Journal of Computer Science

Review

A Comprehensive Survey on Applications, Challenges, Threats and Solutions in IoT Environment and Architecture

[1]Sadia Waheed, [2]Savera Hanif, [1]Rubab Hafeez, [3]Muhammad Imran Sharif,
[4]Kamran Siddique and [5]Zahid Akhtar

[1]*Department of Computer Science, University of Wah, Cantt, Pakistan*
[2]*Department of Computer Science, Comsats University of Islamabad, Abbottabad, Pakistan*
[3]*Department of Computer Science, Kansas State University, Manhattan, USA*
[4]*Department of Computer Science and Engineering, University of Alaska Anchorage, Anchorage, USA*
[5]*Department of Network and Computer Security, State University of New York Polytechnic Institute, Utica, USA*

Article history
Received: 05-10-2023
Revised: 06-11-2023
Accepted: 13-11-2023

Corresponding Author:
Muhammad Imran Sharif
Department of Computer Science,
Kansas State University,
Manhattan, USA
Email: imransharif@ksu.edu

Abstract: The influence of the Internet of Things (IoT) on how people live, interact and conduct business has rapidly increased. Integrating physical objects with electronic networking, or the Internet of Things (IoT), allows for better communication and environment detection. In coming years, higher service levels will be offered by IoT-based technologies, remarkably changing how people would conduct their daily lives. Currently, the number “things” (physical items) connected to the internet exceeds 9 billion. This number is expected quickly to reach around 20 billion. IoT applications in everyday life include smart wearables, smart health monitoring, traffic monitoring, IoT in agriculture with many sensors, smart devices, robots in hospitals, smart grid and water supply and so on. It can help make mobile phone control over homes and cities more intelligent. It provides personal protection as well as improved security. We save a great deal of time by automating tasks. Even when we are far from where we actually are, we can still conveniently get information because it is constantly updated. The internet of things truly has many applications, particularly when paired with other technologies like artificial intelligence and machine learning. This is especially true since it is now possible to put sensors in almost any item, resulting in the creation of a linked internet of things network. This is made possible by the dropping costs of hardware. IoT has numerous uses in supply chain management, manufacturing, smart energy production and wildlife conservation, among other areas. Perhaps, in the end, this growing number of IoT applications will result in a smart planet. Nonetheless, these technologies’ security flaws still cause problems for IoT-based data transmission. IoT inherits the common security problems associated with traditional networks because it is made up of a collection of networks and computing devices. IoT devices have also been vulnerable to other forms of exploitation and cyberattacks. This is because an environment with limited resources makes it difficult to adopt advanced cybersecurity safeguards. Hence, it is imperative to safeguard the entire internet of things architecture from potential vulnerabilities that could jeopardize the confidentiality, privacy and general integrity of the system. Lightweight security solutions are needed since IoT devices have limited resources and the traditional security processes are burdensome. Implementing security measures such as secure authentication, encryption and software upgrades is vital to addressing issues and making sure IoT systems and devices are operating safely and securely. IoT is an area where a lot of work is being done in terms of security and threats. Surveys on IoT security and risks currently available only focus on one aspect of security in IoT at a time. No survey addresses security risks in the architecture and ecosystem of the internet of things along with potential solutions. This survey gives a thorough analysis that addresses potential strategies to deal with security concerns and unites all security-related topics under one heading. It compiled each and every aspect of IoT including applications, Factors affecting security, challenges faced in achieving security along with all security

Science Publications

concern that has been raised and every potential fix. The study also answer the raising question why it is important to secure the network from external influence or attack.

Keywords: Internet of Things, Challenges in IoT, Privacy and Security, Insecure, Encryption

Introduction

The internet is widely used by people across the world nowadays. Its applications range from browsing to online applications like mail, music and video streaming. The emergence of the Internet of Things (IoT) is in the year of 1999. IoT started from the connection of a few computers and now it expands to the connection of billions of intelligent gadgets. The term Internet of Things (IoT) refers to a network of physical objects that are capable of connecting to other systems and devices via the internet and exchanging data with them. These objects have sensors, software and other technology that allow them to exchange data with other devices and systems via the Internet. By collecting and exchanging data automatically, IoT devices can perform operations and processes without the need for human intervention (Seth *et al*., 2021). IoT consists of a centralized architecture that helps in the exchange of information between connecting gadgets and the devices act accordingly to obtain the desired results. IoT is the current hot research topic that enhances the communication between devices and is of economic, social and technical significance. It defines the environment where smart gadgets are interconnected and managed remotely to exchange information with each other. This type of environment enables the connected gadgets so intelligent that they can listen, think talk and act smart in different situations. In IoT environment different technologies are developed such as radio frequency identification, machine to machine communication. Some of examples of smart devices are health care devices, smart watches, temperature sensors and smart locks, autonomous vehicles which have industrial and logistics applications.

Four Layer Architecture of Internet of Things

An architecture is a framework for describing the physical components of a network, their functional arrangement, configuration and the data formats that are utilized throughout its operation. The applications, commercial aspects and technologies employed all influence how the internet of things develops. If we talk about the architecture of IoT it is divides into three parts:

- The gadgets which are: RFID, BLE devices and sensors
- WLANs, cloud and WSNs: Communication network that connects the smart gadgets within an IoT environment
- Big data applications: Using computer systems for transferring information
- For IoT devices, different IoT architectures are available. However, the four-layered architecture is briefly defined in this study

Sensing Layer

Many sensors and actuators are employed at the perception layer to collect important data, such as temperature, moisture content, noises and intrusion detection. This layer’s primary job is to gather information from the environment and transfer it to another layer so that actions can be taken in response to that information. Some of the basic elements of first layer of IoT are:

- Sensors: For the detection of any changes or events within an IoT environment
- Actuators: Associated with controlling the system or a mechanism within a network
- Network: Responsible for the communication between the gadgets

Network Layer

The network layer of an IoT design is in charge of facilitating connectivity and communication amongst IoT system elements. It contains the technologies and protocols that let devices connect to and communicate with the internet as a whole as well as with one another. In the internet of things, popular network technologies include Wi-Fi, bluetooth, zigbee and cellular networks like 4 and 5G. The network layer may also contain security measures like authentication and encryption to guard against unwanted access, as well as gateways and routers that serve as middlemen between devices and the larger internet.

Middleware Layer

Advanced functions including storage, computing, processing and the ability to take action are available in the middleware layer. It stores the entire collection of data and provides the device with the relevant info based on its name and address. Decisions can also be made by it using computations performed on a set of data collected via sensors.

Application Layer

The topmost layer in an IoT design that communicates directly with the end user is called the application layer. It is in charge of offering functions and user-friendly interfaces that let consumers access and manage IoT devices. This layer consists of a variety of programmes and applications that are meant to communicate with the IoT infrastructure underneath, including web portals, smartphone apps and other user interfaces. Additionally, it has middleware services that facilitate easy data sharing and communication between various IoT systems and devices. In order to analyse data and turn it into insightful knowledge, the application layer also has processing and analytics tools. This can include tools for data visualisation, machine learning techniques and other advanced analytics features. The complete architecture is shown in Fig .1 Stergiou *et al*. (2018).

It is clear from the figure that IoT environment has mainly four layers (Stergiou *et al*., 2018). First layer includes the components such as actuators and sensors to receive data to perform different operations. The second layer is a network layer, which is concerned with the collected information. Third layer is the middleware layer; serve as a bridge between the application layer and a network layer. Most of the IoT applications are related to the third layer. Fourth layer contain many end-to-end applications.

In IoT networks, data is circulating between the connected devices, which are millions in number. The data transfer open to attacks helps intruders to steal the information and causes security threats. In 2017, there is an increase of about 600% attacks against the IoT gadgets. IoT devices seem to be the most attacking devices during the construction of IoT environment due to the fact that security and privacy is compromised over the usability, size and cost. Some of companies try to implement the secure environment because some vulnerable facts are exploited and become cause of loss to companies (Lally and Sgandurra, 2018). In some cases the devices are used as a firearm to target other websites but not attacked straight (Alabdulsalam *et al*., 2018). To reduce the effect of threats on IoT environments all the security requirements are need to be fulfilled. Basic concern of the study is to highlight the privacy and security issues within an IoT environment and discuss the possible solutions to overcome the security threats in IoT environment. As all the intelligent gadgets are connected to each other and require to communicate the information with each other, because of sharing information we can say that the issues related to security and privacy arises so the privacy may compromise. Due to these issues, the applications of IoT environment lose their significance.

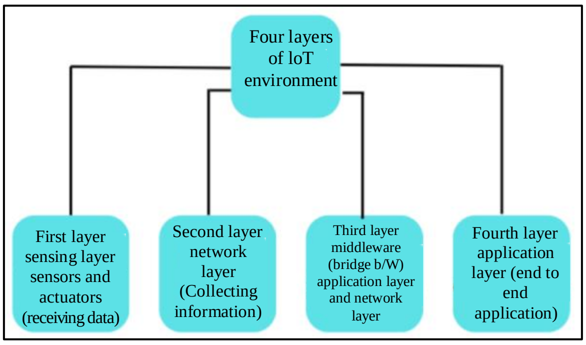
Four layers of loT environment
First layer sensing layer sensors and actuators (receiving data)
Second layer network layer (Collecting information)
Third layer middleware (bridge b/W) application layer and network layer
Fourth layer application layer (end to end application)

Fig. 1: Layered architecture of IoT

This survey examines every facet of security risks in the context of IoT environments and IoT architecture. It also discusses what measures should be taken to ensure that the importance of IoT applications remains uncompromised.

There exist many papers related to the security and privacy issue in IoT environment. I dedicate this section to various authors worked on the field of IoT security, which help the reader to shift to the new work within a field. In the field of IoT security most of the surveys are carried in 2018. Research related to the key management and hurdles within an IoT environment to achieve security related to IoT is discussed in Sicari *et al*. (2016) while other challenges such as integrity, privacy and confidentiality are discussed in Wu *et al*. (2017); Sicari *et al*. (2017).

Some papers discussed security issues in IoT environments. Some of the issues discussed in Sicari *et al*. (2016) are:

- The potential risk for the companies using smart gadgets increases due to the unauthorized access
- How the companies control and monitor these devices and the traffic generating as a result of the information changing between gadgets? One of the French studies reveals that there are 38 vulnerabilities including in IoT gadgets
- These vulnerabilities are deprived of security due to bad encryption techniques used to secure data. By the use of one weak link, thousands of IoT devices can be exposed. The data is automatically collected by the smart gadgets and send this information to the organization or a company
- How the company ensures the integrity of data received and is not manipulated by the unauthorized person during its transmission

In most of the study authors just discuss the challenges related to security without discussing their respective solutions (Joshitta and Arockiam, 2016). In decentralized structures of IoT (Vikas, 2015) discuss most of the security issues and their reimbursements. Security threats related to location-based services are discussed in Joshitta and Arockiam (2016). It is concerned with the problems related to the position of IoT gadgets. The security issue and protocols related to middleware layer are discussed in Chen *et al*. (2017). Other survey papers are related with IoT applications domains. Ngu *et al*. (2016); Dalipi and Yayilgan (2016) describes security challenges and cyber-attacks in smart grids. Donohoe *et al*. (2015) Provides health care applications and industrial IoT applications. Attacks and vulnerabilities are discussed in Liu *et al*. (2015). The development of RFID, communication technologies and a large body of recent scientific literature on wireless sensor networks all indicate to the viability of IoT at different levels of design. However, because these technologies were created from the standpoint of the traditional internet, they must be modified to account for new IoT dimensions of resource efficiency, scalability, security and privacy (Atzori *et al*., 2010). The term "Web of Things" (WoT) was created as a result of the Web's integration of sensors and intelligent devices. Here, the emphasis is mainly on creating apps employing web technologies and intelligent objects (Guinard *et al*., 2010) and representing things on the Web. Some surveys deal with the security issues as well as their promising solutions. In Alaba *et al*. (2017) author investigates about access control and confidentiality and privacy solutions in IoT. However, access control solutions are reviewed by Ouaddah *et al*. (2017) in all the above-mentioned surveys author emphasis on cryptographic approaches without related them to the latest technologies, which are relevant to security measures. Nguyen *et al*. (2015) Different security management techniques such as Network Function Virtualization (NFV) Software Defined Networking (SDN) are discussed. The comparison of cloud computing with edge computing to secure IoT networks is defined in Farris *et al*. (2018). Security vulnerabilities regarding personal IoT environment are discussed in such as smart locks and IP cameras (Yu *et al*., 2017). Some Software Defined Network (SDN) technologies are introduced to cope with security challenges occur within an IoT environment. Such solutions are inexpensive and reduce the hardware. The main idea of SDN is to separate the data plan from the control plan (Yu *et al*., 2017). In Kaur *et al*. (2023) put efforts to compile and contrast intrusion detection system architectures, datasets and machine learning techniques for IoT devices. Author categorize attacks on IoT devices according to various layers and protocols. Research done on IoT devices so far, deals with the present state of the of IoT networks. The purpose of the paper is therefore to summarize the applications and uses of IoT also previous studies on Iot security and privacy challenges and the challenges faced on layered level. Some of the solutions In IoT are also being discussed in this survey.

Applications of IoT

Applications for the Internet of Things (IoT) shown in Fig. 2 span a wide range of industries and are revolutionizing them because of their connection and data-driven capabilities. The way we connect with our environment and systems is changing thanks to IoT technologies, which range from smart homes that increase comfort and security to industrial IoT that optimizes manufacturing processes and healthcare IoT that improves patient care.

Each application mentioned in a figure is explained in detail.

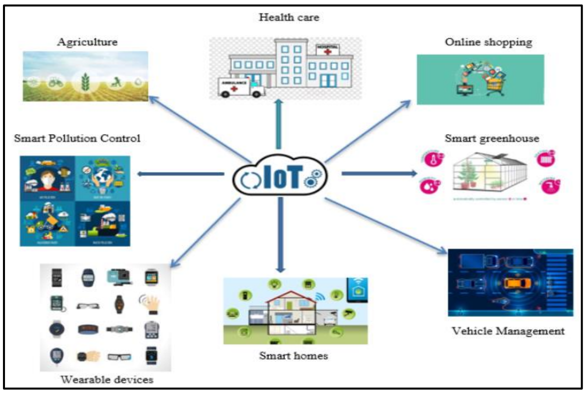

Fig. 2: Applications of IoT

Health Care Applications

Doctors may monitor patients remotely through a network of connected instruments and gadgets without having to be near them thanks to a variety of IoT applications in the healthcare sector. This is especially helpful if the patients do not have any major issues or if they currently have infectious disorders like COVID-19. Robotics is one of the most popular applications of IoT in healthcare. Surgical robots are one such example of how they can assist physicians in carrying out surgery with greater efficiency, control and precision. Additionally, there are disinfection robots that use high-intensity UV light-which is quite helpful these days-to swiftly and completely clean surfaces. Other kinds of robots include nursing robots, which are designed to carry out repetitive duties for numerous patients on a daily basis with minimal harm to the patients.

Smart Home

Smart home applications are the most well-known use of IoT. Who has not heard of the idea of combining all of your household appliances-lighting, air conditioning, locks, thermostats, etc., into a single, smartphone e-controlled system? These days, Internet of Things (IoT) gadgets are growing in popularity because they provide you total control over how you want to customize your house. In fact, there are 127 new IoT devices connecting to the internet every second due to their popularity. A few well-known ones that you may have heard of or perhaps own in your house include the philips hue lighting system, google home and amazon echo plus. You can put a variety of amazing products in your house, such as the August smart lock, foobot air quality monitor, nest smoke alarm and thermostat and more.

Smart City

Cities can be made more resource- and energy-efficient by improving their efficiency. This can be accomplished by utilising a variety of sensors located around the city in various capacities. These sensors can be utilised for a number of purposes, such as traffic management, waste management control, developing smart buildings, streetlight optimisation and more. Numerous global cities, including Singapore, Geneva, Zurich, Oslo and many more, are attempting to integrate IoT and become smarter. Singapore, which is regarded as the world's smartest city, uses the smart nation sensor platform as an example of how to create smart cities. This platform uses sensors in conjunction with IoT to integrate many aspects of public safety, transit, streetlights, urban planning, etc.,

Wearable Devices

Wearable devices that are IoT-enabled, such as smartwatches and fitness trackers, can monitor the user's health and activity levels. These devices can track various metrics such as heart rate, steps taken and calories burned. This data can be used to enhance the user's fitness and overall health (Rahmani *et al*., 2022; Bello and Figetakis, 2023).

Military

With regard to military applications, IoT technology's networked sensors and digital analytic can be leveraged to track supplies and equipment from point of origin to point of need on the battlefield (Gotarane and Raskar, 2019). Integrating sensors and devices into military installations can have a number of advantages. For instance, automated security screening reduces risks while increasing safety. A network of security cameras linked to a central network through the internet and to their surroundings through sensors would also reduce security threats. Effective resource management, such as the use of water and energy, may boost a military base's productivity and capability while guaranteeing the safety of every person residing there. By utilising information from a variety of military platforms, such as planes, weaponry, armoured vehicles and soldiers, the military can improve the efficiency of its intelligence, surveillance and reconnaissance systems. The military forces will be able to recognize major threats more quickly and accurately because to this abundance of information.

Fast Response Against Emergencies

For emergency response services to react swiftly to natural disasters like hurricanes, earthquakes and floods, they must always be on guard. Both wealthy countries and smart cities use technology to anticipate these kinds of events and prepare for them. Firefighters, rescue workers and paramedics can quickly address any kind of scenario with the use of internet of things technologies. In order to achieve this, innovative IoT-enabled emergency response solutions-including flood monitoring-are created by startups and scale ups.

Online Shopping

Retailers cannot ignore the ways in which IoT is transforming the retail industry. To get an advantage over their rivals, offline retailers are coming up with innovative ways to use IoT in e commerce. They have moved to more practical platforms, revolutionising the world of purchasing.

Retailers, for example, are already utilizing internet-connected devices by putting sensors in place to monitor client behaviour or inventory levels. In the retail industry, internet retailers currently hold a significant advantage over traditional brick and mortar establishments.

They can execute smarter marketing plans across all of their stores and make better judgements thanks to IoT. Additionally, customer assistance is more individualised and effective. Retailers now have a more streamlined and transparent supply chain thanks to technology.

Smart Pollution Control

One of the main issues facing most cities worldwide is pollution. It is unclear at times, whether we are breathing in smog or oxygen! IoT can significantly aid in bringing pollution levels down to more bearable levels in such a scenario. This can be achieved by using a variety of sensors in conjunction with the internet of things to gather data on city pollution, such as car emissions, pollen levels, airflow direction, weather, traffic volumes etc., by using this data, machine learning algorithms can estimate pollution levels in various parts of the city, alerting officials to potential issue regions in advance. After that, they can work to reduce pollution till a much safer environment. IBM's China research lab's green horizons initiative serves as an illustration of this.

Standard Production Quality

IIoT builds a network of connected devices and systems to increase productivity and save costs in industries. Through AI integration, predictive maintenance and lean manufacturing, IoT increases production efficiency.

By integrating internal systems with physical processes, the Industrial Internet of Things (IIoT) technology allows for complete visibility into production activities. Systems that are directly linked to one another operate more efficiently and quickly, with almost no downtime, from pre-production to client delivery. Thanks to the sector, the benefits of IIoT are increasing the value of what is predicted.

Agriculture

Using IoT in agriculture can also aid in resolving a number of global problems. UN estimates state that by 2050, agricultural production will need to increase by 200% in order to feed the planet's expanding population. New IoT applications for the agriculture sector are constantly emerging and smart agriculture products and solutions are becoming more and more popular (Xu *et al*., 2022). Every element of greenhouse operations, including air humidity, pest management, lighting, irrigation and fertilization, can be managed by IoT sensors. By doing this, there is a far greater possibility that any changes will be promptly identified and corrected, maintaining ideal plant growth circumstances and guaranteeing good harvests. Convenient dashboards are offered by programmes like farmapp to monitor all the data centrally. Farmers may collect individual data on each animal's diet, blood pressure, temperature, location and a host of other aspects using livestock collars equipped with smart sensors. This makes it simple to keep an eye on the herd, rapidly identify and isolate animals who have a fever from the rest of the herd, find stray sheep or cows in case they become lost and maximise all other areas of dairy production. One example of an internet of things system that collects data and sends it to the cloud is cowlar. Every farm needs a wide range of equipment, including solar panels, engines and water pumps. All of this equipment needs to be maintained since major losses could result from any system failure during harvest season. By utilising IoT technology to facilitate preventive maintenance, farmers may maximise equipment service cycles and avert unplanned system breakdowns.

Power Saving

Building automation systems with IoT capabilities keep an eye on and manage energy users like Heating Ventilation and Air Conditioning (HVAC) systems. By adapting systems to the needs of building users, they aid in energy usage optimisation. Preventing energy loss from ineffective heating or cooling systems is the goal. IoT sensors can also keep an eye on how frequently offices and conference rooms are used. Thus, resources like heating, air conditioning and lighting can be automatically adjusted to actual use, time of day and human presence. IoT-based meteorological forecasts help even more with system optimization.

Autonomous Vehicles

IIoT is a major component of self-driving automobiles, or smart cars, as they are some times known. These cars include a number of integrated features, such navigational sensors, several antennas, speed and slow-down controls, etc., that interact with one another and require communication. The internet of things is essential in this situation, particularly because self-driving cars must be incredibly precise and all of their components must interact with one another in milliseconds while travelling. Tesla motors is developing self-driving automobiles and is a very popular car. The newest developments in artificial intelligence and the internet of things are incorporated into tesla motors vehicles. They are also quite well-liked. The IoT has the potential to revolutionize the automobile industry, while the automobile industry will provide a major boost to the IoT. The prospects for this technology are truly astonishing (Pourrahmani *et al.*, 2022). In order to reduce latency in the internet of Vehicles, SDN-based multi-mediator method based on the CCN was presented. To improve the routing flexibility and heterogeneous device interoperability in an IoV network, an SDN-based controller was used. To maximize network resources, clusters can be formed using a multi-mediator system (Sharif *et al.*, 2023a). A workable plan was put up to lower the response time of traffic control services by utilising heterogeneous network access to enable real-time content distribution in Internet of Vehicles (IoV) systems (Sharif *et al.*, 2023b).

Factors Causing Security Issues

Number of Connected Gadgets

IoT by definition makes networks more vulnerable to hackers. This is due to the fact that it entails linking numerous things or products to the internet that were not before connected to a network. For instance, IoT sensors are connected to factory floor gear by manufacturing enterprises and smart home appliances like light switches, doorbell cameras and thermostats are bought by consumers. Innovation also introduces a new vulnerability. Every linked device, including fitness trackers and subterranean temperature sensors, creates an additional point of entry for hackers, who may use them to take down entire networks. IoT security addresses the unique problems associated with IoT installations in an effort to safeguard devices and networks. However, it's not simple to make sure IoT devices have strong security. A large number of devices are connected and communicating in a difficult way (Sfar *et al.*, 2018). These large number of devices producing a large amount of data which is difficult to handle. Many other problem statements are associated with the aforementioned issue such as:

- How to preserve data privacy and integrity
- How to manage the access control mechanisms
- How to locate the gadgets within a system

Quality of Service

The Internet of Things (IoT) presents challenges for Quality of Service (QoS) due to several factors, such as:

- Network and device heterogeneity: IoT devices come in a wide variety, from basic sensors to intricate actuators. They can also make use of a variety of network technologies, including cellular, bluetooth and Wi-Fi. It is challenging to guarantee constant QoS across all devices and networks due to this diversity
- Restraints on resources: A lot of internet of things devices have restricted resources, such as low memory, processing speed and battery life. Because of this, enforcing and implementing QoS requirements is challenging

- Conditions of a dynamic network: Internet of things devices frequently function in networks that are unexpected and dynamic. Variations in QoS, including delay, jitter and packet loss may result from this

Emerging Technologies and Standards

One of the major challenges in IoT is emerging technologies and standards define for IoT architecture (Čolaković and Hadžialić 2018). Emerging technologies effect the security in following ways: Lack of standardisation: Standards and emerging technologies are frequently not standardised yet, which can cause incompatibility and fragmentation. Because of this, creating and implementing security solutions that function on a variety of platforms and networks is challenging:

- Complexity: It might be challenging to comprehend and securely apply emerging technologies and standards due to their complexity. New network protocols, for instance, might bring along fresh vulnerabilities that call for mitigation
- Quick innovation: As new standards and technologies emerge, it can be challenging for security experts to stay on top of the most recent risks and weaknesses

IoT security is threatened by new standards and technologies in the following specific ways.

Over earlier iterations of cellular technology, 5G networks offer considerable performance and capacity gains. New security issues, such as an expanded attack surface and the possibility of novel sorts of attacks, are nevertheless brought about by 5G.

Edge computing moves storage and processing closer to the devices that produce and use data. For many IoT applications, this can lower latency and increase performance. Edge computing does, however, also provide new security challenges, such as the requirement for edge device and data protection.

Machine Learning (ML) and Artificial Intelligence (AI) are two concepts that are being utilised more and more in internet of things applications to enhance functionality and automate processes. Nevertheless, adversarial attacks against AI and ML models have the potential to disrupt internet of things systems.

Limited Resources

Due to lack of resources such as storage capacities, bandwidth, power and microprocessors, it is difficult to apply encryption algorithm while maintaining the cost in a network (Shamala *et al*., 2021). There are several ways in which having limited resources might make establishing IoT security difficult:

- Hardware limitations: IoT devices frequently have low amounts of RAM, computing power and storage. As a result, implementing and enforcing security measures like intrusion detection, authentication and encryption is challenging
- Software complexity: A multitude of open-source and third party components are frequently used in the complicated software that IoT devices operate. This makes it challenging to find and fix vulnerabilities
- Lack of knowledge: A lot of companies using IoT devices lack the internal knowledge necessary to create and put into practice efficient security measures
- Cost: Security solutions can be pricey and businesses are hesitant to spend money on IoT device security, especially if the devices are inexpensive

Security Threats

IoT network security concerns provide difficulties for a variety of reasons, such as:

- The enormous variety and quantity of IoT device: The internet is home to billions of Internet of Things (IoT) devices, ranging in complexity from basic industrial control systems to simple sensors. Because of this diversity, it is challenging to create and install security solutions that can successfully safeguard all kinds of internet of things devices
- The internet of things' intricacy: IoT networks are frequently dispersed and complicated, with devices linked to several networks and placed in various physical places. Because of this intricacy, it could be challenging to find and fix security flaws
- The many IoT devices' inadequate security features: The low cost and energy efficiency of many IoT devices can restrict their security capabilities. For instance, a lot of internet of things devices are devoid of security features like authentication and encryption
- Threats: Threats such as denial of service, resource constraints, Trojan horses, worms and viruses make it difficult to attain optimal security (Cihan and Akleylek, 2019).

Mobility

Because mobile IoT devices are always moving and connecting to new networks, mobility presents a barrier to ensuring IoT security (Cihan and Akleylek, 2019). This makes it challenging to monitor and track these devices and put in place reliable security measures.

The following are some particular difficulties that mobility presents for IoT security:

- Visibility of devices: Keeping tabs on mobile IoT devices can be challenging, particularly when they are switching across networks. The inability to see security dangers might make it challenging to recognize and counter them

- Authentication of devices: Authenticating mobile IoT devices can be difficult, particularly when they are connecting to unfamiliar networks. This is because mobile Conventional authentication techniques like passwords and certificates are not always compatible with IoT devices
- Data safety: Sensitive data, including location data and personal information, is frequently transmitted by mobile IoT devices. It is necessary to safeguard this data against illegal access and interception
- Safety of networks: Public Wi-Fi networks are among the many networks that mobile IoT devices can connect to. These networks might not be safe and hackers could use them to access mobile IoT networks and devices

Change in Network Topology

The major change of topology is due to mobility. There is often change in topology as the devices rise in lively surrounding (Chen *et al*., 2017). Changes in network topology pose several challenges to the security of IoT devices:

- A larger surface for attacks: Attackers can exploit new attack vectors caused by changes in network configuration or device status
- Diminished visibility: Tracking and keeping an eye on every device on the network is more challenging when the topology of the network changes. As a result, it could be challenging to recognize and address security issues
- A rise in complexity: Network topology changes have the potential to increase network complexity, which could make it harder to secure and maintain
- Decreased effectiveness: Network performance can be affected by changes in topology, which make it more challenging to provide users with services

The following are particular instances of how modifications to network topology pose a threat to IoT security.

A newly connected device is not adequately secured or setup. This increases the device's susceptibility to attacks and opens up a fresh point of attack for hackers to take advantage of. It's possible that a device wasn't fully decommissioned when it was withdrawn from the network. This makes the gadget more open to assault and provides hackers continued access to the network. Modifying the network's configuration results in the addition of new security holes. For instance, introducing a new firewall rule or altering the subnet mask could leave the network vulnerable to attack. A new network segment increases the attack surface and complicates network security and monitoring. Modifying the routing topology affects the network's performance and opens up fresh attack avenues for hackers to take advantage of.

Cloud Computing Risks

Organization of IoT is take place by cloud computing and some security risks are associated with cloud computing. The risks associated with cloud computing can impact IoT security in several ways, such as:

- Breaches of data: Cloud computing services hold a lot of data, including private information from internet of things devices. Attackers might be able to obtain this data if a cloud computing provider is compromised, which could have detrimental effects on IoT security
- Misconfigurations: Many services are provided by cloud computing providers and setting them all up correctly is challenging. Attackers can take advantage of security vulnerabilities caused by misconfigurations
- Insecure APIs: Developers can access cloud computing companies' services through APIs. Attackers might use these APIs, nevertheless, if they are not well secured, to access data or cloud services
- Shared technical resources: Cloud computing companies rent out their infrastructure to several clients. This implies that additional customers are impacted in the event of a security breach in one customer's account
- Insider threats: Many people are employed by cloud computing providers. Some of these workers might be compromised by attackers unintentionally, or they might have malicious intent

Security Challenges

Major cause of security challenge is the wide distribution of smart devices across the network and the type of data that is transferred. Some of security challenges are.

Authentication

Ensuring the authenticity of the data origin node and routing peers involved in data transmission is a crucial task (Yang *et al*., 2016). Authentication poses a challenge in terms of key handling and deployment. Cryptographic key generation and distribution can be used effectively for this purpose, without adding any overhead on the nodes (Bertino *et al*., 2016). Authentication is a crucial process that involves confirming a user or device's identity. In the context of IoT, it is extremely important to authenticate devices and data to prevent unauthorized access. However, several security issues can make it challenging to authenticate IoT devices securely. Access control is providing access to only authorized parties or devices (Yang *et al*., 2017). IoT nodes employ various access control protocols, which may differ from those of other networked devices (Li *et al*., 2017). In a heterogeneous IoT environment management and installment of different access control mechanisms is a challenging task (Lopez *et al*., 2017). Some of the most common security issues in IoT authentication include (Tawalbeh *et al*., 2020):

- Weak authentication and authorization: IoT devices often have weak authentication and authorization mechanisms, which make it easy for attackers to gain unauthorized access. For instance, devices might use default or easily guessable passwords
- Connectivity: IoT devices commonly use insecure internet channels for communication, allowing attackers to intercept and modify data in transit
- Insecure data storage: IoT devices often store sensitive data insecurely, such as unencrypted or on non-volatile memory, leaving it vulnerable to theft by attackers
- Lack of security updates: IoT devices are often vulnerable to known exploits due to infrequent security updates.
- Malicious insiders: Authorized users with access to IoT devices pose a security risk. They could misuse their access to gain unauthorized data or device access

Privacy

In IoT environment installment of autonomous gadgets that senses the people important information introduces a new threat in a network. People’s important data is collected by the connecting IoT gadgets without their knowledge (Kouicem *et al*., 2018). So, privacy is also a challenge in IoT network especially in heterogeneous IoT environments. Some of the challenges facing in privacy are (Nalajala *et al*., 2019):

- Data collection and storage: Internet of Things (IoT) devices gather vast amounts of data, which contain sensitive and personal information. This data can be stored locally on the devices, in the cloud, or both. If the data is not adequately secured, unauthorized individuals are able to access it
- Data exchange: IoT devices frequently exchange data with other gadgets, programmes and services. This information might be distributed without the user’s knowledge or permission
- Tracking and surveillance: IoT devices can be used for tracking and surveillance, which allows for the observation of people’s whereabouts and activities. This might be applied maliciously, like in stalking or discrimination
- Data misuse: The data generated by IoT devices can be misused by individuals or organizations for illegal purposes such as fraud or marketing

Availability

Availability ensures that the system works properly even in the worse situations. Which is quiet challenging because of presence of large number of IoT gadgets (Kouicem *et al*., 2018). Some of the challenges faced in achieving availability are (Sattar and Al-Omary, 2021; Thilakarathne *et al*., 2020):

- Denial-of-Service (DoS) attacks: By saturating IoT devices with traffic or overtaxing them with requests, DoS attacks try to render them inoperable
- Malware attacks: These can seize control of IoT devices, render them inaccessible, or even cause them to harm people or property
- Physical attacks: Physical assaults can harm or even destroy IoT devices, rendering them useless
- Human errors: Availability problems can also result from human error, such as configuration mistakes or misconfigurations

Integrity

Reliable information is needed for any industrial processes to prevent any type of harm to industry. So, there is a need to preserve the important information while exchange of information between the IoT gadgets within a system. Ensuring integrity can lead to certain security challenges such as received data by the devices considered to be true while it is not. Data is not changed during the transmission by intruder intentionally or accidently. Data is transferred among different devices so to keep track of all the data by each device is a challenging task:

- Data tampering: IoT devices collect and process a lot of data, which can be tampered with by attackers. This could lead to inaccurate or misleading information being used to make decisions (Alabdulsalam *et al*., 2018)
- Man in the middle attacks: In a man in the middle attack, an attacker intercepts and modifies data as it is being transmitted between two devices. This can be used to alter the integrity of the data
- Firmware attacks: Firmware is the software that controls the operation of an IoT device. Firmware attacks can be used to modify the firmware and change the way the device operates. This could be used to disable the device or make it do something malicious

Confidentiality and Non-Repudiation

The secret and sensitive data is needed to be prevented by securing the whole system which includes the code, data and all configurations. Information is ambiguous to unauthorized access is confidentiality and non-repudiation is that the sender would not deny that the message is not send by corresponding entity:

- Confidentiality: Confidentiality refers to the ability to keep data private and prevent unauthorized access, such as protecting personal information, financial data, or intellectual property in the context of IoT. IoT devices often collect and transmit sensitive data, such as trade secrets and financial and personal information, which poses a significant challenge to confidentiality. Fraud, identity theft and other crimes can be perpetrated by attackers using this data.

- Non-repudiation: Non-repudiation is the ability to demonstrate that a specific individual or device performed a particular action. In the realm of IoT, this can refer to proving that a device transmitted a specific message or that a user conducted a particular transaction. Non-repudiation is a challenge for IoT devices, as they can be easily hijacked to deliver harmful messages or transactions. An attacker might take control of an Internet of Things device and use it to transmit a fraudulent order to a financial institution

Secure Architecture

The strong IoT architecture is needed to be build that not only overcome the aforementioned security challenges but also deal with the challenges that cause during deployment of IoT gadgets over cloud infrastructure and Software Defined Network (SDN) (Plageras *et al*., 2018; Maple, 2017):

- Weak security features in IoT devices: Default passwords, insecure firmware and inadequate authentication and authorization processes are just a few examples of the lax security features that are frequently built into IoT devices. Because of this, they are more susceptible to attacks such malware infection, unauthorized access and Denial-of-Service (DoS) attacks
- Insecure communication channels: IoT devices frequently communicate across unreliable networks like the internet. Because of this vulnerability, they are
- at risk of being targeted by man in the middle and data tampering attacks (Khan *et al*., 2022)
- Lack of awareness and training: Users and managers of IoT devices frequently are not aware of the security risks that are there. This could lead to mistakes that leave the devices vulnerable to attack
- Complexity of the IoT ecosystem: The industry struggles to adopt newer internet protocols while maintaining backward compatibility, which makes the underlying complexity of IoT frameworks quite difficult and makes it challenging to secure (Seth *et al*., 2021)

How to Overcome Security Challenges in IoT Environment

Encryption

The process of transforming data into a format that cannot be read by anybody without the right decryption key is called encryption. Sensitive data, including financial and personal information as well as intellectual property, is protected by encryption. Data access that is being transmitted or stored IoT networks should be prevented via encryption to stop illegal access. But it also offers protection from other dangers.

One of the best methods for IoT data protection is encryption. Data can be encrypted while it's being utilized, in transit and at rest. Encrypting data while it is kept in a cloud database or on an IoT device is known as encrypting data at rest. If unauthorized users manage to breach the device or database, this stops them from accessing the data. When data is being sent between internet of things devices or between an IoT device and a cloud server, it is referred to as encrypted data in transit. If unauthorized people can monitor network traffic, this stops them from intercepting the data. Encrypting data in use refers to doing so while an internet of things device is processing the data. If unauthorized users manage to breach the device, this stops them from accessing the data.

Here's an illustration of how to use encryption to protect an internet of things network. IoT sensors are used by a company to keep an eye on the humidity and temperature in its warehouses. The sensors send the information to a cloud-based platform, which uses it to produce reports and alarms. The organization employs encryption to safeguard both the data saved on the cloud platform and the data sent between the sensors and the platform. If an attacker gains access to an encrypted device, they will not be able to read the data without the encryption key. This contributes to maintaining the data's integrity and preventing access by unauthorized parties.

Reliable Systems for Authentication and Permission

A reliable system for authorization and authentication can precisely and consistently confirm a user's identity and provide them with the necessary authorizations to utilize resources. Preventing unauthorized access to sensitive data and systems is crucial.

The use of strong authentication and authorization systems, such as Multi-Factor Authentication (MFA), is essential to ensuring the security of IoT devices. For example, IoT sensors and devices are used by hospitals to track patients' records, monitor their vital signs and give prescriptions. To guarantee that only those with permission can access the IoT network and devices, the hospital employs a MFA. Through the use of two or more authentication factors, such as a password and a one-time code produced by a mobile app, MFA provides an additional layer of security. To guarantee that staff members only have the authorization required to carry out their duties, the hospital also employs a permission system. For instance, doctors can examine all patient data and modify prescription regimens, while nurses are restricted to viewing vital signs and administering medication.

The hospital contributes to preventing unwanted access to the internet of things network and devices, enforcing least privilege and enabling audibility by utilizing trustworthy mechanisms for authentication and permission. In addition to ensuring the security and dependability of the IoT network, this serves to protect patient privacy and safety. Hospitals assist in improving the security of their networks and shielding their data from insider threats, unauthorized access and other dangers by implementing trustworthy mechanisms for authentication and permission in IoT networks.

In general, the environment's security can be greatly increased by utilising trustworthy permission and authentication systems, such as Multi-Factor Authentication (MFA), in IoT networks. MFA can assist organisations in safeguarding their data and assets against a range of security threats by making it more difficult for attackers to access the network, guarding against insider threats and adhering to regulatory requirements.

Digital Signatures

Data and communication validity can be confirmed via digital signatures, guarding against manipulation and non-repudiation attacks. A mathematical system used to prove the legitimacy of a digital message or document is called a digital signature. To prevent unauthorized access, alteration, or forging of electronic documents, digital signatures serve as virtual signatures. Digital signatures are individual to the signer and serve the same purpose as traditional handwritten signatures in terms of document authenticity verification. Public key cryptography, which employs a public key and a private key that are mathematically connected, is the foundation of digital signatures. The data is encrypted using the public key and decrypted using the private key. The signer encrypts a hash of the document with their private key to form a digital signature. A document's hash serves as its own digital fingerprint and any modifications to the document will produce a new hash. The digital signature and hash are then sent to the recipient by the signer. Subsequently, the recipient can validate the document's hash and decrypt the digital signature using the signer's public key. The recipient can be sure that the document is from the intended sender and has not been altered if the two hashes match.

Before allowing a device or user access to the internet of things network or its resources, digital signatures can be employed to authenticate the latter. This aids in preventing sensitive data on the network and from being accessed by unauthorized parties. The integrity of data transferred between devices on an IoT network can be guaranteed with the use of digital signatures. This helps to guarantee that the data is received exactly as it was transmitted and stops hackers from altering it while it is in route. The non-repudiation feature of digital signatures ensures that the sender of a message cannot retract their signature. This is crucial for internet of things networks since it can assist in resolving conflicts and preventing fraud.

IoT sensors are used in smart cities to track air quality and traffic. Real-time traffic updates and air quality alerts are produced using the data that the sensors send to a cloud-based platform. To verify the authenticity of the sensors and guarantee the accuracy of the data being transferred between the sensors and the cloud platform, the digital signature can be employed. This contributes to maintaining the accuracy and dependability of the data and preventing unauthorized parties from accessing the network and its contents.

All things considered, deploying digital signatures in IoT networks can greatly increase environmental security. Digital signatures can assist enterprises in safeguarding their IoT networks and data from a range of security risks by verifying devices and users, guaranteeing data integrity and offering non-repudiation.

Secure Development Life Cycle

A methodology called the Secure Development Life Cycle (SDLC) is used to create software that is secure by design. Every phase of the software development process-from gathering requirements to deployment and maintenance is integrated with security. This makes the software more resilient to attacks by assisting in the early identification and resolution of security risks. Since IoT devices are frequently more susceptible to attack than traditional IT systems, the SDLC is very crucial. IoT devices are harder to secure since they are usually more resource-constrained and have fewer attack surfaces. IoT devices are also frequently placed in remote areas, which makes it harder to keep an eye on and secure them.

The following are some particular instances of how the SDLC can be applied to IoT data protection:

- Collecting requirements: The development process should begin with the collection of security needs. A risk evaluation of the IoT device and its planned application should serve as the foundation for these requirements
- Design: It is important to check the IoT device's design for security flaws. Every element of the design, including the software, hardware and communication protocols, should be taken into account in this review
- Implementation: The software of the internet of things device should be implemented using secure coding techniques. This entails avoiding typical security flaws like buffer overflows and SQL injection, verifying user input andutilizingg robust encryption
- Testing: A comprehensive security vulnerability analysis of the IoT device's software is necessary. Both automated and manual tests should be a part of this testing

Organizations can create IoT devices that are more secure and resistant to attacks by adhering to the SDLC.

This contributes to the security of the data that IoT devices gather and send.

Secure Deployment Process

A secure deployment process is a collection of guidelines and practices that institutions can use to safely implement infrastructure and software. Mitigating the danger of security vulnerabilities being brought into the production environment is the aim of a secure deployment process. Devices should be installed safely to reduce the possibility of hacking or unauthorized access. The following are some examples of how an IoT network might be safeguarded using a secure deployment process:

- Through the implementation of robust authentication and authorization protocols, a secure deployment process can effectively hinder unauthorized people from gaining access to or managing internet of things devices. Devices that store sensitive data or have the ability to manage critical infrastructure may find this particularly important
- A safe deployment procedure can limit the transmission of malware and other security risks by separating and isolating internet of things devices from the rest of the network. An attacker will find it more difficult to access additional devices or systems on the network if just one IoT device is compromised
- A secure deployment procedure can aid in preventing network-transmitted IoT data from being intercepted or altered by utilising secure communication protocols
- Through the use of diverse security measures like intrusion detection systems, load balancers and firewalls, a secure deployment procedure can aid in safeguarding IoT networks against denial-of-service attacks and other malevolent activities
- Organisations enhance their overall security posture and safeguard their IoT networks from various attacks by adhering to a secure deployment procedure

Firewalls and Intrusion Detection Systems (IDSs)

Network security tools called firewalls keep an eye on and regulate all incoming and outgoing network traffic by pre-established security regulations. They can be used to defend against denial-of-service attacks, stop malicious traffic from entering or leaving a network and block unauthorised access to networks. Combining firewalls and Intrusion Detection Systems (IDSs) can offer layered protection. IDSs can be used to identify and address unknown risks, whereas firewalls can be used to stop known dangers and stop illegal access to networks. IoT devices can be protected from malware and DoS attacks with the use of firewalls and IDSs. Here are some particular examples of how IDSs and firewalls can support the security of IoT networks:

- Unauthorized access to the web interface of an internet of things device can be prevented by a firewall. By doing this, attackers deterred from using holes in the web interface to access the device
- When malicious traffic is directed at an IoT device, it can be found with an IDS. For instance, traffic attempting to take advantage of a known flaw in the firmware of the device can be found using an Intrusion Detection System (IDS)
- An IoT network can be shielded from a DoS assault by combining an IDS and a firewall. The IDS can be used to identify and notify users of an attack, while the firewall can be used to prevent malicious traffic from entering the network
- Any organization that wishes to defend its network against cyber threats needs to have firewalls and intrusion detection systems installed. Organizations can build a layered security approach that is more successful in identifying and averting attacks by combining various technologies

Update Hardware with the Most Recent Security Patches

The process of applying security updates that fix known vulnerabilities in the firmware of the hardware involves updating it with the most recent security patches. This is a critical step in defending networks and IoT devices against security risks. Maintaining devices with the most recent security updates can assist to reduce the chance of vulnerabilities being exploited. IoT network security can be enhanced by applying the most recent security updates to hardware, as demonstrated by the following specific examples:

- When a router firmware vulnerability arises, a security patch can help stop hackers from using that vulnerability to access the router and the network it is attached to when a camera firmware vulnerability arises, a security patch can help stop attackers from taking use of it to take over the camera and watch the live feed
- When a sensor firmware vulnerability arises, a security patch can help stop attackers from taking use of it to take control of the sensor and alter the data it is gathering
- Organizations can defend their IoT networks from various security risks and make sure their IoT hardware is up to date with the latest security updates by adhering to these guidelines

Use Anonymization Techniques

The process of eliminating or hiding Personally Identifying Information (PII) from IoT data while maintaining the data’s utility is known as anonymization. This is crucial for safeguarding IoT users’ privacy because

IoT devices frequently gather a lot of personal information, including location, health and financial data. Here are some examples of how IoT network security can be enhanced by the use of anonymization techniques: A smart thermostat's location data can be anonymized to help stop hackers from following the thermostat's owner around.

A wearable fitness tracker's heart rate data can be anonymized to help stop attackers from determining the user's health status.

A smart home security system's motion sensor data can be anonymized to stop attackers from pinpointing the precise place where motion is detected.

Employing excellent anonymization strategies to safeguard the IoT networks helps against various security risks and preserves the privacy of IoT users.

Use Privacy-Preserving Technologies

Privacy-Preserving Technologies (PPTs) enable to preserve people's and organizations' privacy while enabling them to gather, share and use data. PPTs function by encrypting or anonymizing data, among other methods, to make it more difficult for outside parties to identify users or follow their whereabouts. PPTs can be used in the following specific ways to safeguard internet of things networks:

- IoT data can be encrypted using homomorphic encryption, allowing third-party service providers to process and analyse it without disclosing the underlying data. This can be helpful for applications like smart home security systems, where customers wish to be able to analyse their data using cloud-based services without having to put their unencrypted data in the hands of the cloud provider
- Before IoT data is shared with third parties, differential privacy can be utilised to introduce noise, which makes it more difficult to identify specific individuals from the data. Applications like traffic monitoring systems may find this helpful, as it allows users to share data with researchers or government organizations without worrying about their privacy being violated
- Several Internet of Things (IoT) devices can work together on projects without disclosing personal information to one another by using secure Multi-Party Computation (MPC). Applications like distributed machine learning, in which internet of things devices work together to build machine learning models without needing to exchange training data

In IoT networks, PPTs are an effective technique for maintaining anonymity. Developers and operators of IoT devices use privacy-preserving technologies to protect user privacy, prevent unauthorized access and usage of IoT data and mitigate potential malicious use of such data.

Educate Users About Privacy

Educating users about privacy entails imparting knowledge about the value of privacy, privacy threats and privacy protection strategies. This involves instructing consumers on the kinds of information gathered about people and how it is applied. The dangers to privacy posed by various technology and services. The controls and privacy options available to them to safeguard their data. How to steer clear of typical privacy hazards. IoT network security is aided by user education regarding privacy in a number of ways. Users are better able to choose which IoT devices and services to use and how to use them when they are aware of the privacy implications of doing so. By doing this, consumers are less likely to expose sensitive information online or leave their devices open to hacking.

Users with more education are better able to recognize and reduce privacy threats connected to IoT networks. Users are less likely to do so, for instance, if they are aware of the dangers associated with using weak passwords or connecting to unsafe Wi-Fi networks.

Users with more knowledge are unlikely to make mistakes that leave their networks or IoT devices vulnerable to attack. Users are less likely to click on fraudulent links or open harmful attachments, for instance, if they are aware of the hazards associated with phishing attacks.

Users with greater education are more likely to support IoT practices that preserve privacy and to be aware of the privacy implications of IoT networks. This can encourage people to value privacy more and put pressure on internet of things companies to implement more privacy-friendly policies.

One of the most crucial steps in defending IoT networks against various security risks is teaching users about privacy. IoT networks can be made more secure by educating users about privacy through enabling them to make knowledgeable decisions about their privacy, assisting them in identifying and mitigating privacy concerns and decreasing the attack surface of IoT networks.

Use Secure Communication Channels

Using communication channels that are impervious to tampering and eavesdropping is known as secure communication channels. This is crucial to prevent unauthorized parties from intercepting or changing sensitive data. IoT networks can be secured by using secure communication channels, as demonstrated by the following examples: Data in transit between Internet of Things devices and the cloud can be encrypted using TLS. This lessens the possibility that hackers will intercept data being sent between the devices and the cloud.

Data in transit between IoT devices and a mobile app can be encrypted using SSL. This lessens the possibility that hackers would intercept data being sent between the mobile app and the devices.

IoT devices and a distant network can be securely connected via a VPN. Because of this, devices that are physically located in various regions of the world can yet communicate with each other as if they were on the same local network.

Implement Least Privilege

A security principle known as "least privilege" argues that users, processes and programmes should only be granted the permissions required to carry out their intended tasks. IoT network security can be enhanced by using least privilege, as demonstrated by the following concrete examples:

- It is possible to stop attackers from taking advantage of security holes in IoT devices to obtain administrator rights by assigning normal accounts to these devices rather than administrator ones
- Attackers can be prevented from accessing sensitive data or taking control of crucial devices by assigning roles to IoT devices and granting them the necessary rights to carry out their jobs. This is done by using role-based access control, or RBAC
- Reducing the attack surface and making it more difficult for attackers to infiltrate the devices can be achieved by using Just-in-Time (JiT) provisioning to provide Internet of Things (IoT) devices access to the resources they require when they need them and to revoke access when necessary

Monitor Devices for Suspicious Activity

Using tools and strategies to identify odd or unexpected activity on devices is known as "suspicious activity monitoring." This can assist in locating possible security risks, including malware infestations, illegal access attempts and data breaches.

IoT network security can be enhanced by keeping an eye on suspicious activity on devices, as demonstrated by the following examples:

- Assaults that target the network, such as denial-of-service assaults, can be found by keeping an eye out for anomalous surges in network traffic
- Tracking unsuccessful attempts at login can assist in identifying brute-force attacks and other account-related threats.
- The detection of malware infections and other device-targeting attacks can be aided by keeping an eye on anomalous file access and configuration changes
- Finding compromised devices that are being used to communicate with attackers might be aided by keeping an eye on contact with known malicious servers

One of the most crucial aspects of defending IoT networks against various security risks is keeping an eye on devices for unusual activity. Quickly identifying and responding to suspicious activities can lower the risk of data breaches, prevent lateral movement across networks and increase compliance with security laws.

Security Threats in IoT Architecture

As discussed in section one IoT environment has four layers:

1. Sensing layer
2. Network layer
3. Middleware layer
4. Application layer

Threats associated with each layer are described briefly.

Threats at Sensing Layer

This layer includes the actuators and sensors. Sensors sense the physical changes in the environment while actuators perform certain actions against the physical changes senses by sensors. Different types of sensors can be used to sense data such as temperature sensors, humidity detecting sensors, ultrasonic sensors etc. the other type of sensors includes electronic or chemical sensors. Different sensing layer technologies are introduced to perform different IoT applications such as RSNs, GPS and RFID. Security threats that can be faced in first layer are.

Node Apprehending

In the context of Internet of Things networks, "node apprehending" refers to the action of locating and isolating a node that is displaying suspicious activity. The traffic, activities and interactions of the node with other nodes on the network can be observed. A node that has been flagged as suspicious can either be disconnected from the network or the source of the threat can be looked into further. The attackers can introduce their own node into the IoT environment by replacing existing ones, giving them control over the introduced node and leaving the system vulnerable to attacks (Kumar *et al*., 2017). A node on an IoT network is deemed suspect for a variety of reasons. A node connecting with known malicious services or sending or receiving abnormally high volumes of data, for instance. A node may exhibit anomalous behavior, such as unauthorized resource access.

It's crucial to take action to lessen the threat posed by a node when it is captured. This could entail restarting, changing the firmware, or removing the node from the network. In certain circumstances, informing the node's owner or maker of the questionable conduct is also necessary.

Nasty Code Addition

A kind of cyberattack known as Nasty Code Addition (NCA) entails infecting IoT devices at the sensor layer with malicious code. The initial layer in an internet of things design is called the sensing layer and its job is to gather environmental data. Network and device security can be breached by NCA attacks, which can also be used to steal confidential information, interfere with operations, or inflict physical harm.

Although NCA assaults can take many different forms, they usually entail taking advantage of weaknesses in IoT networks or devices. For instance, a hacker may use a firmware vulnerability on a device to have access to it and install harmful programmes. Alternatively, a malicious code could be injected into traffic going to internet of things devices by an attacker taking advantage of a security flaw in a network. The security of internet of things devices and networks can be significantly impacted by NCA assaults. NCA assaults have the potential to allow hackers to obtain confidential information, interfere with operations and even physically harm internet of things devices by breaching their security at the sensing layer.

False Data Execution Attack

A cyberattack known as a False Data Execution Attack (FDEA) occurs when a hacker introduces bogus data into an internet of things system at the sensing layer. Vulnerabilities in the communication routes between the sensors and the rest of the system can be exploited, or the sensors themselves can be compromised. Since the sensing layer of an IoT system is where the system first interfaces with the outside world, FDEAs can be especially harmful in these systems. An attacker can essentially poison the entire system by breaching the sensors.

Side Channel Attack

A Side-Channel Attack (SCA) is a kind of cyberattack that takes use of a system’s physical characteristics to obtain private data, including user passwords or encryption keys. Numerous platforms, like as PCs, mobile phones and internet of things devices, can be used for SCAs. Since the sensing layer of an IoT system is the most susceptible to physical attacks, SCAs pose a special risk to these systems. For instance, a side channel attack could be used by an attacker to access a sensor and retrieve the data it is gathering. Sensitive information could then be stolen or the system compromised using this data.

Eaves Dropping

A cyberattack known as “eavesdropping” occurs when a perpetrator listens in on and records conversations between two or more people without the parties’ knowledge or agreement. This can be accomplished by physically breaking into communication connections or by taking advantage of security holes in communication networks or devices.

IoT network security can be significantly impacted by eavesdropping. Attackers can obtain sensitive information, including device credentials, user information and sensor data, by listening in on connections between internet of things devices and the cloud. Then, this data might be utilised to break into systems, pilfer private data, or interfere with daily activities. IoT networks are especially vulnerable to eavesdropping attempts because IoT equipment are frequently placed in unprotected, distant areas.

Attackers will find it simpler to take advantage of communication network weaknesses or to physically access devices as a result.

Denial of Service

In cyberattacks known as Denial-of-Service (DoS) attacks aim to overload a system with requests or traffic so that it becomes inaccessible to authorised users. DoS attacks can be launched against a range of targets, such as servers, websites and internet of things devices.

DoS attacks have the potential to seriously compromise the sensing layer security of internet of things systems. Attackers can stop sensors from gathering data or sending data to the cloud by flooding them with traffic or requests. IoT systems experience disruptions as a result, making it difficult for them to carry out their intended purposes. Denial of service also occurs due to the limited capacity of sensing nodes. In this situation, the nodes are unable to provide their services to users.

Since sensing layer IoT devices are frequently placed in isolated, unprotected areas, DoS attacks pose a special risk to these systems. Attackers will find it simpler to carry out denial-of-service assaults against these devices without being noticed as a result.

Attack During Booting

Cyberattacks that target devices during the starting phase are known as booting attacks. These attacks conducted by taking advantage of holes in the operating system or boot firmware. IoT devices are especially open to attacks during booting because they frequently have few security protections and are installed in isolated, unprotected areas.

IoT security at the sensing layer can be impacted by booting attack vectors in several ways. For instance, a vulnerability in the boot firmware of a sensor could be used by an attacker to access the sensor and change its configuration. This might provide the attacker the ability to stop the sensor from working, steal data from the sensor, or utilise the sensor to start more network-wide attacks. A sensor’s boot firmware could have a vulnerability that an attacker could use to implant malicious code. Then, this malicious code might be used to take advantage of the sensor’s data, interfere with its functionality, or initiate more network-wide attacks. A sensor’s boot code could be altered by an attacker to make the sensor malfunction. This can cause the sensor to either fail to collect data at all or gather data incorrectly. IoT systems that rely on sensor data are not functioning properly as a result. A sensor's encryption keys could be obtained by an attacker by taking advantage of a flaw in the boot firmware of the sensor. The attacker would then be able to decrypt the sensor's data and take confidential data.

Brute Force Attack

A brute-force attack is a kind of cyberattack in which the attacker tries a lot of different combinations until they find the one that works to access a system or data. Brute force assaults are a useful tool for breaking passwords, obtaining encryption keys and breaking into systems and networks without authorization.

Brute-force attacks have a variety of effects on IoT network security at the sensing layer. For instance, a brute-force assault could be used by an attacker to guess a sensor's password and obtain the data stored in the sensor. After then, this data might be taken, altered, or utilized to start more network attacks. A brute-force assault could be used by an attacker to get through a sensor's password and obtain its configuration. This could give the attacker the ability to change the sensor's setup, leading to malfunctions or erroneous data being sent. A brute-force assault could be used by an attacker to guess a sensor's password and take the encryption keys with it. The attacker would then be able to decrypt the sensor's data and take confidential data. A brute-force assault could be used by an attacker to take control of a sensor and utilise it as a springboard for more network-wide attacks. The attacker might, for instance, use the sensor to initiate a denial-of-service attack or send malicious traffic to other networked devices.

Because sensors are frequently installed in remote, unprotected places and have weak passwords, IoT networks are particularly susceptible to brute-force attacks at the sensing layer. Because of this, it is simple for attackers to use brute force attacks against sensors and remain undetected.

Security Threats at Network Layer

The function of network layer is to gather the information collected by the sensing nodes and transfer it to the computational unit for further processing. The major issues at network layer are.

Phishing Attack

Phishing attack is the attack where small effort can target most of the IoT devices. The main concern of attackers is that if few of the devices become the victim then the attack is considered to be successful. Visiting malicious web pages can cause a phishing attack. If a user password is compromised whole IoT environment is exposed to attacks. The network layer is more likely to become the victim of phishing attacks. Phishing attacks have a variety of effects on network layer security in internet of things networks. An attacker might, for instance, send a malicious link-containing phishing email to an internet of things device. Clicking on the link could allow an attacker to gain access to the device or install malware on it. A malicious link to a phoney firmware upgrade could be included in a phishing email that an attacker sends to an internet of things device. An attacker can take control of the device if the user installs the phoney firmware upgrade. An attacker can send a phishing email with a malicious link to a fake configuration file to compromise an internet of things device. The attacker could access the device's data by downloading the phoney configuration file. An IoT device may receive a phishing email from an attacker that contains a malicious link that leads to a fraudulent login page. The attacker can access the device and obtain credentials if the user enters them on the phoney login page.

Unauthorized Access

In unauthorized access, an unauthorized person get the access control by illegal means and stay undetectable within a network for longer period. The attention of attacker in this case is got steal the valuable information without harming the network. As IoT gadgets continuously transmits and receive data so they are highly exposed to access attacks.

At the network layer, unauthorised access to IoT networks can significantly affect security. An attacker can do the following when they get unauthorised access to an IoT network:

- Steal data from internet of things devices, including sensor data, consumer information and intellectual property
- Disrupt or disable internet of things devices to avoid financial losses and operational outages
- Launch additional assaults against systems and devices connected to the network or even outside of it
- Launch denial-of-service attacks on other networks or systems using internet of things devices

Denial of Service (DoS) Attack

A cyberattack known as a Denial-of-Service (DoS) attack occurs when a hacker tries to flood a system or network with traffic such that legitimate users cannot access it. DoS attacks can be launched against a range of systems, such as servers, websites and internet of things networks. DoS attacks have the potential to significantly affect IoT network layer security. An attacker that targets an IoT network with a denial-of-service attack can:

- Stop authorised users from utilising IoT apps and devices
- Disrupt or disable internet of things devices to avoid financial losses and operational outages

- Hide other attacks, including data theft or unauthorised access

Routing by Malicious Nodes

In an attack known as “routing by malicious nodes,” a network attacker hacks a node and uses it to maliciously route traffic in an internet of things network. Attackers can use a variety of techniques to execute routing assaults in internet of things networks. Exploiting routing protocol weaknesses is one popular technique. Another technique is to use malware or other tools to compromise network nodes. Once a node has been breached, an attacker can utilize it to maliciously route traffic, reduce traffic coming from authorized devices, transmit malicious traffic to other networked devices and build network loops that can render devices inaccessible.

Security Threats at Middleware

The network layer and application layer are connected via middleware. Middleware layer also enhance the storage and computing capacities. It provides reliable IoT applications. The attack on this layer takes command on the entire network. Various attacks on this layer are.

Man in the Middle Attack

A cyberattack in which the attacker intercepts communication between two parties and impersonates one of them is known as a Man-in-the-Middle (MitM) attack. Because of this, the attacker can change communications or steal data without the parties’ knowledge. MitM attacks have the potential to significantly affect middleware layer IoT security. The intermediary layer facilitates communication between cloud-based IoT devices and other devices. An attacker can disrupt or disable internet of things devices, steal confidential information, or launch additional assaults against other networked devices and systems by intercepting communication at the middleware layer.

Malicious SQL Commands

The kind of cyberattack in which the attacker inserts harmful code into a SQL query is known as a malicious SQL command. The database may run this code, possibly resulting in harm or jeopardizing security.

Here are some particular examples of how IoT systems might be compromised at the middleware layer by using malevolent SQL commands:

- A malicious SQL command could be injected by an attacker into a middleware programme that controls IoT device setups. This could give the attacker the ability to change an IoT device’s settings, causing it to malfunction or giving the attacker access to private information
- An attacker can insert nefarious SQL statements into a middleware programme that handles and stores sensor data from internet of things devices. This could provide the attacker the opportunity to either alter or steal the sensor data, leading to false alarms or other issues
- A middleware application that is used for IoT device authorization and authentication could be compromised by an attacker using malicious SQL statements. By doing this, the attacker might be able to pretend to be a genuine internet of things device and enter the network without authorization

Signature Wrapping

An attack known as “signature wrapping” occurs when a hacker obtains a valid communication, re-signs it with a malicious signature and then sends it on to the intended recipient. Even though the message has been altered, the recipient’s signature verification procedure will still recognize it as legitimate. At the middleware layer, signature wrapping can significantly affect IoT security. The intermediary layer facilitates communication between cloud-based IoT devices and other devices. An attacker can access Internet of Things devices, take advantage of data and initiate additional attacks against other networked devices and systems by encasing communications in malicious signatures.

Cloud Malware Insertion

An attack known as “cloud malware insertion” occurs when malicious software is introduced into a cloud environment. This might be accomplished via taking advantage of holes in the cloud platform, breaking into a user account, or employing different strategies. The malware can be used to attack Internet of Things (IoT) devices, steal data and launch additional assaults against other networked devices and systems once it has been introduced into the cloud environment. Attackers can introduce malware into cloud environments in a variety of methods. Exploiting cloud platform vulnerabilities is one such technique. Injecting malware using a compromised user account is an additional technique. Through supply chain attacks, in which they breach a third party vendor that supplies software or services to the cloud platform, attackers can also introduce malware into cloud settings.

Flooding

An attack known as “flooding” occurs when an attacker overwhelms a target server or network with a lot of traffic, preventing normal users from accessing it. The middleware layer is one of the several tiers of the network stack where flooding attacks can be executed.

Flooding can cause the middleware layer to become overloaded with traffic, rendering it inoperable for reputable IoT devices. This may stop Internet of Things (IoT) devices from delivering data, getting updates, interacting with the cloud, or carrying out commands. Attackers can increase the effect of other attacks, such DDoS attacks, by using flooding attacks. An attacker might, for instance, use forged source IP addresses to transmit a huge volume of UDP packets to the middleware server. This can result in an excessive amount of answers being sent by the middleware server to the forged IP addresses, flooding the victims with traffic. MitM attacks against IoT devices can be launched by attackers using flooding assaults. An attacker might, for instance, bombard the middleware server with a lot of SYN packets, leading it to generate a lot of half-open connections. The traffic passing across these partially opened connections could therefore be intercepted and altered by the attacker.

Security Threats at Application Layer

Application layer provides services directly to the end users. Different IoT applications such as smart meters, smart homes, smart grids and smart cities lie in application layer. This layer has some security issues not present in other layers. The threats include in this layer are privacy and data thefts issues. Threats faced by this layer are.

Data Thefts

The unlawful acquisition of digital information kept on computers, servers, or other electronic equipment is known as data theft. Sensitive data can contain names, addresses, Social Security numbers, credit card numbers, medical records, financial information, trade secrets and intellectual property. Data from internet of things devices is processed and presented to users by the application layer. An attacker sell or expose private information to criminals if they are successful in obtaining data from the application layer. An attacker might, for instance, take advantage of sensor data, customer information, or intellectual property.

Sniffing

Network packets are captured and examined as part of the process of sniffing, a kind of network traffic analysis. Network traffic can be observed by sniffers for several reasons, such as locating and fixing issues with networks, observing the safety of networks, obtaining information on network behaviour, launching assaults on users or network devices. If implemented security protocols are not secured enough, then it allows the attacker to get access to the confidentiality. The attacker uses some sniffing applications to monitor the IoT network.

End to End Data Encryption

With End-to-End data Encryption (E2EE), only the sender and recipient of a message can decipher the transmission's plaintext content. E2EE uses two cryptographic keys: A public key and a private key. The message is encrypted using the public key and decrypted using the private key. End-to-end data encryption is required to guarantee the confidentiality of data. The application should allow only authentic users to encrypt or decrypt the data. Attackers can access data by using gate-level decryption to get access to the internet of things network. An attacker can access all of the data being encrypted if they are successful in taking advantage of a flaw in the gate level decryption procedure. Sensitive data from sensors, customers and intellectual property can be included in this.

Reprogramming

Reprogramming is the process of altering a device's operating software. This can be carried out for several purposes, including performance enhancement, feature addition and problem fixes.

The application layer of security can be significantly impacted by reprogramming IoT devices. An attacker can take control of an IoT device and use it to conduct attacks against other devices on the network or even the cloud itself if they can reprogram the device. An attacker could reprogram an IoT device to carry malware. This software could start more attacks, impede operations, or steal data. An attacker could reprogram an IoT device to expose security flaws. This can make it simpler to attack the device or provide the attacker access to other networked devices. An attacker could reprogram an IoT device to build a botnet. Large networks of compromised devices known as "botnets" can be used to carry out potent attacks like denial-of-service attacks.

Table 1 displays the security risks present in each IoT layer as described in this study. The distributed nature and complexity of the IoT architecture make it especially open to attack. IoT devices can be challenging to patch or update and they are frequently physically insecure. Furthermore, attackers can take advantage of the frequently weak security of the protocols used by IoT devices. It is crucial to implement security measures to ensure the safety of the IoT network.

Table 1: Summary of security threats at each layer of IoT

Session layer	Network layer	Middle layer	Application layer
Node apprehending	Phishing attack	Man in the middle attack	Data thefts
Nasty code addition	Unauthorized access	Malicious SQL commands	Sniffing
False code execution attack	Denial of Service (DoS) attack	Signature wrapping	End to end data encryption
Side channel attack	Routing by malicious nodes	Cloud malware insertion	Reprogramming
Denial of service	-	Flooding	-
Attack during booting	-	-	-
Brute force attack	-	-	-
Eaves dropping	-	-	-

There are numerous levels of security threats in the IoT ecosystem. Data integrity and privacy are at danger at the sensing layer because of sensor manipulation or data faking. Attacks at the network layer, such as packet sniffing and device impersonation, might jeopardize the integrity of the network and the flow of data. Threats to the middleware layer include message interception and injection, which can stop data flow and possibly jeopardize the dependability of IoT systems. IoT applications are vulnerable to data breaches and unauthorized access due to vulnerabilities at the application layer, such as unsecured APIs or insufficient user authentication. A comprehensive security plan that addresses the specific vulnerabilities and hazards associated with each layer is necessary to protect IoT systems from these threats.

Solutions to Overcome Security Threats in IoT Layered Architecture

It's critical to put security measures in place at every tier of an IoT architecture to ensure its security. Here are a few particular fixes:

- Seals and enclosures: Use sensors and actuators in conjunction with physical security measures like seals and enclosures. Also, use tamper-resistant actuators and sensors
- Spread spectrum approaches: Spread spectrum approaches can be used to make it more difficult for attackers to jam the signals that sensors and actuators use
- Strong authentication and authorization: Make sure all IoT devices have robust authorization and authentication systems in place
- Encryption: To secure data while it's in transit and at rest, use encryption
- Intrusion detection mechanism: To identify and stop malicious activity and to keep an eye out for routing attacks, implement intrusion detection and prevention systems
- Secure communication methods: Use secure communication methods like VPN or HTTPS
- Firewalls and VPNs: In order to manage access to the IoT network, use firewalls and VPNs
- Software updates: Update all software, including operating systems, apps and firmware
- Network segmentation: To lessen the attack surface, divide the IoT network into segments from other networks
- Traffic analysis and monitoring: Use traffic analysis and monitoring to look for anomalies and take appropriate action
- Range of security measures: No single security control is perfect, so it is important to use a variety of controls to protect your system
- Security monitoring: To identify and address security threats, put incident response and security monitoring procedures into practice
- Security frameworks and coding techniques: Make secure applications by utilizing security frameworks and secure coding techniques
- Power management: Use redundancy and power management techniques to make sure IoT networks and devices are always available
- Defense-in-depth strategy: Implement a range of security controls at every tier to establish a defense-in-depth strategy
- Input and output validation: Organizations can enhance the overall security of their IoT deployments and safeguard their systems against various threats by incorporating input and output validation at every layer of the IoT architecture

Putting security measures in place at every layer of the internet of things architecture makes it harder for hackers to access devices, networks and data, hence lowering the risk of cyberattacks. It is possible to stop the collection and transmission of false or misleading data by implementing safety precautions like sensor redundancy and data validation. This is crucial for applications where erroneous data could result in mishaps or other safety incidents, like industrial automation systems and self-driving cars. IoT devices and networks can be protected from malicious actors by implementing security measures like intrusion detection and network segmentation. This is crucial for applications like industrial control systems and medical devices, where unwanted access may result in mishaps like patient injury or equipment damage. Validation of input and output can be applied at every level of the internet of things architecture. For instance, input validation can be used in the sensing layer to look for anomalies or inconsistent sensor data. Input validation can be used at the network layer to scan incoming traffic for malicious packets. Input validation can be used at the application layer to verify that user input is free of malicious code and other threats. Output validation in the middleware layer can be used to scan configuration files for vulnerabilities or sensitive data. Safety features like error handling and input validation can aid in preventing applications from producing inaccurate or deceptive outputs. This is crucial for applications where incorrect outputs could cause disastrous accidents, like flight control systems and nuclear power plant control systems. Physical security and power management are two examples of safety measures that can help guarantee the availability and integrity of IoT networks and devices. This is crucial for applications where a service interruption could have detrimental effects, like emergency response systems and critical infrastructure. The security, dependability and availability of IoT systems are all significantly improved by implementing security measures at the IoT layer. Organizations can lower the risk of cyberattacks, safeguard sensitive data and increase customer trust by implementing these precautions.

Summary and Future Work

The Internet of Things (IoT) is a network of physical items that can connect and exchange data with other devices and systems over the internet. These objects are integrated with sensors, software and other technologies. Without the assistance of a human, these gadgets can gather and share data. The most recent global hot topic is the internet of things. The internet of things promises to make everyday objects smart from light bulbs to train stations. With its rapid growth, the Internet of Things (IoT) now significantly influences how people live, engage and conduct business (Ahmad and Zulkifli, 2020). IoT has made it easier to manage things, from households to big organizations. To provide an example, Internet of Things (IoT) devices have multiple use cases such as:

- Keep track of household items including security systems, lights and thermostats (Alaa *et al*., 2017; Bhat *et al*., 2017)
- IoT allows seamless interconnection among heterogeneous devices, making it a viable solution for disaster management. IoT-enabled systems can detect and monitor potential natural disasters and aid emergency response by utilizing data analytic and AI tools (Ray *et al*., 2017)
- Gather information from medical equipment to track the health of patients (Kashani *et al*., 2021)
- The Internet of Things (IoT) is having a major impact on the automotive industry, with applications in areas such as vehicle manufacturing, fleet management and driver safety (Pourrahmani *et al*., 2022; Karthikeyan *et al*., 2022)
- o The development of big data and the Internet of Things (IoT) is rapidly accelerating and affecting all areas of technologies and businesses by increasing the benefits for organizations and individuals. The growth of data produced via IoT has played a major role in the big data landscape (Marjani *et al*., 2017)

To ensure the IoT sector's continuous expansion and success, numerous difficulties must be overcome. These difficulties have an impact on the growth and development of IoT in numerous industries, ranging from privacy and security concerns to compatibility issues and limited processing power. For the internet of things to succeed and expand, it will be essential to address these issues via the use of data anonymization, encryption, standardization initiatives and other solutions. We attempt to cover every facet of security in this study to educate IoT developers on the need to be aware of the risks and take appropriate action. However, some security precautions that should be taken to maintain the IoT environment's security are not discussed such as securing IoT devices and networks using block chain. It needs to be looked into by researchers how to safeguard IoT networks, devices and data using block chain technology. The restricted resources and capabilities of IoT devices make traditional authentication and authorization procedures unsuitable for them. To ensure the security and scalability of IoT devices, researchers must create new authentication and authorization protocols. The complexity and dynamic nature of IoT networks and devices make security risk management challenging. Researchers must devise innovative strategies to effectively and proactively handle IoT security concerns. Even though the internet of things is still in its infancy, it is expanding quickly. By 2025, it is anticipated that there will be 29 billion IoT devices worldwide. It's critical to understand the possible security and privacy concerns connected to the expanding internet of things. All things considered, IoT security has a bright future. IoT security is becoming more and more important and researchers are working hard to create fresh approaches to reduce the risks. We can make the internet of things a more reliable and safe environment for all users with more research and development.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have not received any financial support or funding to report.

Authors' Contributions

Sadia Waheed Awan: Conceptualized the study, designed the methodology and supervised the research process.

Savera Hanif: Prepared the original draft of the manuscript, reviewed and edited the interim versions.

Rubab Hafeez: Reviewed and edited the interim versions of the manuscript.

Muhammad Imran Sharif and Kamran Siddique: Reviewed the manuscript and provided feedback for finalization.

Zahid Akhtar: Edited the manuscript, reviewed the final version, and ensured the accuracy of the content.

Ethics

The material is the authors' own original work, which has not been previously published.

Conflict of Interest/Competing Interests

The authors declare no conflicts of interest.

References

Ahmad, N., & Zulkifli, A. M. (2022). Internet of Things (IoT) and the road to happiness. *Digital Transformation and Society*, *1*(1), 66-94. https://www.emerald.com/insight/content/doi/10.1108/DTS-05-2022-0009/full/html

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, *97*, 48-65. https://doi.org/10.1063/5.0081996

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002

Alabdulsalam, S., Schaefer, K., Kechadi, T., & Le-Khac, N. A. (2018). Internet of things forensics-challenges and a case study. In *Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers 14* (pp. 35-48). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-99277-8_3

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, *54*(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

Bello, Y., & Figetakis, E. (2023). IoT-based Wearables: A comprehensive Survey. *arXiv Preprint Arxiv:2304.09861*. https://doi.org/10.48550/arXiv.2304.09861

Bertino, E., Choo, K. K. R., Georgakopolous, D., & Nepal, S. (2016). Internet of Things (IoT) smart and secure service delivery. *ACM Transactions On Internet Technology (TOIT)*, *16*(4), 1-7. https://doi.org/10.1145/3013520

Bhat, O., Bhat, S., & Gokhale, P. (2017). Implementation of IoT in smart homes. *Int. j. Adv. Res. Comput. Commun. Eng*, *6*(12), 149-154. https://doi.org/10.1016/j.jnca.2017.08.017

Chen, L., Thombre, S., Järvinen, K., Lohan, E. S., Alén-Savikko, A., Leppäkoski, H., ... & Kuusniemi, H. (2017). Robustness, security and privacy in location-based services for future IoT: A survey. *IEEE Access*, *5*, 8956-8977. https://doi.org/10.1109/ACCESS.2017.2695525

Cihan, A. T. A. Ç., & Akleylek, S. (2019). A survey on security threats and solutions in the age of IoT. *Avrupa Bilim ve Teknoloji Dergisi*, (15), 36-42. https://doi.org/10.31590/ejosat.494066

Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges and open research issues. *Computer Networks*, *144*, 17-39. https://doi.org/10.1016/j.comnet.2018.07.017

Dalipi, F., & Yayilgan, S. Y. (2016). Security and privacy considerations for IoT application on smart grids: Survey and research challenges. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 63-68). IEEE. https://doi.org/10.1109/W-FiCloud.2016.28

Donohoe, M., Jennings, B., & Balasubramaniam, S. (2015). Context-awareness and the smart grid: Requirements and challenges. *Computer Networks*, *79*, 263-282. https://doi.org/10.1016/j.comnet.2015.01.007

Farris, I., Taleb, T., Khettab, Y., & Song, J. (2018). A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Communications Surveys and Tutorials*, *21*(1), 812-837. https://doi.org/10.1109/COMST.2018.2862350

Gotarane, V., & Raskar, S. (2019, April). IoT practices in military applications. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 891-894). IEEE. https://doi.org/10.1109/ICOEI.2019.8862559

Guinard, D., Fischer, M., & Trifa, V. (2010). Sharing using social networks in a composable web of things. In *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* (pp. 702-707). IEEE. https://doi.org/10.1109/PERCOMW.2010.5470524

Shamala, L. M., Zayaraz, G., Vivekanandan, K., & Vijayalakshmi, V. (2021). Lightweight cryptography algorithms for Internet of Things enabled networks: an overview. In Journal of Physics: Conference Series (Vol. 1717, No. 1, p. 012072). IOP Publishing. http://doi.org/10.1088/1742-6596/1717/1/012072

Joshitta, R. S. M., & Arockiam, L. (2016). Security in IoT environment: A survey. *International Journal of Information Technology and Mechanical Engineering*, *2*(7), 1-8.

Karthikeyan, S., Rani, G. J., Ramamoorthy, K., Chelladurai, T., & Thangaselvi, D. E. (2022, May). The industrial internet of things (IIoT): An analysis framework for industry 4.0 applications. In *AIP Conference Proceedings* (Vol. 2418, No. 1). AIP Publishing. https://doi.org/10.1016/j.iot.2022.100579

Kashani, M. H., Madanipour, M., Nikravan, M., Asghari, P., & Mahdipour, E. (2021). A systematic review of IoT in healthcare: Applications, techniques and trends. *Journal of Network and Computer Applications*, *192*, 103164. https://doi.org/10.1016/j.jnca.2021.103164

Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., ... & Ghorbani, A. A. (2023). Internet of Things (IoT) security dataset evolution: Challenges and future directions. *Internet of Things*, 100780. https://doi.org/10.1016/j.iot.2023.100780

Khan, Y., Su'ud, M. B. M., Alam, M. M., Ahmad, S. F., Salim, N. A., & Khan, N. (2022). Architectural threats to security and privacy: A challenge for Internet of Things (IoT) Applications. *Electronics*, *12*(1), 88. https://doi.org/10.3390/electronics12010088

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221. https://doi.org/10.1016/j.comnet.2018.03.012

Kumar, S., Sahoo, S., Mahapatra, A., Swain, A. K., & Mahapatra, K. K. (2017, December). Security enhancements to system on chip devices for IoT perception layer. In *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)* (pp. 151-156). IEEE. https://doi.org/10.1109/iNIS.2017.39

Lally, G., & Sgandurra, D. (2018). Towards a framework for testing the security of IoT devices consistently. In *Emerging Technologies for Authorization and Authentication: 1st International Workshop, ETAA Barcelona, Spain, September 7 Proceedings 1* (pp. 88-102). Springer International Publishing. https://doi.org/10.1007/978-3-030-04372-8_8

Li, F., Hong, J., & Omala, A. A. (2017). Efficient certificateless access control for industrial Internet of Things. *Future Generation Computer Systems*, *76*, 285-292. https://doi.org/10.1016/j.future.2016.12.036

Liu, Y., Li, Z., Li, H., Wang, Y., Li, X., Ma, K., ... & Yang, H. (2015, June). Ambient energy harvesting nonvolatile processors: From circuit to system. In *Proceedings of the 52nd Annual Design Automation Conference* (pp. 1-6). https://doi.org/10.1145/2744769.2747910

Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the Internet of Things. *Future Generation Computer Systems*, *75*, 46-57. https://doi.org/10.1016/j.future.2017.04.045

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155-184. https://doi.org/10.1080/23738871.2017.1366536

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities and open research challenges. *IEEE Access*, *5*, 5247-5261. https://doi.org/10.1109/ACCESS.2017.2689040

Nalajala, S., Kurakula, J. S., Kanumuri, M. K., & Tumma, M. (2019, February). Privacy Preserving using PUP-RUP model. In *2019 International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 115-121). IEEE. https://doi.org/10.1109/ISS1.2019.8908013

Ngu, A. H., Gutierrez, M., Metsis, V., Nepal, S., & Sheng, Q. Z. (2016). IoT middleware: A survey on issues and enabling technologies. *IEEE Internet of Things Journal*, *4*(1), 1-20. https://doi.org/10.1109/JIOT.2016.2615180

Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, *32*, 17-31. https://doi.org/10.1016/j.adhoc.2015.01.006

Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, *112*, 237-262. https://doi.org/10.1016/j.comnet.2016.11.007

Plageras, A. P., Psannis, K. E., Stergiou, C., Wang, H., & Gupta, B. B. (2018). Efficient IoT-based sensor BIG Data collection-processing and analysis in smart buildings. *Future Generation Computer Systems*, *82*, 349-357. https://doi.org/10.1016/j.future.2017.09.082

Pourrahmani, H., Yavarinasab, A., Zahedi, R., Gharehghani, A., Mohammadi, M. H., & Bastani, P. (2022). The applications of Internet of Things in the automotive industry: A review of the batteries, fuel cells and engines. *Internet of Things*, 100579. https://doi.org/10.1016/j.iot.2022.100579

Rahmani, A. M., Szu-Han, W., Yu-Hsuan, K., & Haghparast, M. (2022). The Internet of Things for Applications in Wearable Technology. *IEEE Access*, *10*, 123579-123594. https://doi.org/10.1109/ACCESS.2022.3224487

Ray, P. P., Mukherjee, M., & Shu, L. (2017). Internet of things for disaster management: State-of-the-art and prospects. *IEEE access*, *5*, 18818-18835. https://doi.org/10.1109/ACCESS.2017.2752174

Sattar, K. A., & Al-Omary, A. (2021). A survey: Security issues in IoT environment and IoT architecture. https://digital-library.theiet.org/content/conferences/10.1049/icp.2021.0894

Seth, I., Panda, S. N., & Guleria, K. (2021, October). IoT based smart applications and recent research trends. In *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 407-412). IEEE. https://doi.org/10.1109/ISPCC53510.2021.9609484

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118-137. https://doi.org/10.1016/j.dcan.2017.04.003

Sharif, A., Sharif, I., Saleem, M. A., Khan, M. A., Alhaisoni, M., Nawaz, M., ... & Chang, B. (2023a). Traffic management in internet of vehicles using improved ant colony optimization. *Computers, Materials and Continua*, *75*(3). https://doi.org/10.32604/cmc.2023.034413

Sharif, A., Sharif, M. I., Khan, M. A., Ali, N., Alqahtani, A., Alhaisoni, M., ... & Chang, B. (2023b). SDN-enabled content dissemination scheme for the internet of vehicles. *Cmc-Computers Materials and Continua*, *75*(2), 2383-2396. https://doi.org/10.32604/cmc.2023.033894

Sicari, S., Rizzardi, A., Grieco, L. A., Piro, G., & Coen-Porisini, A. (2017). A policy enforcement framework for Internet of Things applications in the smart health. *Smart Health*, *3*, 39-74. https://doi.org/10.1016/j.smhl.2017.06.001

Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2016). Internet of Things: Security in the keys. In *Proceedings of the 12th ACM Symposium on qos and Security for Wireless and Mobile Networks* (129-133). https://doi.org/10.1145/2988272.2988280

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964-975. https://doi.org/10.1016/j.future.2016.11.031

Tawalbeh, Lo'ai., Fadi, M., Mais, T., Muhannad, Q., (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences 10*(12): 4102. https://doi.org/10.3390/app10124102

Thilakarathne, N. N. (2020). Security and privacy issues in IoT environment. *International Journal of Engineering and Management Research*, *10*. https://doi.org/10.31033/ijemr.10.1.5

Vikas, B. O. (2015). Internet of Things (IoT): A survey on privacy issues and security. *International Journal of Scientific Research in Science, Engineering and Technology*, *1*(3), 168-173.

Wu, F., Xu, L., Kumari, S., Li, X., Shen, J., Choo, K. K. R., ... & Das, A. K. (2017). An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. *Journal of Network and Computer Applications*, *89*, 72-85. https://doi.org/10.1016/j.jnca.2016.12.008

Xu, J., Gu, B., & Tian, G. (2022). Review of agricultural IoT technology. *Artificial Intelligence in Agriculture*, *6*, 10-22. https://doi.org/10.1016/j.aiia.2022.01.001

Yang, Y., Cai, H., Wei, Z., Lu, H., & Choo, K. K. R. (2016). Towards lightweight anonymous entity authentication for IoT applications. In *Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I 21* (pp. 265-280). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-40253-6_16

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250-1258. https://doi.org/10.1109/JIOT.2017.2694844

Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2017). A survey on the edge computing for the Internet of Things. *IEEE Access*, *6*, 6900-6919. https://doi.org/10.1109/ACCESS.2017.2778504