et al.*[81] have presented an online sequential extreme learning machine model for intelligent detection of attacks at the fog nodes to provide a faster, scalable, and flexible interpretation of benign and adversarial traffic coming from the IoT application. Hasan *et al.*[82] have compared the anomaly detection mechanism of various ML techniques (LR, SVM, DT, RF ANN) in a virtual environment producing synthetic data. The dataset DS2OS is publicly available at Kaggle. The dataset has 357952 samples and 13 features. Data preprocessing is performed by performing tasks like cleaning missing data, converting categorical data into numeric using encoders succeeded by application of the techniques on the dataset, and comparing their performances in which random forest outperformed with 99.4% accuracy.

Table 5: Tabular Representation Of Machine Learning Approaches.

Author	Dataset used	Algorithm with implementation platform	Threats	Challenges	Performance evaluation
Anthiet <i>al.</i> [72]	Dataset generated by creating a smart home testbed	Naïve-Bayes Platform: Weka	Network probing, scanning, Dos attacks- SYN, UDP flood attacks.	No clustering of similar devices, limited attacks covered.	scan attack: precision-97.7, recall-97.7, f-measure-97.7 SYN: precision-80.8, recall-68.8, f-measure-65.8
Divyatmika <i>et al.</i> [73]	NSL-KDD	Clustering+ KNN (data classification) + MLP (misuse detection)+reinforcement (anomaly detection) Platform: Weka	Dos, probe, Remote-to-local (R2L), User-To-Root (U2R).	-	Accuracy: 99.95% (with reduced false alarms).
Pajouhet <i>al.</i> [74]	NSL-KDD	PCA+LDA (Feature selection), naïve bayes+CF-KNN (classification)	Dos, probe, Remote-to-local (R2L), User-To-Root (U2R)	Anomaly and intrusion detection at the application and support layer, considering different protocols of the network layer.	Accuracy: Probe Attack: 87.32, Dos Attack: 88.20, U2R-70.15, R2L-42 Detection rate: 84.86, False alarm rate-4.86
Shahid <i>et al.</i> [75]	Dataset generated by creating a testbed.	Random forest, Decision tree, ANN, KNN, GNB (Gaussian Naïve Bayes)	-	Integration of anomaly detection models with a software-defined networking environment.	Accuracy: RF-99.9%, DT-99.5%, SVM-99.3%, KNN-98.9%, ANN-98.6%, GNB-91.6% Accuracy: 97%
Srinivasan <i>et al.</i> [76]	Two random networks	Random forest, MLP, SVM Platform: mininet	Link fault identification.	Testing different ML algorithms.	
[83]	UNSW-NB15, NIMS	Ensemble model (Decision tree + Naïve Bayes + ANN) Platforms and tools: NodeRed middleware, tcpdump, Bro-IDS,	Analysis, backdoor, dos, exploit, fuzzers, generic, Reconnaissance, worms.	Considering other IoT protocols, concentrating on one zero-day attacks.	Accuracy with DNS data source: 99.54%, Accuracy with HTTP data source: 98.97%
Canedo <i>et al.</i> [78]	Dataset generated by creating testbed.	ANN Platform: R (neural-net package).	Invalid data entries.	Generating data entries by creating a testbed with more devices and sensors.	N/A

Ioannouet <i>al.</i> [79]	Networks created with varied placements of sink nodes.	c-SVM platform: RMT tool(Run time monitoring tool).	Routing layer attacks (sinkhole, blackhole, selective forward).	Placement of IDS in high energy gateway nodes.	Accuracy:100% (with the same topology) Accuracy=81%(when the topology is changed)
Zhao <i>et al.</i> [80]	KDD cup 99	PCA(to reduce dimensions) + KNN(classification + Softmax regression(classification) .	Dos, probe, Remote-to- local(R2L), User-To- Root(U2R)		Accuracy: 85.24% with 3 dimensions, 85.19% with 6 dimensions 84.406% with 10 dimensions.
Prabavathyet <i>al.</i> [81]	NSL-KDD	OS-ELM(online sequential extreme machine learning) Platform: MATLAB (R2013a).	Dos, probe, Remote-to- local(R2L), User-To- Root(U2R).	More depth analysis of zero-day attacks is required.	Accuracy:97.16%(forbinary classification) TPR(true positive rate): normal-98.63%, probe-84.2%, Dos-96.61%, U2R-53.81,R2L-71.87%(for multi class classification).
Hasan <i>et al.</i> [82]	DS2OS	LR, SVM, ANN, RF, DT Platform: python with Numpy, pandas, sci-kit learn.	Dos, data type probing, malicious control, malicious control, malicious operation, scan, spying, wrong setup.	More robust algorithmsare required, more attention is required for real-time detection.	Accuracy: LR-98.3% SVM-98.2% DT-99.4% RF-99.4% ANN-99.4%

Lee *et al.*[84] have come up with profiling of abnormal activities of IoT devices via the support of a variety of machine learning algorithms. The approach considers signal injection as a threat to IoT and hence finds it as a principal attack in his research. Two types of datasets were generated, one in which only a single piece of data was faulty and the other in which all parts were defective. The dimensional reduction of the dataset was performed using PCA (principal component analysis along with k-means and SVM for anomaly classification.

Yang *et al.*[85] have proposed a unique human in the cycle intrusion detection via ML to reduce the dependency on a large amount of labeled data for anomaly detection. This approach was performed by the incorporation of techniques like query selection for unlabelled data. Shafi *et al.*[86] have presented a fog-aided SDN(software-defined networking) structure for anomaly detection and prevention for IoT networks, mainly to overcome the pitfalls of screening at the cloud and at the devices. The approach was evaluated by simulating an IoT network using the cooja simulation tool and subsequently training it using the UNSW-NB15 dataset via the E3ML(entropy-based triple machine learning-Knn, MLP, ADT classifiers) approach. However, due to certain limitations like processing power, scalability, manual feature selection,

and heterogeneous data handling pushes us to come with better learning approaches. To deal with some aspects of limitations in ML, DL was implemented and analyzed in the security region of IoT[87].

4.2 Deep Learning-based solutions in IoT security

Deep learning technology is considered to be a successor of ML with the capability of mimicking the human brain, thus falling under the categorization of AI. Deep networks have the potential of achieving better accuracy in terms of predictions and classifications because of the multilayered composition. This composition, when combined with IDS, can achieve performance at a superhuman level for the detection of new attacks and anomalies[88]. The principle benefit of the technology is the omission of manual feature selection and the capability to model non-linear relationships, thereby achieving an edge over ML. Moreover, the ability to handle Big Data, automatic feature extraction further backs the usage of technology in IoT. The essence of the technology revolves around cascading multiple layers for predicting the output. To accomplish the non-linearity activation function plays an important role. Table 6 lists the activation function for deeper networks[89]. Furthermore, Table 7 summarizes the different deep learning-based solutions used to secure IoT systems.

Table6: Activation Functions.

Activation function	Nature	Range	Classification	Mathematical notation	Usage
Sigmoid	Non-linear	0 or 1	Binary classification	$f(x)=1/1+e^{-x}$	Output layer
Tanh	Non-linear	-1 or 1	Binary classification	$\text{Tanh}(x)=2*\text{sigmoid}(2x)-1$	Output layer
Relu[90]	Non-linear	[0,inf]	Multiple classification	$f(x)=\max(0, \max)$	Hidden layer

Swish	Non-linear	-inf to inf	Multiple classification	$f(x)=x*\text{sigmoid}(x)$	Hidden layer
-------	------------	-------------	-------------------------	----------------------------	--------------

Deep learning can be classified into three classes, known as discriminative, generative, and hybrid models.

Discriminative Models: These models belong to the class of supervised learning and thus are used for treating problems of classification and regression. If the input label is X and the corresponding output label is Y , then discriminative models require to learn the conditional probability of target label y , i.e., $p(y|x)$ [91].

- **Convolutional Neural Network (CNN):** It is a feed-forward deep artificial neural network that leverages the concept of convolution for predictions. The notion is to allocate importance to different parts of the image by connecting only a smaller region of a particular layer to the layer, succeeding it. The primary concept is to reduce the size of weights and the neurons. The functionality of CNN revolves around the four layers, namely the convolution layer, to reduce the size of weights followed by the Relu layer to introduce non-linearity into the network[92]. Then come the pooling and the fully connected layer, which subsequently perform the task of shrinking the stack size obtained from the previous layer and performing the actual classification, respectively. Nowadays, the technique is finding usage in the sector of anomaly detection[93][94], the approach is fused with other methods for anomaly detection, thus providing a profitable proposal in this sector.
- **Recurrent Neural Network(RNN):** This type of feed-forward artificial neural network possesses internal memory. The associations between the various units form a digraph, thereby allowing the structure to copy the output and propagating it back to RNN at every timestamp. These associations permit the composition to evince temporal dynamic behavior. The characteristics mentioned above make it appropriate for applications like speech recognition, time series prediction, and anomaly detection[95]. There are many variants to the basic RNN, namely Hopfield network, fully recurrent, Elman and Jordan networks, etc.
- **Long Short Term Memory(LSTM):** It is a type of RNN with an ability to remember long-time dependencies, thus overcoming the limitations of RNN. The composition of LSTM includes memory cells for keeping back the information along with three gates, namely forget, input, and output for memory orchestration[96][97].

Generative Models: These models belong to the class of unsupervised learning. They are used when there is no

presence of labeled data. The model requires calculating the joint probability $p(x,y)$ where x and y are input and output variables, respectively.

Autoencoders: It is a class of deep learning model which relies on the concept of rebuilding the input after performing suitable compression via the application of an encoder followed by a decoder[98]. The prime task is to achieve dimensionality reduction to visualize the data and gather suitable projections from it provided input features are not independent and have some correlation. Vanilla, convolutional, multilayer, regularized are some variants of autoencoders. Meidan *et al.*[99] have presented N-Balot(network-based detection of IoT botnet attacks using deep autoencoders) to detect botnet attacks using autoencoders.

Roopak *et al.*[93] presented a deep learning approach for cybersecurity in the IoT network. Various deep learning models like 1D-CNN, RNN, LSTM, and a hybrid model of CNN+LSTM have been implemented on the CICIDS2017 dataset, particularly for DDOS attack detection and comparison have been made with the standalone Machine learning techniques. McDermatt *et al.*[100] provide a novel bidirectional long short term memory-based RNN for the sensing of botnet activities amongst the consumer IoT device. Packet level detection was performed along with word embedding for recognition of text and conversion of packets into integer format. Rahul *et al.*[88] have proposed a deep neural network-based approach to predict attacks on a NIDS. KDD cup 99 was used for the purpose of training the network. With continuous evaluation and by varying the hidden layer counts, a DNN with 3 layers, 0.1 learning rate running for 1000 epochs generated the maximum accuracy. The system was also tested against many shallow ML algorithms.

Diro *et al.*[101] have presented a deep learning model for the distributed detection of attacks. They try to leverage the self-teaching and compression capabilities of DL by experimenting with using the NSL-KDD dataset to implement the network detection of attacks at fog nodes, unlike following a centralized approach. The results showed that distributed attack detection provided better accuracy compared to the centralized schemes, in accommodation to some double standards being recorded in terms of training time and detection rate.

An attempt to collaborate DL technology with its shallow counterpart was made by Shone *et al.*[102]. They presented a novel unsupervised learning approach named NDAE(non-

symmetric deep autoencoder) for feature engineering combined with random forest for classification. The classifier was implemented in tensor-flow using the benchmark KDD and NSL KDD datasets. Comparisons were made against the traditional Deep Belief Networks and in which NDAE outperformed.

Ullah *et al.*[103] proposed a tensor-flow-based Deep neural network approach to detect software piracy and other malware-based attacks in the industrial IoT network. This DNN is used for capturing pirated software from the source code of different programmers from google code jam followed by an application of CNN to detect footprints via binary visualization on colored images of malware files. Two image ratios 224*224 and 229*229 were considered for evaluation in which 229 *229 gave better accuracy with CNN.

Traffic classification plays a very vital role in ensuring security in IoT networks. Yao *et al.*[104] present an end-to-

end deep learning-based capsule network approach for traffic classification and identification of malware, unlike the conventional DL methods. Telikani *et al.*[105] have proposed a CSSAE technique for intrusion detection, especially in IoT networks. The main focus of the paper is the class imbalance problem in the datasets, which tends to bias the results towards the majority class. They implemented the technique on the NSL-KDD and KDD dataset in the first stage, followed by two-layer stacked autoencoders for feature learning in the second stage. Pajouh *et al.*[106] have deployed LSTM for malware detection in ARM rooted IoT applications and achieved an accuracy of 98%. Liao *et al.*[107] have exploited RNN, and network coding in amalgamation to prevent eavesdropping attacks in heterogeneous IoT environments with highly unreliable storage structures and have proposed two algorithms FAGA() (failure-aware greedy allocation) and FLAGA() (failure-and-load aware greedy allocation) to test the failure condition of storage devices.

Table 7: Tabular Representation Of Deep Learning Approaches.

Author	Dataset used	Algorithm with implementation platform	Threats	Challenges	Performance evaluation
Roopaket <i>al.</i> [93]	CICIDS2017	MLP,1-d CNN,LSTM ,CNN+LSTM Platform: Keras –Tensorflow, machine learning implementation MATLAB2017a.	DDOS	Lack of Deep learning models that can work with highly unbalanced datasets.	Accuracy: 1dCNN-95.14%, MLP-86.34%,LSTM-96.24%, CNN+LSTM-97.16%.
McDermatt <i>et al.</i> [100]	Dataset generated by creating a testbed.	BLSTM	Mirai(scan, infect, control, and attack), UDP.	Lack of comprehensive dataset including more attack vectors.	Accuracy:99.99%(Mirai), 98.58%(UDP).
Rahul <i>et al.</i> [88]	KDD cup 99	DNN with three layers Platform: Keras (Tensorflow).	Dos, probe , User-To-Root(U2R), Remote-to-local(R2L).	Lack of real-time IoT dataset, evaluation of deeper networks.	Accuracy:93%.
Diro <i>et al.</i> [101]	NSL-KDD	Deep learning model with 150, 120, 50 neurons in first, second, and third layer respectively.		Implementation of technique on different datasets.	Accuracy: 96% to 99% 99%(for two class-normal and anomalous) 98.27%(for 4 class(normal, dos, probe, U2R and R2L)
Shone <i>et al.</i> [102]	KDD cup 99, NSL-KDD	NDAE(non-symmetric deep auto-encoders) Platform: GPU enabled tensor-flow.	Dos, probe, User-To-Root(U2R), Remote-to-local(R2L)	Lack of real-time traffic for appropriate analysis.	Accuracy: 94.58%(Dos), 94.67%(probe), 3.82%(R2L), 2.70%(U2R).
Ullah <i>et al.</i> [103]	Google code jam, Leopard Mobile dataset1	Deep neural networks Platform: Tensor-flow	Pirated software and malware threats(industrial IoT).	-	Accuracy: 96%

Yao <i>et al.</i> [104]	UTSC-2016	Capsuleapproach(1-D CNN+ capsule networklayer+LSTM + output layer. Platform:Python2.7, TensorFlow1.8.0	Malware threats.	Higher classification accuracy compared to traditional approaches.
-------------------------	-----------	-----------------------------------------------------------------------------------------------------------	------------------	--------------------------------------------------------------------

4.3 Critical Analysis

The complete inspection and scrutinization of the prevailing ML and DL techniques concerning the survey conducted in this groundwork stipulate the following trends for anomaly detection in the IoT. As a matter of fact, concerning the non-availability of a particularIoT dataset has advocated researchers to orchestrate their experiments either by using some non-IoT series of data or come up with their data records[108][109].The pie-chart below depicts the percentage implementation of various MLand DL approaches at different records, w.r.t the survey conducted in this paper.

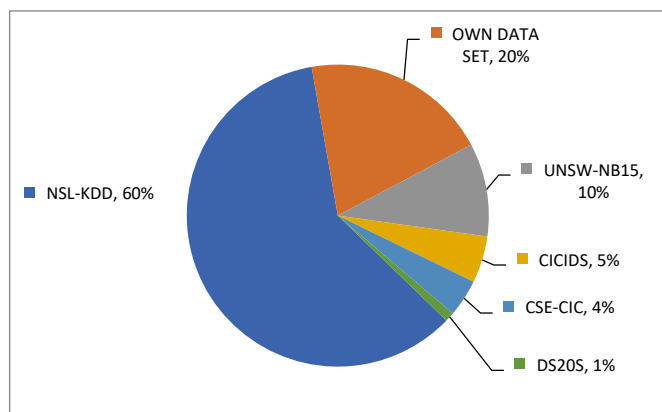


Figure 8: Datasets used.

Figure 8 indicates that the maximum testing of learning approaches are carried out on the KDD cup 99 and its variant NSL-KDD dataset. Also, researchers produced their test records to conduct the implementation, or either utilized datasets like UNSW-NB15, CICIDS, CSE-CIC, and DS2OS for experimentation amongst which only UNSW-NB15 and DS2OS are the most suitable IoT data records, i.e., they represent a real-world scenario of IoT.Further, the survey conducted also helps us to reach some conclusions for the learning approaches which includes their advantages, disadvantages, and their suitability towards the various known attacks which is depicted in Table8.

Table 8: Conclusions about learning approaches.

ML And DL Techniques	Advantages	Disadvantages	Suitability Towards The Attacks
DT	Inherent feature selection, less preprocessing required, simple and easy to implement, can handle missing values, coupling with clustering decreases the processing time in misuse based detection[29].	Large training time, large complexity, small alterations cause significant changes.	C4.0, C5.0 shows very similar results to ANN in[110] with real IoT data. J48 shows a high affinity towards the DOS attack[111].
SVM	The Huge success rate in IDS, best for binary classification, requires small datasets for training, enhanced SVM shows better results in novel and real attacks.	Reveals its weakness in multiclass classification, massive consumption of memory, depends on the kernel function.	It is used in[47] for attack detection. Also useful in spoofing attacks, intrusions in access control[112], online outlier detection[113].
KNN	It has a Fast training phase and makes no assumptions about the data.	It requires abundant storage, expensive, depends on the value of K, and suffers from the dimensionality curse.	Mostly used in combination with other classifiers [33][106]. Useful for access control intrusion detection, malware.

RF	No feature selection, no overfitting problem, usually has the best accuracy.	Time-consuming because of the development of decision trees.	It has achieved 99% accuracy. for the DOS attack [105]. Useful for malware detection,link fault detection[76],access control.
NB	Robust towards the noise,simple and easy to implement	It cannot capture useful information because of the assumption of independence amongst the features.	Used in[34] for intrusion detection, access control.
ANN	Robust model and can handle non-linear data.	It suffers from overfitting, andthe technique is time - consuming, selection of activation function is another overhead and estimating an appropriate number of units in each layer.	Very useful DOS attack detection[114][76].
RNN	Efficient modeling of time-series data	Difficulty in training, cannot remember very long sequences with Relu or tanh activation function[115].	Eavesdropping[106].
LSTM	Reduces a load of feature engineering, effective for unstructured datasets, can remember long sequences of attack patterns.	Difficult to train because of gigantic memory bandwidth requirements.	IoT malware[107], botnet activities, used in [97]for attack detection in fog networks.

The table mentioned above will assist readers with the choice of learning approach they want to implement in their researches based on their advantages, disadvantages, and their suitability towards the various attacks.

5. Case Study: Healthcare and IoT

The innovation in numerous IoT technologies has led to the decentralization of healthcare mechanism from being traditional to a customary localized forum via the assistance of IoT authorized gadgets. These gadgets are based on the concept of a multisensor framework for recording various parameters. These include recording blood sugar, ECG(electrocardiogram), pulse, temperature, etc. of the patient. This customization supports the notion of remote health tracking, which in particular involves at-home medication, elderly care, or any fitness program [116][117][118].

Healthcare in IoT primarily involves four basic entities, which are actors, sensors, communication networks, and applications. The actors include the patients, clinical staff involving the doctors, nurses, experts. Sensors are used for illuminating the actors with paramount requirements and subsequently dispatching the information via a suitable communication network. There are profuse devices prevalent for reading and tracking of vital patient data and other medical statistics. These devices range from smart wearables like smart bands, watches, shoes to intelligent video cameras

and meters. Applications assist with real-time notifications, thus aiding any emergency services. Figure 10 provides a generalized architecture of IoT in healthcare[118].

Figure 9 depicts smart healthcare management with the use of technologies like sensors, wireless sensor networks, cloud storage, along with audio and video interfaces. Sensors are used for reading patient's data and are connected to the microprocessors. These microprocessors are further connected to any wireless communication technology for routing and forwarding the data through the gateway. The data is stored in the virtual machines popular as clouds for preprocessing and analysis. This data can be accessed by doctors, experts, and even the patients. However, a proper security mechanism is required to prevent any kind of damage by the adversaries. The issues and challenges are discussed further.

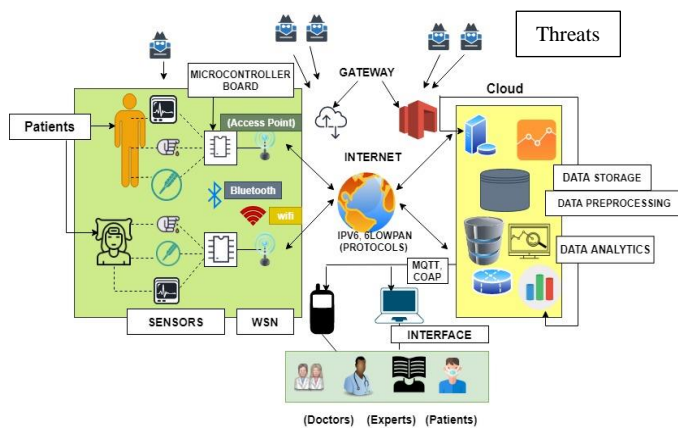


Figure 9: Generalized Healthcare Architecture

Various IoT architectures have progressed over the past years. Some of the prominent architectures are discussed below:

- **mHealth:** It is a primary health care system with a three-layered structure. The layers include a data collection layer for apprehending and collecting the data followed by a data storage layer, which provides for stocking the data in the stack pile racks, and data processing layer for a proper inspection and scanning of data [119].
- **6Lowpan:** It consists of numerous access points with forwarding and routing capabilities. The deployed sensor nodes, along with the access points, lead to the formation of clusters. The connection is achieved via the assistance of IPV6. This approach is preferred over others due to its low energy requirements, which makes it suitable for battery-powered sensors.
- **Zigbee Based:** Gao *et al.*[120] discuss a Zigbee-based structural health monitoring system. Therevolution in WSN allows multiple sensor nodes to communicate wirelessly with the base station. In order to increase the lifetime of the network, a low energy communication channel is necessary. This led to the injection of Zigbee for communication in the health monitoring system.

Despite many benefits, this sector of technology suffers from various loopholes, which are enumerated below.

5.1 Security and Privacy Issues in Smart Healthcare Monitoring

The massive growth in the deadly underlying medical conditions of the population requires well organized, systematic, and efficient healthcare management. Despite the numerous benefits like better diagnosis, treatment, and other facilities, the smart and ubiquitous nature exposes it to multiple cyber threats. Cybersecurity in healthcare is at a nascent stage and thereby requires proactive and improved technologies to protect it from various attacks. Understanding of different security challenges is necessary before dealing with other intricacies of it. There are numerous challenges and issues for contemporary health care applications.

- **Privacy:-** The broadcast nature of communication in healthcare leads to the exploitation of privacy of the patients, thus launching platforms for serious threats like eavesdropping the communication. This aspect, in turn, leads to the exploitation of the confidentiality of the data. Besides, it also gives access to the resources, if any. But for achieving real-time communication, some violations for privacy maintenance are essential, especially in case of emergencies [121].
- **Integrity And Authentication:-** Any change in the data received from the sensors can be life-threatening in the case of a healthcare application. Therefore integrity and authentication are the two major concerns here. Even, end-to-end cryptography and steganography cannot guarantee protection from the attackers due to limited resources in the sensor nodes.
- **Standardization Of Devices:-** As the field of IoT-based Healthcare is advancing day by day, many homogenous devices are fabricated by different manufacturers generating a difference in bandwidth and speed, thus affecting power consumption and efficiency. This leads to an increase in the number of interfaces to maintain standardization, which increases the overhead further. This scenario makes the smart health care systems prone to many attacks.
- **Cloud Storage:-** It refers to using several virtual machines at a single click. This technology increases the flexibility of data storage by storing all the patient's data, thereby reducing the overall expenditure incurred. However, the author in [122] depicts how emergency services can be disrupted and compromised because of a lack of a single cloud-based infrastructure where all e-health records can be accessed. Further security breaches in cloud storage can worsen the situation.
- **Location Tracking:-** Accurate estimation of the patient's location is essential for proper patient care. Security breaches like injection attacks can result in dispatching false information regarding the location of the patients, thereby affecting the treatment process of the actors involved. Thus, a proper smart tracking system is required.

5.2 Machine Learning in Healthcare

To address the above-mentioned flaws, better and improved security frameworks are required that necessitate the amalgamation of machine learning in this sector. Besides fixing critical medical conditions like the identification of tumors, bleeds, etc., this AI tool can solve many security-related affairs and issues by acting as an anomaly detector. Newazet *al.*[123] have suggested the application of health guard: an ML-based security application framework for healthcare systems. This framework leveraged multiple ML algorithms(KNN, Random Forest, DT, ANN) for detecting

malicious activity and was able to achieve an accuracy of 91%. The framework can encapsulate and observe correlations amongst multiple body functionalities and other crucial signs. The structure was tested against threats that included tampered medical devices, DOS, and other false data. To further increase security, research is being carried out to combine ML with blockchain technology.

Tanwar *et al.*[124] have suggested the use of ML in blockchain to improvise data security and privacy. Architecture has been proposed by integrating the two technologies. The learning potential of ML is combined with blockchain technology that will not only make it smarter but also reduce many data-oriented issues. Also, Nilima *et al.*[125] have further backed that the usage of ML with blockchain to make the system smarter and deal with privacy, integrity, and authentication issues. Decentralization, transparency, and immutability are the primary objectives of blockchain technology, which helps to improve the security of the system. This combination will result in incorrect predictions and better security.

6. Research challenges and Future Directions

The expeditious advancement of IoT usage in multiple sectors brings security complications to the forefront. The tremendous volumes of research conducted in the past years still limit IoT to its nascent stage. The prime reason for the multiple challenges IoT is facing that limit its expansion is in the security zone. In this section, the emerging challenges which halt the IoT growth are discussed and pinpointed in Figure 11.

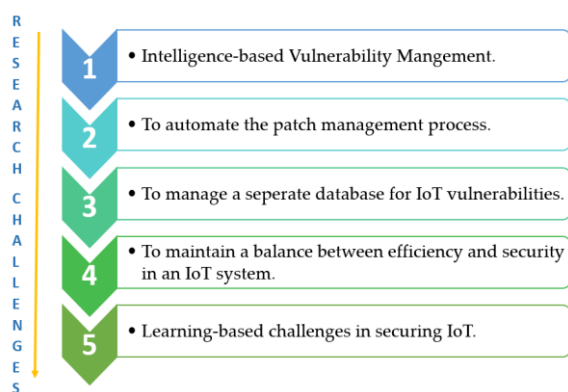


Figure 10: Emerging Challenges and Open Issues.

- **Intelligence-based Vulnerability Management:** Firstly, the heterogeneity of the devices in the smart digitized world limits the automated detection and discovery of the vulnerabilities. Further, adding to this is the lightweight security requirement for their protection. These factors culminate the need to restructure the security analysis platform. The survey conducted in this paper also backs this restructuring by merging AI with IoT and presenting

various solutions offered in this context. However, to further improvise the attack discovery, detection, and mitigation, some problems need to be confronted. These include a lack of real-time datasets. The datasets available for the research purpose do not reflect real-world attack scenarios and are often unbalanced. Further, the continuously changing functionalities of the networking environment require retraining of the system, thereby adding to the overhead.

- **To Automate the Patch Management Process:** The prime challenge to address the vulnerabilities in the smart devices is the lack of a single automated binary code patch generator that is functional across multiple platforms. The leading cause is the generation of devices by different manufacturers. Therefore this prescribes their usability and prevents us from achieving an appropriate and feasible solution for the firmware patching. Further adding to this is the variable nature of the operating system and architectural patterns followed in the numerous devices. Thus, automatic patch generation requires a deep understanding of the entire mechanism, thereby making it a long-term security goal.
- **To manage a separate database for IoT vulnerabilities:** From the studied literature and growing attacks, it is seen that the general IoT devices with inherent known vulnerabilities are flooded to the market. These IoT nodes, in turn, act as a stepping stone for the adversaries to launch various attacks like Mirai, Hijame. Thus, in order to handle the insecure IoT devices, maintaining structured information about the exploits and known vulnerabilities in the smart environment would be of immense use. VARIOt is one such project working exclusively to develop a separate database for managing IoT vulnerabilities.
- **To maintain a balance between Efficiency and Security in an IoT system:** In addition, a balance needs to be achieved between efficiency and data security. Due to the inverse nature, one often gets compromised. Therefore, incorporating ML and DL to the fog nodes must be explored in depth to the intelligence near the data sources to reduce the latency and the bandwidth. Though ML and DL have the capacity to detect multiple attacks, still the challenge for mitigating all possible attack persists. Therefore supplementing the research further is required by exploring the incremental machine learning near the sources.
- **Learning-based challenges in securing IoT:** Machine Learning being known for extracting knowledge from the data have been used for both malevolent and noble

purposes. It is found that the potential adversaries make efficient use of these learning algorithms (machine learning and deep learning-based) to break the cryptographic secrets. For example, Recurrent Neural networks are being used by the authors for the purpose of cryptanalysis. Furthermore, false data input feeds to the machine learning model result in improper functioning of the entire learning-based system. The problem of the oversampling, inadequate training dataset, and feature extraction are also a matter of concern in adding intelligence to smart environments.

7. Conclusion

The extensive study conducted in this research culminates in the various facets of IoT and that include the foundation of the IoT technology to the different architectural approaches. Here the outline is followed by an in-depth security analysis depicting a taxonomy of attacks, anomalies, and vulnerabilities. The technology has already brought and will continue to bring numerous benefits to make Digital Society and Transformation. But the deep contemplation of security aspects of it highlights the raising concerns in this sector. Thus appropriate defense mechanisms are also important here such as access control, IDS, and authentication etc. Due to the non-applicability of traditional security approaches (firewalls, antivirus) primarily because of low memory and computational constraints, other defense mechanisms like IDS have gained popularity. The paper highlights the numerous research efforts in the application of IDS based on the ML and DL algorithm as a security shield in this area. Also, the pros and cons of the various learning techniques are listed with their suitability towards different attacks conducted with critical analysis. Besides all, a case study highlighting the various facets of healthcare and medical infrastructure is also provided which further helps in understanding the practical implementation of IoT and ML in real-world scenarios. In the future, hybrid learning-based techniques need to explore to secure healthy as well as smart environments to reach proper Digital Society and Digital Economy.

REFERENCES

- [1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.
- [2] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, "IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges," *IEEE Access*, vol. 8, pp. 1–1, 2020, doi: 10.1109/access.2020.3022842.
- [3] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K. K. R. Choo, "An Energy-efficient SDN Controller Architecture for IoT Networks with Blockchain-based Security," *IEEE Trans. Serv. Comput.*, vol. 1374, 2020, doi: 10.1109/TSC.2020.2966970.
- [4] A. Čolaković and M. Hadžialić, "PT," *Comput. Networks*, 2018, doi: 10.1016/j.comnet.2018.07.017.
- [5] "IoT Enabling Technologies - IoTbyHVM - Bits & Bytes of IoT."
- [6] X. Xu, J. Zhou, and H. Wang, "Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of things," *Proc. 2013 3rd Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2013*, pp. 825–828, 2014, doi: 10.1109/ICCSNT.2013.6967233.
- [7] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID Technology and Its Applications in Internet of Things (IOT)," pp. 1282–1285, 2012.
- [8] "Importance of Sensors in the Internet of Things | IoT Sensors."
- [9] M. A. Matin, M. N. Islam, M. A. Matin, and M. M. Islam, "Overview of Wireless Sensor Network Chapter 1 Overview of Wireless Sensor Network," Sep. 2012, doi: 10.5772/49376.
- [10] "Embedded systems in the Internet of Things | Embedded system | IoT."
- [11] "What is Cloud Computing."
- [12] S. Gupta, N. Kishore Sharma, and M. Dave, "Internet of Thing: A Survey on Architecture and Elements," *Int. J. Eng. Manag. Res.*, no. 6, pp. 239–242, 2016.
- [13] I. Yaqoob *et al.*, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wirel. Commun.*, vol. 24, no. 3, pp. 10–16, 2017, doi: 10.1109/MWC.2017.1600421.
- [14] D. Navani, S. Jain, and M. S. Nehra, "The internet of things (IoT): A study of architectural elements," *Proc. - 13th Int. Conf. Signal-Image Technol. Internet-Based Syst. SITIS 2017*, vol. 2018-Janua, pp. 473–478, 2018, doi: 10.1109/SITIS.2017.83.
- [15] H. F. Atlam and G. B. Wills, *IoT Security, Privacy, Safety and Ethics*, no. March. Springer International Publishing, 2020.
- [16] M. Bauer, "Internet-of-Things Architecture Project Deliverable D1 . 2 – Initial Architectural Reference Model for IoT," *Architecture*, no. 257521, pp. 1–97, 2011.
- [17] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization," *Comput. Networks*, vol. 56, no. 16, pp. 3594–3608, 2012, doi: 10.1016/j.comnet.2012.07.010.
- [18] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A software defined networking architecture for the internet-of-things," *IEEE/IFIP NOMS 2014 - IEEE/IFIP Netw. Oper. Manag. Symp. Manag. a Softw. Defin. World*, 2014, doi: 10.1109/NOMS.2014.6838365.
- [19] J. Li, Y. Zhang, Y. F. Chen, K. Nagaraja, S. Li, and D. Raychaudhuri, "A mobile phone based WSN infrastructure for IoT over future internet architecture," *Proc. - 2013 IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput. GreenCom-iThings-CPSCOM 2013*, pp. 426–433, 2013, doi: 10.1109/GreenCom-iThings-CPSCOM.2013.89.

- [20] D. Singh, G. Tripathi, and A. J. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services," *2014 IEEE World Forum Internet Things, WF-IoT 2014*, pp. 287–292, 2014, doi: 10.1109/WF-IoT.2014.6803174.
- [21] C. Cecchinel, M. Jimenez, S. Mosser, and M. Riveill, "An Architecture to Support the Collection of Big Data in the Internet of Things," pp. 442–449, 2014, doi: 10.1109/services.2014.83.
- [22] S. Kraijak and P. Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," *Int. Conf. Commun. Technol. Proceedings, ICCT*, vol. 2016-Febru, pp. 26–31, 2016, doi: 10.1109/ICCT.2015.7399787.
- [23] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, 2018, doi: 10.1016/j.jksuci.2016.10.003.
- [24] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," *IEEE Softw.*, vol. 33, no. 1, pp. 112–116, 2016, doi: 10.1109/MS.2016.20.
- [25] D. Priyadarshi and A. Behura, "Analysis of Different IoT Protocols for Heterogeneous Devices and Cloud Platform," *Proc. 2018 IEEE Int. Conf. Commun. Signal Process. ICCSP 2018*, pp. 868–872, 2018, doi: 10.1109/ICCSP.2018.8524531.
- [26] S. Al-sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Review," pp. 685–690, 2017.
- [27] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, 2017, doi: 10.1155/2017/9324035.
- [28] "What is IoT Architecture? Explanation with Example of IoT Architecture."
- [29] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices : Rethinking network security for the Internet-of-Things," 2020.
- [30] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," *Proc. - IEEE Symp. Comput. Commun.*, vol. 2016-Febru, pp. 180–187, 2016, doi: 10.1109/ISCC.2015.7405513.
- [31] O. El Madrasah al-Muhammadīyah lil-Muhandisīn., M. Lahmer, and M. Belkasmī, "E-TI : la revue électronique des technologies de l'information.," *Electron. J. Inf. Technol.*, vol. 0, no. 9, pp. 24–37, 2016, doi: 10.1016/j.fitote.2010.12.007.
- [32] F. Aubet, "Machine Learning-Based Adaptive Anomaly Detection in Smart Spaces Machine Learning-Based Adaptive Anomaly Detection in Smart Spaces Frano," no. January, 2019, doi: 10.13140/RG.2.2.35293.26088.
- [33] W. Meng, "Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling," *Computer (Long. Beach. Calif.)*, vol. 51, no. 7, pp. 36–43, 2018, doi: 10.1109/MC.2018.3011034.
- [34] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," *2016 3rd Int. Conf. Electron. Des. ICED 2016*, pp. 321–326, 2017, doi: 10.1109/ICED.2016.7804660.
- [35] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures," *IEEE Commun. Surv. Tutorials*, vol. XX, no. X, pp. 1–1, 2019, doi: 10.1109/comst.2019.2953364.
- [36] "Into the Battlefield: A Security Guide to IoT Botnets - Security News - Trend Micro IN."
- [37] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 355–373, 2018, doi: 10.14569/IJACSA.2018.090349.
- [38] K. M. Sadique, R. Rahmani, and P. Johannesson, "Towards security on internet of things: Applications and challenges in technology," *Procedia Comput. Sci.*, vol. 141, pp. 199–206, 2018, doi: 10.1016/j.procs.2018.10.168.
- [39] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Networks*, vol. 4, no. 2, 2018, doi: 10.1016/j.dcan.2017.04.003.
- [40] M. binti Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Networks*, vol. 148, pp. 283–294, 2019, doi: 10.1016/j.comnet.2018.11.025.
- [41] I. Gudymenko and M. Hutter, "Security in the Internet of Things Supervisor ;," no. Itt, pp. 1–7, 2011.
- [42] J. Whitter-Jones, "Security review on the Internet of Things," *2018 3rd Int. Conf. Fog Mob. Edge Comput. FMEC 2018*, pp. 163–168, 2018, doi: 10.1109/FMEC.2018.8364059.
- [43] S. Benzarti, B. Triki, and O. Korbaa, "A survey on attacks in Internet of Things based networks," *Proc. - 2017 Int. Conf. Eng. MIS, ICEMIS 2017*, vol. 2018-Janua, pp. 1–7, 2018, doi: 10.1109/ICEMIS.2017.8273006.
- [44] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, pp. 32–37, 2017, doi: 10.1109/I-SMAC.2017.8058363.
- [45] G. Rajendran, R. S. Ragul Nivash, P. P. Parthy, and S. Balamurugan, "Modern security threats in the internet of things (IoT): Attacks and countermeasures," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2019-Octob, 2019, doi: 10.1109/CCST.2019.8888399.
- [46] I. Stelliou, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018, doi: 10.1109/COMST.2018.2855563.
- [47] N. Neshenko, E. Bou-harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security : An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.
- [48] "Top 10 IoT vulnerabilities | Network World."
- [49] M. Bhardwaj, "security in Internet of Things applications.," 2017. .
- [50] "IoT security starts with secure boot."
- [51] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey : A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications," vol. 2014, 2014, doi: 10.1155/2014/357430.
- [52] T. Kothmayr, C. Schmitt, W. Hu, M. Br, and G. Carle, "DTLS

- based Security and Two-Way Authentication for the Internet of Things \$,” no. May, 2013.
- [53] H. Shafagh, A. Hithnawi, and S. Duquenooy, “Talos : Encrypted Query Processing for the Internet of Things,” pp. 197–210, 2015.
- [54] E. Ronen and A. Shamir, “Extended Functionality Attacks on IoT Devices : The Case of Smart Lights (Invited Paper),” 2016, doi: 10.1109/EuroSP.2016.13.
- [55] B. Wei, G. Liao, and W. Li, “A Practical One-time File Encryption Protocol for IoT Devices,” pp. 0–5, 2017, doi: 10.1109/CSE-EUC.2017.206.
- [56] A. Sivanathan, H. H. Gharakheili, and V. Sivaraman, “Can We Classify an IoT Device using TCP Port Scan?,” in *2018 IEEE 9th International Conference on Information and Automation for Sustainability, ICIAfS 2018*, 2018, doi: 10.1109/ICIAfS.2018.8913346.
- [57] L. Markowsky and G. Markowsky, “Scanning for Vulnerable Devices in the Internet of Things,” no. February, 2016, doi: 10.1109/IDAACS.2015.7340779.
- [58] V. J. Ercolani, M. W. Patton, and H. Chen, “Shodan Visualized,” pp. 193–195, 2016.
- [59] C. Konstantinou and M. Maniatakis, “Impact of Firmware Modification Attacks on Power Systems Field Devices,” pp. 283–288, 2015.
- [60] S. Schechter, “The Current State of Access Control for Smart Devices in Homes,” 2013.
- [61] D. Song and D. Wagner, “Smart Locks : Lessons for Securing Commodity Internet of Things Devices,” 2016.
- [62] “5 Simple IoT Devices That Can Become Entry Points for Hackers - CPO Magazine.”.
- [63] M. Saiful, I. Mamun, A. F. M. S. Kabir, S. Hossein, and R. Hayat, “Policy based intrusion detection and response system in hierarchical WSN architecture .,” no. September 2015, 2009.
- [64] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, “Intrusion detection systems for IoT-based smart environments: a survey,” *J. Cloud Comput.*, vol. 7, no. 1, pp. 1–20, 2018, doi: 10.1186/s13677-018-0123-6.
- [65] U. Noor, Z. Anwar, T. Amjad, and K. K. R. Choo, “A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise,” *Futur. Gener. Comput. Syst.*, vol. 96, pp. 227–242, 2019, doi: 10.1016/j.future.2019.02.013.
- [66] J. R. Quinlan, “Induction of Decision Trees,” pp. 81–106, 2007.
- [67] S. Kaplantzis, A. Shilton, and N. Mani, “Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines,” pp. 335–340, 2007.
- [68] M. Martfnez-Arroyo and L. E. Sucar, “Learning an optimal naive Bayes classifier,” *Proc. - Int. Conf. Pattern Recognit.*, vol. 3, pp. 1236–1239, 2006, doi: 10.1109/ICPR.2006.748.
- [69] Y. Electronics, O. Source, A. N. Networks, and A. Ann, “Introduction to Artificial Neural Networks (ANN),” no. February, pp. 1–5, 2009.
- [70] J. Oyelade *et al.*, “Data Clustering: Algorithms and Its Applications,” *Proc. - 2019 19th Int. Conf. Comput. Sci. Its Appl. ICCSA 2019*, no. ii, pp. 71–81, 2019, doi: 10.1109/ICCSA.2019.000-1.
- [71] V. S. Anke Meyer-Baese, “Dimensionality reduction,” in *Pattern Recognition and Signal Analysis in Medical Imaging*, 2014.
- [72] E. Anthi, L. Williams, and P. Burnap, “Pulse: An adaptive intrusion detection for the internet of things,” *IET Conf. Publ.*, vol. 2018, no. CP740, pp. 1–4, 2018, doi: 10.1049/cp.2018.0035.
- [73] Divyatmika and M. Sreelesh, “A two-tier network based intrusion detection system architecture using machine learning approach,” *Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016*, pp. 42–47, 2016, doi: 10.1109/ICEEOT.2016.7755404.
- [74] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K. K. R. Choo, “A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks,” *IEEE Trans. Emerg. Top. Comput.*, vol. 7, no. 2, pp. 314–323, 2019, doi: 10.1109/TETC.2016.2633228.
- [75] M. R. Shahid, G. Blanc, Z. Zhang, and H. Debar, “Machine Learning for IoT Network Monitoring,” *RESSI (Rendez-Vous la Rech. l’Enseignement la Sécurité des Systèmes d’Information)*, 2019.
- [76] S. M. Srinivasan, T. Truong-Huu, and M. Gurusamy, “Machine Learning-Based Link Fault Identification and Localization in Complex Networks,” *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6556–6566, 2019, doi: 10.1109/JIOT.2019.2908019.
- [77] N. Moustafa and J. Slay, “The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,” *Inf. Secur. J.*, vol. 25, no. 1–3, pp. 18–31, 2016, doi: 10.1080/19393555.2015.1125974.
- [78] J. Canedo and A. Skjellum, “Using machine learning to secure IoT systems,” *2016 14th Annu. Conf. Privacy, Secur. Trust. PST 2016*, pp. 219–222, 2016, doi: 10.1109/PST.2016.7906930.
- [79] C. Ioannou and V. Vassiliou, “Classifying security attacks in IoT networks using supervised learning,” *Proc. - 15th Annu. Int. Conf. Distrib. Comput. Sens. Syst. DCOSS 2019*, pp. 652–658, 2019, doi: 10.1109/DCOSS.2019.00118.
- [80] S. Zhao, W. Li, T. Zia, and A. Y. Zomaya, “A dimension reduction model and classifier for anomaly-based intrusion detection in internet of things,” *Proc. - 2017 IEEE 15th Int. Conf. Dependable, Auton. Secur. Comput. 2017 IEEE 15th Int. Conf. Pervasive Intell. Comput. 2017 IEEE 3rd Int. Conf. Big Data Intell. Compu*, vol. 2018-Janua, pp. 836–843, 2018, doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.141.
- [81] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, “Design of Cognitive Fog Computing for Intrusion Detection in Internet of Things,” *J. Commun. Networks*, vol. 20, no. 3, pp. 291–298, 2018, doi: 10.1109/JCN.2018.000041.
- [82] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” *Internet of Things*, vol. 7, p. 100059, 2019, doi: 10.1016/j.iot.2019.100059.
- [83] N. Moustafa, B. Turnbull, and K. K. R. Choo, “An ensemble intrusion detection technique based on proposed statistical

- flow features for protecting network traffic of internet of things,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, 2019, doi: 10.1109/JIOT.2018.2871719.
- [84] S. Y. Lee, S. R. Wi, E. Seo, J. K. Jung, and T. M. Chung, “ProFiOT: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach,” *2017 27th Int. Telecommun. Networks Appl. Conf. ITNAC 2017*, vol. 2017-Janua, pp. 1–6, 2017, doi: 10.1109/ATNAC.2017.8215434.
- [85] K. Yang, J. Ren, Y. Zhu, and W. Zhang, “SECURITY AND PRIVACY IN THE WIRELESS INTERNET OF THINGS: EMERGING TRENDS AND CHALLENGES Active Learning for Wireless IoT Intrusion Detection,” *IEEE Wirel. Commun.*, vol. 25, no. December, pp. 19–25, 2018, doi: 10.1109/MWC.2017.1800079.
- [86] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, “Fog-Assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network,” *IEEE Access*, vol. 6, pp. 73713–73723, 2018, doi: 10.1109/ACCESS.2018.2884293.
- [87] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, “Machine Learning in IoT Security: Current Solutions and Future Challenges,” no. June, 2019.
- [88] V. K. Rahul, R. Vinayakumar, K. Soman, and P. Poornachandran, “Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security,” *2018 9th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2018*, pp. 1–6, 2018, doi: 10.1109/ICCCNT.2018.8494096.
- [89] D. S. Gupta, “Fundamentals of Deep Learning – Activation Functions and When to Use Them?,” 2020. .
- [90] “A Practical Guide to ReLU - Danqing Liu - Medium.” .
- [91] A. Shrestha and A. Mahmood, “Review of deep learning algorithms and architectures,” *IEEE Access*, vol. 7, pp. 53040–53065, 2019, doi: 10.1109/ACCESS.2019.2912200.
- [92] S. Albawi, T. A. M. Mohammed, and S. Alzawi, “A DATA-DRIVEN APPROACH TO PRECIPITATION PARAMETERIZATIONS USING CONVOLUTIONAL ENCODER-DECODER NEURAL NETWORKS Pablo,” *Ieee*, 2017.
- [93] M. Roopak, G. Yun Tian, and J. Chambers, “Deep learning models for cyber security in IoT networks,” *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, pp. 452–457, 2019, doi: 10.1109/CCWC.2019.8666588.
- [94] D. H. Kim and J. E. Ha, “Multi-lane detection using convolutional neural networks and transfer learning,” *J. Inst. Control. Robot. Syst.*, vol. 23, no. 9, pp. 718–724, 2017, doi: 10.5302/J.ICROS.2017.17.0107.
- [95] “Understanding RNN and LSTM - Towards Data Science.” .
- [96] “Deep Learning | Introduction to Long Short Term Memory - GeeksforGeeks.” .
- [97] A. Diro and N. Chilamkurti, “Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications,” *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 124–130, 2018, doi: 10.1109/MCOM.2018.1701270.
- [98] M. R. Shahid, G. Blanc, and Z. Zhang, “Anomalous Communications Detection in IoT Networks Using Sparse Autoencoders.”
- [99] Y. Meidan *et al.*, “N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders,” vol. 13, no. 9, pp. 1–8, 2018.
- [100] C. D. McDermott, F. Majdani, and A. V. Petrovski, “Botnet Detection in the Internet of Things using Deep Learning Approaches,” *Proc. Int. Jt. Conf. Neural Networks*, vol. 2018-July, pp. 1–8, 2018, doi: 10.1109/IJCNN.2018.8489489.
- [101] A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for Internet of Things,” *Futur. Gener. Comput. Syst.*, vol. 82, pp. 761–768, 2018, doi: 10.1016/j.future.2017.08.043.
- [102] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A Deep Learning Approach to Network Intrusion Detection,” *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, 2018, doi: 10.1109/tetci.2017.2772792.
- [103] F. Ullah *et al.*, “Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach,” *IEEE Access*, vol. 7, pp. 124379–124389, 2019, doi: 10.1109/access.2019.2937347.
- [104] H. Yao, P. Gao, J. Wang, P. Zhang, C. Jiang, and Z. Han, “Capsule Network Assisted IoT Traffic Classification Mechanism for Smart Cities,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7515–7525, 2019, doi: 10.1109/JIOT.2019.2901348.
- [105] A. Telikani and A. H. Gandomi, “Cost-sensitive stacked autoencoders for intrusion detection in the Internet of Things,” *Internet of Things*, p. 100122, 2019, doi: 10.1016/j.iot.2019.100122.
- [106] H. HaddadPajouh, A. Dehghantanha, R. Khayami, and K. K. R. Choo, “A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting,” *Futur. Gener. Comput. Syst.*, vol. 85, pp. 88–96, 2018, doi: 10.1016/j.future.2018.03.007.
- [107] C. H. Liao, H. H. Shuai, and L. C. Wang, “RNN-Assisted Network Coding for Secure Heterogeneous Internet of Things with Unreliable Storage,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7608–7622, 2019, doi: 10.1109/JIOT.2019.2902376.
- [108] S. Siboni *et al.*, “Security Testbed for Internet-of-Things Devices,” *IEEE Trans. Reliab.*, vol. 68, no. 1, pp. 23–44, 2019, doi: 10.1109/TR.2018.2864536.
- [109] Y. Teranishi, Y. Saito, S. Muro, and N. Nishinaga, “JOSE: An Open Testbed for Field Trials of Large-scale IoT Services,” *J. Natl. Inst. Inf. Commun. Technol.*, vol. 62, no. 2, pp. 151–159, 2015.
- [110] F. Alam, R. Mehmood, I. Katib, and A. Albeshri, “Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT),” *Procedia Comput. Sci.*, vol. 58, no. DaMIS 2016, pp. 437–442, 2016, doi: 10.1016/j.procs.2016.09.068.
- [111] R. R. R. Robinson and C. Thomas, “Ranking of machine learning algorithms based on the performance in classifying DDoS attacks,” *2015 IEEE Recent Adv. Intell. Comput. Syst. RAICS 2015*, no. December, pp. 185–190, 2016, doi: 10.1109/RAICS.2015.7488411.
- [112] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, “IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?,” *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, 2018, doi: 10.1109/MSP.2018.2825478.
- [113] M. A. Alsheikh, S. Lin, D. Niyato, and H. P. Tan, “Machine

- learning in wireless sensor networks: Algorithms, strategies, and applications,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014, doi: 10.1109/COMST.2014.2320099.
- [114] R. C. Deo and B. K. Nallamothu, “Learning about Machine Learning: The Promise and Pitfalls of Big Data and the Electronic Health Record,” *Circ. Cardiovasc. Qual. Outcomes*, vol. 9, no. 6, pp. 618–620, 2016, doi: 10.1161/CIRCOUTCOMES.116.003308.
- [115] “Recurrent Neural Networks and LSTM explained - purnasai gudikandula - Medium.” .
- [116] E. Fazeldehkordi, O. Owe, and J. Noll, “Security and privacy in iot systems: A case study of healthcare products,” *Int. Symp. Med. Inf. Commun. Technol. ISMICT*, vol. 2019-May, pp. 1–8, 2019, doi: 10.1109/ISMICT.2019.8743971.
- [117] I. Singh and D. Kumar, “Improving IOT Based Architecture of Healthcare System,” *2019 4th Int. Conf. Inf. Syst. Comput. Networks, ISCON 2019*, pp. 113–117, 2019, doi: 10.1109/ISCON47742.2019.9036287.
- [118] S. Lavanya, G. Lavanya, and J. Divyabharathi, “Remote prescription and I-Home healthcare based on IoT,” *IEEE Int. Conf. Innov. Green Energy Healthc. Technol. - 2017, IGEHT 2017*, pp. 1–3, 2017, doi: 10.1109/IGEHT.2017.8094069.
- [119] N. Kumar, “IoT architecture and system design for healthcare systems,” *Proc. 2017 Int. Conf. Smart Technol. Smart Nation, SmartTechCon 2017*, pp. 1118–1123, 2018, doi: 10.1109/SmartTechCon.2017.8358543.
- [120] A. C. Tokognon, B. Gao, G. Y. Tian, and Y. Yan, “Structural Health Monitoring Framework Based on Internet of Things: A Survey,” *IEEE Internet Things J.*, vol. 4, no. 3, pp. 629–635, 2017, doi: 10.1109/JIOT.2017.2664072.
- [121] S. Alromaihi, W. Elmedany, and C. Balakrishna, “Cyber security challenges of deploying IoT in smart cities for healthcare applications,” *Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2018*, pp. 140–145, 2018, doi: 10.1109/W-FiCloud.2018.00028.
- [122] S. Poorejbari and W. Mansoor, “Smart healthcare systems on improving the efficiency of healthcare services,” *2019 2nd Int. Conf. Signal Process. Inf. Secur. ICSPIS 2019*, pp. 1–4, 2019, doi: 10.1109/ICSPIS48135.2019.9045894.
- [123] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, “HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems,” *2019 6th Int. Conf. Soc. Networks Anal. Manag. Secur. SNAMS 2019*, pp. 389–396, 2019, doi: 10.1109/SNAMS.2019.8931716.
- [124] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W. C. Hong, “Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward,” *IEEE Access*, vol. 8, pp. 474–448, 2020, doi: 10.1109/ACCESS.2019.2961372.
- [125] N. V. Pardakhe and V. M. Deshmukh, “Machine Learning and Blockchain Techniques Used in Healthcare System,” *2019 IEEE Pune Sect. Int. Conf. PuneCon 2019*, pp. 1–5, 2019, doi: 10.1109/PuneCon46936.2019.9105710.