A Survey on IoT Security: IoT Architecture, Security Issues, Challenges, and Solutions

Ghadi Shaheen
Faculty of computing and Information Technology
King Abdulaziz University, Saudi Arabia

Fatmah Alahmadi
Faculty of computing and Information Technology
King Abdulaziz University Saudi Arabia

Amjad Alsulami
Faculty of computing and Information Technology
King Abdulaziz University, Saudi Arabia

Shaimaa Salama
Faculty of computing and Information Technology
King Abdulaziz University, Saudi Arabia

ABSTRACT
The Internet of Things (IoT) technologies have expanded in diverse domains to create smart environments. According to the distribution of IoT, security aspects must be concerned and improved. The IoT uses different kinds of technologies to produce results. Therefore, it presents new different challenges and issues in security. Several researchers have examined various security issues, threats, challenges, and solutions to increase security in IoT devices. This survey paper presents an introduction to IoT and its purposes. IoT includes three different layers of architecture classified as perception, network, and application layers. The security issues, threats, and challenges in each layer of IoT. The possible solutions to solve the IoT security issues. Moreover, a comparison between IT and IoT security.

Keywords
Internet of Things, IoT security, Security Solutions, Lightweight Cryptography, NOS

1. INTRODUCTION
The Internet of Things (IoT) has grown due to rapid development in the new era of technology and the increasing of smart devices with high-speed networks. The Internet of Things concept defines by Kevin Ashton in 1999 as devices connected to each other through the internet [1] . The internet of things is an interconnected system that aims to exchange information between the internal devices within the IoT environment via network protocols. It uses a new generation of the internet supported by technologies such as Radio Frequency Identification (RFID). The IoT is smart infrastructure with constrained devices connected to each other at anytime and anywhere such as smart homes, healthcare, and smart cities. According to [2], IoT is a smart device that transfers data and resources within the environment. Moreover, it is able to be organized automatically by enabling sensor devices to sense the environment. Therefore, it is qualified to understand the complexity and respond quickly. The IoT devices are controlled remotely to provide services and exchange information through network protocols. Smart devices/objects can be small wearable accessories (e.g., smartwatches) or large machines such as smart cars, refrigerators, and emergency alarms. IoT meets the society requirements such as communication in cars, smart cities, connected healthcare systems, and tracking camera monitoring. The internet of things has become essential in daily life with the rapid development of the economy as it is widely used in public security, healthcare, intelligent fire control, and smart home [3]. Nowadays, the internet of things is not just computers and smartphones, it includes devices with sensors within the environment. According to the popularity of IoT, the security, reliability, and confidentiality of data traveling to and from IoT devices have become a major concern. In IoT, every object can be connected to each other through the internet. Therefore, contains a large amount of personal and important data which requires performing security policies and techniques. Many research papers study the security of IoT, its challenges, and solutions. Unfortunately, today there are many potential problems and challenges. Based on [4], IoT networks and devices confront many security challenges such as authentication, information leakage, privacy, and eavesdropping. This research [5], describes the importance of the security aspect in IoT and defines the security requirements to understand and protect the IoT environment that must be taken into mind.

2. BACKGROUND
Based on [6], the research focuses on IoT issues and their experiences such as denial of service attacks and eavesdropping. Moreover, it considers the network of unsecured devices as bots that can be easily attacked by third parties. The privacy issue in IoT is mentioned in [7] by describing the private issue of IoT in the reference model. It evaluates the impact of technologies and features on the privacy of IoT devices through the recent years of 2020. Moreover, this research [8] discusses security and privacy issues in IoT and mentioned the limitations in each layer of IoT architecture. It describes the privacy constraints related to the IoT and identified some solutions to overcome these issues such as firewalls, encryption, and access control. The internet of things infrastructure was discussed in [9], IoT infrastructure has clear features and various technologies such as Radio Frequency Identification (RFID). RFID is an electromagnetic device containing a chip that allows data transmission depending on the type of application, whether it could be active or passive. The data sent using radio frequencies are passed to the processors, and that is required to implement the services in IoT devices. Moreover, it discusses a number of related threats in IoT applications such as smart agriculture, and a number of sensor applications including natural disasters, temperature measurement, or air pollution. This research [5], indicated several applications that help in daily life, such as smart homes, smartwatches, monitor cameras, and microwave devices. Based on the expansion of the internet of things, the services increasing per day. Moreover, they connect via the internet. As well as the increase in the use of IoT devices to facilitate daily life so, the chances of malicious attacks on these devices increase.

3. INTERNET OF THINGS ARCHITECTURE
The IoT architecture defines as three main layers which are the

perception layer, network layer, and application layer. The points below illustrate each layer [10, 11, 12]:

3.1 Perception or Sensor Layer

It is a physical layer, and it defines as the bottom layer of IoT infrastructure. This layer interacts with different technologies such as sensors, actuators, and edge devices. It comes in different forms like using RFID, and Wireless Sensor Networks (WSN) to collect information. The goal of this layer is to connect data and pass digital signals into the network layer [13].

3.2 Network Layer

The data collected from the perception layer must be filtered and distributed. This layer connects the perception with the application layer by taking data to and from the perception layer, then routing messages to IoT devices in the application layer. It is implemented using Wi-Fi, Bluetooth, or Long-Term Evolution (LTE) [10].

3.3 Application Layer

This layer defines as the top layer in IoT infrastructure which the user can communicate with. It is responsible to deliver information to different users. It is the interface of users in IoT such as when the user uses an application to control his smart house. In this layer, the purpose of creating a smart environment is accomplished [14].

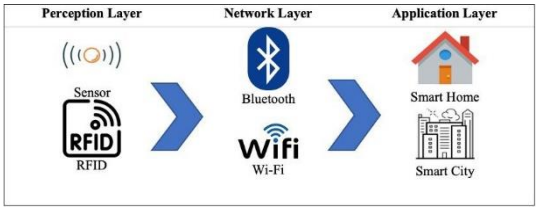

Fig. 1. IoT Architecture.

4. IOT SECURITY ISSUES AND THREATS

Every technical system needs to be concerned about its security requirements to achieve a secure and trusted environment. Nowadays, The IoT contains different types of technologies. Therefore, it presents new different security threats and issues in our life. For example, when data is communicating with different networks, it will open a lot of security issues and threats on the network layer [5].

The following points are security issues in IoT that most researchers include[9]:

1) Confidentiality

Data confidentiality is a very important concept that must be concerned to ensure the security of data. It allows authorized users and objects to access and modify data. There are two aspects of data confidentiality that must be addressed: The first one is an access control mechanism and the second one is an object authentication process. Moreover, the management of data representation is an issue in data confidentiality. For example, in the network layer, the data transmission can be exposed to phishing attacks to steal sensitive data [11, 15].

2) Integrity

According to [16] said, integrity is to ensure that the data has not been modified or changed in transit. The integrity of data in IoT may be difficult because of the data transaction through different layers using different devices. Moreover, the difficulty of knowing the source of data. For example, rerouting the data transmission through another path in the network layer.

3) Availability

Availability is to ensure the data is accessible whenever the devices are connected to the internet. Therefore, users can be tracked without their knowledge [9]. To avoid this issue, an appropriate algorithm must be improved to achieve the assurance of data availability.

4) Heterogeneity

The IoT communicates with different technologies, vendors, and complexity. Each one has different capabilities, releases, versions, and technical interfaces. Therefore, the IoT must be designed to work with all these different components by using suitable protocols between heterogeneous devices [5].

5) Policy

The policies in IoT are very important because of dealing with different types of technologies [17]. The Service Level Agreements (SLAs) of each service involved must be clear and obvious. The issue in IoT is due to its heterogeneous nature that the policies may not be applicable.

The following points are security threats in the IoT [5]:

1) End-to-End Life Cycle Protection

Data is obtained from various devices and shared with each other. Therefore, to ensure the confidentiality and protection of data, it must include a framework to manage the lifecycle of data.

2) Secure Planning

The different uses of devices and their communication with each other in IoT can cause a complication in security policies. External and internal devices must be performed on the same security policy.

3) Usable Privacy and Security

Users need to focus on configuring the security and privacy in order to avoid misconfiguration of it and complex security in IoT.

4) Weak Passwords

Using weak guessable passwords leads the unauthorized party to be accessing the system easily and exploits IoT components. The passwords must be strong and changed frequently to raise the level of security [8].

5. SECURITY CHALLENGES IN EACH LAYER OF IOT

IoT layers are exposed to security challenges and attacks. The attacks impact IoT layers by denying the services or espionage the data. Moreover, some attacks can impact one or more layers instead of being special for one layer. The following section describes the attacks in each layer of IoT.

5.1 Perception Layer

- **Node Capture Attack**: According to [19], the attacker capture and acquire the data physically of the sensor node at the perception layer. Node capture attack enables to manipulation of the node or device of IoT to a malicious node controlled by the attacker. Therefore, if it is accomplished, the sensitive information is stolen or manipulated by the attacker [10]. Unfortunately, this attack impacts some nodes of IoT which are in an unguarded environment, and when the monitors' devices are costly to

equip [19].

- **Replay Attack**: Based on [20, 21], the perception layer is vulnerable to attack by replay attack. It occurs when the attacker intercepts the session and stores the messages. After that, sends the old message as a legitimate user to gain access to unauthorized devices or resources. This attack aims to thieve the identity of legitimate users, intercept the session or messages, and replay it for malicious purposes [22].

- **Sleep Deprivation Attack**: According to [23], the sleep deprivation attack impacts the sensor node of IoT devices that are in low-power sleep mode. Moreover, the attacker attempts to exhaust the battery of these sensor nodes. This attack causes a denial of service due to decrease power by running a lot of requests to the IoT devices [10]. Therefore, IoT infrastructure becomes unavailable because IoT devices consume their battery [24].

5.2 Network Layer

- **Denial of Services (DoS)/Distributed DoS (DDoS) Attacks:** Based on [25, 26], DOS/DDoS are the most attacks that impact IoT at the network layer. It makes the servers unavailable and disrupts service to legitimate users by sending a lot of requests. Moreover, if the requests are from multiple sources so, it is known as a Distributed Denial of Services attack (DDoS) [10]. According to the weakly configuration of IoT devices and the complexity of the network layer, IoT is the exposition to attacks [24].

- **Man in the Middle Attack:** MitM occurs by the internal user when controlling the communication between two devices in IoT [10]. It appears as a normal exchange of information and the real devices cannot detect the malicious device. Its goal could be for manipulation or eavesdropping such as to steal information or to edit and forward data [27]. Therefore, it considers as a big challenge to the IoT at the network layer due to the weak validation of certificates. Moreover, if eavesdropping on the IoT device is accomplished, the communication will be compromised entirely. This attack violates the integrity, and confidentiality of data [11].

- **Sinkhole Attack:** Based on [28], a sinkhole attack is a specific type of routing attack and considers the most serious attack at the network layer in IoT. It occurs when the attacker installs a malicious node between the IoT nodes [29]. Therefore, the attacker can manipulate the routing of the packets or messages, send a false notice report of the attack, and disable the network itself to serve the IoT devices [28]. The sinkhole attack impacts the performance of IoT networks and violates the confidentiality of data. Moreover, it can be vulnerable to further attacks such as DOS/DDoS attacks [10].

5.3 Application Layer

- **Phishing Attack**: Phishing attack is the most common attack to steal sensitive data for illegitimate use. It occurs when the attacker acts as a trusted user or entity and deceives the real user to send personal information to a fake website [30]. According to [31], the attacker can gather sensitive information by bypassing IoT devices. Therefore, it becomes a serious issue because all IoT devices are machines that lack intelligence [29].

- **Malicious Viruses:** Malicious viruses are used to compromise the devices or operations, steal personal information, and unauthorized access to the system or device [32]. Moreover, the attacker impacts the IoT devices with malicious SW in order to deny IoT services or corrupt information [33]. Malicious scripts are scripts added or deleted from the software to make damage to the IoT services and devices [10]. The IoT services usage through the internet, thereby easily harms and damages when the user requests the services [29].

- **Sniffing Attack:** Sniffing attack captures the data through the sniffing process of the packets that are transmitted over the channel. Based on [34], the sniffer attack is known as a network protocol analyzer, and it occurs when the sniffer steals data from all devices connected to the host system. The attacker sniffs the IoT application to gain access to the sensitive information and harm it or for illegitimate usage [24].

6. SECURITY SOLUTIONS FOR IOT

The previous sections discuss in detail the security issues, threats, attacks, and challenges of each layer in it. This section introduces the proposed security solutions based on various research. The most important solutions that are effective in IoT environments and devices are stating the following:

6.1 Framework of Weak Password Detection for IoT Devices

Web-based applications are used for device managers in order to function, manage and display the information of IoT devices. Using a password is one of the critical authentication methods to log in. In this case, the password must be unguessable [18]. Based on [36], the research has developed a framework to detect weak passwords that are used in IoT devices automatically through a web-based application. The analysis was designed to scan and then detect weak passwords based on web applications depending on IoT devices in Beijing, Zhejiang, and Shandong. The results were able to detect 12,1279 devices using weak web passwords in it. The framework has improved the detection process of weak

passwords and worked effectively.

6.2 Dynamic Policies and Synchronization System in IoT

The IoT is a combination of different technologies to produce the purpose goal. Each technology has its own policy, and it must be updated to prevent attacks as much as possible. Based on [17], the research focused on how to enhance the policies in IoT by using Networked Smart Objects (NOS). The definition of NOS is to manage and control heterogeneous sources and the flow of data in IoT. Moreover, it can raise the security and quality of data [36]. The solution of the paper has been integrated into distributed IoT sources through NOS, and NOS based on Message Queuing Telemetry Transport (MQTT) protocol. MQTT protocol uses in IoT to large-scale, exchange information, and ensure the quality of messages. It applied special algorithms to identify which policy is under the synchronization process. Moreover, the research is concerned with the loaded time to update policies in real time. The concept of the framework is needed in IoT to raise security while using heterogeneous sources.

6.3 Lightweight Cryptography

Cryptography is the most effective solution to protect important and sensitive data in systems. Unfortunately, not all cryptographic types efficiently secure IoT infrastructure and devices. Therefore, the researchers suggest Lightweight cryptography (LWC) as a new branch to ensure security in IoT environments [37]. Lightweight cryptography is one of the cryptographic algorithms with a low cost of implementation and convenience with IoT-constrained architecture and devices [38]. Based on [22, 39], the researchers recommend LWC as a solution for IoT. Each layer of IoT requires encrypted data to generate and transferred by them. Moreover, it discusses the two factors to choose LWC as a solution. The first factor is the weight of the software which is dependent on time and memory. The second factor is the weight of hardware that depends on the cipher area of data and required power. LWC requires low space for RAM and ROM. It balances the throughput and performance with power.

6.4 Datagram Transport Layer Security (DTLS)

Based on [40], the research recommends Datagram Transport Layer Security (DTLS) based architecture as a solution to build a strong architecture and secure end-to-end communication in IoT and discusses its benefits. DTLS is a protocol to transport data securely in communication within the IoT environment. It is based on Transport Layer Security (TLS) protocol. Moreover, it protects the communication between the constrained devices/users to prevent manipulating and eavesdropping in IoT layers [41]. It implements a handshake mechanism by using the Internet of Things Security Support Provider (IoTSSP) device to provide a secure session for IoT devices [40].

7. IT SECURITY VS IOT SECURITY

Security is the most important factor in IT and IoT infrastructure and devices. It considers as a strong role in succeeding the infrastructure. The table below discusses the differences between IT security and IoT security in devices and infrastructure [11, 12, 42]

TABLE 1. IT security vs IoT Security

IT Security	IoT Security
The internet connects users with devices within the infrastructure.	The internet connects the user and devices with devices remotely, known as machine to machine (M2M).
The devices can protect by adding security policies and tools in order to secure their infrastructure [43].	The devices and infrastructure should be designed and built-in security to be secure and reliable.
The security solutions efficiently work within the infrastructure.	The normal security solutions such as in IT devices do not work well to secure IoT devices and infrastructure because all devices connect remotely.
The IT infrastructure can overcome security issues, easily stop its effects, and eliminate distributed damage.	IoT experienced some difficult issues to overcome, stop or eliminate the attacks because the infrastructure depends on the internet.

8. DISCUSSION

Security is an important factor that must be performed in IoT layers. Each layer in IoT has its own functions and operations that should address the security requirements at each step. According to the used of heterogeneous nodes in IoT, the security has become more complicated and difficult to consider. Several studies have shown different solutions to raise the security in IoT systems and close its security gaps. Despite these critical solutions, there are new different technologies connected to perform IoT tasks. Therefore, new threats, issues, and challenges could be introduced. The growth of IoT needs new security solutions to be updated and secured as much as possible. There are different security requirements in IoT infrastructure that can be considered for future research, depending on the type of application such as, data confidentiality is important to allow authorized users to access smart cities, and data integrity is important to ensure the data has not been modified in smart health. A number of researchers found that the policies in IoT are one of the critical issues that must be concerned. Due to the heterogeneous nature of IoT, the policies may not be applicable. Furthermore, the physical devices of IoT including mobiles or computers can be stolen. The dashboard of the IoT is an essential component that must be protected and considered by third parties because it is able to control the whole system. There must be a critical solution when the IoT devices are stolen such as, the application should verify the logged user every 5 minutes and if there is no use for a while the application will log out automatically. The research found a solution for dynamic policies and synchronization systems in IoT that can enhance the policy issue using NOS [17]. The solution was helpful to synchronize and update policies and it needs more improvements to match heterogeneous devices. Using a weak password to log in to a dashboard permits attackers to access the IoT system. The research found a solution to detect weak passwords in IoT devices based on web-based applications [36] that could be used. Moreover, to detect weak passwords in mobile applications, multi-factor authentication can be implemented. Multi-factor authentication uses two different ways or more to allow accessing the authorized user such as face recognition and password. Other research found a solution that is DTLS to secure end-to-end communication through using TLS protocol and implementing a handshake mechanism. A handshake mechanism uses IoTSSP. DTLS aims to present a secure session for IoT devices [41]. According to the data transmission between layers, the data must be encrypted in each layer of IoT. There are several studies focusing on Lightweight Cryptography solutions. LWC is using a cryptographic

algorithm to encrypt data [39]. It is implemented with low cost and low storage space. This survey paper attempts to group the recent research in IoT security. The gaps in IoT security are not fully considered and need to be improved in each layer and component such as the security in physical devices, data transmission, access control, and hardware/software of IoT.

9. CONCLUSION

The Internet of things (IoT) plays a vital role in the new era of technology. It enables the devices, systems, or users to be connected with each other anywhere at any time using the internet. This survey paper presents the IoT architecture, security issues, threats, and challenges in each layer of IoT. Moreover, outlines four of the most effective security solutions in IoT components. In addition to providing a section for a comparison between different solutions in IoT in order to facilitate future research work for other researchers.

10. REFERENCES

[1] Kevin Ashton, ”That ’Internet of Things Thing”, RFID Journal, 2009

[2] Madakam, Somayya, et al. "Internet of Things (IoT): A literature review." Journal of Computer and Communications, 2015

[3] B. Li and J. Yu, “Research and application on the smart home based on component technologies and internet of things,” *Procedia Engineering*, 2011.

[4] Jurcut, A., Coffey, T., Dojen, R. and Gyorodi, R., “Analysis of a key- establishment security protocol”, Journal of Computer Science and Control Systems, 2008.

[5] Razzaq, Mirza Abdur, et al. "Security issues in the Internet of Things (IoT): A comprehensive study." International Journal of Advanced Computer Science and Applications, 2017

[6] Ebraheim Alsaadi, and Abdallah Tubaishat, "Internet of Things: Features, Challenges, and Vulnerabilities", International Journal of Advanced Computer Science and Information Technology, 2015

[7] Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges." Security and Communication Networks, 2014

[8] Vikas, B. O. "Internet of things (IoT): A survey on privacy issues and security." International Journal of Scientific Research in Science,

[9] Engineering and Technology, 2015

[10] Joshitta, R. Shantha Mary, and L. Arockiam. "Security in IoT environment: a survey." International Journal of Information Technology and Mechanical Engineering, 2016

[11] Lin, Jie, et al. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE internet of things journal , 2017

[12] Mahmoud, Rwan, et al. "Internet of things (IoT) security: Current status, challenges and prospective measures." 2015 10th international conference for internet technology and secured transactions (ICITST).

[13] IEEE, 2015

[14] Neshenko, Nataliia, et al. "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet- scale IoT exploitations." IEEE Communications Surveys & Tutorials, 2019

[15] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, 2015

[16] Sarker, Iqbal H., et al. "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions." Mobile Networks and Applications, 2022

[17] Daniele Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, "Internet of Things: Vision, applications and research challenges", Ad Hoc Networks, 2012

[18] Md Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", SERVICES, 2015, IEEE World Congress on. IEEE, 2015.

[19] Sicari, Sabrina, et al. "Dynamic policies in internet of things: enforcement and synchronization." IEEE Internet of Things Journal, 2017

[20] Seyum Wolde, Mehir, and Adeel Hussain. "Password Security Assessment of IoT-Devices." 2022

[21] Wang, C. . “Understanding node capture attacks in user authentication schemes for Wireless Sensor Networks,” *IEEE Transactions on Dependable and Secure Computing*, 2022

[22] Damghani, H. “Classification of Attacks on IoT,” In 4th International Conference on Combinatorics, Cryptography, Computer Science and Computation 2019.

[23] Jurcut, A., Ranaweera, P. and Xu, L. (2020) “Introduction to IoT Security.”

[24] Williams, P. “A survey on security in internet of things with a focus on the impact of emerging technologies,” *Internet of Things*, 2022

[25] Pirretti, M. “The sleep deprivation attack in sensor networks: Analysis and Methods of Defense,” *International Journal of Distributed Sensor Networks*, 2006

[26] Hassija, V. “A survey on IOT security: Application areas, security threats, and solution architectures,” *IEEE Access*, 2019

[27] Anand, P. “IOT vulnerability assessment for sustainable computing:

[28] Threats, current solutions, and open challenges,” *IEEE Access*, 2020

[29] Abughazaleh, N. “DOS attacks in IOT Systems and proposed solutions,” *International Journal of Computer Applications*, 2020

[30] Aliyu, F., Sheltami, T. and Shakshuki, E.M. “A detection and prevention technique for man in the middle attack in fog computing,”

[31] *Procedia Computer Science*, 2018

[32] C. Ioannou and V. Vassiliou, “Accurate detection of sinkhole attacks in IOT networks using local agents,” *2020 Mediterranean Communication and Computer Networking Conference (MedComNet)*, 2020.

[33] I. Ahmad, M. Niazy, R. Ziar, and S. Khan, “Survey on IoT:

Security Threats and Applications ," *Journal of Robotics and Control*, 2021.

[34] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IOT: A survey on attacks and countermeasures," *IoT*, 2021

[35] S. G. Abbas, I. Vaccari, F. Hussain, S. Zahid, U. U. Fayyaz, G. A. Shah, T. Bakhshi, and E. Cambiaso, "Identifying and mitigating phishing attack threats in IOT use cases using a threat modelling approach," *Sensors*, 2021.

[36] M. Shobana and S. Rathi, "IOT Malware : An Analysis of IOT Device Hijacking," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2018.

[37] T. Aziz and E.-ul Haq, "Security challenges facing IOT layers and its protective measures," *International Journal of Computer Applications*, 2018.

[38] B. Prabadevi and N. Jeyanthi, "A Review on Various Sniffing Attacks and its Mitigation Techniques," *Indonesian Journal of Electrical Engineering and Computer Scienc*, 2018.

[39] Qu, Jia. "Research on password detection technology of IOT equipment based on Wide Area Network". In: ICT Express ,2022

[40] S. Sicari, C. Cappiello, F. D. Pellegrini, D. Miorandi, and A. Coen- Porisini, "A security-and quality-aware system architecture for internet of things," Information Systems Frontiers,2014.

[41] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight cryptography for internet of insecure things: A survey," *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019.

[42] Katagi, Masanobu, and Shiho Moriai. "Lightweight cryptography for the internet of things." sony corporation 2008.

[43] Dhanda, Sumit Singh, Brahmjit Singh, and Poonam Jindal. "Lightweight cryptography: a solution to secure IoT." Wireless Personal Communications 2020

[44] Dos Santos, Giederson Lessa, et al. "A DTLS-based security architecture for the Internet of Things." *2015 IEEE symposium on computers and communication (ISCC)*. IEEE, 2015.

[45] Kothmayr, Thomas, et al. "DTLS based security and two-way authentication for the Internet of Things." *Ad Hoc Networks*, 2013

[46] D. Singh, P. Singh, M. Mishra, A. Lamba, and S. Swagatik, "Security Issues In Different Layers Of IoT And Their Possible Mitigation," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, 2020.

[47] Chakrabarti, A., & Manimaran, G. Internet infrastructure security: A taxonomy. IEEE network, 2002