Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA

Proceedings of the Cyber Secure Nigeria Conference – 2023

Internet of Things (IoT) Security and Private Concerns: An Overview

Mosud, Y.O., Ajulo, E.B. & Yinusa, A.B.
[1&3]Department of Computer Science, Caleb University, Lagos, Nigeria
[2]Dep of Computer Science/Mathematics, Mountain Top University, Ibafo, Ogun State, Nigeria
E-mails: myolumoye@yahoo.com; emmanuelajulo@gmail.com; bukky4muda@yahoo.com
Phone: +234-8035804475

ABSTRACT

The number of Internet of Things (IoT) applications has greatly increased during the last two decades. Globally, more than half a billion electronic devices are connected. Due to their constant connection to the Internet, IoT applications are frequently targeted by a wide range of conventional threats, such as Trojan horses, worms, malware, spyware, and malicious code injections. It is apparent that traditional threats offer services like accountability, authorization, authentication, and these factors are typically used to identify a subject and determine whether the person is qualified to access the object. With the large numbers of connected devices, it is likely that IoT systems may become more vulnerable to threats and attacks with high-frequency electromagnetic radiation and more advanced viruses. Therefore, there is a pressing need to address these privacy and security concerns because it is insufficient to rely on currently used conventional procedures. This study identifies the knowledge and research gaps in this field by exploring the various dangers that IOT devices are vulnerable to, how these dangers operate and create a recovery mechanism to mitigate the harms. The study concludes by suggesting cutting-edge authentication methods like one-time password (OTP) ID- and password-based, three-factor/multi-factor and blockchain.

Keywords: Architecture, Authentication, Internet of Things, Privacy, Security

Proceedings Citation Format
Mosud, Y. O., Ajulo, E.B. & Yinusa, A.B. (2023): Internet of Things (IoT) Security and Private Concerns: An Overview. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria. 11-12th July, 2023. Pp 49-58 https://cybersecurenigeria.org/conference-proceedings/volume-2-2023/
dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P7

1.. INTRODUCTION

Kelvin Ashton coined the phrase "The Internet of Things (IoT)" in 1999 with the intention of advancing communication and fostering interpersonal connection in a virtual setting. A poll claims that by the end of 2020, there will be 50 billion linked devices, and by 2023, there will be 14.7 billion (Sharma, Shamkuwar & Singh, 2019). Gillis (2023) describes the internet of things, or IoT, as an interconnected network of computing devices, mechanical and digital machines, objects, animals, or people who are given unique identifiers (UIDs) and the capacity to transfer data over a network without the need for human-to-human or human-to-computer interaction. The International Telecommunication Union, ITU (2023) defines IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies".

IoT technology is now mostly used in business and industrial sectors. Intelligent devices come in a variety of interrelated, varied forms, ranging from small equipment to basic wearable and home appliances. This technology can also be employed in intelligent initiatives, such as smart farming, housing, cities, and healthcare systems. Chips are present in these items, which are utilized to examine and investigate the information. By the end of 2020, the IoT market is anticipated to reach 5.8 billion units, a 21% increase from 2019 (Muhammad et al, 2022). The Internet of Things (IoT) is one of the most recent technologies that has undergone a significant evolution and has become an indispensable tool in our daily lives. This development has positively impacted many sectors, such as agriculture, water management, social security, house security, education, smart grid, to mention but a few (Assiri & Almagwashi, 2018). As a result, more and more gadgets are becoming connected every day. The Strategy Analytics (2021) predicts that there will be more than 30 billion by the end of 2025 and 50 billion by 2030 of connected objects.

IoT technology enables the development of networks linking various things, whether in the real world or the digital one (Patel, Patel & Scholar, 2016; Assiri & Almagwashi, 2018; Strategy Analytics, 2021). As a matter of reality, the client-server architecture networks, the World Wide Web (WWW), e-mail, file sharing, etc. were all developed as a result of the development of a simple computer network connecting personal computers. It then makes its way to a wide-area network that connects billions of intelligent things that were built into complex systems.

For the benefit of people, it is important to comprehend and deal with these challenges. IoT security and privacy issues may be handled by people to their advantage. The Internet of Things (IoT) foresees a world in which common objects can communicate with one another and link to the internet to create self-configuring, intelligent systems. In spite of the benefits of IoT development, security and privacy are still seen as significant barriers to IoT design, adaptation and advancement. Concerns over security and privacy are the main issues that needs to be addressed in each IoT. For security-related issues, a number of research have provided solutions. In order to safeguard IoT, security concerns at the layer relating to IoT must be addressed. In the sections that follow, a brief review of the literature is presented, which is then followed by the architecture of IoT, security and privacy concerns of IoT, security attacks and authentication methods.

2. LITERATURE REVIEW

IoT security and privacy concerns have lately received a great deal of attention and efforts. To address these concerns and difficulties associated with IoT security, several papers and surveys have been released. The survey conducted by Yang, Wu, Li and Zhao (2017) address the personal and safety concerns with clear implications for low-end systems (Muhammad et al, 2022; Yang, Wu, Li and Zhao, 2017). The risks and difficulties related to IoT security that affect networks, devices, and systems are briefly covered by many writers (Hukkeri & Goudar, 2019). In their surveys, Weber, Gopi, and Rao broke down security-related difficulties and challenges into four categories: IoT device constraints, such as battery life extension; (Hukkeri & Goudar, 2019) lightweight computation; (Soumyalatha, 2016) categorization of security threats; and (Genadiarto, Noertjahyana, & Kabzar, 2018) control access mechanisms and architecture [Muhammad et al, 2022; Rao, 2018; Weber, 2015; Mosud, 2013). The presentation, network, transport, and application layers of the IoT architecture are also covered in the dialogue.

Another survey regarding issues with IoT security was published by Tewari and Gupta (2020). This study layered architecture of IoT devices and sheds light on fresh security concerns. They presented tools and methodologies for IoT research as well as highlighted the cross-layer heterogeneous integration difficulties. Noor and Hassan (2019) compared several research in a number of areas (simulation tools, procedures, IoT device security, and privacy). It examines the IoT security measures in place at the moment, including authentication, security encryption, trust management, and new technologies.

Research on personal and safety-related issues with IoT devices is also offered, and it emphasizes how privacy is distinct from other industries. It includes information gathered by IoT experts who attempted to understand security and privacy issues and made fresh security protocol suggestions for effective security and privacy mechanisms (SPMs) (Muhammad et al, 2022; Bamasag & Youcef-Toumi, 2015). Almost all linked devices are at high risk, pose dangers and are vulnerable to hacking.

The number of linked devices is expanding, but so are the problems and difficulties. To address these problems, several cutting-edge technologies, such as blockchain, AI, and fog computing, are combined with IoT. IoT and these cutting-edge technologies are utilized together to address security and privacy concerns. Researchers are paying attention to these technologies, particularly blockchain, which serves as a reliable third party. Safety-critical data, IoT devices, and security may all be protected by the blockchain (Muhammad et al, 2022). IoT device concerns and security and privacy-related problems may both be successfully addressed by combining blockchain with IoT technologies.

3. ARCHITECTURE OF IoT

IoT connects numerous heterogeneous things, such as computers, smartphones, TVs, vehicles, industrial machines, refrigerators, irrigation system or medical tool (Kumar, Tiwari & Zymbler, 2019). IoT is not standardized, hence there are different layered architectures [Burhan, Rehman & Kim (2018) that can be employed during implementation. This varies from three-, five- to seven-layer architectures.

Each IoT layer differs from the others in terms of the technology and functions it is integrated with, and as a result, each layer has security concerns (Assiri & Almagwashi, 2012; Mohammadi et al., 2015). This study discusses the three-layer architecture (figure 1) which consists of the perception layer, the network layer and the application layer.

- Perception Layer: This layer is also referred to as "sensors layer", and is the first of IOT architecture. It is the layer that connects the real world to sense and collect data from the surroundings, and prepares the data before sending it to the network layer. The layer primarily makes use of sensors, Global Positioning System (GPS) and Radio Frequency Identification (RFID) technologies (Azrour et al. 2021; Assiri & Almagwashi, 2018).

- Network Layer: It is the second layer that connects to multiple servers, gateways and smart devices. It is in charge of sending the recorded data to other IoT network elements. This is why the Internet of Things (IoT) uses a variety of communication standards and protocols such as Wi-Fi, Bluetooth, 4G/5G, WiMAX, ZigBee, 6LoWPAN and others. This layer is a target for some attacks such as denial-of-service attacks, destruction, illegal access, data eavesdropping, man-in-the-middle attack, virus etc. Attackers can analyze the traffic and eavesdrop to attack the network confidentiality and privacy. The remote access mechanisms of the IoT and data exchange increases the probability of such attacks. The key exchange mechanism must be in a high-security manner to protect it from any attacker (Azrour et al. 2021; Atlam, Walters & Wills. 2018).

- Application Layer: The Application Layer is in charge of offering the user application-specific services. In order to achieve this, it specifies how the IoT may be used, for example, in smart homes or autos. At this layer, the IoT clearly serves its intended function by offering a variety of smart environment applications. Common IoT applications include smart cities, smart homes, smart offices, smart transportation, etc. IoT has both personal uses, like those for mobile apps or smart wearable gadgets, industrial ones, and in autos (Atzori et al, 2012).

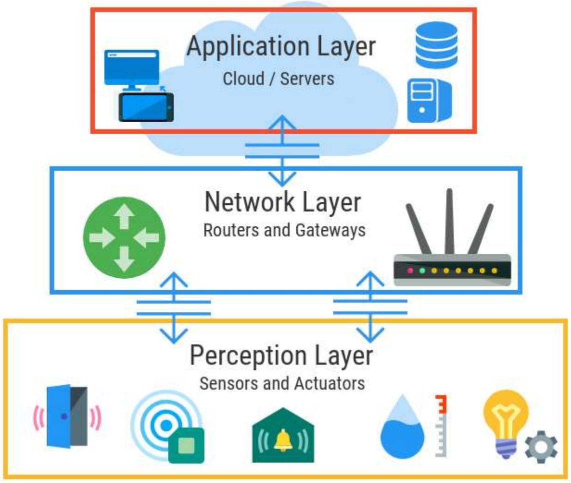

Figure 1: The Three-Layer Architecture

4. IoT SECURITY AND PRIVACY CONCERNS

The Internet security glossary (2023) describes privacy in IoT as "the right of an entity (often a person), acting on its own behalf, to decide the extent to which it will engage with its surroundings, such as how willingly it is willing to divulge information about itself to others (Assiri & Almagwashi, 2018). In the Internet of Things, a network of devices seeks to collect data from the surrounding area before broadcasting it along with some events to a server that houses apps. Privacy must be controlled throughout each stage, including in the device, storage, communication, and processing. One of the crucial concerns that has to be resolved in the IoT is the privacy and protection of sensitive data (Kumar & Chouhan, 20021).

As billions of devices are linked to the internet and billions of data points are used, it is necessary to protect all of these connections and data points in the internet of things. IoT security and IoT privacy are mentioned as important problems because of its larger attack surface. One of the most infamous recent IoT attacks was Mirai, a botnet that hacked domain name server provider and temporarily brought numerous websites offline in one of the largest distributed denial-of-service (DDoS) assaults ever recorded. Utilizing inadequately protected IoT devices, attackers obtained access to the network.

The capacity to incorporate sufficient security protections is a critical challenge for the IoT. Hackers have previously gained access to video surveillance systems, Internet-connected baby monitors, medical equipment, and even autos, as well as business networks, using unsecured IoT devices. Other crucial factors are data privacy and individual privacy. Data loss, theft, or improper usage may result from inadequate security, including confidential financial and health information. The number of vulnerability points rises as a result of connected devices and systems and cloud-stored data. Due to their susceptibility to hacking, the US Food and Drug Administration (FDA) recalled over 500,000 pacemakers in 2017. A hacker, for instance, may deplete the battery or shock the patient (Samuel, 2023).

The same year, criminals broke into a casino and stole a significant amount of data from a poorly secured "smart" fish tank which had Internet capabilities that allowed it to be controlled remotely for temperature, salinity, and food distribution but also exposed the casino's data system to attack (Samuel, 2023). Another issue is the tracking of people's movements using surveillance cameras, as it is possible to determine where someone has been or what they have done at any given time by combining video data with other types of data produced by sensors, cameras, cellular records, computer logs, and other systems. Law police, governments, companies, and others may use or misuse this information (Samuel, 2023).

5. IoT SECURITY ATTACKS AND AUTHENTICATION METHODS

5.1 IOT Security Attacks

Attacks usually experienced in IOT can be classified as physical, network, software and web.

These are discussed as follows:

i). Physical Attack

Examples of physical attacks are invasive, noninvasive, semi-invasive, object replication, sleep denial and fake node injection.

- Invasive Attack: This is an example of physical attacks that require the attacker to physically approach the chips or disconnect the targeted devices. Depending on the sort of attack that is to be launched and the IoT device, advanced knowledge and specific tools are needed (Azrour et al., 2021).

ii). Network Attack

Examples of network attacks include the RFID spoofing, RFID unauthorized access, sinkhole, wormhole, sybil, routing information, man-in-the-middle, selective forwarding, traffic analysis, routing information and replay attack

- DoS/DDoS attacks: It is an example of network attacks. A security attack known as denial of service (DOS) tries to block permitted access to network resources by legitimate users and entities. It is regarded as the most common and effective assault. Attackers can often utilize flooding attacks to deplete a system's memory, CPU, and bandwidth. 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, authorized users are blocked from using services (Azrour et al., 2021; Archana &. Harini, 2019; Ahmed et al, 2018).

iii). Software Attack

These are malicious programs or codes that are intentionally installed on a target's device to cause harm, damage, or allow unauthorized access. Examples include the following: operating system, worms, viruses. trojan horse, phishing, backdoor and brute force

- Back Door: It is a harmful and intricate code that can get past authentication checks to access system resources from a distance. Back doors in IoT operating systems like RTOS and Contiki can be leveraged to get unwanted access. This kind of attack is intended to penetrate an IoT system's security defenses, including authentication and cryptography, using a variety of methods.

iv). Web Attacks:

There are many flaws in IoT web app as a result of poor coding. These flaws allow hackers to get access to the servers or databases of these IoT web apps that hold sensitive personal or financial data. Sometimes, infected apps are connected to IoT web applications, making these software programs exposed to a variety of assaults. Examples of web attacks are DDoS attacks, explication of a misconfiguration, SQL injection, malicious code injection, path-based DoS attacks, malware, spyware.

- Malware: Malware is an acronym for malicious software. It is a software purposedly designed to damage computers and IoT devices in order to steal personal data, bypass access controls, and harm computers and IoT devices without the user's permission. IoT malware like Aidra, Mirai and Bashlite are IoT malware families that scan the machine to look for open ports to gain access.

5.2 IoT Authentication Methods

IoT authentication is a methodology for increasing trust in the identification of IoT machines and devices to safeguard data and manage access as it travels across an insecure network, like the Internet. Strong IoT authentication is required so that linked IoT equipment and devices can be relied upon to guard against control requests from untrusted persons or devices. In order to get access to data on servers, such as audio recordings, pictures, and other potentially sensitive information, attackers may pretend to be IoT devices. This is another reason why authentication is helpful. A robust authentication can be implemented to protect connections between IoT devices using a number of techniques:

i). A One-Time Password (OTP)

This is sometimes known as a dynamic password, and is a password that is only good for one transaction of authentication. Several OTP authentication mechanisms are suggested in the literature review for protecting communication in an IoT setting. These protocols are built on a variety of methods, including RSA cryptography, hash groups (MD5, SHA1, and SHA256), and time synchronization. Additionally, they are all based on Lamport's OTP algorithm [101–104]. Unfortunately, these protocols are weak to some attacks (Azrour et al., 2021; Shivraj et al., 2015; Lee & Kim, 2013).

ii). ID- and Password-Based Authentication

The technique for separating legitimate from unauthorized organizations is ID-based authentication. The user's access to the resource is either approved or refused based on their ID. All characteristics that distinguish one person from another, such as a username, email address, phone number, IP address, etc., are referred to as user IDs. Numerous protocols are suggested (Azrour et al., 2021; Park et al., 2015) in the IoT context based on this method. However, the server/client authentication architecture often uses this approach. A server is therefore necessary in an IoT context in order to store the user's ID and secret in the server's database.

However, using an ID-based authentication strategy has several problems, which are described as follows. How are user data kept on the server? Is the server able to protect them from insider and stolen verifier attacks? Additionally, users could forget their authentication credentials. As a result, they cannot carry out their authentication. Saving personal ID on a computer, tablet, or smartphone in this situation is inappropriate, even if the device is not linked to a public network. Another difficulty is the user ID communication via public networks. Hash functions or a cryptographic scheme are advised in this case (Azrour et al., 2021).

iii). Three-factor/Multi-factor Authentication

This method takes security to the next level by combining multiple mechanisms to authenticate: Something you know (e.g., a password), something you are (e.g., fingerprint or iris scan), something you possess (e.g., a one-time code or password generator). While providing a better degree of security, two-factor and multi-factor authentication may cause some user experience (UX) friction since they make the user work harder to gain access.

iv). Blockchain: A blockchain is a special form of database. It varies from a typical database because of how it saves data in a special way. Data is stored in a sequence of blocks called "blocks" on a blockchain. Utilizing this cutting-edge technology, several writers have recently suggested an authentication system for the Internet of Things (Azrour et al., 2021; Alzubi, 2021; Narayanan, 2021; Pajooh, 2021). Because the data preserved in the blockchain is reliable and long-lasting, transparency, anonymity, and traceability are all made possible, thereby providing users the assurance to use the data recorded accurately in the future (Azrour et al., 2021).

6. CONCLUSION

The Internet of Things has been a major factor in the recent fast growth of technology. The communication of data is now simpler as a result of these technologies. The security of user data should not be disregarded, though. In light of this, the study conducted is primarily concerned with the security of IoT technology. As a result, as already said, IoT is vulnerable to a number of threats, including DOS, password guessing, replay, and insider assaults. The study outlined some of the authentication methods used for IoT because it is the first security function that IoT must provide. One-time password (OTP), ID- and password-based, three-factor/multi-factor and blockchain are the mechanisms most often used to enforce authentication. Lastly, the study proposes effective and safe IoT authentication method in our future work in an effort to improve the security of the IoT ecosystem.

REFERENCES

1. Ahmed, A., Latif, R., Latif, S., Abbas, H., & Khan, F. A. (2018). Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review. *Multimedia Tools and Applications*, *77*, 21947-21965.
2. Alzubi, J. A. (2021). Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare. *Computer Communications*, *170*, 200-208.
3. Archana, K. C., & Harini, N. (2019). Mitigation of spoofing attacks on IOT home networks. *International Journal of Engineering and Advanced Technology*, *9*(1S), 240-245.
4. Assiri, A., & Almagwashi, H. (2018, April). IoT security and privacy issues. In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-5). IEEE.
5. Assiri, A., & Almagwashi, H. (2018, April). IoT security and privacy issues. In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-5). IEEE.

6. Atlam, H. F., Walters, R., & Wills, G. (2018). Internet of things: state-of-the-art, challenges, applications, and open issues. *International Journal of Intelligent Computing Research (IJICR)*, *9*(3), 928-938.
7. Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Computer networks*, *56*(16), 3594-3608.
8. Azrour, M., Mabrouki, J., Guezzaz, A., & Kanwal, A. (2021). Internet of things security: challenges and key issues. *Security and Communication Networks*, *2021*, 1-11.
9. Bamasag, O. O., & Youcef-Toumi, K. (2015, October). Towards continuous authentication in internet of things based on secret sharing scheme. In *Proceedings of the WESS'15: Workshop on Embedded Systems Security* (pp. 1-8).
10. 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.
11. Genadiarto, A. S., Noertjahyana, A. and Kabzar, V. (2018). Introduction of Internet of Thing technology based on prototype, *Jurnal Informatika*, vol. 14, no. 1, pp. 47–52, 2018.
12. Gillis, A.S. (2023). What is the internet of things (IoT)? https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT
13. Gopi, A., & Rao, M. K. (2018). Survey of privacy and security issues in IoT. *International Journal of Engineering & Technology*, *7*(2.7), 293-296.
14. Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for internet of things. *Sensors*, *21*(3), 772.
15. Hukkeri, G. S. and Goudar, R. H. (2019) "IoT: issues, challenges, tools, security, solutions and best practices," *International Journal of Pure and Applied Mathematics*, vol. 120, no. 6, pp. 12099–12109, 2019.
16. International Telecommunication Union, ITU (2023). Internet of Things Global Standards Initiative. Accessed https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
17. Internet Security Glossary (2023). Internet Security Glossary. Retrieved May 30, 2023 from https://www.ietf.org/rfc/rfc2828.txt.
18. Javed, Y., Khan, A. S., Qahar, A., & Abdullah, J. (2017). Preventing DoS attacks in IoT using AES. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *9*(3-11), 55-60.
19. Kumar, P., & Chouhan, L. (2021). A privacy and session key-based authentication scheme for medical IoT networks. *Computer Communications*, *166*, 154-164.
20. Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big data*, *6*(1), 1-21.
21. Lee, Y., & Kim, H. (2013). Insider attack-resistant otp (one-time password) based on bilinear maps. *International Journal of Computer and Communication Engineering*, *2*(3), 304.
22. Mohammadi, M., Aledhari, M., Al-Fuqaha, A., Guizani, M. & Ayyash, M. (2015). Internet of Things: A Survey on Enabling, IEEE, 5 NOV 2015.
23. Mosud, Y. O. (2013). Cybercrime and Technology Misuse: Overview, Impacts and Preventive Measures, *The European Journal of Computer Science and Information Technology (EJCSIT),* Vol. 1, Issue 3, pp. 10-20.Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review*, *31*(5), 618-627.

24. Narayanan, U., Paul, V., & Joseph, S. (2021). Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec. *Journal of Ambient Intelligence and Humanized Computing*, 1-19.
25. Noor, M. B. M. & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: a survey, *Computer Networks*, vol. 148, pp. 283–294.
26. Park, K., Lee, S., Park, Y. & Park, Y. (2015). An ID-based remote user authentication scheme in IoT, *Journal of Korea Multimedia Society*, vol. 18, no. 12, pp. 1483–1491, 2015.
27. Patel, K. K., Patel, S. M., & Scholar, P. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, *6*(5).
28. Samuel, G. (2023). Internet of Things. Encyclopedia Britannica, 28 Apr. 2023, https://www.britannica.com/science/Internet-of-Things. Accessed 16 June 2023.
29. Sharma, N., Shamkuwar, M., & Singh, I. (2019). The history, present and future with IoT. *Internet of things and big data analytics for smart generation*, 27-51.
30. Shivraj, V. L., Rajan, M. A., Singh, M., & Balamuralidhar, P. (2015, February). One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)* (pp. 1-6). IEEE.
31. Soumyalatha, S. G. H. (2016). Study of IoT: understanding IoT architecture, applications, issues and challenges, *International Journal of Advanced Networking & Applications*, vol. 478, 2016.
32. Strategy analytics (2021). Internet of things now numbers 22 billion devices but where is the revenue?" strategy analytics online newsroom." https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where (accessed March. 18, 2021).
33. Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future generation computer systems*, *108*, 909-920.
34. Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future generation computer systems*, *108*, 909-920.
35. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal*, *4*(5), 1250-1258.