International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

IoT Security: The vulnerabilities in internet of things devices and securing IoT ecosystem

Gaurav Malik [1,*] and Prashasti [2]

[1] *The Goldman Sachs Group, Inc. Dallas,Texas, USA.*
[2] *Application security engineer, The New York Times, Dallas, United States.*

International Journal of Science and Research Archive, 2023, 08(01), 1071-1093

Publication history: Received on 17 December 2022; revised on 31 January 2023; accepted on 02 February 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.8.1.0093

Abstract

The Internet of Things (IoT) has reached the top of most people's minds in modern society, with countless advantages widespread in healthcare, manufacturing, and smart cities. This increased number of connected devices is an extremely serious security problem. They examine aspects vulnerable to security breaches in IoT devices, especially the sources of security breaches, such as weak authentication mechanisms, insecure communication protocols, and lack of device updates. The paper also analyzes how these vulnerabilities affect privacy, safety, and business operations. The study, by pointing out actual world security breaches, such as Distributed Denial of Service (DDoS) attacks and data breaches, emphasizes the necessity of reliable security measures to secure confidential data and the system's integrity.

It also considers the various approaches to securing an IoT vecosystem, including secure device design, highly advanced cipher protocols, and multi-factor authentication. The study discusses emerging technologies in IoT security, such as blockchain, artificial intelligence (AI), and machine learning, which have recently been leveraged. 5G networks and technology in future IoT security are also covered, emphasizing increased connectivity and the security challenges that increased data transfer speed brings. The study presents a complete framework that outlines how IoT security challenges can be curbed, advocating for a proactive, multi-layer approach to prevent risks and achieve IoT systems' continued growth and trustworthiness.

Keywords: IoT Security; Vulnerabilities; Authentication; Encryption; Blockchain

1 Introduction

Because of the Internet of Things (IoT), devices in the digital world communicate and behave differently. They represent convenience, efficiency, and fulfillment, especially when most IoT devices are smart home appliances or industrial machinery. These devices, with sensors and connection features, allow real-time data collection and analysis and hence help make decisions more effectively for various sectors. IoT has been incorporated into people's everyday lives, fostering innovation in the healthcare, manufacturing, and smart city industries. While IoT security challenges seem quite vast, they directly result from the rapid increase in IoT's use. They are raising the question of the vulnerability of these interconnected systems. Most IoT devices are created with a priority to function more than security, which results in holes that cybercriminals would exploit. As a consequence, IoT security is an increasingly pressing matter, because any breach may result in severe privacy violations, data hacks, or even physical damage. With the increasing number of IoT devices in today's world comes more attack surfaces, and attackers can easily intrude on the network and steal sensitive data or disrupt the services.

* Corresponding author: Gaurav Malik.

IoT security is important since these devices keep and transmit delicate individual and venture data, such as health data and monetary exchanges. IoT security is important not only for protecting devices but also for assuring data integrity, confidentiality, privacy protection, and critical infrastructure reliability. Suppose the emerging technologies of IoT are to be deployed and the IoE realized. Our IoT ecosystems should be secured and protected by authorized access and risk mitigation, and trust in these technologies should be fostered. Since IoT should be fostered as an interconnected system, failure to secure one will have far-reaching consequences as all systems remain in control of the sensing and action of other systems in the network. There are some challenges and concerns in securing the IoT ecosystem. The first challenge is IoT device security protocol standardization, which is plagued by the lack of uniform implementation of security across various platforms and devices. Most IoT devices have weak authentication mechanisms, making them vulnerable to hacking attempts. Further compounding the problem is the lack of frequent software updates and patches on many devices, beginning to accumulate vulnerabilities where fixes have not been addressed. Many IoT devices use insecure communication channels as well. They are susceptible to interception and manipulation. Since the IoT networks are also complex (varying range of devices and access levels of users), ensuring security gets harder.

This study explores the vulnerabilities in IoT devices and suggests measures for ensuring the safety of the IoT ecosystem. This research attempts to elucidate why outbreaks of security breaches can happen, how effective the existing security parameters are, and how they can enhance the security of IoT networks. The first part of the study will be dedicated to a deep understanding of the vulnerabilities existing in IoT devices and the causes behind the security flaws. It will explore present solutions, best practices in IoT network protection, and case studies of effective uses. The last sections will present some advanced techniques in IoT security and insights into what IoT security will be like in the coming days when the scenery transforms digitally.

2 Understanding iot Vulnerabilities

2.1 Definition and Types of Vulnerabilities in IoT Devices

Most IoT devices have the capacity to connect and give up data once over the Internet. Due to their inherent connectivity, those devices tend to be exposed to a variety of security vulnerabilities. They can categorize the vulnerabilities of IoT devices into software vulnerabilities, hardware vulnerabilities, and network vulnerabilities (Meneghello et al., 2019). Many IoT devices run on embedded systems with outdated or no patches, and industrial software vulnerabilities are a common concern. Such devices may not have security mechanisms as strong as encryption and secure boot processes that protect them from malicious attacks. Many IoT devices have also been built in with very few resources, so they are denied the ability to implement many more defense protocols, thus making them solicit common holes like buffer serrate, SQL injection, or cross-site scripting (XSS).

Critical among them is the provider of hardware vulnerabilities. Some IoT devices are weakly or even completely unprotected in physical terms, for example, unencrypted firmware or poorly designed hardware components that could be easily compromised. Hardly did the device come out; malicious actors can get to a device unauthorizedly by physically splicing or through hardware-based key extraction and side-channel attacks. Such vulnerabilities can leak sensitive information, such as encryption keys, that can then be used to break encrypted communications or a database. Network vulnerabilities are the absence of secure communications protocol or unsafe network connections, which may open the door to unauthorized interception or data tampering (Butun et al., 2019). Basic communication protocols of IoT devices like HTTP or MQTT do not encrypt the data by default. It facilitates the hacking of IoT devices by hackers who can use Man in the Middle (MITM) to attack, intercept, and modify the communication between IoT devices and users. Most IoT networks are developed to be highly interoperable; devices with different manufacturers can be easily communicated. Now, this makes the possibility of the existence of a vulnerability from the third party's device without the necessary security measures.

Table 1 Definition and Types of Vulnerabilities in IoT Devices

Vulnerability Type	Description	Example Devices Impacted	Common Attack Methods
Software Vulnerabilities	Issues in embedded systems with outdated patches or poor coding.	IoT sensors, industrial control devices	Buffer overflows, SQL injection
Hardware Vulnerabilities	Poorly protected physical components, firmware, or hardware keys.	Routers, smart cameras	Side-channel attacks, key extraction

Network Vulnerabilities	Insecure communication channels, lack of encryption.	Smart thermostats, industrial IoT	Man in the Middle (MITM), packet sniffing

2.2 Common IoT Security Breaches and Attacks

There has been plenty of documentation of several IoT-related security breaches and attacks, and they have a high level of risk due to insecure devices. One of the most notorious examples is distributed denial of service (DDoS) attacks, whereby a group of (compromised) IoT devices will utilize their bandwidth to ''deny service to a target server by flooding it with traffic and making it unavailable. IoT is the victim of the disabled devices in the Mirai botnet attack in 2016, the attack that exploited millions of IoT devices to disrupt internet services on a broad scale (Geenens, 2019). In other words, the botnet exploited weak passwords and unsecured devices to crash the target network in this instance. Another common attack on IoT devices is data breaches. That is because many IoT devices gather sensitive information, such as personal health data, financial transactions, and where a person is located, and such data is ripe for cybercriminals to exploit for rewards.

Attackers can also infiltrate cloud platforms or databases containing IoT-gained data and get access to personal and sensitive information. For example, in 2019, they breached thousands of smart security cam company users, gaining access to the contents of video footage and personal information. Such breaches damage reputation and may facilitate identity theft or unauthorized access to critical systems. There is also man in the Middle (MitM) attacks in IoT ecosystems (Farrah & Dacier, 2021). In attacks such as these, malicious actors intercept the communication between IoT devices and cloud servers and replace or inject some harmful data into the communication channel. The players of these attacks can send the wrong information to a device, such as feeding a smart thermostat the wrong information or telling a connected vehicle the wrong commands. Since the communication channel of IoT devices contains no encryption, the system is highly vulnerable to MitM attacks, which may distort its integrity and reliability.

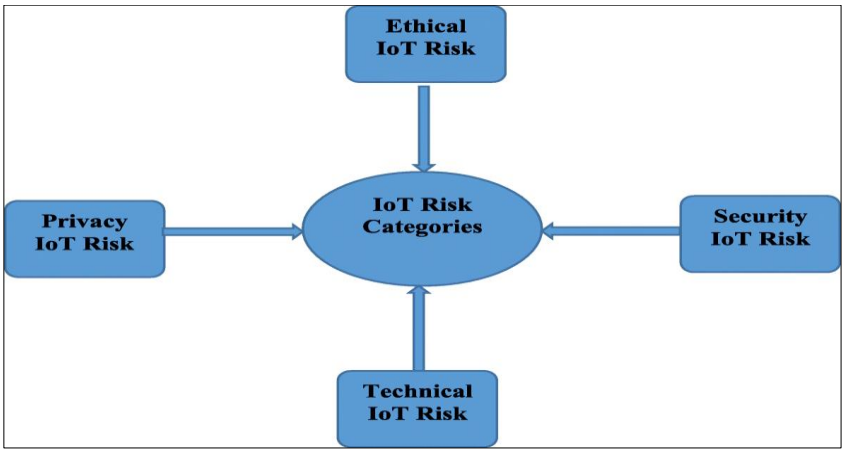

Figure 1 IoT risk categories

2.3 Impact of IoT Vulnerabilities on Privacy, Safety, and Business Operations

If they amplify their [the vulnerabilities of IoT devices] impact on privacy, safety, and other business operations, then inevitable consequences would be high. Privacy breaches are often directly followed up by the fact that IoT devices sometimes collect data about personal. For example, if your smart home assistant is not secured and there are any insecure channels for communication, for example, your conversation with that smart home assistant or your schedule could be leaked to the hacker. In the case of IoT devices such as wearable health trackers in healthcare, sensitive patient data, such as heart rate and medication history, can inadvertently be exposed if not secured properly. Moreover, breach of IoT privacy breaches an individual's privacy and erodes trust in IoT systems, which in turn causes much lower adoption of such systems (Bibri & Bibri, 2015).

In the case of IoT vulnerability, safety is also a very important concern. Many IoT devices control or monitor critical systems in manufacturing, transportation, or the healthcare industry. The consequence of a compromised IoT device can be fatal (physical). An example of such an industrial setting would be an attacker who gains access to a connected industrial control system (ICS) that could be used to manipulate video in operations, causing accidents, equipment damage, or personal injury. IoT vulnerabilities can help hackers change medical device settings, putting patient lives on the line.

IoT vulnerabilities also hit business operations. Such cyberattacks against IoT devices can induce considerable operational disruption, loss of sensitive data, and potential financial losses. For example, a DDoS that brings down an IoT-controlled smart grid may result in blackouts that may cause widespread power outages in areas, thereby rendering the entire region crippled by business operations. IoT network data breaches could lead to the theft of pertinent proprietary information that can destroy the company's competitive advantage. IoT vulnerabilities also have compliance issues in industries pending strict data protection regulations like healthcare and finance. It is concluded that the risks to privacy, safety, and business operations are severe in IoT devices and ecosystems. While these are technical vulnerabilities, they are not technical problems but have real-world practical consequences. They can affect the effectiveness and trustworthiness of IoT systems (Lv et al., 2020). Addressing these vulnerabilities is important to guarantee the safe and sensible integration of IoT technologies into the community.

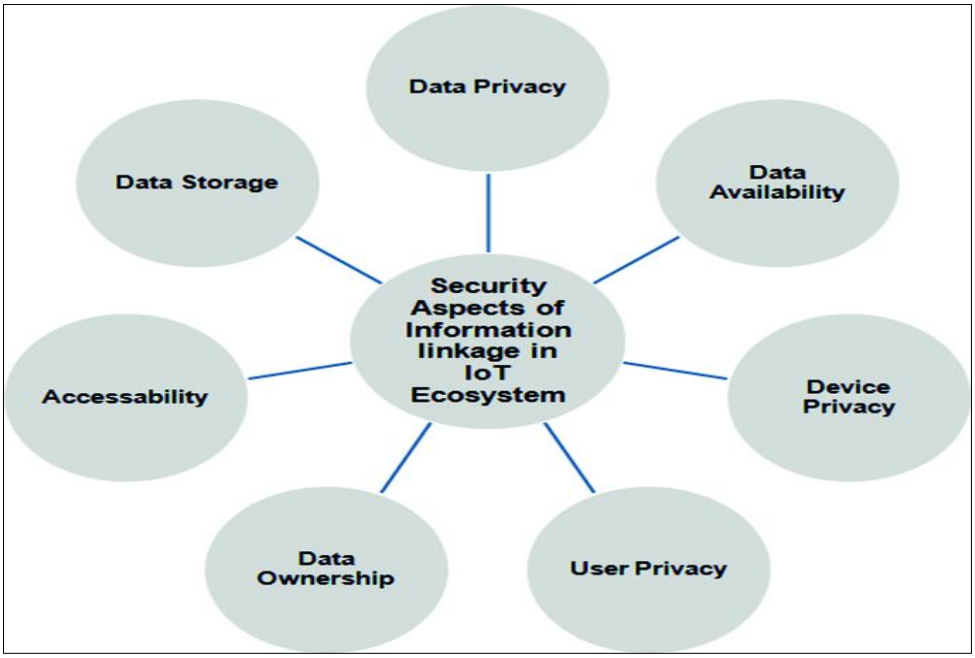

Figure 2 IoT Data Management

3 Root Causes of IoT Security Vulnerabilities

There are multiple reasons why IoT devices are so vulnerable to security attacks, all of which combine to make IoT ecosystems insecure. It is generally recognized that IoT offers many beneficial aspects, but the underlying security issues are still a major barrier to safe and wide deployment. Several root causes regarding technical, operational, and design flaws are often involved. The accompanying section talks about the main factors that cause IoT security vulnerabilities, which are the absence of a standard, weak authentication protocols, an insecure protocol, insufficient updates, and privacy issues for data (Frustaci et al., 2017).

Table 2 Root Causes of IoT Security Vulnerabilities

Root Cause	Description	Impact
Lack of Standardization	No uniform security guidelines across manufacturers.	Vulnerabilities across platforms
Weak Authentication Mechanisms	Default or weak credentials without proper user validation.	Unauthorized access, data leaks
Insecure Communication Protocols	Use of outdated or non-encrypted communication methods.	Data interception, MITM attacks
Insufficient Updates	Lack of firmware and software patches or automated updates.	Exploitation of known vulnerabilities

Data Privacy Risks	Sensitive data exposed due to lack of encryption and access control.	Personal information theft, misuse

3.1 Lack of Standardization in IoT Device Security

IoT ecosystems are secured, but uniform security standards are not provided. Unlike traditional computing devices, many manufacturers who produce IoT devices have different approaches to security and, hence, have different and inconsistent security postures. Because of the lack of industry-wide security standards, manufacturers follow no common framework when designing their IoT products. Many devices are constructed with few security measures if any at all. IoT devices 'security varies between brands, products, and models depending on whether they have standardized guidelines for device design, firmware updates, and encryption methods (Zandberg et al., 2019). The lack of such standardization compounds security, as digital devices of various manufacturers cannot easily communicate

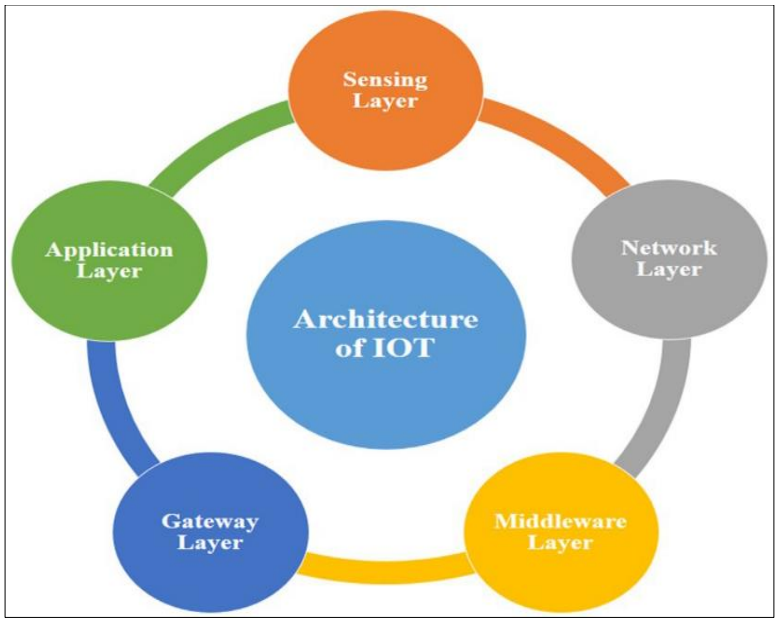

Figure 3 The architecture of the IoT framework

3.2 Weak Authentication and Authorization Mechanisms

The first line of defense in accessing the network and the resources is authenticating and authorizing users or devices. Many IoT devices lack proper authentication practices or are weak in their authentication practices. These devices have default credentials, or the password is simple to guess, and the password is rarely changed, making these devices vulnerable to brute force or dictionary attacks. Some IoT devices do not have multi-factor authentication (MFA), another type of protection that can further prevent access (Ometov et al., 2019). At times, devices lack appropriate mechanisms that would allow them to ascertain the identity of users and applications, leaving them open to manipulation outside of authorized control. The absence or weakness of authorization protocol can lead to unauthorized data exposure or a potential takeover of critical systems by an unauthorized user. Because IoT devices are often placed in critical infrastructure settings, weak authentication can have quite negative impacts in the healthcare or industrial industry, from vulnerability to data breaches, service interruptions, or even physical damage.

3.3 Insecure Communication Protocols

The ability of IoT devices to communicate with each other makes communication protocols necessary for the devices to transmit data. Most IoT devices could transmit across insecure communication channels or outdated protocols with no encryption or data integrity check (Abosata et al., 2021). One notable example of communication using a protocol like HTTP is forked, although it is commonly abused because attackers can intercept and manipulate the communication. Suppose proper encryption or communication protocols like those offered by HTTPS or the newer and more modern TLS/SSL are not in place. In that case, the data transmitted between devices can be intercepted, modified, or stolen. Many IoT networks are also based on closed communication protocols that are not sufficiently secure. MITM attackers can intercept and alter communication between IoT devices or between devices and central servers because they use

insecure protocols. Other IoT devices transfer data exchanged on unencrypted wireless networks such as Wi-Fi, Zigbee, and Bluetooth, which are prone to eavesdropping or interference. One of the major vulnerabilities of IoT ecosystems is the lack of secure communication protocols that break data confidentiality and data integrity during the data in transit (Frustaci et al., 2017).

3.4 Insufficient Device and Software Updates

The lack of updating the device's firmware and software is another critical root cause of IoT security vulnerabilities. It can become extremely difficult to patch security flaws, address vulnerabilities, and keep IoT devices running without regular updating. Many IoT devices, particularly those deployed at large scale, lack an automated update mechanism, and even updates from manufacturers are not timely. This leaves the rest of the devices in the open with known vulnerabilities and may operate for extended periods before being patched. Some IoT manufacturers do not establish clear processes to deliver patches or updates, or where updates are made available to users, they are not informed or incentivized to install them. This problem further compounds when such devices are embedded in faraway or distant locations that are hard to reach, let alone have physical updates done (Andersson & Weigand, 2015). Some devices do not have an internal mechanism to roll back to previous software versions after an update fails and risks malfunctioning or being exposed to attacks. Regularly updating IoT devices is crucial because failing to do so creates a massive security gap that cybercriminals are keen to exploit.

3.5 Data Privacy Risks

Gathered and transmitted in huge volumes, IoT devices 'personal, health, and operation data are considered the sweet spot for cybercriminals to exploit sensitive information. Because many IoT devices fail to implement sufficient data protection such as encryption, data anonymization, and strict access control, users are exposed to data privacy risks. Since no secure data storage and transmission protocols exist, sensitive information (such as customer records) can be accessed and intercepted when stored or traversing a network. The IoT device may not be able to entirely dispose of the personal information securely, so it is still at risk of being accessed without authorization even after the device is decommissioned or redeployed. Some of the data collected and IoT devices may store the data in a centralized cloud platform, lacking strong controls for securing the data, which adds to the privacy worries. With the increase of data privacy regulations such as GDPR, organizations have a legal and financial risk of not securing the data gathered by IoT devices (Chaudhuri, 2016). The data privacy risks are very real in healthcare, where devices generate sensitive patient information, and in smart home settings, where personal behavior and preferences are continuously monitored.

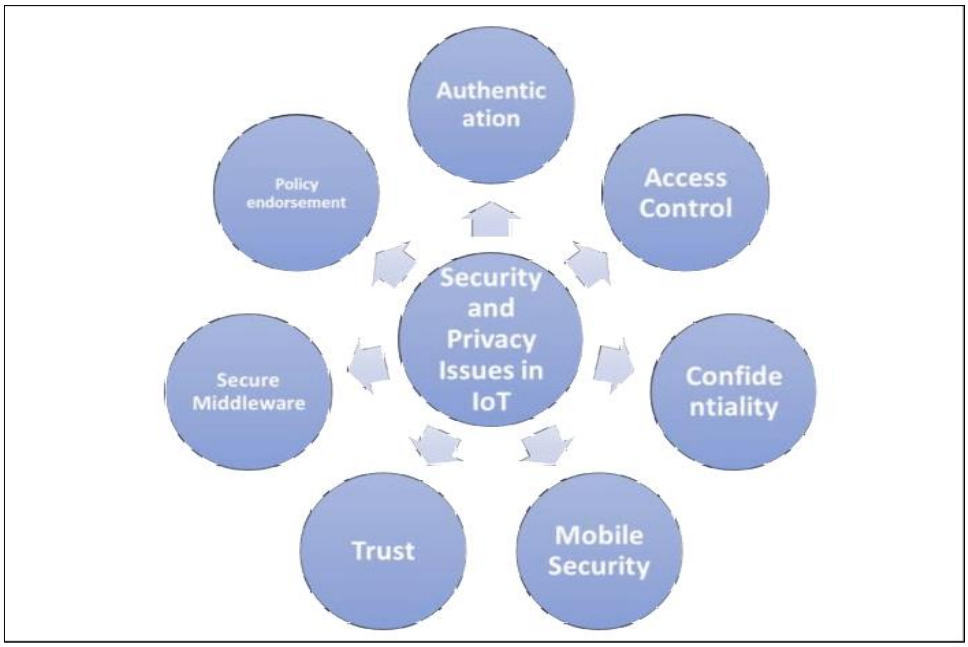

Figure 4 Security and Privacy issues in IoT

4 Securing IoT Ecosystems

The development of modern technology is impacted by the Internet of Things (IoT), and securing the devices and networks in the Internet of Things (IoT) ecosystem is an important challenge. The security in the IoT ecosystem is focused on creating security in the device lifecycle framework, security in detecting threats and incident response, and security in using such technologies as edge computing and cloud security (Krishnan et al., 2019). These components are discussed in the latter part of this section.

4.1 IoT Device Security Lifecycle

The IoT device security life cycle includes the design, development, deployment, operation, and decommissioning stages. At each stage, security must be integrated to provide strong protection for the device over its life. The security should be built into the device architecture when the device is being designed. The first step is just a couple of lines. It refers to choosing secure communication protocols to implement fast and strong encryption methods and verifying that the hardware and software of the device itself are resistant to being hacked (Mousavi et al., 2021). This phase helps avoid integrating weak or outdated technologies that the attackers could exploit. Secure coding is crucial in the development stage. To reduce the chances of common coding vulnerabilities in IoT, developers should follow industry standards like the Open Web Application Security Project (OWASP) for IoT. The software should be checked for exploitable weaknesses using regular code reviews, security testing, and vulnerability assessments.

With the deployment of the device, its security must continuously be actively managed. Updating regular software and firmware is crucial to patching, especially vulnerabilities, and improving the device's overall resilience. Secure update mechanisms should be supported in devices such that an update applied to a device is applied safely and reliably. There should be the need to continuously monitor the device for unusual activities, as surrounding families and institutions would be flagged in case of a threat by intrusion detection devices (Loukas et al., 2019). The device should be securely decommissioned when it becomes obsolete; it should be ensured that data stored on the device are wiped and cannot be recovered by an unauthorized party.

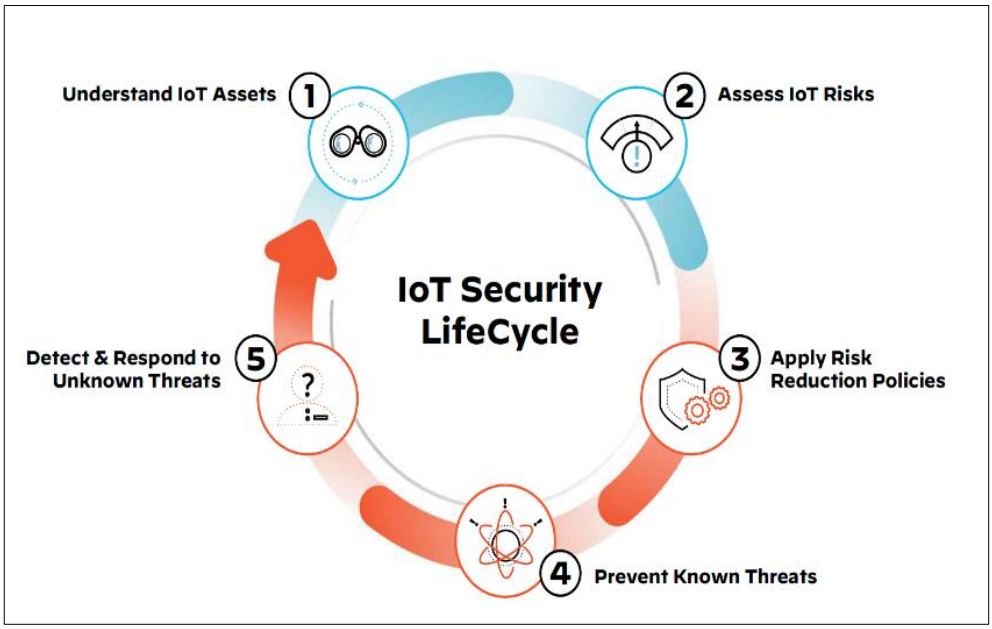

Figure 5 Secure Across the 5 Stages of the IoT Security Lifecycle

4.2 Security Frameworks and Protocols for IoT Ecosystems

A standardized security framework and protocols would be necessary to secure an IoT ecosystem effectively; a standard enables the structure for security management within IoT networks. One such framework is the IoT Security Foundation (IoTSF) Security Framework, which has a checklist for secure lifecycle management, risk assessment, and continuous security monitoring.

Security protocols are essential to secure the communication between IoT devices and networks. Popular protocols using which the data can be sent securely are Transport Layer Security (TLS), Secure Socket Layer (SSL), or Datagram Transport Layer Security (DTLS). They also ensure the network data's confidentiality and integrity during their transmittance through the network. In transit and at rest, data will be encrypted with strong levels. It will stop data breaches and unauthorized access. The next key protocol is the authentication and authorization protocol (OAuth), indicating how to request IoT resources to prevent people or IoT devices from accessing data if they do not get authorization. The IoT Security Architecture (IoTSA) and the Industrial Internet Consortium (IIC) Cybersecurity Framework should be applied to such standards for securing data (Buchheit et al., 2021). These are common language security bases for different industries and use cases in smart cities and industrial IoT (IIoT). These are ways to stay ahead of evolving threats and maintain parity for corresponding security posture in IoT networks.

4.3 Threat Detection and Incident Response in IoT Networks

Because the IoT network is dynamic, it is crucial to have efficient mechanisms for detecting threats and incident response. The bulk of IoT devices have created a world of large interconnectivity, where traditional security systems struggle to detect the appropriate threats (Makhdoom et al., 2018). Specialized tools and techniques for IoT threat detection are needed. Anomaly-based detection is mainly used in IoT threat detection. It monitors normal network behavior and detects any variance indicating an attack. One common example in IoT ecosystems is a Distributed Denial of Service (DDoS) attack, which can be indicated by unusual traffic patterns or abnormal device activity. Such intrusion detection systems for IoT can assist in detecting possible security breaches early and before the damage done is excessive.

Incident response plans must be implemented to mitigate the attack once the threat is detected. Our incident response covers the steps of containing the breach, investigating the root cause, and taking corrective actions. The attack impact should be minimized so the response plan structure will be well-formed. The first point of concern is quick containment. It could entail isolating the compromised devices, blocking the evil traffic, or turning off affected services. All actions should be well documented for post-incident analysis or to fine-tune future defense strategies. In addition to enabling good threat detection and incident response, IT and IoT security teams must coordinate with each other (Bernal et al., 2021). Between most organizations and IoT devices, devices are not typically managed with traditional IT infrastructure, but this ''separate'' approach can often mean longer business disruption from incidents. As the IoT is becoming mature and the number of connected devices grows, the number of traditional IT devices involved in the breach also rises, making unified threat management systems (which monitor both traditional IT devices and those in the IoT) essential to a complete security posture.

4.4 Role of Edge Computing and Cloud Security in IoT

Cloud computing and edge computing solutions that contribute to decentralized and centralized security are crucial to IoT ecosystem security. For instance, edge computing is good for increasing the responsiveness and security of IoT devices (processing data closer to where it is created, at the “edge” of the network). Edge computing reduces the risk of exposing data in transit when the data is sent to centralized data centers (Bilal et al., 2018). It can relieve cybersecurity bottlenecks by implementing real-time threat detection and filtering at the device or gateway level. It also enables security at the edge, reducing latency and bandwidth consumption by limiting the need to transfer all the data from the edge to the cloud. This is very important for time-sensitive applications such as autonomous vehicles or any other system with industrial automation. By most definitions, edge computing also adds an extra security layer over that since even if an attacker gains access to a device, he may never get to his intended target due to added security measures implemented locally.

Building cloud security into IoT devices becomes very important in dealing with the high volume of data these devices can generate. Scalable storage and processing power in the cloud is possible and must be secure. Strong access controls, encryption, and multi-factor authentication (MFA) are necessary for cloud services. The utilization of a cloud-based IoT management platform can provide visibility of the entire IoT network to reduce issues of real-time monitoring and automated detection of threats, as well as centralized management of security policies (Alam, 2021). Holistic security for IoT is achieved by integrating it with edge and cloud security to protect local and centralized resources and assist both. These technologies work together to address specific aspects of the security issues faced within IoT networks, obtaining a more resilient and comprehensive IoT network.

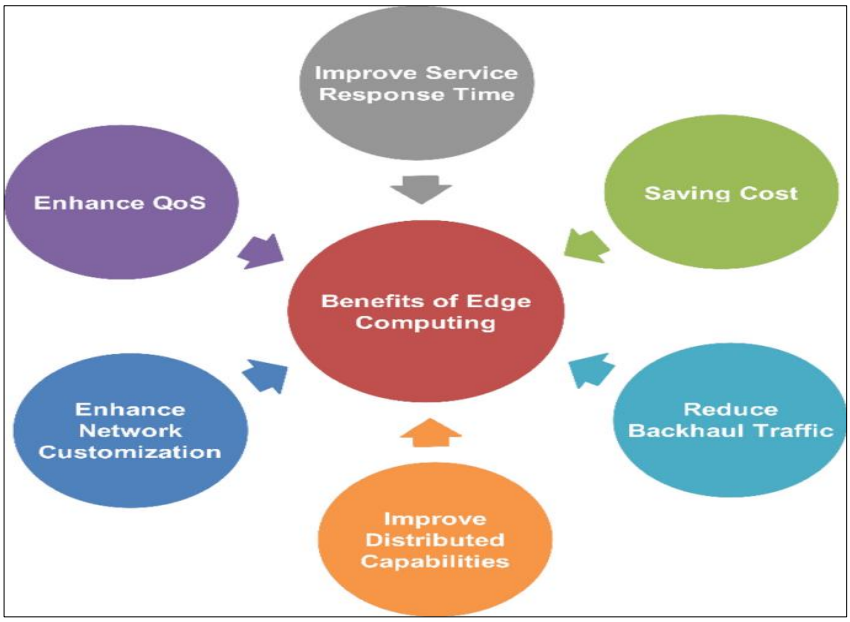

Figure 6 Edge Computing for Real-Time Internet of Things Applications

5 IoT Security Challenges in Different Sectors

With the sheer amount of IoT products used in many different industries, securing this success is becoming increasingly important. Unlike each sector, each sector has its own set of unique IoT security challenges for its devices and networks.

Table 3 IoT Security Challenges in Different Sectors

Industry Sector	IoT Security Challenges	Example IoT Devices Affected	Impact
Healthcare	Weak protocols, tampered data, insecure medical devices	Wearable health monitors, insulin pumps	Misdiagnosis, patient safety risks
Smart Homes and Buildings	Weak authentication, unsecured communication protocols	Smart thermostats, security cameras	Data leaks, unauthorized access
Industrial IoT (IIoT)	Integration of legacy systems, insecure remote access	Industrial sensors, smart machines	Operational disruption, financial loss
Retail and E-commerce	Insecure point of sale (POS) systems, unsecured payment devices	POS terminals, smart payment systems	Financial data theft, service disruption

5.1 IoT Security in Healthcare Devices

Technology like remote healthcare IoT devices such as wearable fitness trackers, remote patient monitoring systems, and connected medical devices transformed patient care into a continually monitored and real-time data-transmitted process. Such devices are not integrated into healthcare networks without security issues. These devices are often hacked because of their weak and/or nonexistent protocols, which give hackers easy access to data that is pretty sensitive when it comes to patients. For these and many other reasons, security for such devices is an easy cyber-criminal conquest, thanks to the prevalence of encryption, outdated operating systems, and, in many cases, no encryption in many healthcare IoT devices. The second obstacle is to guarantee the integrity of the data collected by healthcare IoT devices. With the misdiagnosis or providing an incorrect treatment plan, tampered data can jeopardize the data (Mirsky et al., 2019). If the insulin pump or the pacemaker is in the wrong hands, these other devices have life dangers accompanying them and can change the device's functionality. The services of medical institutions are provided to a wide spectrum of networks, requiring fast and comprehensive access to those data, which complicates the deployment of a whole set of security solutions by medical institutions. Healthcare IoT was designed to grow in number and sophistication. It should not be taken for granted that securing patient data and maintaining medical devices' safe operability are the main concerns (Isler et al., 2018).

5.2 IoT Security in Smart Homes and Buildings

IoT devices such as smart thermostats, security cameras, and connected lighting systems offer ease and energy efficiency in smart homes and buildings. These devices pose several security risks. Hackers often target them because they are popular, and their exploitation is simple. Many smart homes devices ship with weak default passwords, out-of-date software, and few security features, making them easy prey to Distributed Denial of Service (DDoS) or even remote hijacking.

Smart homes and buildings also suffer from the security risks caused by insecure communication protocols. For example, many IoT devices transmit data unencrypted, so an attacker can easily cozy up to some data. The last reason is that many connected devices in smart homes provide extended attack surfaces. A breach of one device, such as a smart door lock or surveillance camera, could result in voluntary or unauthorized access to other systems in the home, such as personal devices or the home's Wi-Fi network (Pattanasri, 2018). The IoT ecosystem also lacks standardized security protocols, so whilst manufacturers must not offer an unsafe service, the opportunity to prioritize convenience and the cost are not ideally balanced with security. This starts with ensuring that smart homes are end-to-end encrypted, making continuous device updates, and educating on the user's side.

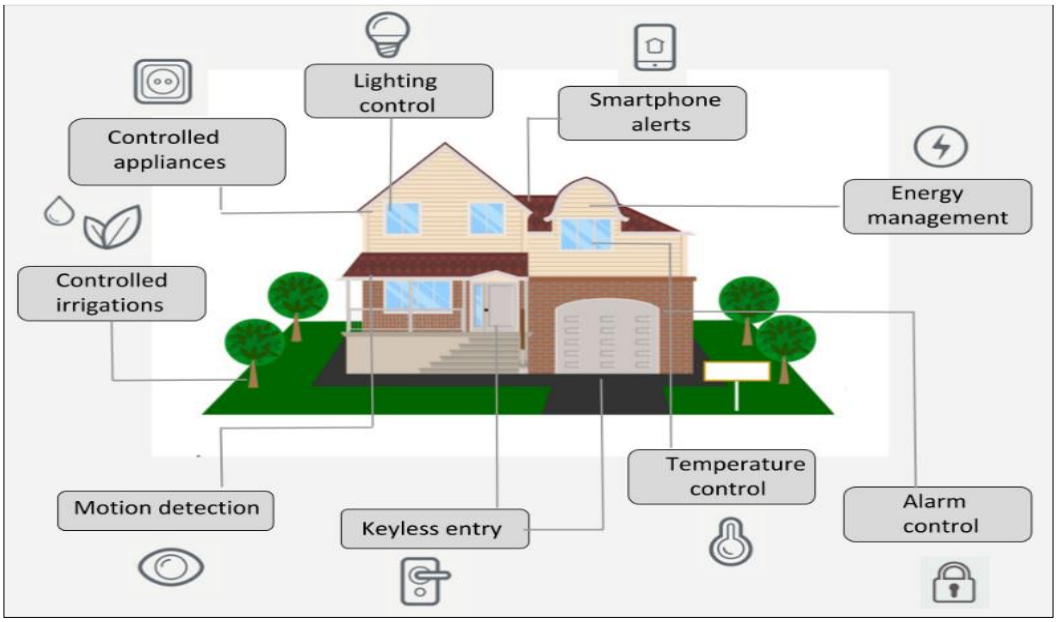

Figure 7 An IoT-based smart home depicting the use of smart sensing devices for different purposes

5.3 IoT Security in Industrial IoT (IIoT)

The industry has been drastically changed by the Industrial Internet of Things (IIoT), which brings the most critical infrastructure together on the networks that allow business decisions based on data and real-time optimization of processes. Beyond gaining awareness of IoT threats, IIoT systems have some of the biggest security challenges in the IoT simply because they introduce new entities that interoperate with legacy IT infrastructures, which raises the bar for the number and type of security threats. These systems include old, legacy equipment that was never planned to have network connectivity and never be secured. Many IoT devices are often placed inside remote or hard-to-reach locations, making monitoring and securing them uneasy.

The impacts of a breach in an IIoT network are severe. Disruption, or major loss of functionality, of both manufacturing operations is possible, as well as incurring a financial loss, damaging the environment, or even creating harm to employees. IIoT systems tend to comprise or integrate cloud platforms and vendors in the third tier, thereby increasing supply chain attacks (Costa et al., 2020). A vulnerability in a third-party component being used on an IoT device could allow cyber attackers to enter the whole network. To ensure the security of IIoT networks, it is necessary to enable robust access control mechanisms and real-time monitoring and use security protocols specifically suitable for industrial network networks as security protocols in the Operational Technology (OT).

5.4 IoT Security in Retail and E-commerce

IoT devices are widely used in the e-commerce and retail industry to provide ease of customer shopping and streamline operations. Smart connected point of sale (POS) systems, inventory tracking systems, and connected payment devices can offer better services. These devices are just as appealing to cybercriminals because they handle sensitive customer data, such as credit card information, personal details, and what a customer has purchased. Retail IoT devices are susceptible to cyberattacks that can cause serious financial damage from direct theft and the expenses incurred in money for reputation damage and regulatory penalties (Stellios et al., 2018).

The retail sector also hopes to achieve success in securing IoT-enabled payment systems. One such problem is that attackers cannot steal customer payment data using the common method enabled by lots of payment terminals: secure authentication methods. Suppose the devices are not well secured or do not meet compliance standards such as Payment Card Industry Data Security Standards (PCI DSS). This increases the risk of data breaches when more and more retail businesses bring out IoT-based supply chain management solutions. In order to secure IoT in retail, different layers, ranging from end-to-end encryption of the data to always updated software, having tighter access control to highly sensitive data, and having payment systems that are not attacked, are required.

6 Best Practices for iot Security

In the rapidly growing world of IoT, the security of devices and their networks is paramount. IoT devices are spreading across every industry niche, and it is important to build strong security protocols to safeguard data and privacy and the industry's core business activities. The following is a practical and technical approach to IoT security.

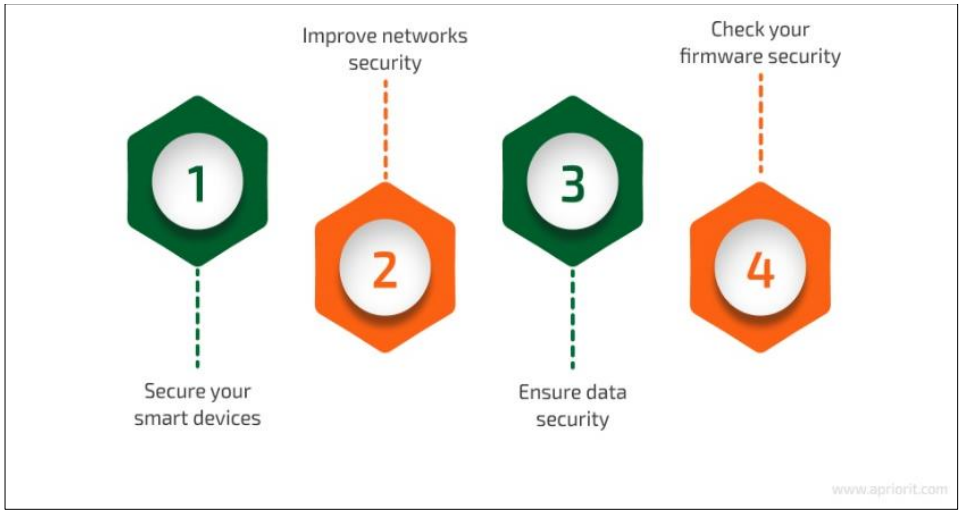

Figure 8 IoT Security Challenges and Best Practices

6.1 Secure Device Design and Development

Security should be embedded into IoT devices' design and development stages, not added as an afterthought. When designing a secure device begins, the least privilege and the notion of defense in depth are the ideas behind it. Hardware, software, and firmware must be designed with security in mind, and device manufacturers must do so. To prevent physical attacks and unauthorized tampering of sensitive information, devices should incorporate secure boot mechanisms, TEEs, and hardware-based security features such as Trusted Platform Modules (TPM). Hardcoding credentials or using default passwords are often exploited, so device developers must avoid this (Chandavarkar, 2020). It should use unique device identifiers to make devices authentic and secure. When the development teams follow strict secure coding practices and vulnerability assessment on an ongoing basis, any wall of mass is found early in the development lifecycle. Device firmware should be designed to be secure concerning known and emerging threats, and security flaws should not compromise the system when deployed.

6.2 Strong Authentication and Access Control Practices

Robust authentication and access control mechanisms are the most important parts of securing an IoT ecosystem. To allow any IoT device to access any network or resource, all devices must use strong authentication protocols to verify users and devices. Multi-factor authentication (MFA), which involves something the user knows (password), something

the user has (security token), and something the user is (biometric authentication), can be used to achieve this. Each user's privilege should be role-based, and no one should be given much more than he needs. This is known as access control. Policies should be enforced in IoT networks to allow only authorized personnel to access sensitive data and control some functionalities (Ali et al., 2019). Communication between devices and servers also needs to be protected with good encryption so that attackers cannot intercept sensitive information as it is being transmitted. Periodic rotation of credentials should be used in IoT systems to prevent unauthorized access since they should frequently force users and devices to update passwords and security keys.

6.3 Regular Software and Firmware Updates

Updating the software and firmware of IoT devices regularly is necessary to counter new vulnerabilities that are discovered. Device manufacturers and network admins must participate in security work and develop timely patches to address security flaws and provide adequate protection against the latest threats. This should include an automated mechanism that notifies users when an update is available and a smooth installation process. Not updating devices leaves they open to known exploits and security risks. Out-of-date firmware can be a vulnerability for cyber attackers to exploit to gain unauthorized access or disrupt operations (Bompos, 2020). This risk can be mitigated with IoT devices designed to have a robust update mechanism that supports over-the-air (OTA) firmware updates for remote and secure patching of IoT devices.

6.4 Encrypting Data in Transit and at Rest

An IoT ecosystem, like any other ecosystem, is secured by encryption. In such a case, all the data transmitted between IoT devices, servers, and cloud platforms has to be encrypted using strong crypto protocols like Transport Layer Security (TLS) or Secure Socket Layer (SSL). It ensures that the intercepted communication, if any, remains unreadable. The information remains intact and confidential. The data encryption stored on devices and servers is equally important (Bokefode et al., 2016). Many IoT devices collect sensitive information, including wearable devices' personal health data and smart factory industrial control data. Data at rest encryption is the protection of data. Suppose an adversary has direct access to a device or a server to attempt to access your data without the right decryption keys. Organizations have to practice end-to-end encryption for any sense of security for unauthorized data access and leaks.

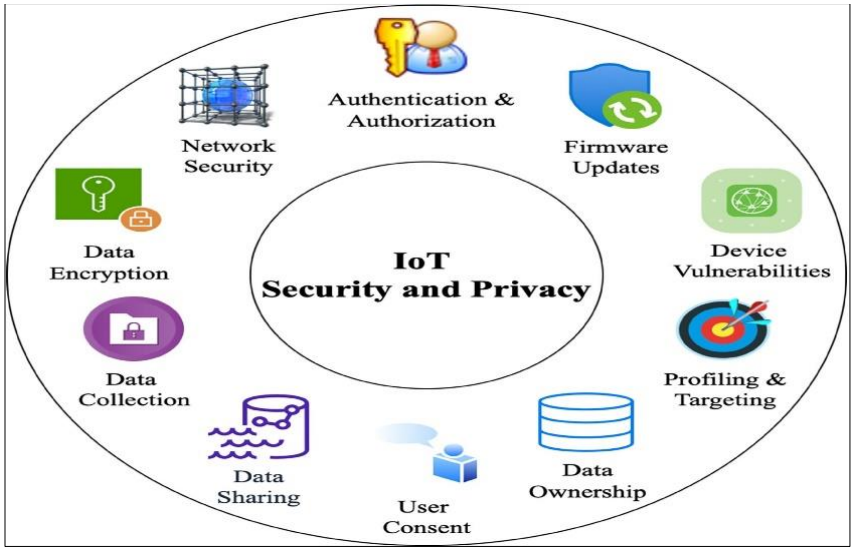

Figure 9 Exploring security and privacy enhancement technologies in the Internet of Things

6.5 Secure Communication Protocols and Firewalls

Communication protocol in an IoT is used for network security. Insecure protocols make it easy for attackers to attack many IoT devices. They use secure communication protocols (HTTPS, MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), which give us better security than normal HTTP and TCP/IP protocols. Moreover, secure protocols, firewalls, and intrusion detection systems (IDS) should be used to monitor and filter traffic in IoT networks. A firewall is a security line of defense between an external network and your internal network (Alsaqour et al., 2021). IDS tools also examine the network traffic and seek any indication of dubious activity. These security measures further enhance protections against IoT system attacks such as DDoS that overwhelm IoT systems and disrupt service.

6.6 User Awareness and Training on IoT Security

For instance, attention is overlooked to user awareness and training in the case of IoT security. This is the most insufficient (and hence the fault) way to diminish the most common security vulnerability, the human fallacy. IoT devices must understand the risks and what they can and cannot do to protect themselves.

Such include reactivating default passwords, recognizing a phishing attack, and the significance of regularly updating the device. It should be trained to the needs of different user groups, such as technical personnel and end users. Technical staff should be trained in-depth to secure IoT infrastructures, nontechnical, and nontechnical, given basic security protocols to follow (Brandon, 2020). They should be thinking about maintaining their training sessions, and it should be regular to make users aware of the new security threats and how to protect themselves. With the advancements of IoT systems being an integral part of our everyday lives, it is more important for us to have a culture of awareness in the security aspect of the IoT world.

7 Real-world successful case study

Table 4 Real-World Successful Case Study: Securing IoT in Healthcare

Security Measure	Description	Implemented In	Result
Data Encryption	Strong encryption (e.g., AES-256) to protect data in transit.	Remote patient monitoring systems	Protected sensitive patient information
Multi-Factor Authentication (MFA)	Layered authentication to ensure authorized access.	Healthcare providers, patients	Reduced unauthorized system access
TLS for Communication	Secure communication between IoT devices and cloud platforms.	Device-server communication	Prevented man-in-the-middle attacks
Network Segmentation	Isolated IoT devices from critical systems to mitigate risks.	Healthcare networks	Minimized the lateral movement of attackers

7.1 Case Study: Securing IoT in Healthcare (Remote Patient Monitoring Systems)

Internet of Things (IoT) technologies have entered the healthcare market, where they have been used for remote monitoring and patient management. Remote patient monitoring (RPM) systems are one of the most important applications of IoT in healthcare, where healthcare providers can collect, monitor, and analyze patient data in real time from a distance. The use of these systems is compared with people who do not use them, and I have to say that people who do use these systems have been very successful at using these systems, especially with chronic conditions like diabetes, hypertension, and heart disease, where continuous monitoring is so great. The usage of IoT in healthcare has potential issues from the standpoint of data security and privacy (Awotunde et al., 2021). Among the healthcare IoT systems that handle PHI, such systems are a prime target for PHI. These systems should be secured because protecting patient data from unauthorized parties accessing data, cyberattacks, data breaches, and deep water is vital. In this case study, Robusta's IoT RMS security strategy is used to secure critical patient data, and the system continues to be strengthened to address cyber threats and become more resilient.

7.2 Key Security Measures Implemented

While deploying the healthcare provider's remote patient monitoring system, the provider took several important security measures to handle the growing security concerns about IoT-based healthcare systems. In that sense, the measures included were designed to mitigate risks directly related to the interaction between the IoT devices, networks, and communication protocols in the healthcare ecosystem. The provider encrypted all data from IoT devices to the cloud-based monitoring platform. This meant sending blood pressure readings, glucose levels, and other ECG results without being able to read those sensitive patient data from unauthorized access during transmission. All data was confidential using strong encryption algorithms such as AES-256 and was secured and intact (Nyati, 2018). All these were integrated into the system with robust authentication and access control mechanisms (Usman et al., 2017). Multifactor authentication (MFA) was given to patients and healthcare providers, so the only people who could access the system were the ones authorized. It mitigated the risks of the login credentials being taken.

Besides accepting the secure communication protocols such as Transport Layer Security (TLS) for the communication between IoT devices and the backend servers, the healthcare provider also installed the data exchange between these

devices. TLS prevents man in the middle, no data can be intercepted or attacked, and the communication channel is secure (Alwazzeh et al., 2020). The devices have also updated the security patch for the latest system vulnerabilities and new threats that may crop up in time. Another important security measure included segmentation of the network used by the IoT devices. If any IoT device was compromised, the provider mitigated this risk of lateral movement by establishing an IoT device from a separate network with other critical healthcare infrastructure. This network segmented attackers out of sensitive hospital systems if a device was infiltrated.

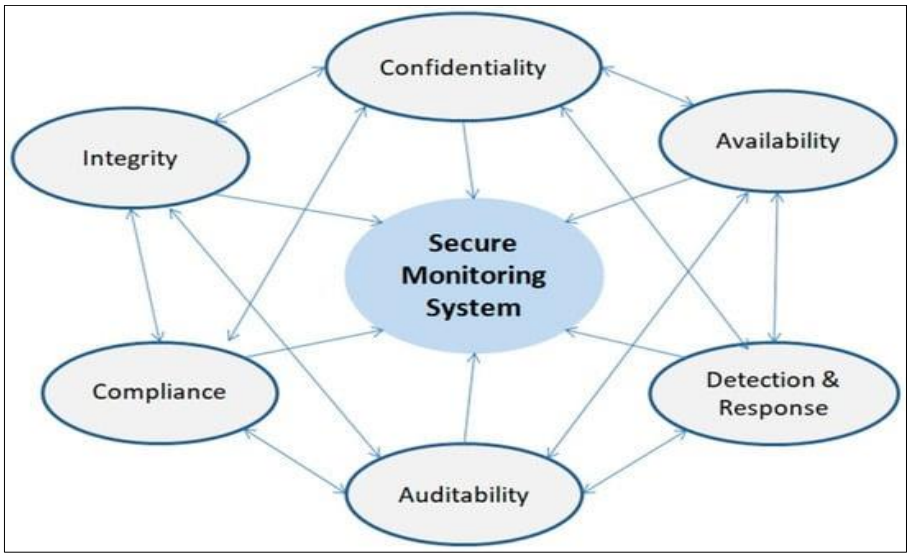

Figure 10 The primary goals of the proposed system

7.3 Results and Benefits of IoT Security in the Case Study

The security measures were adopted, and a few good things happened to healthcare providers. The first contribution is that the RPM greatly improved security. Data breaches or cyberattacks were limited. Communication protocols for the patient data are encrypted and secure to remain confidential and meet standards such as the United States Health Insurance Portability and Accountability Act (HIPAA) (Hoffman, 2020). In healthcare and its environments where the patient's private information is critical, implementing multifactor authentication and access controls significantly decreases the risk of unauthorized access. The adoption of IoT technologies had to be encouraged in the healthcare domain to safeguard patient-sensitive health information, and the provider would be able to maintain patient trust.

Adopting IoT security also led to the operational efficiency of the healthcare provider. IoT devices and platforms will be used securely in the healthcare domain to increase remote and patient monitoring and decrease visits and the load on healthcare facilities. Because of abnormalities that occurred, continuous monitoring and early intervention lowered costs and led to better patient outcomes. The provider could do all this by remaining compliant with the regulatory frameworks that are quite strict on data protection. Since healthcare providers integrated it's IoT systems with secure practices, they followed the relevant privacy regulations and avoided fines and bad reputations.

7.4 Lessons Learned and Practical Insights

The lessons from this case study and the related practical insights are key to healthcare organizations intending to secure their IoT systems. The key takeaways are regarding the layer security approach and the fact that it is specific to the IoT device. The perimeter security sweep and base-level password protection are not enough to protect healthcare data. A strong holistic security method such as encryption, a secure communication protocol, and strong authentication are very important to protect from cyber threats. The third lesson is always to have continuous monitoring and updates. IoT devices are not very secure and are never updated; therefore, cybercriminals can access them. The healthcare provider urged for software that gets regularly updated and patched for already existing vulnerabilities. Installing embedded firmware can make it difficult for unpatched IoT devices to get infected (Arakadakis et al., 2021).

The case study also sheds light on the repercussions of network dichotomization for mitigating possible security breaches. By isolating IoT devices on a separate network, the healthcare provider reduces the risk of an attacker gaining access to critical systems even if one of the IoT devices is compromised. This can be done in any industry to prevent IoT devices from being used as a gateway for cyber-attacks against more sensitive infrastructure. Healthcare IoT systems

security is a holistic approach involving multiple security measures (Sun et al., 2019). Both healthcare providers and IoT technology providers learn how to use evolutionary strategies to prevent IoT security failures. They should implement strategies such as this case study to help address important subjects such as patient data protection, compliance with regulations, and building trust with emerging technologies. These lessons learned apply to any sector that has leveraged IoT to help bring innovations and efficiencies to how and when an individual interacts with people and provides services to a company.

8 Advanced iot Security Solutions and Technologies

A large number of security issues in this ecosystem will continue to grow. Modern IoT systems can be serviced by traditional security measures, just not in a vast diversity of devices, big-scale networks, and special security requirements of different segments. Advanced IoT security solutions and technologies have been created aimed at advanced IoT security solutions for innovative and practical methods to secure IoT devices and IoT networks (Hassija et al., 2019). This section covers some of the most effective and new modalities for securing IoT surroundings, Blockchain, AI and machine learning, Zero Trust Architecture, IoT intrusion identification devices (IDS), and next-era firewalls and VPNs.

Table 5 Advanced IoT Security Solutions and Technologies

Solution/Technology	Description	Application in IoT Security	Potential Benefits
Blockchain	Decentralized ledger for secure, immutable data transactions.	Device authentication, data integrity	Improved transparency, tamper-proof data
AI and Machine Learning	Algorithms for real-time threat detection and anomaly prediction.	Network traffic monitoring	Proactive threat detection, response
Zero Trust Architecture	No default trust, constant validation of devices and users.	Device network access control	Reduced unauthorized access risks
Intrusion Detection Systems (IDS)	Monitors IoT network for anomalies and malicious activities.	Real-time security monitoring	Early breach detection and containment
Next-Generation Firewalls	Advanced firewall with application layer filtering and deep packet inspection.	Filtering IoT traffic	Block unauthorized or malicious traffic

8.1 Blockchain for Securing IoT Networks

Blockchain technologies decentralized and immutable nature has made it attractive for the need for secure IoT. At its core, blockchain's greatest strength is to store and communicate between IoT devices securely, transparently, and not open to tampering. They treat each device in an IoT network as a node on the blockchain, particularly if they want the records of any transactions or data exchanges of an IoT network to be recorded securely with a distributed ledger. Eliminating the need for central servers, which said attacks can target, is beneficial (Mahjabin et al., 2017). Blockchain helps enhance the security of IoT by overcoming some fundamental challenges like device authentication, data integrity, and transparency. An example is that devices can automatically check each other's identities and exchange data based on smart contracts without the risk of any unauthorized access. Blockchain encryption ensures that the data transmitted within the IoT network is kept safe and not manipulated without the information being detected. With IoT devices generating huge amounts of sensitive data, blockchain can be used to build a transparent and secure environment for data these days to mitigate the risk of data breaches and malicious interference.

8.2 AI and Machine Learning in IoT Security

Artificial Intelligence and Machine learning can modernize the solutions with security by taking proactive measures for detection and response to threats. AI and ML algorithms can process massive amounts of data generated in real-time from IoT devices and detect anomalies and patterns, indicating that some form of threat may be going on. These models continuously learn this data and eventually teach the models to become more effective in detecting and predicting new attacks such as Distributed Denial of Service (DDoS), man in the middle, unauthorized access attempts, and more. Security tasks, patch management, vulnerability assessments, and incident response are also ready to be done by AI

(Kumar, 2019). Machine learning can automatically identify an IoT device as having a vulnerability and then suggest updates that keep it secure as it evolves (Al-Garadi et al., 2020). With AI-driven security solutions and automated processes, human error is reduced, and security operations are becoming more efficient. AI systems can respond quickly to threats, causing less harm from cyber-attacks and downtime for important IoT networks.

8.3 Zero Trust Architecture in IoT Ecosystems

Zero Trust Architecture (ZTA) is an extra security model in which no device, user, or system in the network or outside it should be trusted by default. All requests made for access must be verified before the access is granted, even if they come from an internal source. Now, more than ever, it becomes even more important to follow this principle in IoT environments, given the number of devices and diversity they produce and the fact that traditional security models fail here. When it comes to IoT devices in Zero Trust, they are constantly monitored, and strong authentication and authorization checks verify their activities. Based on roles, there are rules of what can be accessed to which devices and how much they can access the data or network resources required for performing their function. Speaking of which, ZTA also highlights the importance of micro-segmentation. This technique splits the IoT network into smaller parts to restrict the propagation of the enemy in the system (Ashraf & Habaebi, 2015). An attacker cannot easily get to other devices or critical systems if he gains access to that one part of the network. This model of approach to the security of IoT networks makes them more secure from internal and external threats.

8.4 IoT Intrusion Detection Systems (IDS)

An intrusion detection system or IDS for IoT networks is a collection of tools designed to monitor IoT networks for any anomaly, such as malicious attack access or malware. However, any unusual communication activity also flows on the network. As IoT devices have features, specific IDS for IoT environments is required. In IoT communication, traditional IDS is inefficient in detecting urgent threats as the traffic of IoT is sporadic and uses reduced protocols such as MQTT and CoAP. The reality of the advanced IoT IDS solution for real-time analysis of the data traffic generated by IoT devices through behavior-based analysis to identify the abnormal activities that may threaten security (Asharf et al., 2020). IoT networks benefit from exploiting the dynamic nature inherent in such networks by learning common patterns of device communication and using these patterns to signal abnormal behavior that may signal a threat. IoT IDS systems are finally integrated with access control systems and other security solutions such as firewalls, anomaly detection systems, and so forth to guarantee total safety and fast incident response.

8.5 Next-Generation Firewalls and VPNs for IoT

Firewalls such as next-generation firewalls (NGFWs) and VPNs are employed to protect IoT networks. While traditional firewalls apply packet filtering from the predefined rules, the NGFW is more advanced as it includes application layer filtering, deep packet inspection, and intrusion prevention. These above features are indispensable for providing IoT subject matter determination and blockage over IoT-specific threats, including botnet assaults and protocol misuse. The NGFW also improves visibility into IoT traffic and lets the administrators watch the communication patterns, detect anomalies, and have tighter security policies. Using VPNs is another critical security factor for the IoT ecosystem (Ali et al., 2020). The encrypted tunnels of VPNs allow IoT devices to communicate with them and protect the sensitive data that goes over them. Virtual private networks or VPNs are useful in keeping your data safe when it passes through insecure networks like the public internet in a geographical area or when there is a remote device. Similar options are available to communicate with an IoT network, as with regular TCP clients. VPN protects the IoT device from location tracking and unauthorized access, which is a part of how it secures data in transit.

Given the high evolution of IoT networks, their networks need advanced technologies for security that evolve quickly enough with growing threats. IoT ECS security takes off when blockchain, AI, Zero Trust Arch, IDS, and next-generation firewalls and VPN come into the picture. These technologies are practical, scalable, and effective ways of protecting IoT devices, networks, and the data these devices generate. As IoT grows within industries, organizations need to put these high-tech security measures in place as this safeguards the digital infrastructure and paves the path for LO success more than what can be imagined.

9 Regulatory and Compliance Considerations in iot Security

They live in a modern world where the Internet of Things (IoT) is growing chaotically, and the demand for regulations of IoT devices and IoT data privacy and security is increasing. Due to the recent expansion of IoT devices in such facets of the economy and society where life and capital are on the line, researchers cannot be too careless with security in this respect in defending personal information and public import.

Figure 11 Regulatory compliance and IOT security standards

9.1 International IoT Security Regulations

Internationally, several regulations in the domain of security challenges for IoT have been established. Out of these two frameworks, the GDPR and the CCPA are the two most influential global frameworks. The EU's 2018 GDPR is today's biggest data protection law for IoT devices. The rule applies to any company that performs data processing for EU citizens regardless of company location. GDPR also requires businesses to provide technical and organizational measures to be adopted and secure personal data under custody. A critical element is ensuring that the IoT is built fundamentally secure and that data is ended. At the same time, it occurs, and proper controls are required to restrict access to sensitive data from unauthorized personnel (Burhan et al., 2018).

Under GDPR, businesses are also responsible for data processing activities to inform people and individuals to obtain explicit consent before collecting data. In response to IoT manufacturers and service providers who have access to personal data and exercise the related rights through IoT devices, transparency (as well as the exercise of user rights, including the right of access, rectification, and erasure of user data) must be guaranteed to them. This also means that for IoT ecosystems that can lead to many devices breaching simultaneously, the GDPR also sets the obligation to inform affected persons and regulators of such a data breach within 72 hours. The second important regulation in the US that impacts IoT security practices is the CCPA, which has been in force since 2020. Redacting or deleting personally identifying information is problematic under the GDPR, and the CCPA is similar, whereby the CCPA relates to data privacy and the rights granted to California residents about knowing such data is being collected, to be deleted, and to opt out of the sale of that information. It is the law in California only. As many businesses decide to spread the board CCPA under their business practices, its impact is felt beyond their borders. The CCPA's data security and consumer protection requirements and breach notification requirements collectively directly impact IoT device manufacturers and service providers in California.

9.2 Industry-Specific Compliance Standards

There are many industry-specific standards for IoT security, especially in sectors such as healthcare, finance and critical infrastructure, and international regulations. The Health Insurance Portability and Accountability Act (HIPAA) is one of healthcare IoT devices' most well-known compliance frameworks. HIPAA sets the standards for how patient data can be held private and secure, as patient data includes data from a connected IoT device in a healthcare setting. As such, healthcare organizations must implement safeguards to protect electronic health records (EHRs) and limit unauthorized access to IoT devices like wearables or remote patient monitoring systems.

With HIPAA, there are requirements upon healthcare organizations to evaluate how risks to patient data will be mitigated, implement access controls, and ensure that IoT devices will also use encryption and be audit compliant. Considering that patient data is always considered important to protect and is always on devices and also transmitted to healthcare providers, it becomes important in the context of IoT to make sure the data is protected both when it is stored on devices and also when it is transmitted so that no unintentional vulnerabilities are created. If not in compliance with HIPAA regulations, organizations can be fined and penalized, and the loss of reputation can damage damaged organizations. The Payment Card Industry Data Security Standard (PCI DSS) applies to IoT devices in financial transactions (Razikin& Widodo, 2021). The responses to the above snippets indicate that any IoT device that processes

payment card information should comply with PCI DSS requirements. Encryption of payment data, secure authentication, and regular vulnerability assessments. These standards particularly affect retailers and financial institutions as they often use IoT to build point of sales (POS) systems, mobile payments, and digital wallets.

9.3 Implications of Noncompliance on Businesses and Consumers

Failure to comply with IoT security regulations can hurt businesses and consumers badly. There are also financial costs associated with noncompliance for businesses. Over these past years, the size and severity of the organization's breach determine how penalties come with violating regulations such as GDPR and CCPA, which can be in the millions. Besides regulatory fines, businesses may have to undertake lawsuits from consumers whose data was compromised, further impairing the businesses. Noncompliance can also greatly affect a company's reputation outside of direct financial costs. Consumers today are more worried about their privacy and security. Any breach or inability to meet regulatory compliance may erode customer trust, resulting in customer and revenue loss.

The consequences of noncompliance to consumers can be indeed even more personal and harmful. Data breaches in the case of IoT devices can misplace sensitive personal information, including health records, finance information, and even location information, and thus expose them to identity theft, fraud, and even body harm. IoT devices, specifically in the healthcare sector, serve a key role in monitoring patients if compromised, which can result in patient safety crises without affecting the quality of constant care. This, calls for compliance with IoT security regulations to protect business interests and consumer rights and safety.

The final point in the discussion is that compliance and regulatory considerations are critically important for IoT security. The GDPR and CCPA are world standards, and HIPAA and PCI DSS are specific industry standards for security needs. Big financial, personal, and reputational consequences await businesses and consumers for not complying. A non-negligible necessary component for such investments is that organizations prioritize IoT security and adhere to these regulations to protect their stakeholders and their operational integrity.

10 Future Considerations and the Evolution of iot Security

The importance of secure Internet of Things (IoT) security becomes even more evident as it grows. Technological advancements, the development of 5G networks, changing cybersecurity threats, and the emergence of IoT device security are factors that shape the future of IoT security. They look at the primary steps to secure IoT ecosystems in the future by configuring 5G networks, examine security trends briefly, and explain how this new readiness is important in dealing with future challenges.

10.1 The Future of IoT in the Context of 5G Networks

With the start of 5G networks, the IoT is set to revolutionize the future of IoT in the same way because, with 5G, it is possible to send data at up to ten times faster speeds than before and to reduce the latency and increasing the reach of the connection of the Internet of Things devices to our surroundings making this a better way to connect with the actual environment in which a user lives. 5G will enable more seamless interconnectivity among IoT systems, and the related industries will enjoy the advantages of new capabilities that 5G networks provide, such as autonomous vehicles, smart cities, and industrial automation.

5G will also bring challenges in terms of security due to the large volume of data and the number of connected devices in the 5 G-enabled environment. As 5G networks offer an ultra-low latency, making real-time decision-making quicker, these can also assist attackers in conducting faster and more sophisticated attacks (Loghin et al., 2020). The volume of data that will be exchanged in 5G is larger than that of 4G due to huge bandwidths, which makes it much harder to monitor and secure these transactions. On the contrary, to overcome these challenges, security measures are needed to incorporate advanced encryption techniques, real-time threat detection systems, and enhanced network segmentation to surround areas where vulnerable devices are located. IoT combined with 5G will require more secure authentication and access control mechanisms to safeguard sensitive data and critical infrastructures from unauthorized access.

10.2 Upcoming Trends in IoT Device Security

Many emerging trends will make the future landscape of IoT device security. One of the main use cases in which IoT security is improving is artificial intelligence (AI) and related machine learning engines (ML). AI-driven solutions respond to IoT devices' huge amounts of data and detect plugins, threats, or security incidents in real time. It can also greatly increase the ability to forecast and stop attacks from escalating to an extent where they cannot be addressed quickly. Blockchain technology has been applied to ensure IoT ecosystems. Blockchain is an excellent object for

authenticating the IoT device and taking measures for authenticating data transactions. Through blockchain, IoT networks may record a transparent and secured verification of device identity, monitoring, and recordable interaction of devices. This approach will protect IoT devices and data from being tampered with by malicious actors. There is also a greater need for more secure communication protocols. Could traditional communication protocols not be as well protected as they once were since IoT networks grow in complexity? In the IoT, advanced encryption standards and data transmission techniques will be implemented so that information will not be delved into in the case of an attack.

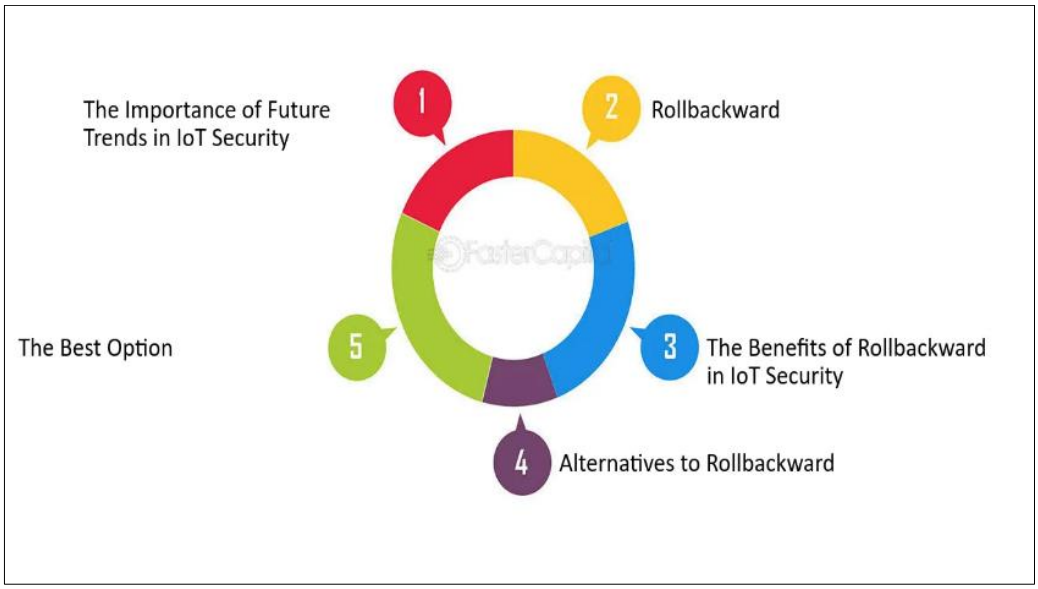

Figure 12 Future Trends in IoT Security and Roll backward - Roll backward in IoT

10.3 Evolving Cybersecurity Threats in the IoT Ecosystem

With the expansion of IoT ecosystems, IoT networks become sophisticated in the way that the threats targeting those networks grow. Cybercriminals are exploiting IoT device vulnerabilities, which are increasing due to Distributed Denial of Service (DDoS) attacks, data theft, or commanding connected systems. Botnets have risen to the forefront of the IoT space due to the number of compromised devices that can be networked to form an infected network of IoT devices for malicious purposes. Such botnets are already the engines powering several large-scale cyberattacks, and they are expected to become more numerous as more devices connect themselves to the internet.

IoT devices are also targets of ransomware attacks. As the reliance on IoT devices in critical infrastructure and business operations increases, attackers can encrypt the data or disrupt operations to extort a ransom (Butt et al., 2019). Attacks on industrial control systems and healthcare devices have shown that physical manipulation or hijacking of IoT devices can lead to damage. Supply chain attacks are another emerging threat in which the manufacturers or distributors of IoT devices are compromised to introduce those vulnerabilities at the source. Third parties produce many IoT devices, and therefore, the security of the supply chain has become an important aspect of IoT security. It will be necessary to collaborate across industries to ensure that devices are tamper-proof from the point of origin to their deployment in the field.

10.4 Preparing for Future Challenges in IoT Security

Organizations must devise a proactive and holistic IoT security preparation for imminent security challenges. Implementing a strong security framework, which includes continuous monitoring, regular updates of the software and firmware, and a multi-layered defense mechanism, is one of the first steps to secure IoT ecosystems. They will help identify these vulnerabilities before the attackers can exploit them (Chavan, 2021). Organizations must educate their employees and consumers about the meaning of IoT security. Awareness through training and best practice guidelines is necessary to prevent such vulnerabilities, as many IoT security breaches are due to human error. Furthermore, companies must also adhere to solid identity and access management (IAM) policies that restrict access to important services to only authorized users and devices.

As the IoT matures, more emerging technologies such as AI, machine learning, and blockchain will be relied upon to strengthen security measures. However, that will not be enough to reduce risks. Clear security standards must be

established, complied with, and shared, as threat intelligence will likely require a collaborative approach of industry stakeholders, government, and consumers (Vitunskaite et al., 2019). The security of IoT will depend on how well it adapts to the fast pace of technological progress, how it can respond to new threats, and how it ensures that an unbelievable number of connected devices are added daily. The top priority will be to see the next generation of security measures successfully rolled out, which, in turn, will help ensure that IoT ecosystems grow and remain trustworthy

11 Conclusion

The Internet of Things (IoT) is now one of the fastest-growing industries where every device is connected to another, and they play a crucial role in measuring data in a new way, adding value to the customer, and creating innovative products and solutions. As IoT ecosystems grow, so do the security challenges, and IoT devices face several vulnerabilities and threats? These include software, hardware, networks, weak or missing authentication mechanisms, insecure communication protocols, and insufficient updates. As there is no standard across devices and manufacturers regarding security protocols, these issues make networks more prone to breaches and attacks, leading to loss of privacy, safety, and business operations. The nature of defense against these vulnerabilities requires the IoT ecosystem to rely on sound, many-layered security and reactions that will work on a persistent but fast-changing threat landscape. Therefore, real-time threat detection, strong authentication mechanisms, encryption, secure communication protocols, and regular software updates are some solutions that are required to mitigate these. Promising is the integration of advanced technologies like artificial intelligence, machine learning, blockchain, and zero trust architecture into security. With these innovations, proactive threat detection and secure device authentication, which will increase the integrity of data, would be possible to fight against future cyberattacks.

The challenges that security will face in this space will only get bigger as the IoT space evolves, especially with the introduction of 5G networks. 5G integration will increase data volumes and interconnectivity, making monitoring and securing IoT transactions harder. The 5G has an enhanced capability of faster threat detection and more efficient security protocols. To take hold of the IoT benefits when they are set while mitigating IoT risks, businesses must take a holistic strategy for securing the gadgets they utilize and the organizations they utilize, for example, the system, putting away information, and transmission channels. There will be a growing sophistication of cyber threats, such as botnets, ransomware attacks, and supply chain vulnerabilities. Creating unified security standards, complying with the same needs, and periodic collaborative approaches between network providers, security professionals, regulatory bodies, and manufacturers. Businesses invest in continuous training for employees and customers on security, as human error factors contribute the most to data breaches.

The security of the IoT ecosystem is paramount to maintaining privacy, safety, and operational integrity, while the IoT becomes an integral part of everyone's life. The combination of emerging technologies such as blockchain and AI and the development of efficient security frameworks will be important to make IoT networks resilient against changing threats. An aggressive, coordinated effort towards IoT security will aid in securing sensitive data, building trust with consumers, and advancing the growth of IoT in the diet industries safely.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors, 21(11), 3654.

[2] Alam, T. (2021). Cloud-based IoT applications and their roles in smart cities. Smart Cities, 4(3), 1196-1219.

[3] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE communications surveys & tutorials, 22(3), 1646-1685.

[4] Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309.

[5] Ali, M. I., Kaur, S., Khamparia, A., Gupta, D., Kumar, S., Khanna, A., & Al-Turjman, F. (2020). Security challenges and cyber forensic ecosystem in IOT driven BYOD environment. IEEE Access, 8, 172770-172782.

[6] Alsaqour, R., Motmi, A., & Abdelhaq, M. (2021). A systematic study of network firewall and its implementation. International Journal of Computer Science & Network Security, 21(4), 199-208.

[7] Alwazzeh, M., Karaman, S., & Shamma, M. N. (2020). Man in the middle attacks against SSL/TLS: Mitigation and defeat. Journal of Cyber Security and Mobility, 449-468.

[8] Andersson, R., & Weigand, F. (2015). Intervention at risk: the vicious cycle of distance and danger in Mali and Afghanistan. Journal of Intervention and Statebuilding, 9(4), 519-541.

[9] Arakadakis, K., Charalampidis, P., Makrogiannakis, A., & Fragkiadakis, A. (2021). Firmware over-the-air programming techniques for IoT networks-A survey. ACM Computing Surveys (CSUR), 54(9), 1-36.

[10] Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics, 9(7), 1177.

[11] Ashraf, Q. M., & Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in Internet of Things. Journal of Network and Computer Applications, 49, 112-127.

[12] Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. In The fusion of internet of things, artificial intelligence, and cloud computing in health care (pp. 105-134). Cham: Springer International Publishing.

[13] Bernal, A. E., Monterrubio, S. M. M., Fuente, J. P., Crespo, R. G., & Verdu, E. (2021). Methodology for computer security incident response teams into IoT strategy. KSII Transactions on Internet and Information Systems (TIIS), 15(5), 1909-1928.

[14] Bibri, S. E., & Bibri, S. E. (2015). Ethical implications of AmI and the IoT: risks to privacy, security, and trust, and prospective technological safeguards. The shaping of ambient intelligence and the Internet of Things: historico-epistemic, socio-cultural, politico-institutional and eco-environmental dimensions, 217-238.

[15] Bilal, K., Khalid, O., Erbad, A., & Khan, S. U. (2018). Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers. Computer Networks, 130, 94-120.

[16] Bokefode, J. D., Bhise, A. S., Satarkar, P. A., & Modani, D. G. (2016). Developing a secure cloud storage system for storing IoT data by applying role-based encryption. Procedia Computer Science, 89, 43-50.

[17] Bompos, K. (2020). Development time of Zero-Day cyber exploits in support of offensive cyber operations (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

[18] Brandon, J. M. (2020). Educating for Security: A Qualitative Study of Non-technical Information Security Policies in Association of American Universities Member Institutions (Doctoral dissertation, Indiana University of Pennsylvania).

[19] Buchheit, M., Hirsch, F., & Martin, R. A. (2021). The Industrial Internet of Things trustworthiness framework foundations. Industrial Internet Consortium. Available online: https://www. iiconsortium. org/pdf/Trustworthiness_Framework_Foundations. pdf (accessed on 30 December 2021).

[20] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. sensors, 18(9), 2796.

[21] Butt, U. J., Abbod, M., Lors, A., Jahankhani, H., Jamal, A., & Kumar, A. (2019, January). Ransomware Threat and its Impact on SCADA. In 2019 IEEE 12th international conference on global security, safety and sustainability (ICGS3) (pp. 205-212). IEEE.

[22] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.

[23] Chandavarkar, B. R. (2020, July). Hardcoded credentials and insecure data transfer in IoT: National and international status. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.

[24] Chaudhuri, A. (2016). Internet of things data protection and privacy in the era of the General Data Protection Regulation. Journal of Data Protection & Privacy, 1(1), 64-75.

[25] Chavan, A. (2021). Eventual consistency vs. strong consistency: Making the right choice in microservices. International Journal of Software and Applications, 14(3), 45-56. https://ijsra.net/content/eventual-consistency-vs-strong-consistency-making-right-choice-microservices

[26] Costa, F. S., Nassar, S. M., Gusmeroli, S., Schultz, R., Conceição, A. G., Xavier, M., ... & Dantas, M. A. (2020). Fasten iiot: An open real-time platform for vertical, horizontal and end-to-end integration. Sensors, 20(19), 5499.

[27] Farrah, D., & Dacier, M. (2021, May). Zero conf protocols and their numerous man in the middle (MITM) attacks. In 2021 IEEE Security and Privacy Workshops (SPW) (pp. 410-421). IEEE.

[28] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of things journal, 5(4), 2483-2495.

[29] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of things journal, 5(4), 2483-2495.

[30] Geenens, P. (2019). IoT Botnet Traits and Techniques: A View of the State of the Art. Botnets, 101-164.

[31] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEe Access, 7, 82721-82743.

[32] Hoffman, S. A. E. (2020). Cybersecurity Threats in Healthcare Organizations: Exposing Vulnerabilities in the Healthcare Information Infrastructure. World Libraries, 24(1).

[33] Isler, Y., Olcuoglu, L. T., & Yeniad, M. (2018). Data security and privacy issues of implantable medical devices. Natural and Engineering Sciences, 3(3), 12-22.

[34] Krishnan, P., Duttagupta, S., & Achuthan, K. (2019). SDNFV based threat monitoring and security framework for multi-access edge computing infrastructure. Mobile Networks and Applications, 24(6), 1896-1923.

[35] Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. International Journal of Computational Engineering and Management, 6(6), 118-142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf

[36] Loghin, D., Cai, S., Chen, G., Dinh, T. T. A., Fan, F., Lin, Q., ... & Zhang, Z. (2020). The disruptions of 5G on data-driven technologies and applications. IEEE transactions on knowledge and data engineering, 32(6), 1179-1198.

[37] Loukas, G., Karapistoli, E., Panaousis, E., Sarigiannidis, P., Bezemskij, A., & Vuong, T. (2019). A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. Ad Hoc Networks, 84, 124-147.

[38] Lv, Z., Han, Y., Singh, A. K., Manogaran, G., & Lv, H. (2020). Trustworthiness in industrial IoT systems based on artificial intelligence. IEEE Transactions on Industrial Informatics, 17(2), 1496-1504.

[39] Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), 1550147717741463.

[40] Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21(2), 1636-1675.

[41] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal, 6(5), 8182-8201.

[42] Mirsky, Y., Mahler, T., Shelef, I., & Elovici, Y. (2019). {CT-GAN}: Malicious tampering of 3d medical imagery using deep learning. In 28th USENIX Security Symposium (USENIX Security 19) (pp. 461-478).

[43] Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks, 27(2), 1515-1555.

[44] Nyati, S. (2018). Revolutionizing LTL carrier operations: A comprehensive analysis of an algorithm-driven pickup and delivery dispatching solution. International Journal of Science and Research (IJSR), 7(2), 1659-1666. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203183637

[45] Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y., & Gerla, M. (2019). Challenges of multi-factor authentication for securing advanced IoT applications. IEEE Network, 33(2), 82-88.

[46] Pattanasri, T. (2018). Mandatory data breach notification and hacking the smart home: A legal response to cybersecurity? QUT Law Review, 18(2), 268-289.

[47] Razikin, K., & Widodo, A. (2021). General cybersecurity maturity assessment model: Best practice to achieve payment card Industry-Data security standard (PCI-DSS) compliance. CommIT (Communication and Information Technology) Journal, 15(2), 91-104.

[48] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 20(4), 3453-3495.

[49] Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: A survey. IEEE Access, 7, 183339-183355.

[50] Usman, M., Jan, M. A., & He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. Information Sciences, 387, 90-102.

[51] Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Computers & Security, 83, 313-331.

[52] Zandberg, K., Schleiser, K., Acosta, F., Tschofenig, H., & Baccelli, E. (2019). Secure firmware updates for constrained iot devices using open standards: A reality check. IEEE access, 7, 71907-71920.