International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

IoT Security Challenges and Their Solutions: An Analysis Using AI and Machine Learning

Deepak Kumar[1], Lekha Kumari[2], Anmol Kumar[3], Gurjeet Singh[4]

Ms. Taruna Chopra[5] Assistant Professor

Department Of Computer Science And Information Technology[1,2,3,4,5],
Kalinga University, Raipur, Chhattisgarh, India
aptechprogramming@gmail.com[1], lekhakumari67457@gmail.com[2], anmolaarya7@gmail.com[3], jarsotiaabhi@gmail.com[4], taruna.chopra@kalingauniversity.ac.in[5]

Abstract - The Internet of Things (IoT) has completely changed how we interact with technology, bringing more connectedness and ease into our daily lives. However, because IoT devices provide fresh and challenging security issues, This increasing connectivity also increases the potential of cyber assaults. With the help of artificial intelligence (AI) and machine learning (ML), This research paper addresses the key IoT security issues, such as authentication, data privacy, and device tampering, and makes recommendations for solutions. IoT security measures can be greatly improved by AI and ML by examining behaviour patterns, identifying weaknesses, and foreseeing possible threats. This research paper cover current IoT security assaults and looks at how AI and ML might have been able to stop them. It also looks at the current limitations and potential future directions of AI and ML in IoT security. The study concludes that although AI and ML are promising technologies for addressing IoT security concerns, they must be utilised in conjunction with other security measures, and continued innovation and investment in IoT security is important for a safer and more secure futureThe limitations of conventional security measures will then be discussed, and possible solutions to these problems will be suggested using AI and machine learning (ML). The analysis of AI and ML applications in IoT security will include threat prediction, intrusion detection, and anomaly detection, among other topics. Additionally, it will look at how AI and ML may be used to protect IoT networks from Distributed Denial of Service (DDoS) assaults, which have been more frequent in recent years. The article will show case studies of recent assaults on IoT devices and networks, like the Mirai botnet attack in 2016, and look at how AI and ML may have been able to avoid or mitigate these attacks. The paper will also discuss the difficulties and restrictions associated with using AI and ML to IoT security, such as the requirement for huge datasets and computing capacity as well as the possibility of bias in machine learning algorithms. The paper will finish by summarising the potential advantages of employing AI and ML in IoT security, such as enhanced accuracy and efficiency in threat detection, and the necessity for continued investment in research and development to address the quickly changing IoT security scenario.

***Key Words*:** Internet of Things (IoT), security challenges, data privacy, threat prediction, Mirai botnet attack, cybersecurity, network security, privacy concerns, cloud computing, healthcare

1.INTRODUCTION

The Internet of Things (IoT) is a constantly growing network of networked systems, sensors, and devices that is revolutionising how we live and conduct business. The potential for increased productivity, comfort, and connectivity is enormous given that there are predicted to be 75 billion IoT devices by 2025. However, because IoT devices provide fresh and challenging security issues, this increasing connectivity also increases the potential of cyber assaults [1].

IoT devices are becoming increasingly commonplace, which makes them more desirable targets for cybercriminals who may use their flaws to obtain private data, disrupt services, or even kill people directly. These dangers vary from device tampering and remote hacking to data breaches and DDoS assaults, and conventional security methods frequently fall short in defending against them . The Internet of Things has enabled smart meters, remote monitoring, process automation, smart homes, smart cities, and smart businesses [2].

The purpose of this research paper is to analyse the main IoT security issues and suggest solutions that make use of machine learning (ML) and artificial intelligence (AI) technologies. IoT security measures can be greatly improved by AI and ML by examining behaviour patterns, identifying weaknesses, and foreseeing possible threats. With the help of artificial intelligence (AI) and machine learning (ML), this research paper will analyse the main IoT security issues and suggest solutions. The paper will begin by giving a thorough overview of the present status of IoT security and outlining the different threats and vulnerabilities that IoT systems are currently subject to. The limitations of conventional security measures will then be discussed, and possible solutions like AI and ML will be suggested. Detecting intrusions, identifying anomalies, and predicting threats are just a few of the uses of AI and ML in IoT security that will be examined in this research.

The paper will finish by summarising the potential advantages of employing AI and ML in IoT security, the need for continual innovation, and the necessity for investment in IoT security. It will then discuss the difficulties and constraints of using AI and ML in IoT security.

Application domains, security concerns, and the methodology used to design solutions are all taken into account by the writers. The authors outline the classification of IoT security issues using attack vectors, vulnerabilities, and other pertinent methods. The writers look into a variety of issues, such as potential attack vectors and the needs for IoT network security. Examining the use of computers and deep learning to safeguard the IoT. To determine how the IoT's expanding capabilities affect security and privacy, researchers have examined known and unknowable hazards, attainable remedies, and barriers.

The Internet of Things (IoT) regulates connectivity by determining how and what happens when things communicate. This implies that IoT networks are always accessible, wherever they may be. Because IoT devices are continually being added and withdrawn, networks must continue to be responsive and adaptable . The biggest problem with industrial IoT networks is wireless communication. For sensitive applications like traffic monitoring, production on an assembly line, and medical equipment, highly dependable, low-latency communication is required[3]. In industrial IoT networks, wireless communication presents the biggest challenge. Sensitive applications like traffic surveillance, assembly line production, and medical equipment require highly reliable, low-latency connectivity. An internet of things (IoT) device is a piece of hardware containing a sensor that transmits information across places. Because a complex system application uses several sensors, the systems should be configured to consume less resources and be less expensive [4].

1.1. Lack of research

Numerous factors, including the relative novelty of IoT technology and the complex and dynamic nature of IoT security threats, can be blamed for the paucity of research in the area of IoT security issues and related AI and machine learning-based solutions. If the next-generation IoT system is to have a continuously evolving and modern security system, the capabilities of artificial intelligence, in particular machine and deep learning solutions, must be leveraged. Lack of standardised security protocols for IoT devices, which makes it challenging to compare and assess various security solutions, may be another factor contributing to the paucity of study. Additionally, there may be a lack of understanding of how to deploy AI and ML successfully among organisations and individuals, as well as a lack of awareness of the potential advantages of using these techniques in IoT security.

1.2. Structure of Our research

The remainder of the paper is divided into the following sections. The background of the domain is covered in Section 2 & 3, along with a research of related works. In Section 4, We look at the security issues and IoT system architectures, as well as our study approach.The findings of our research are presented in Section 8, along with possible machine learning and deep learning-based security solutions for IoT contexts.

2. APPLICATION OF IOT

The Internet of Things (IoT) is crucial to the development of technology. The phrase "Things" refers to electronic items that are connected to the internet, while "IoT" stands for "Internet of Things." Increased automation of conventional industrial and manufacturing processes characterises the

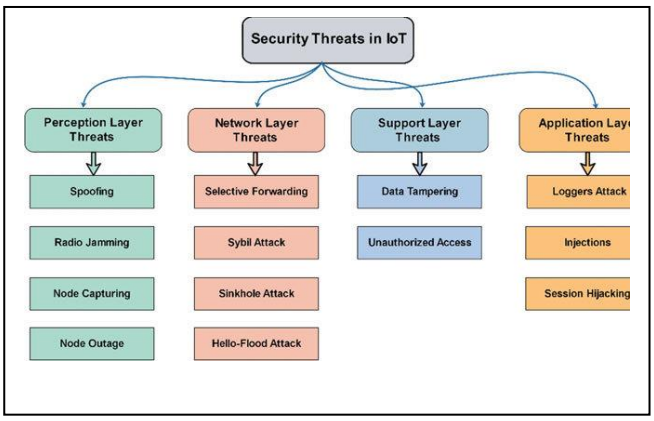


Fig -1: Security Threats In Iot

Fourth Industrial Revolution, often known as Industry 4.0. One of the sophisticated technologies being developed for this movement is the Internet of Things [5]. IoT is now become very exciting and challenging technology for applications developer due to its diverse nature which covers different aspects of life. IoT application domain not restricted to one aspect of human life like building concept as a smart building or smart homes but also dominant in other fields [6].

One of the most promising sectors for the use of IoT technology is the healthcare sector because it has the ability to transform the way treatment is provided and enhance patient outcomes. The usage of IoT devices in healthcare, however, also poses substantial security problems, including the possibility of cyberattacks that could jeopardise patient safety and the risk of data breaches.

These problems may be solved using artificial intelligence (AI) and machine learning, according to some. For instance, academics have suggested using machine learning algorithms to find behavioural patterns that could point to a future cyber assault and to find anomalies in network traffic that could point to a security breach [7One of the numerous challenges the Internet of Things faces is safeguarding user privacy and thwarting attacks like spoofing, denial of service (DoS), jamming, and eavesdropping. The Internet of Things connects a variety of things to networks to enable complex and intelligent applications [8].

The privacy of data analysis focuses on ML-based methods for recognising viruses, authenticating IoT devices, and restricting access to such devices. The adoption of IoT in the future will have a big impact on business, society, and the economy. Smart environment includes smart homes, smart buildings, and smart city. Smart homes equipped with IoT infrastructure gives us a comfortable life and more importantly, this technology gives the concept of efficiently utilizing the resources. Smart home [9]

The difficulties of protecting IoT systems have been identified, and viable solutions using AI and ML have been put forth. A machine learning-based intrusion detection system for IoT networks, for instance, was proposed by Li et al. (2019) and demonstrated great accuracy in identifying hostile traffic. Similar to this, Singh and Sharma (2021) suggested a deep learning-based approach for recognising IoT botnet traffic, which showed good accuracyAdditional difficulties that need to be solved include the possibility of bias in algorithms and the difficulty of integrating AI and ML with current security infrastructure. Additionally, by examining data from sensors

and other IoT devices to identify potential security risks and weaknesses, AI and machine learning can be used to enhance the security of medical equipment. Machine learning techniques, for instance, can be used to analyse the activity of medical equipment in real-time and spot trends that can point to a security breach.

One of the application scenarios of IoT in this regard is the fire detection mechanism or monitoring the fire. It also includes the safety of human with the technology. For example, with the help of IoT sensors, temperature sensors sense the fire and quickly inform the rescue team. Further, it also incorporates the other data like a number of human beings, assets, the intensity of the fire, material present over there and some other related information that help people for better rescue as well as it reduces the damage [10]. Additional difficulties that need to be solved include the possibility of bias in algorithms and the difficulty of integrating AI and machine learning with current security infrastructure . One of the numerous challenges the Internet of Things faces is safeguarding user privacy and thwarting attacks like spoofing, denial of service (DoS), jamming, and eavesdropping. The Internet of Things connects a variety of things to networks to enable complex and intelligent applications.

The author investigates IoT system problems and potential solutions for IoT network security using machine learning methods like supervised learning, unsupervised learning, and reinforcement learning (RL). Security is an important aspect when we integrate the different technologies under the single management system. IoT gives us more secure world by using its innovative technologies. Security includes the security of homes, buildings, shops and car parking are now easy to manage with the help of IoT [11].

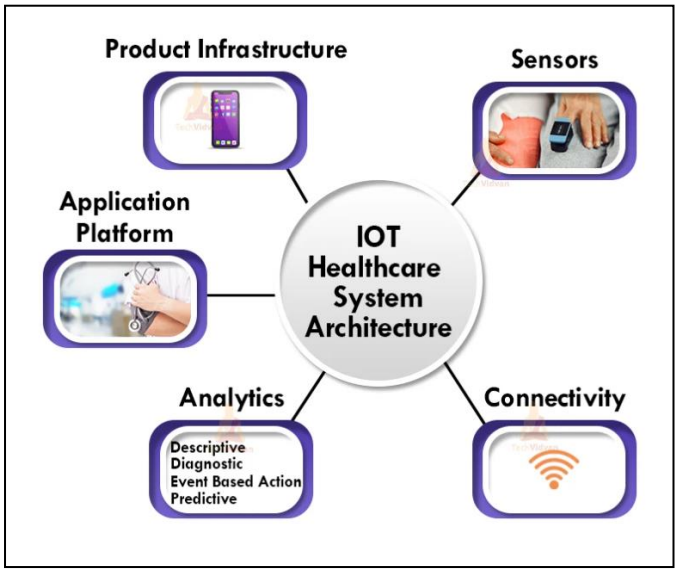
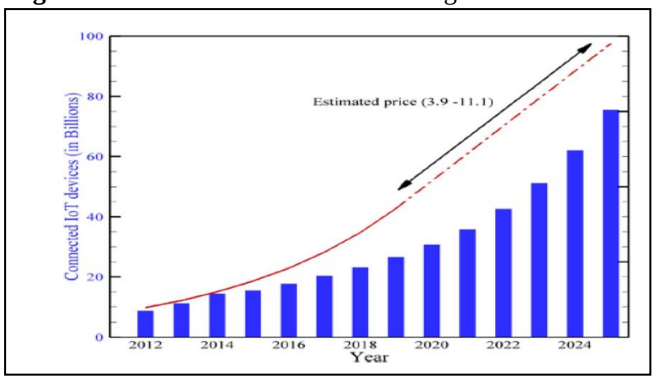


Fig -2: The IoT risk management model in healthcare [12].

The IoT is a technique to create intelligent surroundings, such as smart cities, healthcare systems, and building management systems. This is as a result of recent advancements. It also demonstrates how significant IoT applications can impact the economy and the market share they are anticipated to hold by 2025. Figure 3 shows the total number of connected devices with the IoT.

These smart environments' main objective, which has a big impact on business, society, and the economy, is to provide services based on intelligent techniques and sensor data enabled by the Internet of Things. According to a Statista research, there are about 25 billion IoT devices linked globally as of 2021, and this figure is projected to rise to 75 billion by 2025. According to a different MarketsandMarkets analysis, the size of the global IoT market is anticipated to increase from USD 622.6 billion in 2020 to USD 1,386.06 billion by 2026, at a compound yearly growth rate (CAGR) of 13.2% during the forecast period . The usage of cloud computing is growing, wireless networking technology is advancing, and the demand for real-time data analytics and predictive maintenance is rising. These and other factors are driving the growth of the IoT market. The COVID-19 epidemic has also sped up the adoption of IoT technology as businesses search for solutions to boost operational effectiveness and remote monitoring capabilities.

Fig -3: Total connected IoT devices and global IoT market so



far and future prediction [13].

The Internet of Things (IoT) market is anticipated to expand over the next few years as more businesses implement IoT solutions to boost productivity and gain a competitive edge. Furthermore, it is anticipated that the adoption of IoT devices and solutions would be further accelerated by technological advances like 5G, edge computing, and AI. But as the IoT market expands, security issues are also going to become more prevalent. To deal with these issues, efficient security protocols and solutions will need to be developed. Cloud computing is being used at an increasing rate. As a result, businesses can now store and handle massive amounts of data produced by IoT devices, which has stimulated the creation of new IoT applications and use cases. Organisations may extend their IoT projects more easily and affordably thanks to cloud computing. IoT device deployment in remote or difficult-to-reach places has been made possible by advancements in wireless networking technologies, such as 5G and LPWAN.

Faster speeds, greater bandwidth, and lower latency provided by these technologies are essential for enabling real-time communication and data sharing amongst IoT devices. Real-time data analytics and predictive maintenance are becoming more and more popular. The IoT market is primarily driven by the capacity to gather, store, and analyse data in real-time. Real-time data analytics empowers businesses to take quicker, more educated decisions, and predictive maintenance lengthens asset lifespans and minimises downtime. COVID-19 pandemic: As businesses sought to enhance remote monitoring capabilities and lessen the need for in-person interactions, the COVID-19 pandemic has pushed the adoption of IoT technology. For instance, remote patient health monitoring has been done using IoT devices like wearables and remote monitoring systems. Innovations in technologies like 5G, edge computing, and AI: Innovations in technologies like 5G, edge

computing, and AI are projected to accelerate the uptake of IoT products and services. For instance, edge computing and 5G offer real-time data processing and analysis at the network's edge while enabling quicker and more dependable connection between IoT devices. IoT devices generate a lot of data, which AI may be used to analyse and deliver insights that can be utilised to improve operations and decision-making.

3.METHODS OF IOT ATTACK AND SECURITY

3.1. Research Method

The use of AI and machine learning necessitated a thorough review of the literature using pertinent keywords and databases, the collection of data from a range of sources, including research papers, industry reports, and case studies, analysis using both qualitative and quantitative techniques, the use of case studies to demonstrate the application of these techniques, simulation to gauge their effectiveness, and the use of various tools and technologies, including programming.

The information gathered covered the many IoT system and device types, the threats and attacks these systems and devices faced, and the various AI and machine learning techniques employed for IoT security. Overall, this research paper employed a variety of techniques and resources to present a thorough review of IoT security issues and their AI and machine learning-based solutions.

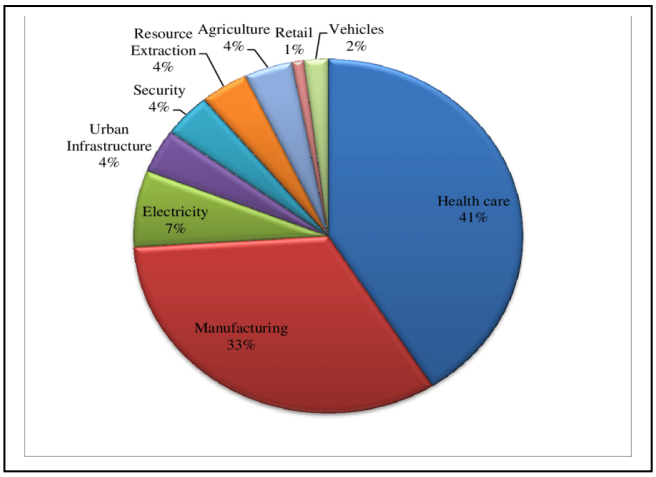


Fig -4: By 2025, what the main IoT applications could mean for the economy

3.2. Research Questions

The following are the study's research questions:

1.What are the principal IoT security issues and dangers that organisations are currently facing?

2.What are the most recent applications of AI and machine learning to these problems?

3.What are the IoT security performance KPIs for these AI and machine learning methods?

4.What are the most typical IoT device categories that are prone to security flaws?

5.What advantages and disadvantages do AI and machine learning have as tools for enhancing IoT security?

6. How can businesses strike a balance between the demands of IoT security, data privacy, and user convenience?

3.3. Initial reconnaissance

Initial reconnaissance is the first phase of a cyberattack, during which the attacker learns as much as possible about the target system and hunts for potential weaknesses. This can involve obtaining details about the system's software and hardware configuration, probing open ports to find out which services are active, and scanning the network to find connected devices [14].

Port scanners, vulnerability scanners, and social engineering techniques like phishing emails or pretexting are some of the tools and methods that attackers may use during the early reconnaissance phase. System administrators for the Internet of Things (IoT) must be aware of these technologies and approaches and take precautions to safeguard their networks from potential threats. The application processor should be installed in a tamper-resistant environment because it includes sensors, actuators, a power source, and communication. Hardware-based security can also be used for device authentication, enabling the device to demonstrate its authenticity to the server to which it is connected.

3.4. Physical Attacks

Physical access to devices or systems is required for physical attacks on IoT systems, which can range from device theft to physical manipulation with sensors or other parts. These assaults may lead to data theft, device manipulation, or service interruption. Theft, damage, or tampering with IoT equipment or sensors are just a few of the various physical attacks that might occur. For instance, a hacker could take an IoT device to access private information or tamper with sensors to change the information being gathered. In order to acquire private information or stop services, attackers may also try to physically modify the system.

Physical security measures, such as locks, security cameras, and access controls, should be put in place to avoid physical attacks on IoT equipment. In the event of a physical attack, data encryption and reliable authentication procedures can also help prevent data theft and modification [15].

3.5. False data injection attacks

False data injection attacks are a form of cyberattack that include tampering with data gathered by sensors or IoT devices to provide erroneous results. This kind of attack can have major repercussions, especially when the data acquired is utilised to make important decisions [16].

An IoT device or sensor may transmit data, and in a fake data injection attack, an attacker may intercept the stream and insert bogus data. Additionally, in order to produce false results, the attacker may modify the sensor's data collection. This may cause incorrect inferences to be made from the data, which may have major repercussions like inaccurate medical diagnoses or inaccurate readings in crucial infrastructure systems.

3.6. Denial of service attacks

Cyber attacks known as denial of service (DoS) attempts include flooding a network or system with traffic or requests in order to prevent legitimate users from accessing it. A DoS attack might target a single IoT device or a whole network of IoT

devices in the context of the internet of things. A DoS attack involves flooding an IoT device or network with a lot of traffic or requests, which makes the target device or network overloaded and unresponsive. Critical infrastructure systems may suffer severe effects as a result, including service interruptions and downtime for authorised users [17].

3.7. Architectures of IoT Systems and Security Issues

THE hardware components, such as sensors, and the cloud-based software platform and networking network. Although these elements offer a number of advantages, such as real-time data monitoring and analysis, they also raise security issues that need to be resolved in order to stop unauthorised access, data breaches, and other security threats. Device security is one of the main security issues, as IoT devices may be susceptible to cyberattacks because of weak passwords, out-of-date firmware, or other vulnerabilities. Implementing device authentication, encryption, access control, and intrusion detection is necessary to reduce this risk. Concerns about network security also exist since IoT networks may be exposed to a variety of security risks, including DoS attacks, man-in-the-middle attacks, and eavesdropping. To assist defend against these dangers, employ VPNs, firewalls, and encryption. Another issue is cloud security, as cloud-based IoT platforms may be open to virus infestations, data theft, and unauthorised access [18]. These dangers can be reduced with the aid of security measures like multi-factor authentication, data encryption, and routine security audits. Finally, IoT data analysis can use AI and machine learning to spot anomalies that could indicate security breaches. IoT system architects may develop reliable and secure IoT systems that offer users secure services by adopting a variety of security measures and utilising AI and machine learning approaches.

3.8. Security issues and architectural concerns.

IoT technology adoption has given rise to a number of security problems and architectural challenges. IoT devices' susceptibility to cyberattacks as they could not have the essential security safeguards to stop unauthorised access or data breaches is one of the main security concerns. These security worries can be reduced by implementing security features like multi-factor authentication, intrusion detection, encryption, and regular security audits. In addition, using AI and machine learning to analyse IoT data can aid in the detection of anomalies and the avoidance of security breaches. IoT systems can offer users secure and dependable services by adopting a thorough security policy and resolving architectural issues.

4.RESULTS

4.1. IoT Layered Architectures and Security Attacks

There isn't a single, universal IoT design that researchers and people throughout the world agree upon. Researchers have proposed a wide variety of architectures. Some academics claim that the IoT design has three layers, while others advocate for a four-layer architecture. They believe that the three-layer architecture cannot satisfy the needs of applications because of improvements in the IoT. The five-layer design has also been suggested as a solution to the security and privacy issue that the Internet of Things faces. It is believed that a

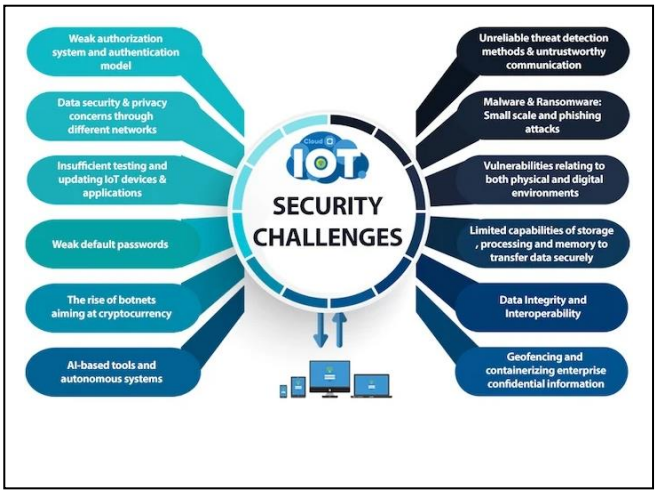


Fig -5: Security Challenges of IoT

recently proposed architecture can satisfy the IoT's security and privacy needs [19].

4.1.1. Three Layer Architecture

Its very simple architecture satisfies the IoT's core principles. When the Internet of Things was first being developed, it was proposed. It has three layers.

The names of these three layers are perception, network and application layer. The three-layer architecture, which consists of the perception or sensor layer, networking and data transfer layer, and middleware or support layer, is a frequently used design paradigm in IoT systems. Data is sensed from many sources, including sensors and actuators, and is converted into a digital signal that can be transferred over a network via the perception or sensing layer. By offering capabilities for intrusion detection, threat prediction, and risk assessment, AI and machine learning approaches can help in solving these security concerns. Some of the methods frequently utilised in IoT security solutions based on AI and ML include clustering, classification, regression, and rule-based algorithms.

Data transmission between the middleware layer and the perception layer is handled by the networking and data communication layer, which guarantees an effective and dependable data transfer. The processing and management of the data received from the perception layer, as well as the provision of services like storage, analytics, and security, are the responsibilities of the middleware or support layer. While the scalability, flexibility, and efficiency of this three-layer design are unquestionably advantageous, it also presents a number of security issues that must be resolved.

4.1.2. Perception Layer

The IoT system's perception layer is in charge of gathering data from sensors and gadgets. Vulnerabilities in the sensors or the communication protocols used to collect data can cause security problems at this tier. For instance, a hacker might attempt to use a sensor's vulnerability to access the data it gathers without authorization. By inserting bogus data or changing the sensor inputs, they might also try to tamper with the sensor readings. These sensors can gather data regarding position, changes in the atmosphere, the environment, motion, vibration, etc. However, attackers who want to use them to replace the sensor with their own are primarily after them.

4.1.3. Network Layer

The network layer in an IoT architecture is in charge of facilitating communication between IoT devices and a server or cloud. It deals with the transfer of data packets over several networking protocols, including as TCP/IP, ZigBee, Wi-Fi, LoRaWAN, etc., from the source device to the destination device. The network layer, however, has grown to be a

significant point of vulnerability in IoT systems as a result of the growing number of devices.

- Attacks against legitimate users of devices or other network resources are known as denial of service (DoS) attacks. In order to prevent some or all real users from using the targeted devices or network resources, it is often performed by flooding them with repetitive requests.

- MiTM (Main-in-the-Middle) Attack: A MITM attack occurs when the attacker deceives the sender and receiver into thinking they are speaking directly to one another by secretly intercepting and changing their communication. An attacker can alter messages to suit their needs because they have control over the communication.

- Attack using an exploit: An exploit is any immoral or unlawful attack using software, data chunks, or a series of commands. It makes use of security flaws in software, hardware, or operating systems. It typically arrives with the intent of taking over the machine and takes data saved on a network.

4.1.4. Application Layer

The uppermost layer in the IoT architecture, the application layer, is in charge of providing end users with services like data collection and processing, insight generation, and interfaces for control and interaction. The IoT apps and services are really installed at this layer, making it the one that end users can see the most [20].

Common security threats and problem of application layer are:

- An injection attack is cross-site scripting. It gives an attacker the ability to insert a client-side script, like java script, onto a reliable website that other users are seeing. An attacker can then totally alter the application's contents to suit his demands and use the original data in an unauthorised manner.

- Ability to handle Mass Data: Due to the sheer volume of devices and data being transferred between users, it is unable to handle the processing of data in accordance with the requirements.

4.2. Security Problems in the Sensing or Perception Layer

An IoT system's first layer, perception or sensing, is in charge of gathering data from sensors and other devices. The application layer, network layer, and perception layer make up the three layers of a typical Internet of Things design. However, as the significance of data processing and intelligent decision making increases, the support or middleware layer between the network and application levels becomes increasingly crucial. IoT systems may contain a number of levels, such as a network layer and a support layer. In various studies of IoT systems, cloud computing has been deployed as the foundational support layer.

The perception layer, also known as the sensing layer, is composed of numerous sensors and other devices. Limited computing, memory, storage, and communication resources are available at this layer. Node authentication, insecure encryption, and access control are the primary security measures this layer uses in an Internet of Things network. In the actual world, privacy invasions and crimes against the perceiving layer are all too common. Taking over a node is one method of carrying this out. Other methods include side-channel attacks, replay attacks, data injection, and malicious code usage. For instance, if a node is taken over by an attacker, it can stop providing legitimate network data and even stop using the IoT security programme.

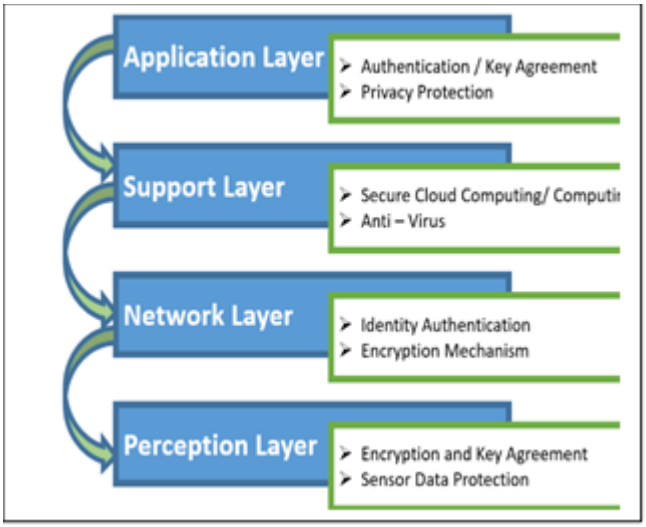


Fig -1: layers of IoT

4.2.1. Network And Data Communications Layer Security Problems An IoT system's networking and data communications layer is essential for transferring data between devices and applications. This layer is, however, extremely susceptible to a number of security problems. Man-in-the-middle attacks, which allow attackers to eavesdrop, change, or inject data by intercepting the data being transmitted between devices and apps, are a widespread problem.

Compatibility, privacy, and secrecy are the major objectives of this layer. Criminal activity, including as phishing, distributed denial-of-service assaults, attacks on data transit, routing attacks, identity authentication, and encryption, is anticipated to happen at this layer. These assaults have the potential to jeopardise system integrity and grant unauthorised access to private information. Another security flaw that attackers might use to collect and replay previously transmitted data and force devices or programmes to carry out undesirable or dangerous activities is replay attacks. Unauthorised access and data breaches can also result from spoofing attacks, in which attackers pretend to be an authorised device or programme.

4.2.2. Security Issues in the Middleware or Support Layer The middleware or support layer, which manages interactions between sensing and actuating devices and cloud servers, offers a variety of services, including data aggregation, filtering, processing, and communication with other devices. However, this layer is also prone to various security issues that can jeopardise the integrity and confidentiality of the system. The absence of procedures for access control and authentication in the middleware layer is one of the main issues. Unauthorised users have access to the middleware and can alter the data flow without sufficient authentication. Data loss, bogus data injection, and even denial-of-service attacks can result from this. Similar to how the absence of access control restrictions can give attackers access to the middleware and prevent the system from operating normally. The IoT system's middleware, also known as the support layer, is a significant component, and the security of this layer is essential to the system's overall security. The confidentiality, integrity, and availability of the data may be compromised by a number of security vulnerabilities caused by improper authentication, access control, encryption, and secure coding practises. Because of this, it is crucial to develop strong security methods to safeguard the middleware layer and guarantee the IoT system's smooth operation.

4.3. IoT Security Solutions Based on AI and ML

Artificial intelligence (AI) and machine learning (ML)-based IoT security solutions are gaining popularity because of their capacity to recognise and respond to threats in real-time. The ability of AI and ML to quickly analyse massive amounts of data and identify anomalies that could be signs of an attack is one of its main advantages. Additionally, these technologies can be used to strengthen data encryption, identify and stop cyberattacks, and improve access control systems.

Different methods, including anomaly detection, behaviour analysis, and predictive modelling, can be used by AI and ML-based security solutions. Finding peculiar patterns or behaviours that might point to an assault is known as anomaly detection. With the use of this technique, you can spot strange network activity, odd login patterns, and other peculiar behaviours that could be signs of an attack.

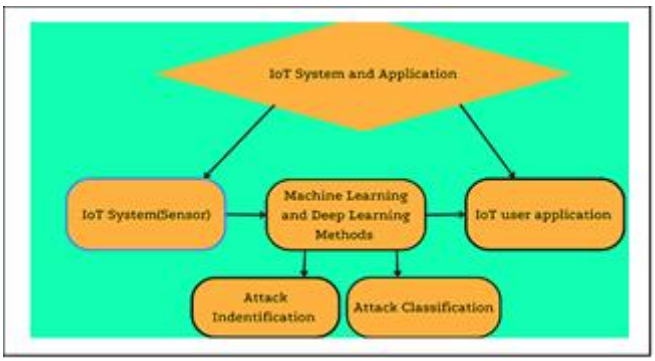


Fig -7: A machine learning security framework for IoT systems

4.3.1. Regression and Classification Techniques

One of the most popular machine learning methods for IoT security solutions is classification, followed by regression. To forecast the class or category of a new data point in classification, a model is trained on a labelled dataset.

This can be used to identify well-known security concerns and categorise fresh data as either safe or possibly dangerous. In regression, a model is trained on a collection of numerical values to forecast a continuous output variable. This can be used to identify anomalies or unusual behaviour in IoT devices or networks, which may point to a security compromise.

These are some examples of how these strategies are used.

1. The SVM classification approach monitors IoT devices for anomalous behaviour and Android malware to ensure the dependability of IoT services. 2. The random forest approach is used to identify anomalies, denial-of-service attacks, IoT invasions, and irregularities in smart cities.

3. A Naive-Bayes-based classification model and a linear-regression-based method for identifying

malicious IoT harmful nodes are two further techniques for discovering anomalies.

4.3.2. Clustering Methods

Without any prior knowledge of the groupings, clustering techniques can be used to group data points based on similarity or dissimilarity.

Clustering can be used to spot anomalies or outliers in network traffic or device behaviour in the context of IoT security. For instance, if it is discovered that a group of devices exhibits anomalous data traffic patterns in comparison to the rest of the network, this may point to a potential security risk. Clustering of system log data enables cybersecurity programmes to more quickly discover useful information or insight. By revealing previously hidden patterns and structures in IoT security data, clustering algorithms may be very useful in resolving IoT security concerns, such as recognising outliers, anomalies, signatures, fraud, and cyberattacks [21].

4.3.3. Rule-Based Approaches

Rule-based strategies entail formulating a set of guidelines that specify what to do in specific circumstances. These rules might be derived from professional knowledge or extracted from data using methods like association rule mining or decision tree induction. Rule-based strategies can be used in the context of IoT security to identify and address security threats in accordance with specified rules. For instance, if a sensor reading exceeds a specific threshold and signals a potential physical attack, a rule may be established to sound an alarm. To increase the precision and efficacy of security solutions, rule-based techniques can also be utilised in combination with other techniques, such as machine learning.

5.CONCLUSIONS

The Internet of Things (IoT) has revolutionized the way we interact with technology. The increased use of IoT devices has brought up important questions regarding the security of these devices and the data they handle, though. Effective security solutions are more important than ever as the number of IoT devices increases. In-depth study of the security issues IoT systems face and potential solutions using machine learning (ML) and artificial intelligence (AI) techniques have been provided in this research. IoT system architectures must be carefully examined, as well as the cyberattacks that can disassemble them layer by layer, in order to identify and safeguard IoT devices and systems. We looked into different machine learning and deep learning techniques that could be applied to enhance IoT security.Our study has demonstrated that AI and ML can significantly improve IoT security by enabling quicker threat detection and response as well as by offering predictive analytics for better risk management. The many AI and ML techniques discussed in this work, including classification, regression, clustering, and rule-based techniques, show their potential to handle a range of IoT security issues. The performance and efficacy of these procedures can be improved, but more research is necessary. Overall, this paper offers a thorough assessment of the current state of IoT security and the potential contribution of AI and ML to risk mitigation. In the future, we hope that other academics and practitioners will use our research on AI and ML-based security solutions to find and implement IoT security solutions.

REFERENCES

[1] Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 2019, 7, 82721–82743. [CrossRef]
[2] Slusarczyk, B. Industry 4.0: Are we ready? ´ Pol. J. Manag. Stud. 2018, 17, 232–248. [CrossRef]
[3] Ma, Z.; Xiao, M.; Xiao, Y.; Pang, Z.; Poor, H.V.; Vucetic, B. High-Reliability and Low-Latency Wireless Communication for Internet of Things: Challenges, Fundamentals, and Enabling Technologies. IEEE Internet Things J. 2019, 6, 7946–7970. [CrossRef]
[4] Li, S.; Xu, L.D.; Zhao, S. The internet of things: A survey. Inf. Syst. Front. 2015, 17, 243–259. [CrossRef] 16. Asim, M.; Arif, M.; Rafiq, M. Applications of Internet of Things in university libraries of Pakistan: An empirical investigation. J. Acad. Libr. 2022, 48, 102613. [CrossRef]

[5] Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Commun. Surv. Tutor. 2020, 22, 1686–1721. [CrossRef]
[6] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[7] Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Commun. Surv. Tutor. 2020, 22, 1686–1721. [CrossRef]
[8] Rawat, D.B.; Doku, R.; Garuba, M. Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security. IEEE Trans. Serv. Comput. 2019, 14, 2055–2072. [CrossRef]
[9] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," J. Clean. Prod., vol. 140, pp. 1454– 1464, 2017.
[10] A. Q. Gill, N. Phennel, D. Lane, and V. L. Phung, "IoTenabled emergency information supply chain architecture for elderly people: The Australian context," Inf. Syst., vol. 58, pp. 75–86, 2016
[11] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[12] Alshamrani, M. IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. J. King Saud Univ. Comput. Inf. Sci. 2021, 34, 4687–4701. [CrossRef]
[13] Tahsien, S.M.; Karimipour, H.; Spachos, P. Machine learning based solutions for security of Internet of Things (IoT): A survey. J. Netw. Comput. Appl. 2020, 161, 102630. [CrossRef]
[14] Woo S. The right security for IoT: physical attacks and how to counter them. In: Minj VP, editor. Proft From IoT. http://www.iot.electronicsforu .com/headlines/the-right-security-for-iot-physical-attacks-and-how-to-counter-them/. Accessed 13 June 2019.
[15] Akram H, Dimitri K, Mohammed M. A comprehensive iot attacks survey based on a building-blocked reference mode. Int J Adv Comput Sci Appl. 2018. https://doi.org/10.14569/IJACSA.2018.090349
[16] Mode G, Calyam P, Hoque K. False data injection attacks in Internet of Things and deep learning enabled predictive analytics; 2019.
[17] Herberger C. DDoS fre & forget: PDoS—a permanent denial of service. Radware Blog, Radware Ltd. http://www.blog.radware.com/secur ity/2015/10/ddos-fre-forget-pdos-a-permanent-denial-of-service/. Accessed 12 Sept 2016.
[18] Mendonça, R.V.; Silva, J.C.; Rosa, R.L.; Saadi, M.; Rodriguez, D.Z.; Farouk, A. A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms. Expert Syst. 2021, 39, e12917. [CrossRef]
[19] Deep, S.; Zheng, X.; Jolfaei, A.; Yu, D.; Ostovari, P.; Bashir, A.K. A survey of security and privacy issues in the Internet of Things from the layered context. Trans. Emerg. Telecommun. Technol. 2020, 33, e3935. [CrossRef]
[20] Yassein, M.B.; Shatnawi, M.Q. Application layer protocols for the Internet of Things: A survey. In Proceedings of the 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 22–24 September 2016; pp. 1–4.
[21] . Sarker, I.H. Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. Ann. Data Sci. 2022, 1–26. [CrossRef].