IoT Security : Challenges & Solutions

SHRUTI NANAWARE, URWASHI PATIDAR, AJEET SINGH RAJPUT
Department of Computer Science and Engineering
Medi-Caps University
Indore, INDIA

Abstract: The Internet of things (IOT), is the present and future of today's generation, as with passing time our closeness to this device is increasing, which is giving a boost to the IOT related threats and challenges. As we know, the dependency of these devices to data is huge and data is a big asset in today's days so everyone had to ensure the safeguard of this data in any possible way. In this paper we will talk about what are these challenges and what is the solution for these challenges. As we know with an individual's duty to safeguard yourself it is also the duty of the government to make precise rules and regulations with well mentioned punishments for any crime via IOT and detailed specific IOT Guidelines.

Keywords: Internet Of Things(IOT), Security, Challenges, Solutions

Received: May 29, 2022. Revised: October 9, 2023. Accepted: November 11, 2023. Published: December 27, 2023.

1. Introduction

The concept of Internet Of Things (IOT) was introduced by Kevin Ashton, a co-founder of the Auto-ID Centre at MIT, in 1998.The vision is that objects ("things") are connected to each other and thereby they create IoT in which each object has its distinct identity and can communicate with other objects. IoT objects can vary dramatically in size from a small wearable device to a cruise ship. IoT transforms ordinary products such as cars, buildings, and machines into smart, connected objects that can communicate with people, applications and each other.[1]

IOT is basically a network of physical devices, home appliances, vehicles, etc. that are

embedded with sensors, connectivity via network and different kinds of software to share and use the database in the best possible way over the internet. The term is made up of internet which defines network connection and things here refers to the wide variety of objects from simple sensors to the very complex machinery and vehicles. It is used to automate the things around ourselves with the use of different features of Artificial Intelligence.[2]

The aim of this research is to look for challenges and security of IOT and IOT related technologies and how can we secure the IOT related technologies. As we all know these devices play an important role in our daily lives and due to which the intensity of the threats due to lack of security will be major on anyone's life. As IOT is beginning to play the basic utility role in our life in this modern developed society, one must be aware of the threat generated due to this and how to safeguard yourself from these threats.

2. Literature Review

"Internet of Things Security: A Review" by Abomhara et al. (2017)
This review article examines numerous IoT security issues and suggests potential fixes

such as secure booting, encryption, and authentication. Confidentiality, integrity, availability, authenticity, and non-repudiation are the five main IoT security goals listed by the authors. Moreover, they stress the significance of regulation and standardisation for IoT security, pushing for the creation of standards and policies. The authors draw attention to the importance of secure software upgrades, device identification, and communication protocols.[3]

"Security and Privacy Challenges in the Internet of Things" by Roman et al. (2013)
Authentication, access control, and data encryption are all part of the security architecture this study suggests in order to address the security and privacy issues in the IoT. The authors place a strong emphasis on the value of secure software updates, device identification, and communication protocols. They urge the creation of policies and educational initiatives to increase knowledge of the dangers and best practices in IoT security. They also talk about how crucial user awareness and education are to IoT security.[4]

"A Survey on Internet of Things: Security and Privacy Issues" by Alaba et al. (2017)
This survey study provides an overview of IoT security and privacy challenges and suggests solutions such as intrusion detection systems, blockchain technology, and secure communication protocols. The authors point out the difficulties in implementing security solutions in IoT devices with limited resource availability and provide resource-light security techniques. They also stress the significance of data privacy in the IoT and suggest fixes like data anonymization and encryption.[5]

"Internet of Things Security Issues and Solutions: Review" by Aazam et al. (2014)
IoT security issues are covered in this review article along with potential solutions, including safe routing protocols, network segmentation, and threat modelling. The authors stress the need for creating security architectures that can change to accommodate the dynamic nature of IoT networks and offer solutions that can identify and address security risks in real-time. Moreover, they go through the difficulties of implementing security solutions in IoT devices with limited resources and provide lightweight security mechanisms that may effectively function in these conditions.[6,7]

"Security in the Internet of Things: A Review" by Aji et al. (2017)
This research article presents an overview of the security issues with IoT and suggests solutions including biometric authentication, intrusion detection systems, and security analytics. The authors stress the significance of cooperation amongst various IoT security players, including device makers, service providers, and regulators. They also suggest using machine learning methods to enhance IoT security and identify security concerns in real-time.[8]

"IoT Security: Review, Blockchain Solutions, and Open Challenges" by Alotaibi et al. (2019)
This paper provides a comprehensive review of IoT security and highlights the potential of blockchain technology to address IoT security challenges. The authors discuss the various blockchain-based solutions for IoT security and highlight the benefits of decentralisation and immutability provided by blockchain technology. They also identify open challenges in blockchain-based IoT security,

such as scalability, interoperability, and regulatory frameworks.[9]

"Security and Privacy in Internet of Things: Challenges and Solutions" by Kumar et al. (2018)
This article explores the numerous security and privacy issues that the Internet of Things (IoT) faces and suggests solutions including secure communication protocols, access control, and data anonymization. The authors recommend a risk-based approach to IoT security and emphasise how important risk assessment and threat modelling are to IoT security. They also stress the requirement for regulation and uniformity in IoT security, pushing for the creation of security standards and recommendations.[10]

"Security Challenges for the Internet of Things" by Gubbi et al. (2013)
This essay examines the security issues with IoT and suggests remedies including access control, encryption, and security standards. The authors stress the significance of safe data transmission and storage in the Internet of Things and recommend the implementation of resource-efficient, lightweight security techniques. They also talk about the difficulties of protecting IoT devices in dynamic and diverse settings and provide solutions like device identification and trust management.[11]

"Security and Privacy Issues in IoT: A Comprehensive Review" by Siddique et al. (2020)
An overview of the security and privacy issues with IoT is given in this review article, along with suggested solutions such as secure communication protocols, intrusion detection systems, and blockchain technology. In their article, the authors stress the need of end-to-end security in the Internet of Things, including safe device provisioning, secure communication, and secure data storage. Moreover, they stress the value of user privacy in the IoT and suggest fixes such as data encryption and anonymization.[12]

"Internet of Things Security: A Survey" by Kumar et al. (2019)
An overview of IoT security issues is provided in this survey report, along with suggested solutions including device authentication, access control, and secure communication protocols. The authors stress the need of protecting the IoT ecosystem, which includes devices, networks, and applications. They also address the possibilities of AI and machine learning to boost IoT security, and they recommend using blockchain technology to improve data security and privacy.[13]

"Internet of Things Security: Review of Risks and Solutions" by Al-Fuqaha et al. (2015)
This review paper discusses the security risks in IoT and proposes solutions such as intrusion detection systems, secure communication protocols, and encryption. The authors highlight the importance of end-to-end security in IoT, including secure device authentication, data integrity, and data confidentiality. They also discuss the challenges of implementing security solutions in resource-constrained IoT devices and propose lightweight security mechanisms that can operate efficiently in such environments.[14]

"Security and Privacy in Internet of Things (IoT): A Review" by Abbas et al. (2019)
An overview of the security and privacy issues with IoT is given in this review article, along with suggested solutions including access restriction, encryption, and secure communication protocols. The authors stress the need of device authentication and trust

management for IoT security, and they suggest using blockchain technology to improve data security and privacy. Moreover, they talk about the difficulties in protecting IoT devices in dynamic and diverse settings and provide solutions like device profiling and behaviour analysis.[15]

"IoT Security: A Comprehensive Survey" by Aashma Uprety et al. (2017)
An overview of IoT security issues is provided in this thorough survey article, along with suggested solutions including encryption, authentication, and intrusion detection systems. The authors talk about the difficulties in protecting IoT devices with constrained resources and provide resource-light security solutions. Moreover, they emphasize the significance of protecting the channels of communication used by IoT devices and suggest the usage of secure communication protocols.[16]

"A Survey on IoT Security: Review, Challenges, and Solutions" by Siddiqui et al. (2021)
This review of IoT security issues makes recommendations for solutions, including device authentication, access control, and secure communication protocols. End-to-end security, including safe device provisioning, secure communication, and secure data storage, is emphasised by the authors as being crucial in the Internet of Things (IoT). They also stress the significance of ongoing IoT device monitoring and analysis in order to identify security issues and take appropriate action.[17]

3. IoT elements

Users can benefit from a variety of IoT services and amenities. They thus require certain components in order to be used effectively. IoT elements are covered in this section. Figure 1 illustrates the components required to offer IoT capabilities. These elements' names are as follows.

Fig-1 The IoT elements

3.1 Identification

Identification provides each object in a network with a clear identification. Identification involves the two processes of naming and addressing. Naming is the name of the thing, whereas addressing is its particular address. Because two or more items may share the same name, but always have a separate and unique address, these two phrases are extremely different from one another. There are several techniques that may be used to give network objects a name, including electron products codes (EPC) and ubiquitous codes [18]. IPv6 is used to give each item a special address. First, IPv4 was used to issue addresses, but owing to the high number of IoT devices, it was unable to satisfy the requirement for addressing.Therefore, IPv6 is used because it uses a 128 bit number addressing scheme.

3.2 Sensing

Sensing describes the process of gathering data from things. The gathered data is transferred to the storage medium. Actuators,

RFID tags, smart sensors, wearable sensing devices, and many more types of sensors are available to gather data from things.

3.3 Communication

One of the primary goals of the Internet of Things is communication, which is accomplished by connecting various devices and enabling communication between them. Devices used for communication may transmit and receive data such as files and messages. Numerous technologies, such as Long Term Evolution (LTE)[19], Near Field Communication (NFC)[20], Bluetooth[21], WiFi[22], and Radio Frequency Identification (RFID)[23].

3.4 Computation

By employing sensors, computation is done on the data that has been gathered from the objects. It is employed to get rid of information that is not required. To carry out the processing of IoT applications, several hardware and software platforms have been created. Audrino, Raspberry Pi, and Intel Galileo are employed as hardware platforms, but the operating system is crucial in the processing of software systems. Operating systems of many kinds, including Tiny OS[24], Lite OS[25], Android, etc., are used.

3.5 Services

The IoT apps offer four different sorts of services. An identity-related service is the first. It is used to determine which objects sent the request and who they are. Another service that gathers all of the data from objects is information aggregation. The aggregation service further handles processing. The third service is a collaborative service that decides based on the data gathered and communicates the proper replies to the devices. The final service is a ubiquitous service, which uses real-time responses from devices without regard to location or time constraints.[26,27]

3.6 Semantics

IoT is accountable for assisting people by carrying out their responsibilities. It is the most crucial component of IoT to carry out its duties. It functions as the IoT's brain. It gathers all the data and takes the necessary actions to decide what replies to send to the devices.

4. IoT Architecture

There isn't one globally accepted IoT design that everyone agrees upon. A three-layer high-level design, however, is the most often used. As seen in Fig. 2, this architecture is composed of three layers: the perception layer, the network layer, and the application layer.[29]

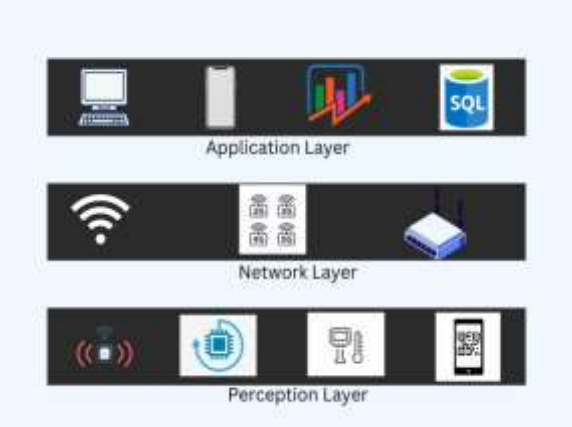

Fig-2 Three Layer Architecture

Perception layer (PL): The physical layer known as the perception layer (PL) is equipped with sensors for sensing and acquiring environmental data. It detects certain physical characteristics or locates other intelligent items in the surrounding area.

Network layer (NL): The network layer (NL) is in charge of establishing connections with other smart objects, network components, and servers. Additionally, it transmits and processes sensor data using its characteristics.

Application layer (AL): The application layer is in charge of providing users with services tailored to their particular applications. It outlines numerous IoT deployment scenarios, including smart homes, smart cities, and smart healthcare.

5. IoT Security Challenges

5.1 DOS Attack

A security attack known as denial of service (DOS) tries to block authorised access to network resources by legitimate users and entities. It is considered as the most common and effective assault. Attackers can often utilise flooding attacks to deplete a system's memory, CPU, and bandwidth [30-35]. As a result, he either stops the system from providing a service or renders it useless. Pirates can employ a variety of techniques in this assault, including delivering erroneous packets and flooding the network with messages. As a result, authorised users are blocked from using services.

5.2 Replay Attack

Replay attacks are among the most established types of assaults on communication networks, particularly against protocols for key exchange and authentication. It enables the pirate to record and save part or the entire recorded session in a genuine flow [36, 37]. As soon as the attacker has gained the confidence of the public network, he or she transmits the message that was captured to the origin session's participant or to a new destination [38]. Replay attacks are therefore regarded as a security flaw in IoT networks since they involve the unauthorised storage of specific data before it is transmitted back to the recipient. To trap the victim in an unauthorised operation is the aim of this assault [39]. For example, a temperature sensor in a smart home system measures the temperature and sends the results to the controller. The device may start or stop the air conditioner based on these parameters to adjust the air temperature to the preferences of the staff. The day's readings, however, can be saved and sent at night if an attacker has obtained the temperature of the sensor. Consequently, the air conditioner won't be operating correctly.

The three primary strategies now employed by solutions to replay attacks are the timestamp, nonce, and response-challenge. The first one is a system that looks at the message's freshness to identify replay attacks. However, ensuring time synchronisation between IoT items is challenging [40]. The nonce, which consists of a string of random numbers, is the second mechanism. The issue with this technique is that the node doesn't have enough memory to store the list of received nonces. The challenge-response mechanism is the last mechanism. Verifying that the other party can overcome some obstacles is one of its goals. However, this method requires that the two parties reveal a secret beforehand.

5.3 Password Guessing Attack

Pirates have developed different methods to get the right password because of the significance of passwords in the authentication process and the widespread usage of them by many authentication protocols. The most common attack is hence password guessing. This assault, in particular, may be carried out both online and offline. In this technique, the attacker listens in on two domains' communication during the authentication step in order to gather some helpful information. To successfully complete the authentication,

the attacker must then guess every likely password [32, 41].

5.4 Spoofing Attack

In the context of network security, a spoofing attack occurs when an unauthorised actor creates a fabricated parameter [76]. The purpose of this attack is to trick servers into thinking the attacker is a legitimate organisation [62]. Consequently, the pirate wins the government's trust. For instance, in smart health, the pirate might transmit false information to the server used for authentication. In other words, if he completed the authentication process successfully, he might ask for the victim's sensor and subsequently get the victim's confidential health information [38, 77–79].

5.5 Insider Attack

When a legitimate party with authorised access tries to compromise the system, it is known as an insider attack in the field of cyber security. The authorised entity's activity may have been unintentional or purposeful. Both times, the system is regarded as being weak, therefore an immediate fix has to be found. More than 57% of sensitive company information is reportedly the target of insider attacks. On the other hand, the analysis supports the fact that insiders were responsible for more than 60% of current attacks.

IoT Security is examined using 5 different categories referred to in below table[1].

S. No	Category	Category Description
1	Authenticity	Only the authenticated user is allowed to access information.
2	Authorization	The data available is limited and may differ for every user.
3	Confidentiality	The data shared via the network should be one to one with no intruder in between.
4	Integrity	The data is not tampered with while it is shared via network.
5	Availability	The data is available or not when the user needs it.

Table-1

6. Security Incidents

1. The security incidents brought on by IoT devices in real life are already shocking: The media reported that the Eastern United States was subjected to the worst DDoS attack in history on October 21, 2016, with attack bandwidth exceeding 1 Tbps. The

U.S. network was targeted, rendering over half of it unusable. The incident was brought on by micro-smart gadgets, such as cameras, home routers, and digital video recorders, which were widely used yet easily overlooked in daily life (DVR). These devices were infected with the Mirai malware, which led to attacks that for many hours rendered hundreds of popular websites such as Twitter and Amazon unusable.

2. On December 23, 2015, a hacker used BlackEnergy and some other malicious code related to it as their primary attack tools. They remotely controlled the power control system node to deliver the power cut-off instructions and prevented the system from recovering by erasing and covering data, shutting down, and interfering with service calls. A brief power outage that impacted more than half of the Ivano-Frankivsk region in Ukraine has a huge number of customers.
3. In 2015, a security expert from HackPWN demonstrated how to use BYD cloud service flaws to start a BYD car, open the trunk, and unlock the door [43].

7. IoT Security Tools & Technology

As we now know what are the security issues and to cope up with these issues there are different technologies to resolve the vulnerabilities of IoT.

7.1 Side-channel analysis

This approach detects both hardware malicious and trojan firmware and software which are installed by them on the device. During this process side-channel signals are analysed along with some more parameters like timing, power, and temperature. With these parameters side-channel signals are used to look for abnormal behaviour of the device, which looks for system health and if any significant character of malicious or trojan firmware is found it notifies.

7.2 Trojan activation

The aim of this strategy is to activate the trojan circuitry to detect the trojan.

7.3 Intrusion detection system (IDS)

It is a policy-based system approach. If there is any violation of any essential policies, IDS detects it in a continuous manner. It ensures that general rules and regulations are followed, and encourages a reliable approach to defend against battery-draining and sleep deprivation attacks.

7.4 Circuit modification

It counted among most used and effective methods which gives safety against the side-channel and trojan attacks.

7.5 Securing firmware update

In the process of firmware update the base broadcast announces the new version to neighbour nodes via CMD. A new advertisement (ADV) is sent to the neighbour node of this firmware update. Whichever node is willing to update this node compares the existing and ADV firmware and sends a request (REQ) if they need it. During this whole process there are many chances of DoS attack during each step, so it is most important to secure the firmware update via authentication and authorization which we have discussed in the above section.

7.6 Kill/Sleep command

It is built during the manufacturing process of RFID tags. An RFID tag has a unique PIN, e.g., a 32-bit password. Tag can be killed by receiving the unique PIN from RFID reader, for example future information is not transferred. Also, there is a process to make

command sleep for a period of time. As we know, effective pin management schemes are needed in a technique[44].

8. Solutions By Experts

We will discuss some of the points given by theoretical experts, practical experts, technical experts.

8.1 Theoretical experts

Based on a broad understanding of the security concerns for the Internet of Things' perception layer, they suggested an effective authentication and access control mechanism (IoT). A benefit of the suggested approach is that it uses elliptic curve cryptography to establish session keys (ECC). This improves intermediary procedures and mutual authentication between user and sensor nodes. On the other hand, this approach addresses the resource-constrained issue in the Internet of Things' perception layer [45].

Elliptic Curve Cryptography can be used by smart IoT devices which ensures optimization of point and field arithmetic for precise calculations and also is used in implementation of a security and access control mechanism like DCCapBAC. These designs are embedded on devices enabling distributed security approaches for IoT for end-to-end security and accessibility [5].In large-scale sensing networks, big data streaming has emerged as a key paradigm for the real-time processing of vast, ongoing data flows. A Data Stream Manager (DSM) must constantly check the security (i.e., authenticity, integrity, and confidentiality) when working with massive sensing data streams in order to guarantee end-to-end security and maintain data quality. Because real time imposes a delay in the data stream, existing solutions are not suited. We suggest a Dynamic Prime Number Based Security Verification (DPBSV) method for massive data streams in this paper. Our system is built on a shared common key that is dynamically updated by creating synchronised prime numbers. After a handshake, the common shared key updates at both ends, including source sensing devices and DSM, without additional communication [46].

It has recently been demonstrated that Public-Key Cryptography (PKC) is indeed possible on resource-constrained nodes utilising Elliptic Curve Cryptography (ECC). Yet, because the outcomes are still insufficiently pleasing, this viability does not necessarily imply appeal. In this study, we show implementation findings for Pairing-Based Cryptography (PBC), a relevant emerging topic, and ECC on two of the most widely used sensor nodes. By doing so, we demonstrate that PKC is not only practical but also appealing to WSNs. According to our knowledge, the pairing computation results on the MICA2 (8-bit/7.3828-MHz ATmega128L) and Tmote Sky (16-bit/8.192-MHz MSP-430) nodes are the most effective [47].

8.2 Practical experts

I believe that the IoT provides the following three primary dangers to consumer privacy that Ramirez likes to focus on: (1) the widespread data collection, (2) the potential for unexpected consumer data uses that could have negative repercussions, and (3) increasing security concerns. They believe the following three measures are essential for companies to implement in order to enhance user privacy and security and subsequently boost customer confidence in IoT devices: Using "security by design," "data minimization," and "increasing transparency" are the first two, while "security by design" and "giving customers notice and a choice" are the third and fourth. I believe that these steps are essential for both the growth of IoT business models and the preservation of client data privacy.[48].

A secure computing environment that is tamper-resistant is provided by security measures that are taken into account when building a device. According to the article, updates and patches, firewalling and intrusion prevention systems (IPS), device authentication, access control, and secure booting are only a few of the security measures that IoT devices must be protected against throughout their whole existence, from design to operational phases. Businesses should prioritise security above all else, and security ought to come as standard on all gadgets. In particular, businesses should: (1) conduct a privacy or security risk assessment as part of the design process; (2) test security measures prior to product launch; (3) use smart defaults, such as requiring users to change default passwords in the setup process; (4) consider encryption, particularly for the storage and transmission of sensitive information; and (5) use smart defaults.[49].

Determine the appropriate proportions to help you plan out the design area for privacy notices. This offers a taxonomy and uniform terminology of notice approaches to encourage comprehension and reasoning about notice choices available in the context of certain systems. Our knowledge systematisation and the created design space can assist designers, developers, and researchers in identifying notice and choice requirements and in creating a thorough notice concept for their system that takes into account the requirements of various audiences as well as the system's opportunities and limitations for providing notice [50].

8.3 Technical experts

Organisations and governments must alter their perspectives on security in order to reduce the growing security dangers to businesses. With this paradigm shift, security is addressed on a far more comprehensive scale at all levels of contact. The challenges, hazards, and technological benefits and disadvantages specific to the environments for the product or service must be highlighted by organisations. They need to be aware of internal capabilities, current procedures, strategies, governance, and security controls, as well as what is lacking and where the gaps are. Harbor Research is supporting this change.

The Internet of Things (IoT), also known as connected world solutions, uses machine-to-machine (M2M) technologies (such as sensors, GPS, and RFID tags) to connect physical assets to analytics and control systems through the Internet. An online study of IT and business decision-makers in 593 international companies representing the retail, manufacturing, consumer products, transportation, healthcare, government, oil/gas, and hospitality industries was commissioned by Zebra Technologies in October 2014 and was carried out by Forrester Consulting. In this study as well as a related study carried out in 2012, a few major issues were investigated.They concentrated on determining organisations' interest in IoT solutions, the deployment schedule for IoT applications, and the technical aspects of IoT solutions for which businesses seek outside help.All poll participants in these studies had decision-making or persuasion authority over their company's IoT solutions. International businesses are aware of how IoT solutions can revolutionise industries. IoT solution deployment is gaining traction among multinational corporations. IoT solutions often include Wi-Fi, real-time location monitoring, and security sensors. Using IoT solutions can help businesses reap a variety of advantages. International businesses are aware of how IoT solutions can revolutionise industries. Global enterprises have a lot of interest in deploying IoT solutions. Plans for IoT solution implementation are readily apparent among businesses and government agencies. IoT solutions are useful for asset tracking, security, and surveillance across a wide range of businesses [51].

9. Conclusion

The Internet of Things has been a major factor in the recent fast growth of technology. The communication of data is now simpler thanks to these technologies. The security of user data should not be disregarded, though. In light of this, the study conducted for this article is primarily concerned with the security of IoT technology. As a result, as we've already said, IoT is vulnerable to a number of threats, including DOS, password guessing, replay, and insider assaults. We have outlined the authentication methods used for IoT because it is the first security function that IoT must provide. One-time passwords, ECC-based mutual authentication, ID-based authentication, certificate-based authentication, and blockchain are the mechanisms most often used to enforce authentication.We found that the bulk of contemporary authentication procedures are based on encryption cryptography after comparing them.

Finally, we will propose effective and safe IoT authentication techniques in our future work in an effort to improve the security of the IoT ecosystem.

10. Future Scope

The purpose of this research was to present an overview of the most important elements of IoT with an emphasis on the difficulties and security concerns related to IoT devices. There are still a number of issues and difficulties with the IoT's security. Future research and development in IoT security will have many intriguing potentials as a result of the combination of IoT and cloud computing. Listed below are some possible areas of concentration on this subject:

1. **Secure data transfer:** Secure data transfer between IoT devices and the cloud will become more and more important as more of these devices are linked to cloud platforms. New methods for safeguarding data flow in IoT systems, such as encryption and secure communication protocols, might be the subject of research. The usage of hybrid encryption techniques, including symmetric and asymmetric encryption, may be investigated in order to increase the security of data transit in IoT systems.

2. **Scalability and performance:** There will be a need for new methods of organising and analysing data in the cloud as IoT systems expand. New cloud-based architectures and algorithms that can effectively manage enormous amounts of data from IoT devices might be the subject of research. In order to allow real-time processing of IoT data while simultaneously assuring the scalability and dependability of cloud-based IoT systems, this might entail investigating the usage of distributed computing and edge computing.

3. **Multi-tenancy:** There will be a demand for multi-tenancy solutions that can securely isolate data from various users and apps as more businesses utilise IoT devices and cloud platforms. Research should concentrate on creating fresh methods, such virtualization and containerization, for establishing multi-tenancy in IoT systems. Investigating the usage of microservices architectures to provide safe data and application separation in cloud-based IoT systems might be one way to do this.

4. **Cost and energy efficiency:** Cost- and energy-effective methods of connecting IoT devices with the cloud

will be required as these devices become more widely used. Study findings might focus on creating fresh methods for decreasing the price of cloud-based services and optimising the energy usage of IoT devices. In order to identify energy-intensive activities and optimise the use of resources in IoT systems, this might include investigating the use of machine learning and data analytics.

5. **Privacy and data protection:** Privacy and data protection will be more and more crucial as more and more data is gathered by IoT devices and stored in the cloud. Study findings may focus on creating novel methods, such as data anonymization and access control mechanisms, for safeguarding sensitive data in cloud-based IoT systems. Investigating the use of blockchain technology to provide safe, decentralised IoT data management and storage might be part of this.

6. **Cloud-based security solutions:** Cloud-based security solutions that are capable of handling security risks in IoT systems will be required due to the complexity of IoT security concerns. New strategies for adopting cloud-based security solutions, such as intrusion detection and prevention systems and security information and event management (SIEM) systems, might be the subject of research. This might entail investigating the application of AI and ML to automate threat detection and response in cloud-based IoT systems.

References

[1] The Future of IoT: Trends and Predictions for 2023 and Beyond https://www.geekcoders.store/2023/02/the-future-of-iot-trends-and.html?m=1

[2] R&D Department, Vestel Electronic Inc., Manisa, Turkey 2011 https://www.scirp.org/journal/paperinformation.aspx?paperid=73675

[3] "Internet of Things Security: A Review" by Abomhara et al. (2017) https://www.researchgate.net/publication/269687360_Security_and_privacy_in_the_Internet_of_Things_Current_status_and_open_issues

[4] "Security and Privacy Challenges in the Internet of Things" by Roman et al. (2013) https://www.nics.uma.es/pub/papers/1633.pdf

[5] "A Survey on Internet of Things: Security and Privacy Issues" by Alaba et al. (2017) https://www.sciencedirect.com/science/article/abs/pii/S1084804517301455

[6] "Internet of Things Security Issues and Solutions: Review" by Aazam et al. (2014) https://khu.elsevierpure.com/en/publications/cloud-of-things-integration-of-iot-withcloud-computing-2

[7] "Internet of Things Security Issues and Solutions: Review" by Aazam et al. (2014)https://www.researchgate.net/publication/315835782_Internet_of_things_Security_A_Survey

[8] "Security in the Internet of Things: A Review" by Aji et al. (2017)

[9] “IoT Security: Review, Blockchain Solutions, and Open Challenges" by Alotaibi et al. (2019) https://www.researchgate.net/publication/321017113_IoT_Security_Review_Blockchain_Solutions_and_Open_Challenges

[10] "Security and Privacy in Internet of Things: Challenges and Solutions" by Kumar et al. (2018) https://www.researchgate.net/publication/357393481_A_Systematic_Literature_Review_on_the_Cyber_Security

[11] "Security Challenges for the Internet of Things" by Gubbi et al. (2013) https://www.researchgate.net/publication/344417463_THE_INTERNET_OF_THINGS_CHALLENG

ES_-_COUNTRY_AND_INDUSTRY_ANALYSES

[12] "Security and Privacy Issues in IoT: A Comprehensive Review" by Siddique et al. (2020)

https://ieeexplore.ieee.org/abstract/document/8035317

[13] "Internet of Things Security: A Survey" by Kumar et al. (2019) https://www.researchgate.net/publication/315835782_Internet_of_things_Security_A_Survey

[14] "Internet of Things Security: Review of Risks and Solutions" by Al-Fuqaha et al. (2015) https://arxiv.org/abs/1805.11011

[15] "Security and Privacy in Internet of Things (IoT): A Review" by Abbas et al. (2019) https://www.researchgate.net/publication/340893540_Security_and_Privacy_in_the_Internet_of_Things_IoT_Survey

[16] "IoT Security: A Comprehensive Survey" by Aashma Uprety et al. (2020) https://www.researchgate.net/publication/347188214_Reinforcement_Learning_for_IoT_Security_A_Comprehensive_Survey

[17] "A Survey on IoT Security: Review, Challenges, and Solutions" by Siddiqui et al. (2021) https://www.sciencedirect.com/science/article/pii/S2542660522000592

[18] Koshizuka, N.; Sakamura, K. Ubiquitous ID: Standards for ubiquitous computing and the Internet of Things. *IEEE Pervasive Comput.* **2010**, *9*, 98–101. https://ieeexplore.ieee.org/document/5586696

[19] Crosby, G.V.; Vafa, F. Wireless sensor networks and LTE-A network convergence. In Proceedings of the IEEE 38th Conference on Local Computer Networks (LCN), Sydney, Australia, 21–24 October 2013; pp. 731–734. https://ieeexplore.ieee.org/abstract/document/6761322

[20] Want, R. Near field communication. *IEEE Pervasive Comput.* **2011**, *10*, 4–7. https://ieeexplore.ieee.org/document/5958681

[21] McDermott-Wells, P. What is bluetooth? *IEEE Potentials* **2004**, *23*, 33–35. https://ieeexplore.ieee.org/document/1368913

[22] Ferro, E.; Potorti, F. Bluetooth and Wi-Fi wireless protocols: A survey and a comparison. *IEEE Wirel. Commun.* **2005**, *12*, 12–26. https://ieeexplore.ieee.org/document/1404569

[23] Want, R. An introduction to RFID technology. *IEEE Pervasive Comput.* **2006**, *5*, 25–33. https://ieeexplore.ieee.org/document/1593568

[24] Levis, P.; Madden, S.; Polastre, J.; Szewczyk, R.; Whitehouse, K.; Woo, A.; Gay, D.; Hill, J.; Welsh, M.; Brewer, E.; et al. TinyOS: An operating system for sensor networks. *Ambient Intell.* **2005**, *35*, 115–148. https://link.springer.com/chapter/10.1007/3-540-27139-2_7

[25] Cao, Q.; Abdelzaher, T.; Stankovic, J.; He, T. The liteos operating system: Towards unix-like abstractions for wireless sensor networks. In Proceedings of the International Conference on Information Processing in Sensor Networks, 2008 (IPSN'08), St. Louis, MO, USA, 22–24 April 2008; pp. 233–244. https://ieeexplore.ieee.org/abstract/document/4505477

[26] Xing, X.J.; Wang, J.L.; Li, M.D. Services and key technologies of the Internet of Things. *ZTE Commun.* **2010**, *2*, 011. https://www.scirp.org/journal/paperinformation.aspx?paperid=6306

[27] Gigli, M.; Koo, S. Internet of things: Services and applications categorization. *Adv. Internet Things* **2011**, *1*, 27. https://www.scirp.org/journal/paperinformation.aspx?paperid=6306

[28] M. Wu, T.J. Lu, F.Y. Ling, et al., "Research on the architecture of Internet of Things," In 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Vol. 5, pp. V5-484–V5-487, IEEE, 2010

[29] P. Sethi, S.R. Sarangi, "Internet of things: architectures, protocols, and applications," Journal of Electrical and Computer Engineering, 2017.

[30] S. Prabhakar, "Network security in digitalization: attacks and defence," International Journal of Research in Computer Applications and Robotics, vol. 5, no. 5, pp. 46–52, 2017.

[31] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702–2733, 2019.

[32] H. C. Hasan, F. N. Yusof, and M. Daud, "Comparison of authentication methods in internet of things technology," International Journal of Computer and Systems Engineering, vol. 12, no. 3, pp. 231–234, 2018.

[33] A. Ahmed, R. Latif, S. Latif, H. Abbas, and F. A. Khan, "Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review," Multimedia Tools and Applications, vol. 77, no. 17, pp. 21947–21965, 2018.

[34]] K. C. Archana and N. Harini, "Mitigation of spoofing attacks on IOT home networks," International Journal of Engineering and Advanced Technology, vol. 9, no. 1S, pp. 240–245, 2019.

[35] Y. Javed, A. S. Khan, A. Qahar, and J. Abdullah, "Preventing DoS attacks in IoT using AES," Journal of Telecommunication, Electronic and Computer Engineering, vol. 9, no. 3–11, pp. 3–11, 2017.

[36] H. C. A. van Tilborg and S. Jajodia, Encyclopedia of Cryptography and Security, Springer US, Boston, MA, 2011.

[37] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027–2051, 2016.

[38]] S. Behrooz and S. Marsh, "A trust-based framework for information sharing between mobile health care applications," in Proceedings of the IFIP International Conference on Trust Management, pp. 79–95, Darmstadt, Germany, July 2016.

[39] P. Rughoobur and L. Nagowah, "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare," in Proceedings of the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), pp. 811–817, Dubai, United Arab Emirates, December 2017.

[40] Y. Feng, W. Wang, Y. Weng, and H. Zhang, "A replay-attack resistant authentication scheme for the internet of things," in Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), pp. 541–547, Guangzhou, China, July 2017.

[41] M. Azrour, Y. Farhaoui, and M. Ouanan, "Cryptanalysis of farash et al.'s SIP authentication protocol," *International Journal of Dynamical Systems and Differential Equations*, vol. 8, no. 1/2, 2018.

[42] A. K. Sahoo, A. Das, M. Tiwary, "Firewall engine based on graphics processing unit," In 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, IEEE, pp. 758–763, 2014.

[43] Zhejiang Dahua:Security of the Internet of Things Technical White Paper:DAHUA TECHNOLOGY CO., LTD.(2017)

https://www.dahuasecurity.com/asset/upload/uploads/soft/20181120/IoT-Security-Technology-White-Paper_V1_0_0-20180104.pdf

[44]A Comprehensive Study of Security of Internet-of-Things

https://ieeexplore.ieee.org/ielaam/6245516/8128656/7562568-aam.pdf

[45]Ye, N., et al.: An efficient authentication and access control scheme for perception layer of internet of things. Appl. Math. Inf. Sci. 8(4), 1617 (2014)

https://www.researchgate.net/publication/258509303_An_Efficient_Authentication_and_Access_Control_Scheme_for_Perception_Layer_of_Internet_of_Things

[46]Puthal, D., et al.: A dynamic prime number based efficient security mechanism for big sensing data streams. J. Comput. Syst. Sci. 83(1), 22–42 (2017)

https://www.sciencedirect.com/science/article/pii/S0022000016000209

[47]Szczechowiak, P., et al.: NanoECC: testing the limits of elliptic curve cryptography in sensor networks. In: Wireless Sensor Networks, pp. 305–320. Springer, Berlin (2008)

https://www.researchgate.net/publication/221420440_NanoECC_Testing_the_Limits_of_Elliptic_Curve_Cryptography_in_Sensor_Networks

[48]Ramirez, E.: Privacy and the IoT: Navigating Policy Issues. US FTC, Washington (2015)

https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf

[49]Shipley, A.: Security in the Internet of Things. Wind River, September 2014 (2015)

https://events.windriver.com/wrcd01/wrcm/2016/08/WP-IoT-security-in-the-internet-of-things. pdf

[50]Schaub, F., et al.: A design space for effective privacy notices. In: Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (2015)

https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf

[51] Zebra Internet-Of-Things Solution Deployment Gains Momentum Among Firms Globally,

A Forrester Consulting Thought Leadership Paper Commissioned By Zebra Technologies,

October 2014

https://halberdbastion.com/sites/default/files/2018-01/Forrester-IoT-Gains-Momentum-Globally-2014.pdf