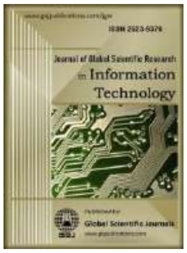
Contents lists available at www.gsjpublications.com

Journal of Global Scientific Research
in Information Technology

journal homepage: www.gsjpublications.com/jgsr



A Review of IoT Applications, Attacks and Its Recent Defense Methods

Nafea Ali Majeed Alhammadi, Khalid Hameed Zaboon

Department of Computer Sciences, Shatt Al-Arab University College, Basrah, Iraq.

ARTICLE INFO

Received: 16 Feb 2022,
Revised: 16 Feb 2022,
Accepted: 18 Feb 2022,
Online: 1 Mar 2022

Keywords:
IoT Applications, Cybersecurity, Cyberattacks, Defense methods

ABSTRACT

Nowadays, the technology become an important part from our live. Moreover, Internet of Things (IoT) is expressed by mixed technologies at the system level in many applications domains. The IoT can be applicated in several environments. Therefore, the security of Internet of Things (IoT) has become a critical concern. Recently, it is observed that there are several types of sophisticated attack could target the IoT and make the services useless from the legitimate users. In this work, the IoT applications, IoT security which include the most common attack and the proposed solution. The majority of the offered solutions have various downsides and restrictions. However, the most suitable and reliant protection features, processes, strategies, and approaches for dealing with sophisticated threats targeting the IoT environment remain unknown. This review paper focuses on the most common and effective solution for securing the IoT environment against the cyberattack that adopt the traditional and modern approaches. Finally, this research gives a framework and potential areas of convergence for constructing enhanced DDoS defensive solution models.

1. Introduction

The Internet of Things (IoT) has received a lot of interest in recent years. Kevin Ashton was the first to propose the Internet of Things idea in 1999.Communications within IoT devices have become more accessible than ever before because to significant improvements in mobile communication, Radio Frequency Identification, cloud computing, and Wireless Sensor Networks [1]. Smart phones, laptops, PDAs, and other hand-held embedded devices are all part of IoT. To connect with one another and convey useful data to the centralized system, IoT devices rely on wireless communication networks. [2].

The data by IoT devices is handled in a centralized system before being distributed to the designated recipients. Our everyday routines are more focused on a fictitious realm of virtual world due to the fast rise of communication and internet technologies. [3]. People can shop, work, communicate, and nurture pets and plants in the network's virtual environment, but humans must live in the actual world [4]. [4]. As a result, replacing all human tasks with totally automated life is extremely tough. The better services for future development of internet there is restriction of frictional space bounding limit. The Internet of Things has effectively brought the fictitious world and the actual world both on the same interface [5].

The adoption rate of IoT devices is now quite strong, with an increasing number of devices linked to the internet. According to estimates [6,]

Corresponding author:
E-mail addresses: nafeaalhamadi@yahoo.com (Nafea), khalid.Hameed842@gmail.com (Khalid)

there will be 35 billion related objects with around 300 billion linkages by 2021, generating income of over 800 billion euros. In China, nine billion devices currently is connected and the number predicted to rise to 24 billion by 2020. The IoT will allow personals and devices to communicate anywhere, anytime with any device by using any services or networks under ideal conditions [4], [7]. The basic aim of IoT is better future for human beings with a superior world. Fig. 1 shows the architecture of IoT environment. However, the substance of apps and devices are not built to withstand confidentiality threats, which raises a slew of privacy and security issues in IoT networks, including secrecy, identification, data integrity, and access control [5]. [5]. Attackers and intruders target IoT devices on a daily basis.

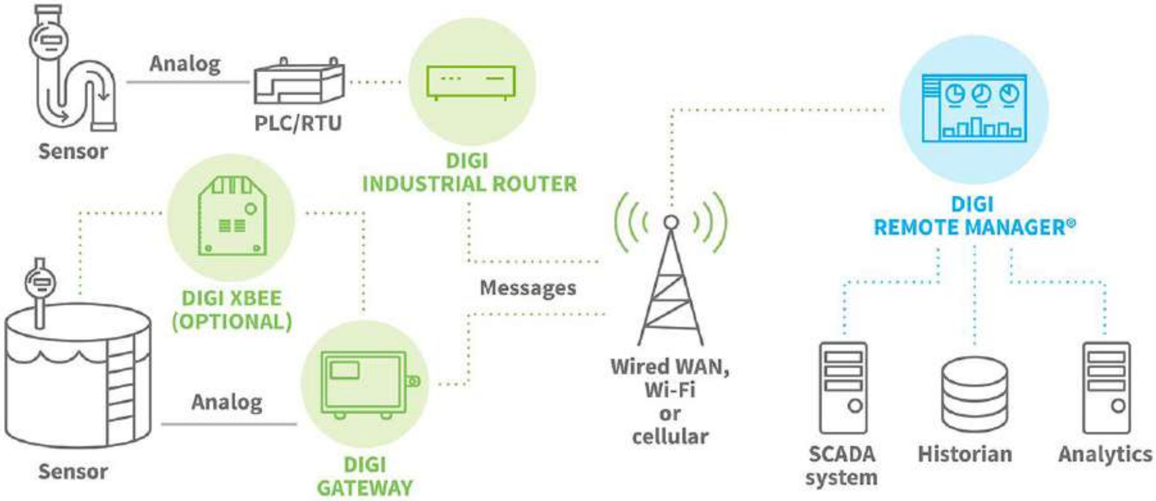


Fig. 1 the architecture of IoT environment [4], [7].

In this work, the IoT environment background with it is application in our live have been illustrated. Also, the most common and effective types of attack and recent defense methods have been presented. The work is segmented into 4 sections as: Section 1 presents the introduction which it gives the background on the IoT environment, IoT applications, IoT attack and defense methods. Whereas, the IoT applications have been discussed in detail in under section 2. Furthermore, Section 3 presents the IoT security. Finally, section 4 concludes the work.

2. IoT Applications

The Internet of Things has a huge possible for environmental social effect as it adapts. Some IoT-based concepts include smart grid, mobility, smart buildings, public safety and medical, environment monitoring, healthcare, agriculture, industrial processing, and breeding, and independent living [8]. Each of these services are connected to us in some manner. The use of these apps and their numerous advantages play an essential role, and their existence has become increasingly reliant. Their availability and usage have acquired a visionary size in recent years and became of essential importance. It would not be wrong to say that the Internet's future is solely built on the notion and vision of Internet of thing, which essentially propels us into the future. [9]. In Figure 10, many IoT application areas are presented. The study is focused on the fundamentals of functional aspects of applications, with notable work done by many researchers throughout the years being discussed in the next section of the article. The IoT can be applicated in several environments such as displayed in Fig. 2 [10].

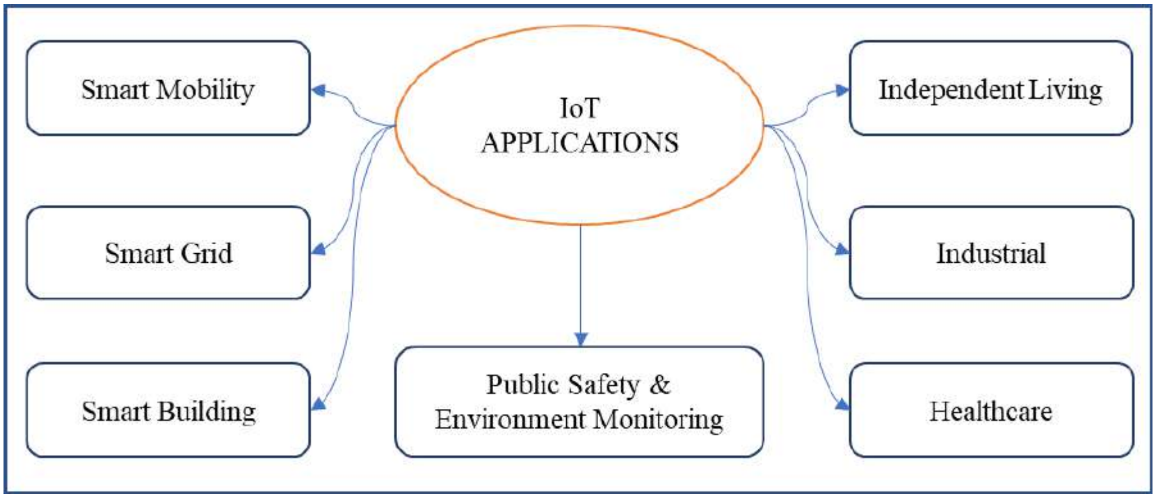


Fig. 2 The IoT Applications.

2.1. *Smart Mobility*

Numerous modes can be accessed by utilizing the methodology of smart mobility which is efficient and flexible with the passage of time and the ever-increasing needs of society, Vehicular Ad-hoc Networks (VANETs) have received a lot of attention. As a result, it might be described as a paradigm shift toward a more adaptable and multimodal transportation system. It is, after all, the foundation for the IoV, which aims to enhance road awareness to prevent or decreasing accidents and providing innovative solutions for more efficient transportation modes. There are countless more difficulties relating to traffic congestion and traveling from one location to another that are being researched and improved by various experts. Researchers in the field of mobility have developed fresh strategies based on current resources [10].

2.2. *Smart Grid*

Smart Grid detects the local changes in usage of electricity supply and reacts accordingly through digital communication technology. It is also called a two way communication between a customer and utility enabling customer to prioritize their energy usage and demand. The energy is sent via the grid according to the calculated requirement [11].

2.3. *Smart Building*

A Smart Building is a residential habitat that is outfitted with lighting, heating, and other technological equipment, comparable to any other living environment. They can be operated remotely via a smart phone or a computer, which is a huge distinction from ordinary homes. Smart homes/buildings have emerged in recent years as a result of the integration of numerous technologies with the Internet [12].

2.4. *The Public Safety & Environment Monitoring*

The practice of careful observation on weather patterns, endangered species preservation, water management, and several other characteristics that are directly or indirectly related to our environment is known as public safety and environmental monitoring. To monitor timely changes in environmental factors, applications are integrated with various sensors and other observational equipment. [9].

2.5. *Medical and Healthcare (IoMT)*

The IoMT is an organized integration strategy that integrates medical services to the IT system via multiple computer networks that are connected online. Medical equipment have built-in Wi-Fi systems that enable machine-to-machine communication using the IoMT principle [1].

2.6. *The Industrial Processing*

In recent years, the Internet of Things (IoT) has grown in popularity in the realm of industry. The functional capabilities of IoT are either molded or created in specific to respond to the demands of the industry in today's industrial equipment and requirements. [13].

2.7. Independent Living

Independent living attempts to assist older people as much as possible in their everyday activities, allowing them to live a self-sufficient and secure lifestyle. With considerable scientific efforts and contributions in this arena, the notions of IoT have been evoked. [14].

3. IoT Security

As IoT applications continue to expand and evolve, assaults against those apps are becoming more common. For both manufacturers and customers, securing IoT devices is becoming increasingly difficult. Several studies have been highlighted the key security concerns as being default, weak, or storing data online without a password. The password used for IoT devices are very simple, default and sometime no password is given. Such a flaw puts users' security at danger and permits hackers to execute large-scale cyberattacks like DDoS using IoT devices According to Bashar et al. in [7], an unencrypted medical record of 6 million harmed individuals in the United States and other regions is publicly available. [8].

3.1. The Most Common IoT Attacks

Several types of attack could target the IoT environment, in this section we focus on the most common and dangers types of them. Fig. 2 Shows the most common types of IoT attack.

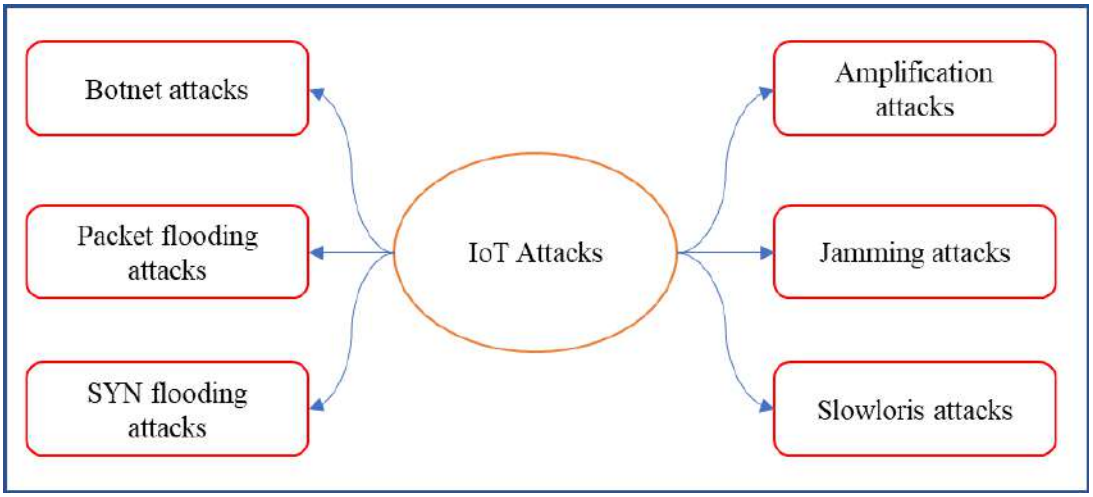


Fig. 3 IoT applications

3.1.1. Botnet attacks

The attacker commands the hacked IoT devices, which are known as bots or zombies, with the aid of the handler. A botmaster (an hacker in charge of the bots) might employ a variety of IP addresses to perform large-scale assaults such as spam emails for financial gain or DDoS attacks on key infrastructure or websites to render them unavailable In 2016, one of the most well-known large-scale IoT botnet assaults, "Mirai," rendered high-profile websites such as the New York Times, Twitter, Netflix, GitHub, and others unavailable [7].

3.1.2. Packet flooding attacks

Another sort of large-scale assault is packet flooding. Because web hosts have no authority over the packets they receive, these attacks can occur [7], [8]. Because IoT devices have internet access, they are subject to flooding assaults, and IoT traffic might go through numerous hops before a gateway or an IDS is achieved the sequence of routers packets travelled from are not included in packets received at a router. Opponents can use this to counterfeit the internet Protocol and bombard the victim with bogus packets, leading the victim to crash. The UDP flooding assault, in which UDP datagrams flood and congest the network is an example of a flooding attack. [8]. ICMP flooding is also another tactic in which a constant stream of ping packets is broadcast to the recipient without getting a response, overloading network resources.

3.1.3. SYN flooding attacks

A conventional TCP three-way protocol is overcome in a SYN flooding attack, and attacker uses fake IP addresses to transmit multiple SYN packets to various ports on the target. The source seldom answers with the intended ACK message when the destination responds to the SYN request with SYN-ACK, forcing the target to remain waiting for a response until its connection limit is exceeded, it times out, and it prevents reacting to genuine requests [8].

3.1.4. Slowloris attacks

Slowloris is a DDoS assault that targets HTTP servers. This technique opens a large number of HTTP connections to the target web server. By sending fractional and continuous HTTP requests, these connections are maintained open for an endless amount of time. The targeted web server leaves the connections open, steadily reducing its resources until they are totally depleted [6]. DDoS assaults that penetrate slowly are difficult to detect.

3.1.5 Jamming attacks

These attacks have major ramifications for IoT devices because they can rapidly deplete battery capacity by interrupting data transmission and retransmitting it frequently [8]. A jammer attack is one of the biggest dangers to the IoT ecosystem due to the resource constraints of IoT devices. Jamming attacks have a detrimental impact on Distributed systems because they interrupt communication, reduce IoT performance, cease communication, and deplete the limited energy resources of IoT devices. [1], [8].

3.1.6 Amplification Attacks

The adversary enhances assault force by amplification in this form of attack. Attackers can carry out these attacks by exploiting protocol flaws and impersonating source IP addresses. DNS amplification, ICMP amplification, and UDP amplification are examples of amplification attacks. [6].

4. The Proposed Solution

Several solutions have been proposed to secure the IoT environment against the cyber-attack. However, in this section we summarized the most common and effective of them as shown in the below Fig. 4.

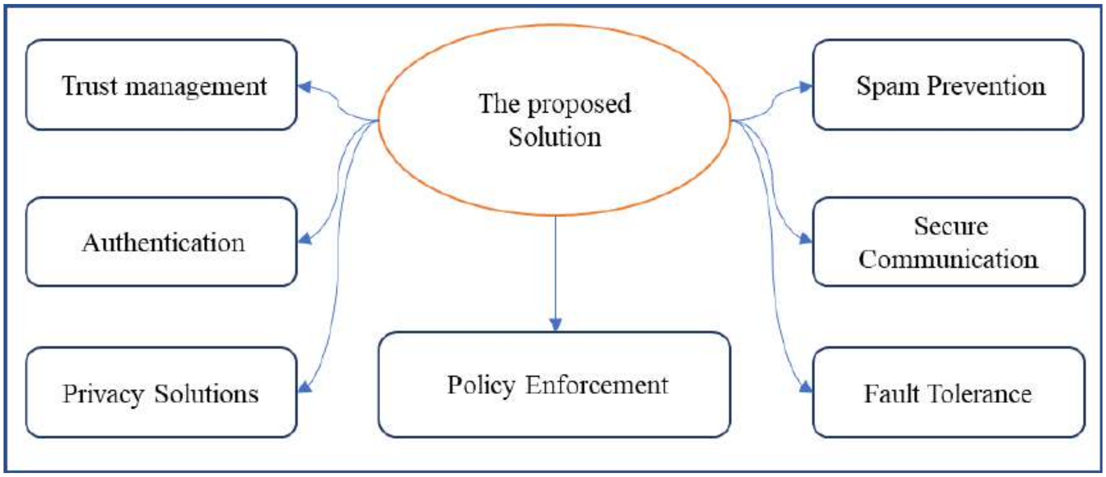


Fig. 4 The most effective defense methods.

4.1. Trust Management

In IoT security, trust management is critical. The importance of trust management in the IoT system was demonstrated in research by [6]. People may benefit from trust managers to assist them overcome the dangers and uncertainties associated with the Internet of Things. Trust may be thought of as a term that includes both privacy and security. Trust management is discussed as a requirement for IoT in research by [7]. Authors in [15] also acknowledged that trust refers to how people feel while interacting with IoT devices. That is, consumers have the right to manage their resources at any time and from any location, as well as gadgets that allow them to comprehend their engagements with IoT systems. More Furthermore, they state that good management can promote IoT trust.

4.2. Authentication

The development of different authentication mechanisms for IoT can aid in the security and privacy of data. the authors in [6, 15] illustrate authentication approaches for the security and privacy of IoT and privacy in previous work. Authentication can be done via a gateway security token, a global trust tree, or a trust chain. Furthermore, each model has its advantages and disadvantages. Henceforth the author in [56] proposed in IoT end user authentication a two-level key management session. The work contributes to the development of a two-level session key (TKS) based IoT security authentication method.

4.3 Privacy Solutions

According to the literature, there are numerous solutions to privacy concerns. Furthermore, in previous work [16] provides innovative solution for privacy challenges in the IoT. The data should be managed by every user proposed tools. As a result, privacy is considered during the design process; this is known as the principle of privacy by design. There is also a transparency principle. Transparency in the context of IoT means that consumers need to know who or what is handling their data, as well as how and when it is used.As a result, regulations requiring transparency must be implemented in order to protect privacy. Another option that has been proposed is data management. That is, determining who is in charge of managing the confidential data. Different data management strategies, as well as policy-enforcement methods for privacy solutions, are required.

4.4. Policy Enforcement

In today's world, policy enforcement is seen as a critical tool for addressing any security issue in any community. Data protection is vital to people's privacy, according to EU regulation; that is, private rights should be maintained during every party's contact in the digital world of IoT. In literature [17] research focuses on a software-based solution to IoT security. It provides a security architecture solution that includes micro security functionalities known as boxes. The architectural approach includes a centralized IoT Sec controller which can observe the environment and establishes a common knowledge of cross-technology implementations. From the generated general understanding, network managers may represent and configure innovative boxes and their transmission techniques.

4.5. Fault Tolerance

The IoT fault tolerant systems have been proposed for different requirements. The author in [16] focuses on safeguarding the IoT by establishing an innovative solution for safe and ethical usage, in response to the increasing number of assaults on the Internet and its gadgets. They mentioned a variety of conditions for IoT devices to attain fault-tolerance in their methodology. It comprises three needs, according to their research. To begin with, all devices should be set to be secure initially. Second, all IoT devices must be turned on so that the network and functions can be monitored. Finally, any device or object should be capable of protecting itself against network outages and threats. When a service is disrupted, the devices must respond quickly and recover from or endure any harm [7].

5. Conclusion

Considerate the value, amount of devices, and cost of data created by the connected devices known as IoT helps merchants and organizations to design efficient solutions that can expand, preserve their data, and function optimally in this increasing data-driven IoT industry. It also aids in comprehending various trends in data consumption, utilization, and storage. However, public and private safety issues, such as confidentiality, accessibility and integrity, among others, have hampered the quick, strong, and widespread adoption of the IoT, despite its enormous potential. Using the foregoing concepts, this research investigates the works to categorize the security issues in the IoT revolution. It discussed IoT security and privacy issues, concerns, obstacles, and potential solutions for minimizing identified vulnerability issues and attaining secure networks.

6. References

[1]. Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: challenges and solutions. *Wireless Personal Communications*, *119*(3), 2603-2637.

[2]. Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

[3]. Sivapriyan, R., Sushmitha, S. V., Pooja, K., & Sakshi, N. (2021, December). Analysis of Security Challenges and Issues in IoT Enabled Smart Homes. In *2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-6). IEEE.

[4]. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-484). IEEE.

[5]. Hua, W., Dai, F., Huang, L., Xiong, J., & Gui, G. (2019). HERO: Human emotions recognition for realizing intelligent Internet of Things. *IEEE Access*, *7*, 24321-24332.

[6]. Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. *IEEE Access*, *7*, 51691-51713.

[7]. Khalaf, B. A., Mostafa, S. A., Mustapha, A., Ismaila, A., Mahmoud, M. A., Jubaira, M. A., & Hassan, M. H. (2019). A simulation study of syn flood attack in cloud computing environment. *AUS journal*, *26*(1), 188-197.

[8]. Mohan Kumar, U., Siva SaiManikanta, P., & AntoPraveena, M. D. (2019). Intelligent security system for banking using Internet of Things. *Journal of Computational and Theoretical Nanoscience*, *16*(8), 3296-3299.

[9]. Udoh, I. S., & Kotonya, G. (2018). Developing IoT applications: challenges and frameworks. *IET Cyber-Physical Systems: Theory & Applications*, *3*(2), 65-72.

[10]. Kiran, S., Kumar, U. V., & Kumar, T. M. (2020, September). A review of machine learning algorithms on IoT applications. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 330-334). IEEE.

[11]. Zheng, L., Chen, S., Xiang, S., & Hu, Y. (2012, August). Research of architecture and application of Internet of Things for smart grid. In *2012 International Conference on Computer Science and Service System* (pp. 938-941). IEEE.

[12]. Rokonuzzaman, M., Mishu, M. K., Amin, N., Nadarajah, M., Roy, R. B., Rahman, K. S., ... & Pasupuleti, J. (2021). Self-sustained autonomous wireless sensor network with integrated solar photovoltaic system for internet of smart home-building (IoSHB) applications. *Micromachines*, *12*(6), 653.

[13]. Li, X., Zhou, Z., Guo, J., Wang, S., & Zhang, J. (2019). Aggregated multi-attribute query processing in edge computing for industrial IoT applications. *Computer Networks*, *151*, 114-123.

[14]. Baig, M. M., Afifi, S., GholamHosseini, H., & Mirza, F. (2019). A systematic review of wearable sensors and IoT-based monitoring applications for older adults–a focus on ageing population and independent living. *Journal of medical systems*, *43*(8), 1-11.

[15]. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications*, *42*, 120-134.

[16]. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

[17]. Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE access*, *8*, 32031-32053.

[18]. Ali M. Jasim, A. M. (2020). An IoT Based Smart Agricultural Field Monitoring and Irrigation System. *Journal of Global Scientific Research*. 1, 307-316.