Journal of Advances and Scholarly Researches in Allied Education
Vol. 21, Issue No. 5, July-2024, ISSN 2230-7540

Internet of things (IOT) Security: Challenges & Solutions

Akshat Gupta*

Student, Class 12th, St Joesph's Academy, Dehradun, Uttarakhand, India

Email: heyitsakshatt@gmail.com

Abstract - The fast expansion of the Internet of Things (IoT) has led to the transformation of several sectors via the connectivity of devices and the ease of real-time data collecting. However, important security vulnerabilities have emerged as a consequence of the expansion of Internet of Things systems, putting their availability, confidentiality, and integrity at risk. A comprehensive overview of the primary security issues related to the Internet of Things (IoT) is the goal of this write-up. Faults in software integrity, network connection, data encryption, and device authentication are among these issues. This essay delves into the peculiar threats posed by resource-constrained Internet of Things devices and the prospect of widespread cyberattacks. Modern, state-of-the-art methods for avoiding these threats are also included in the research. Some examples of these frameworks include blockchain-based cryptographic protocols, intrusion detection systems, robust access control methods, and lightweight cryptographic protocols. By reviewing the current state of affairs and looking ahead to future developments, this paper aims to provide academics and practitioners with the knowledge they need to enhance the security of the Internet of Things (IoT) and make it possible to safely implement IoT technologies in many different industries.

Keywords - Internet of Things, Cyber-attacks, encryption, Challenges, Solution.

----------X----------

1. INTRODUCTION

In the technological industry, things have changed drastically in recent years. And now it's a part of our everyday lives, which is much more vital than before. Among these more contemporary inventions, the IoT has been attracting an increasing number of users while also advancing at a steady rate. This growth has benefited several areas, such as smart grid, water management, education, social security, agriculture, and home security, to name a few. As a result, the number of internet-enabled devices continues to rise every day. In 2025, there will be over 38 billion connected products; by 2030, that number will rise to 50 billion. Strategy Analytics is the source of this data.

The relatively new concept of the Internet of Things (IoT) allows for the possible connection of various digital and physical items. The truth is that the Internet originated as a small network connecting personal computers. The Internet eventually gave rise to a slew of associated technologies, such as the World Wide Web, electronic mail, file sharing, and client-server architecture networks. Next, the information is sent to a wide area network, which links together a multitude of smart devices integrated into complex systems, numbering in the billions. Their ability to see, respond to, and manipulate their physical environment is derived from the sensors and actuators that comprise their core functioning.

Despite its many benefits, the Internet of Things (IoT) has three major drawbacks: data gathering, data transfer, and data security. In order to facilitate data collection by means of IoT devices, a multitude of sensing technologies have been developed and adapted. Several protocols have been created and improved so that Internet of Things devices may talk to one other and to networks that already exist. The objective is to streamline the process of sending the gathered data. Having said that, the final one doesn't get nearly enough love and attention. There are a lot of current and past security difficulties that are inherently tied to authentication, data security, authorization, and the Internet of Things (IoT). Actually, authentication flaws may lead to a wide variety of attacks, such as replay attacks, Denning-Sacco attacks, DOS assaults, password guessing attacks, and many more.

Nevertheless, authenticating IoT devices across several coupled protocols is a significant difficulty. Issues pertaining to the limitations of Internet of Things devices must also be considered by these protocols, including power consumption, memory restrictions, and computational capacity.

The Internet of Things (IoT) has emerged as a paradigm shift that has the potential to revolutionise the way we interact with common items by converting them into intelligent gadgets that are networked and capable of interacting and

exchanging data. On the Internet of Things (IoT), applications may be found in a broad variety of fields, ranging from smart homes and wearable gadgets to industrial automation and smart cities. These applications promise to improve efficiency, convenience, and innovation. The fast expansion of Internet of Things devices, on the other hand, has simultaneously generated substantial security issues. In light of the fact that billions of devices are linked to one another, each of which is susceptible to cyberattacks, Making sure that networks connected to the Internet of Things are secure has become paramount.

There is a vast array of issues related to Internet of Things security, such as the protection of data privacy, the authentication of devices, the integrity of networks, and the ability to withstand hostile assaults. These difficulties are made much more difficult by the variety and resource restrictions of Internet of Things devices, as well as by the broad deployment of these devices in areas that are often insecure. It is common for traditional security techniques, which were developed for normal computer systems, to be insufficient for the specific needs of Internet of Things ecosystems. Consequently, to ensure the security of infrastructures supporting the Internet of Things, it is necessary to use innovative methodologies and comprehensive tactics. When it comes to Internet of Things security, one of the most significant difficulties is the sheer number and variety of devices. Integrating a wide range of sensors, actuators, and processing units, each of which has a unique set of capabilities and vulnerabilities, is what Internet of Things systems do. Solutions that are strong and scalable, as well as those that are able to adapt to a variety of settings and use cases, are required in order to guarantee the safety of such a wide variety of devices. In addition, Internet of Things devices usually function with limited computing power and battery life, which necessitates the implementation of lightweight security methods that do not compromise performance.

An additional crucial aspect is ensuring the data's secrecy and integrity. Devices connected to the internet regularly gather and transmit a broad range of sensitive data, including medical records and signals used in industrial control systems. Identity theft, financial loss, and disruption of vital services are just a few of the serious consequences that may emerge from unauthorised access to sensitive data. Providing end-to-end encryption, secure data storage, and effective access control techniques is vital for maintaining an efficient Internet of Things security architecture.

Also, many other types of cyber-attacks may compromise Internet of Things (IoT) devices due to their interconnected design. Some examples of these dangers include malware, Distributed Denial of Service (DDoS) attacks, and vulnerabilities in older systems that hackers exploit. Cybercriminals may take over IoT devices as they try to steal information, halt operations, or target other computer systems connected to a network. Complete threat detection and response systems must be implemented to strengthen Internet of Things networks and make them less vulnerable to these dangers.

In order to effectively handle these difficulties, it is essential to use a multi-layered security strategy. The implementation of strong device authentication and authorization procedures, the guarantee of secure communication routes, the deployment of frequent software updates and patches, and the cultivation of a culture of security awareness among users and stakeholders are all included in this. Moreover, cutting-edge innovation like blockchain, AI, and ML could bring fresh approaches to bolstering the safety of the IoT.

This essay delves into the many security issues associated with the IoT and offers several solutions to these challenges. The goal of this study is to offer a full overview of how to properly protect Internet of Things (IoT) systems by analysing the dangers that are now present and assessing the different security frameworks and solutions. The purpose of this research is to provide a contribution to the current efforts to develop Internet of Things ecosystems that are both safe and robust. This will be accomplished via a mix of theoretical insights and practical suggestions.

2. LITERATURE OF REVIEW

Mazhar et al. (2023) A widely recognised technology, the Internet of Things (IoT), greatly impacts several fields, including networking, employment, healthcare, and the economics, among others. Internet of Things (IoT) devices have the ability to automate tasks, increase productivity, and decrease anxiety in many places, including smart cities and schools. Cyberattacks and other forms of cyber danger have a significant impact on what the Internet of Things deems as intelligent applications. Many traditional approaches to protecting the IoT have proven insufficient due to the proliferation of new vulnerabilities and threats. The future of the Internet of Things (IoT) depends on AI-powered deep learning and machine learning to keep security measures intact. It is critical to use the capabilities of artificial intelligence, namely machine and deep learning solutions, to guarantee that the security system of the next-generation Internet of Things system is updated and adaptable. Internet of Things security intelligence is examined in this study from every possible angle. An new strategy for protecting Internet of Things devices against various attacks is to use machine learning and deep learning to extract information from raw data. We wrap up by discussing the important areas for further study and suggest some next steps that may be based on our findings. Finding attack patterns in unstructured data and safeguarding Internet of Things devices is the goal of this article's investigation into machine learning and deep learning. We use these findings as a springboard to discuss the challenges

researchers face and the potential solutions for this area of study moving forward. Anybody interested in cybersecurity or the Internet of Things (IoT) may use this website's content as a technical reference and resource.

Rajmohan et al. (2022) The security of smart systems built on the Internet of Things (IoT), which include sensors, actuators, and distributed control loops, is very important yet difficult to manage. The foundation of information security patterns is time-tested, domain-agnostic security expertise. In the context of developing IoT-based smart systems, why are they crucial? Do any existing designs provide enough protection for the Internet of Things? The purpose of this study is to systematically review the literature on IoT security designs and patterns (including privacy). Conversely, we want to analyse the research environment so that we can give solutions to our research questions. Following these well-established guidelines allows us to conduct thorough systematic literature reviews. We have meticulously sorted through and evaluated thirty-six (36) peer-reviewed articles published between 2010 and 2020 concerning IoT security and privacy patterns and designs. We started our search with thousands of potential papers, and these were among the ones we ultimately found. From what we can see, there has been a rise in the amount of articles covering designs and patterns for IoT security in the previous three years. So far, we haven't found a solution that takes into account both architectural and network/Internet of Things device level security (and privacy) issues by methodically applying designs and patterns together. Furthermore, we looked at how the primary studies' research contributions deal with the different issues included on the OWASP IoT top ten vulnerabilities list. Finally, we address the current knowledge gaps in this area and propose solutions to promote the adoption of patterns for privacy- and security-by-design in the Internet of Things (IoT).

Azrour et al. (2021) In computing, the phrase "Internet of Things" (IoT) describes a vast network that allows many smart devices and objects to exchange data and instructions remotely. In order for the Internet of Things to function, there must be sensing, processing, and data transfer. Domestic, healthcare, telecommunications, environmental, industrial, building, water management, and energy are just a few of the many sectors that are already making use of the new Internet of Things technologies. Embedded devices are at the heart of Internet of Things technology, which is distinct from traditional computing platforms. The possibility of connecting the physical and virtual worlds, as well as the flow of personally identifiable information generated by sensors, makes security a critical concern for IoT devices. The Internet of Things also need solutions for lightweight encryption. So, to help design authentication systems that will guarantee the security of IoT services, this article aims to predict the main security concerns and challenges surrounding the IoT.

Afzal et al. (2021) The Internet of Things paradigm envisions a future in which billions of networked devices are endowed with artificial intelligence, internet connection, sensing and actuation capabilities, and other capabilities. Instead of having a limited number of powerful computer devices in our life, the theory makes the assumption that we should have a vast number of gadgets that are relatively less powerful than the others. To put it another way, incorporating the power to do computations and access the internet into almost every commonplace item that we own. On the other hand, "ubiquitous computing" was a term that was used in the past to refer to the same concept. The Internet of Things has lately improved the idea of internet convergence. Internet of Things security is a complex and challenging topic. It is possible for integrity breaches to originate from a wide number of sources, none of which are incompatible with one another. As a result of the fact that this technology is still in its earlier phases, both customers and vendors are searching for the most advantageous choices. There are many different types of security problems that may arise with the Internet of Things. Some examples include malware threats and system hijacking, inadequate consumer awareness owing to a lack of understanding, a lack of approved fixes, and malicious Internet of Things apps. For example, users should take precautions to ensure that the Internet of Things network is kept separate from other networks in order to reduce the impact of inadequate security. You will be able to save both time and money if you steer clear of plug-and-play capabilities. When cloud computing is not used Passwords for Internet of Things devices need to be unique and difficult to guess.

Litoussi et al. (2020) In a major way, the Internet of Things (IoT) impacts every facet of our everyday lives. It includes a broad variety of technology, from small wearable gadgets to large-scale industrial networks. Constructing Internet of Things (IoT) technology should improve people's quality of life. Securing the Internet of Things requires intricate solutions, yet there are many risks against it. Among the primary goals of Internet of Things (IoT) security is the protection of customer data and personal information, the upkeep of secure infrastructure and devices, and the assurance of service availability within an IoT ecosystem. Examining the potential dangers of the Internet of Things (IoT) and providing ways to avoid them is the focus of this book.

3. ARCHITECTURE OF THE (IoT)

A proposed definition of the phrase "Internet of Things" is a standard for describing a vast network that links many various types of embedded sensors, actuators, and microcontrollers. The Internet of Things (IoT) encompasses a wide variety of interconnected objects, such as mobile phones, computers, irrigation systems, cars, medical equipment, industrial gear, cellphones, and refrigerators. Further, although earlier designs consolidated both traditional, mobile, and sensor-

based Internet networks into a single entity, the Internet of Things is a more recent innovation that separately addresses these issues. Many hybrid terminals are used by the Internet of Things. Internet connectivity means that many of these devices can communicate with common web protocols like HTTP, JSON, and XML. Because of its widespread acceptance, this technology may be tailored to work with a wide range of preexisting infrastructures, which is a major plus. And there are a number of potential new protocols for the IoT that are being considered. The HTTP protocol has equivalents like CoAP and MQTT, while the IPv4 and IPv6 network protocols have alternatives like 6LoWPAN.

When it comes to the Internet of Things (IoT), there are several designs that are distinct from one another. However, the emphasis of this article is on two well-known architectures, which are three- and five-layer structures respectively. The three-layer architecture is comprised of three levels, which are the perception layer, the networking layer, and the application layer, as shown in Figure 1. The following is a description of the function that each layer serves.

1. The initial layer of the Internet of Things architecture is called the perception layer. It is linked to the physical world in order to sense and gather data from their surroundings based on their surroundings. This layer is made up of sensors and actuators that are able to detect certain functionalities, such as motion and location, and to quantify variables like light, gas, temperature, pH, and so on.

2. The second layer is known as the network layer, and its primary function is to establish connections with a variety of smart devices, gateways, and servers. It is in charge of transmitting the values that have been collected to other components of the Internet of Things network. Due of these factors, When it comes to communication, the Internet of Things uses a plethora of protocols and standards, such as 4G/5G, Wi-Fi, ZigBee, Bluetooth, 6LoWPAN, WiMAX, and many more.

3. The service the user has requested may be delivered by the application layer. Some patient health measures, for

4. instance, may be made available to doctors under this scheme. The applications that may be deployed are determined by this layer. Some examples of these applications are water monitoring, smart homes, and smart environments.

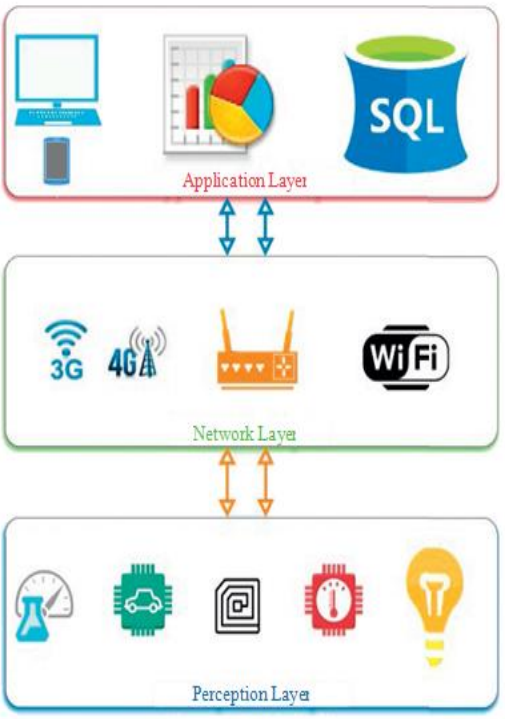
5. 

Figure 1: The architecture with three layers

However, the five-layer architecture incorporates not just the three levels carried over from the previous design, but also the processing and business layers. The five levels are shown in Figure 2. These layers are the perception, transport, processing, application, and business layers. Each of the three levels of a three-layer architecture performs the same functions as its corresponding layer. This includes perception, transport, and application. The roles played by the addition layers are described in detail below:

1. The processing layer goes by many names than just that; one of them is the middleware layer. Furthermore, it is accountable for the management, analysis, processing, and storage of the data that has been received. Without the need for human interaction, it is able to make judgements based on the data that is being processed. Cloud computing, big data, and database management are some of the present solutions that are beneficial to this layer.

2. It is the job of the business layer to manage the whole of the Internet of Things (IoT) systems. Application, business, and profit model control is its primary purpose. Further, this layer may control the limitations that users have on their privacy.

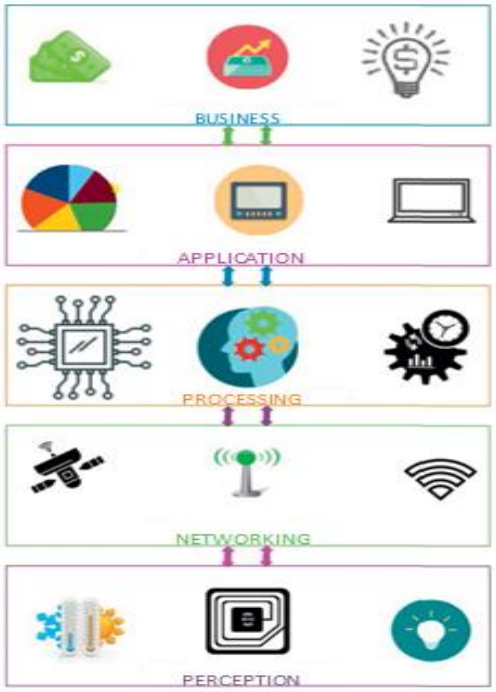


Figure 2: The architecture with five-layer

4. IoT SECURITY CONCERNS

- **DOS:** The goal of a (DOS) attack is to prevent legitimate users and organisations from gaining access to a network's resources. Most people agree that it's the best and most common attack. In order to exhaust a system's resources, such as memory, CPU, and bandwidth, attackers often use flooding assaults. Consequently, he either makes the system useless or completely disables it. As part of this attack, pirates may use a number of methods, such as flooding networks with messages or delivering unwanted packets. Therefore, legitimate customers are unable to utilise the services.

- **The Attack by Replay:** One of the older forms of assaults on communication networks is the replay attack, which targets protocols for key exchange and authentication. With this function, the pirate may capture a lawful traffic session and save it in part or in its whole. With the support of the general population.

- **Attack via Guessing Password:** Because passwords are crucial to the authentication process and are widely used by many authentication protocols, pirates have developed a number of methods to figure out the proper one. As a result, password guessing is the most popular attack. In particular, this assault may be carried out offline or on the internet. In this method, the hacker listens in on the authentication discussion between two parties in order to steal sensitive information. Then, the attacker has to try every possible password until they succeed with the authentication procedure.

- **Spoofing Attack:** A spoofing attack occurs when an unauthorised party generates a false parameter in the context of network security. This attack aims to fool servers into thinking the attacker is a legitimate party. Thus, the authority begins to trust the pirate. For instance, a pirate may provide fictitious information to an authentication service in the smart health space. Thus, if he completed the authentication process successfully, By requesting the victim's sensor, he could access the victim's private medical records.

- **Insider Assault:** Within the realm of cyber security, an insider attack transpires when an authorised entity with lawful access attempts to compromise the system. An authorised entity's activity may be unintentional or purposeful [80–84]. The system is deemed insecure in both situations, thus we need to quickly identify a fix. More than 57% of sensitive company data are the target of insider attacks.

5. IoT REQUIRES SECURITY SERVICES

This section discusses a few security services after discussing different security assaults used by attackers. Therefore, the purpose of this part is to go over the essential steps for Internet of Things device security. The most important components of any Internet of Things (IoT) system's security are listed in Table 1. Among these components are the following: non-repudiation, availability, secrecy, authenticity, and permission.

Table 1: Security Requirements of basic IoT Layer

Security services	Perception	Networking	Application
Authentication	✓	✓	✓
Authorization	✓	✓	✓
Confidentiality	✓		
Availability	✓	✓	
Integrity	✓	✓	✓
Non-repudiation		✓	

- **Private information:** As a rule of thumb, the capability to prevent unauthorised access to personal information is what constitutes confidentiality. Therefore, it guarantees and assures that no unauthorised parties will be able to access, modify, or delete personal data. Particularly, secrecy is a crucial security feature in the IoT network. The most focused service, however, is privacy. Trojan horses, spyware, and viruses are examples of malware software that may infiltrate a user's system and steal sensitive data. They might use scripts or executable software to get illegal access to the machine. To protect sensitive information gathered by sensors and prevent unauthorised parties from accessing it, cryptographic methods and algorithms may be used within the framework of the Internet of Things. Consequently, encryption is a must for any data sent between devices.

Consequently, the message can only be understood by approved entities.

- **Availability:** Internet of Things security services also include making resources available to legitimate organisations at all times, no matter where they are or what time of day it is. For resources and data to be considered available, they must be accessible to authorised users at all times. On top of that, sensors may find a home in the IoT framework if they could provide their perceived data in real time. The existence of an actuator also suggests that it can react quickly and accurately to human commands. Disruptions to the availability of particular resources may occur as a consequence of using multiple networks, protocols, and data transmission methods. However, there are three main malicious techniques that attackers might utilise to threaten availability: denial of service (DOS), flooding, and black hole. For the first, it's usually used in an availability situation. Pirates have access to technologies such as distributed denial of service (DDOS) attacks, which include several resources working together, and simple denial of service (DOS) attacks. By sending out an excessive amount of unwanted messages and requests, an attacker may overload a device's resources in a flooding attack. In addition to targeting bandwidth, this attack decreases CPU and memory capacity. This means that either the device is unreachable or the connection is slow. To make sure the resources we need are available, we may use one of several platforms that facilitate remote system integration or choose for a distributed approach to system operation.

- **Verification:** One of the biggest problems with an IoT network is the authentication service. One component of it is the verification of identity. On the one hand, devices need to be able to authenticate remotely via a public network and confirm the legitimacy of the use. On the other hand, authentication ensures that only authorised persons may join a private, encrypted chat. One element, a simple password, was used by earlier authentication mechanisms. But there are a lot of password-related issues that these solutions have to address. Password forgetting is a common problem among users. Passwords that users use could be inadequate. After much research and a dictionary attack, hackers manage to figure out the correct password. Therefore, authentication using passwords alone cannot ensure safety. Authentication methods based on smart cards now provide multifactor authentication. In most cases, a functional smart card and the correct preshared secret are required by the system. However, fingerprint biometrics are a part of it. The next two sections will discuss various authentication techniques and analyse many proposed IoT authentication schemes, both of which are essential for the security of the Internet of Things.

- **Validation:** With more and more devices becoming online, authentication is becoming an increasingly pressing issue for IoT systems. In reality, it's a reference to the security agency that determines the level of access permissions (read, write, and delete) for each user. In addition, the criteria for access control that are used to authorise or deny IoT devices are laid forth in it. Consequently, it is problematic to allow limited users to acquire additional permissions that would allow them to get illegal access to devices and their data.

- **Fairness:** By maintaining its integrity, a message ensures that no unauthorised third party changed it while it was in transit. Hence, it verifies that the receiver has received the exact identical message as the sender. Keeping an unapproved item from being illegally changed is the main objective. For Internet of Things (IoT) networks to keep smart devices secure, the system must guarantee data integrity. Consequently, it is imperative that neither unauthorised users nor items be permitted. Additionally, cryptography and encryption methods may be used while transferring crucial data. As an example, in order to guarantee data integrity, the authors of suggested using the HMAC-SHA 256 approach.

- **The Ignorance of Truth:** One of the security features that guarantees that participants in a communication may communicate or receive information in its entirety is non-repudiation. Furthermore, it ensures that there is no denying the unquestionable transmission of identify or data between two IoT items. Non-repudiation ensures that a source node will provide its data and that a receiving node will verify that the data received matches the original source.

6. METHODS FOR IoT AUTHENTICATION

The privacy of users must be safeguarded from malevolent attacks as a result of IoT's capacity to access all user data. Unauthorized users should also not be able to access the devices. Thus, verifying the user's identity is required prior to granting authority. Therefore, there are various methods available for verifying the identity of a user. Still, the most popular is the authentication system that uses previously shared passwords, keys, or secrets. As a result, we examine the methods used to strengthen authentication in an Internet of Things context in this section.

- **Authentication with One-Time Password:** A dynamic password, or one-time password (OTP), is a password that only has to be entered once in order to authenticate a single transaction. To protect data transfer in an Internet of Things (IoT) environment, the reviewed literature suggests many OTP authentication techniques. The construction of these protocols incorporates a number of

methods, including time synchronisation, hash fractions (MD5, SHA1, and SHA256), and RSA cryptography. However, as they are all based on Lamport's OTP algorithm, these protocols are open to many kinds of attacks. On the flip side, in 2013, Lee and Kim introduced a bilinear map based OTP method that is immune to insider attacks, which strengthens OTP authentication. However, it requires complex computation. Given the gravity of the situation, Shivraj et al. put up a strong OTP solution tailored to the IoT. Slim identity-based elliptic curve encryption and Lambport's One-Time Password (OTP) technique form the basis of the suggested protocol.

- **Mutual Authentication Using ECC:** Internet of Things devices often have limited resources. Nodes, objects, actuators, and sensors all need real-time communication capabilities. Because of these reasons, offering a lightweight authentication solution for the Internet of Things is vital. Because of this, Azrour et al. proposed a reliable authentication method for the Internet of Things. This protocol's backbone, elliptic curve cryptography (ECC), beats the standard RSA encryption method in terms of measurements. Furthermore, other authentication schemes that rely on ECC. For computers with limited memory and processing power, elliptic curve cryptography is believed to be the most secure and effective option.

- **Authentication with ID and Password:** As a security measure, ID-based authentication may help distinguish between legitimate and fraudulent users. The resource's access is either approved or rejected depending on the user's ID. User IDs include all attributes that may be used to identify an individual, including but not limited to email addresses, phone numbers, IP addresses, etc. This technique is the backbone of several proposed protocols for the Internet of Things. The server/client authentication architecture, however, is where this mechanism is most often used. Since the user's ID and secret need to be stored in the server's database, an IoT ecosystem cannot function without a server.

Nevertheless, the following paragraphs will go into further depth about the several downsides of using the ID-based authentication approach. To begin, what is the server-side storage mechanism for user data? Are they secure against server-side intrusions and stolen verifier attacks? It is also possible for users to forget their login settings. As a result, they can't complete the following authentication. It is not acceptable to store personal information on a device in this case, regardless of whether it is linked to a private or public network. Thirdly, it's not easy to transmit user IDs over public networks. Here, you should use a cryptographic technique or hash function.

- **Certificate-Based Verification:** An alternate method was suggested to address the issues with ID- and password-based authentication. We refer to this method as certificate-based authentication. Numerous applications have widely embraced certificate-based authentication. For instance, to verify a user's identity in financial apps, Hiltgen et al. proposed a new method based on certificates for authentication. This tactic has also been used by the Internet of Things. Internet of Things devices may lack the computing capacity necessary to execute the algorithms and device certificates, even if certificate-based authentication provides more security. Therefore, items connected to the Internet of Things should not be treated using this manner.

- **Blockchain:** Blockchain represents a certain type of database. Its unique approach to data storage sets it apart from a conventional database. Blockchains store information in a collection of blocks that are connected to one another. Utilising this new technology, several writers have proposed an IoT authentication scheme in recent years. Additionally, the blockchain provides traceability, privacy, and transparency while also assuring future usage of correctly recorded data via sustainability and verification of data kept in the network.

- In the Internet of Things context, various authentication techniques are employed. Most suggested IoT authentication systems are based on encryption cryptography, as Table 2 shows. Two different forms of cryptography are applied here. Asymmetric encryption algorithms, like ECC, are the first kind; symmetric encryption algorithms, like AES, are the second. Additionally, some authentication systems use hash algorithms to hash important parameters. Finally, because they can be used to guarantee that messages are received fresh, random numbers are also incorporated in certain protocols.

Table 2: Categorization of certain IoT authentication protocols.

Protocol	Proposed for securing		Method used			
	IoT	WSN	Encryption algorithm	Random number	Hash function	Others
[128]	—	✓	—	—	✓	—
[129]	✓	—	—	—	—	Time synchronization
[110]	✓	—	ECC	—	—	Lamport's OTP algorithm
[109]	—	—	—	✓	—	Zero-knowledge proof
[104]	—	—	AES-based MAC	—	—	—
[130]	✓	✓	ECC	—	✓	—
[131]	✓	✓	ECC	—	✓	Smart card
[132]	✓	—	ECC	✓	✓	—
[133]	✓	—	—	—	✓	—
[134]	✓	—	AES	—	—	—
[83]	✓	—	Symmetric encryption	—	—	—
[15]	✓	—	—	✓	✓	Fuzzy extractor mechanism
[20]	✓	—	ECC	✓	✓	Challenge-response
[135]	✓	—	Symmetric encryption	✓	✓	Blockchain machine learning
[136]	✓	—	ECC	✓	✓	-

ECC: elliptic curve cryptography; AES: Advanced Encryption Standard; OTP: one time password; WSN: wireless sensor network.

Conversely, Table 3 illustrates the benefits and drawbacks of a few chosen IoT authentication systems. As we can see, a protocol is only deemed effective if it satisfies all security requirements and is lightweight. In conclusion, we can say that because of the limitations of IoT devices, processing and running times are significant.

Table 3: One Internet of Things (IoT) authentication scheme's benefits and drawbacks

Protocol	Advantages	Limitations
[113]	Is lightweight	Uses only hash function
[114]	Can detect man-in-the-middle attacks	Uses certificates that need an important space in memory
[90]	Can be implemented in real-time IoT networks Based on two-factor authentication	Vulnerable
[89]	Can deal against insider attack based on bilinear maps	Needs complex computation Is heavyweight Not efficient for IoT devices
[84]	Surpasses HOTP	Vulnerable against some attacks
[115]	Offers mutual authentication	Does not cover all IoT service requirements
[116]	Guarantees authentication and session key exchange	Cannot resist all attacks
[74]	Can be used with cloud servers	Based only on one hash function
[117]	Very lightweight	Operates only in CoAP-based IoT environment
[118]	Lightweight mutual authentication	The running time of protocol is not very fast
[119]	Can be used for authentication protocol for IoT-based RFID systems	

7. CONCLUSION

Modern technological advancements would not have been possible without the Internet of Things. The transport of data has been made easier by these technological advancements. However, user data security should not be overlooked. The safety of Internet of Things (IoT) systems is the major emphasis of the research presented in this piece. Accordingly, the IoT is susceptible to several forms of attacks, such as replay, Denial of Service (DOS), and password guessing, as mentioned before. The most important security function for the Internet of Things is authentication. As a result, we have given you a thorough rundown of the authentication techniques used by the Internet of Things. Blockchain, ID-based authentication, certificate-based authentication, one-time passwords, and ECC-based mutual authentication are the main methods used to improve authentication. We found that most modern authentication techniques use encryption cryptography after analysing them.

REFERENCES

1. Ahammad, D. S. K. H. (2022). Microarray Cancer Classification with Stacked Classifier in Machine Learning Integrated Grid L1-Regulated Feature Selection. Machine Learning Applications in Engineering Education and Management, 2(1), 01–10.

2. Ashwin, K. V., Kosuru, V. S. R., Sridhar, S., & Rajesh, P. (2023). A passive islanding detection technique based on susceptible power indices with zero non-detection zone using a hybrid technique. International Journal of Intelligent Systems and Applications in Engineering, 11(2), 635-647.

3. Burgos-Artizzu, X. P., Dollár, P., Lin, D., Anderson, D. J., & Perona, P. (2012). Social behavior recognition in continuous video. In: 2012 IEEE Conference on Computer Vision and Pattern Recognition. IEEE; pp. 1322-1329.

4. Chen, L. C., Papandreou, G., Kokkinos, I., Murphy, K., & Yuille, A. L. (2018). DeepLab: Semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected CRFs. IEEE transactions on pattern analysis and machine intelligence, 40(4), 834-848.

5. Chen, Z., & Gupta, S. (2020). Deep learning for object detection: A comprehensive review. Journal of Visual Communication and Image Representation, 68, 102768.

6. Chinthamu, N., Gooda, S. K., Venkatachalam, C., Swaminathan, S., & Malathy, G. (2023). IoT-based secure data transmission prediction using deep learning model in cloud computing. International Journal on Recent and Innovation Trends in Computing and Communication, 11, 68-76.

7. Deng, J., Dong, W., Socher, R., Li, L. J., Li, K., & Fei-Fei, L. (2009). ImageNet: A large-scale hierarchical image database. In: 2009 IEEE conference on computer vision and pattern recognition. IEEE; pp. 248-255.

8. Everingham, M. et al. (2010). The Pascal visual object classes (VOC) challenge. International Journal of Computer Vision, 88(2), 303-338.

9. Girshick, R. (2015). Fast r-cnn. In: Proceedings of the IEEE International Conference on Computer Vision. pp. 1440-1448.

10. Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2014). Rich feature hierarchies for accurate object detection and semantic segmentation. Proceedings of the IEEE conference on computer vision and pattern recognition, 580-587.

11. Guo, J., He, H., He, T., Lausen, L., Li, M., Lin, H., et al. (2019). GluonCV and GluonNLP: Deep Learning in Computer Vision and Natural Language Processing. arXiv preprint arXiv:1907.04433.

12. Gupta, A., Singh, R., Sharma, A., & Das, S. (2023). Influence of cultural factors on consumer behavior in India. Journal of Consumer Research, 50(1), 112-129.

13. He, K., Gkioxari, G., Dollár, P., & Girshick, R. (2017). Mask R-CNN. Proceedings of the IEEE international conference on computer vision, 2961-2969.

14. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. Proceedings of the IEEE conference on computer vision and pattern recognition, 770-778.

15. Henriques-Alves, A. M., & Queiroz, C. M. (2016). Ethological evaluation of the effects of social defeat stress in mice: Beyond the

social interaction ratio. Frontiers in Behavioral Neuroscience, 9, 364.

16. Inman, J. J., & Nikolova, H. (2018). Shopper-facing retail technology: A retailer adoption decision framework incorporating shopper attitudes and privacy concerns. Journal of Retailing, 94(3), 377-389.

17. Jhuang, H. et al. (2010). Automated home-cage behavioural phenotyping of mice. Nature Communications, 1, 68.

18. Kamau, J., Goldberg, R., Oliveira, A., Seo-joon, C., & Nakamura, E. (2023). Improving Recommendation Systems with Collaborative Filtering Algorithms. Kuwait Journal of Machine Learning, 1(3).

19. Lin, T. Y., Dollár, P., Girshick, R., He, K., Hariharan, B., & Belongie, S. (2017). Feature pyramid networks for object detection. Proceedings of the IEEE conference on computer vision and pattern recognition, 2117-2125.

20. Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C. Y., & Berg, A. C. (2016). SSD: Single Shot MultiBox Detector. European conference on computer vision, 21-37.

21. Norouzzadeh, M. S. et al. (2018). Automatically identifying, counting, and describing wild animals in camera-trap images with deep learning. Proceedings of the National Academy of Sciences of the United States of America, 115(25), E5716-E5725.

22. Peixoto, H. M., Teles, R. S., Luiz, J. V. A., Henriques-Alves, A. M., & Santa Cruz, R. M. (2019). Mice Tracking Using the YOLO Algorithm. PeerJ Preprints, 7, e27880v1.

23. Raj, R., & Sahoo, D. S. S. (2021). Detection of Botnet Using Deep Learning Architecture Using Chrome 23 Pattern with IoT. Research Journal of Computer Systems and Engineering, 2(2), 38-44.

24. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. Proceedings of the IEEE conference on computer vision and pattern recognition, 779-788.

25. Redmon, J., & Farhadi, A. (2017). YOLO9000: Better, faster, stronger. Proceedings of the IEEE conference on computer vision and pattern recognition, 7263-7271.

26. Redmon, J., & Farhadi, A. (2018). YOLOv3: An incremental improvement. arXiv preprint arXiv:1804.02767.

27. Ren, S., He, K., Girshick, R., & Sun, J. (2015). Faster R-CNN: Towards real-time object detection with region proposal networks. Advances in Neural Information Processing Systems, 91-99.

28. Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556.

29. Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., & Wojna, Z. (2016). Rethinking the inception architecture for computer vision. Proceedings of the IEEE conference on computer vision and pattern recognition, 2818-2826.

30. Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press.

Corresponding Author

Akshat Gupta*

Student, Class 12th, St Joesph's Academy, Dehradun, Uttarakhand, India

Email: heyitsakshatt@gmail.com