Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 10. No. 4, December 2022 – Special Issue on Cryptography & Security Mechanisms

Article Citation Format
Abanga, E.A. (2022): A Review of Internet Of Things (Iot) and Security Concerns. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology.
Vol. 10, No. 4. Pp 121-130
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P13

A Review of Internet of Things (IoT) and Security Concerns

Abanga Ellen Akongwin
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: ellen.abaga@st.gimpa.edu.gh
Phone: +233540337659

ABSTRACT

Wireless technology networks are particularly vulnerable to security attacks. Wireless communication networks are widely used in education, defense, industry, healthcare, retail, and transportation. These systems rely on wired and cellular networks. In society and industry, wireless sensor networks, actuation networks, and vehicle networks have garnered a lot of attention. The Internet of Things has gotten a lot of research attention in recent years. The Internet of Things is regarded as the internet's future. IoT will play an important role in the future, changing our lifestyles, standards, and business structures. The use of IoT in various applications is likely to skyrocket in the next years. The Internet of Things enables billions of devices, people, and services to communicate and exchange information. IoT networks are vulnerable to several security vulnerabilities as a result of the rising use of IoT devices. It is crucial to implement effective privacy and security protocols in IoT networks to guarantee, among other things, confidentiality, authentication, access control, and integrity. This paper provides a thorough analysis of the security and privacy challenges in IoT networks.

Keywords: Internet of Things, Security, Security Concerns, Attacks, Networks, Internet

1. INTRODUCTION

Internet-enabled devices have received top priority in recent technological breakthroughs since they offer much more value than earlier models. To enable smart functions, nearly all consumer electronics now have internet connectivity capabilities. The term "Internet of Things" refers to these internet-capable objects or equipment that can communicate with one another online (IoT) (Ding et al., 2020). The term "Internet of Things" (IoT) refers to technologically advanced objects that are connected to the internet; each of these items is individually identified, reachable via a network infrastructure, and capable of real-time perception, data analysis, and help users (Singh & Singh Tomar, 2019). The concept of the Internet of Things was first used in 1982 by a specially designed soda machine that could comment on the beverages it held and if they were cold thanks to its internet connection.

The earliest contemporary idea of IoT was introduced in 1991 by Mark Weiser as a form of pervasive computing. However, Bill Joy's 1999 taxonomy of the internet included a tip about communication from device to device. The phrase "Internet of Things" was coined by Kevin Ashton to describe a network of interconnected gadgets in the same year (Iera et al., 2010). Using cutting-edge technologies like Radio-Frequency IDentification (RFID) and Wireless Sensor Networks (WSNs), which are sensed by sensor devices and then processed for decision-making, based on which an automated action is performed, the fundamental idea behind the Internet of Things is to enable the autonomous exchange of useful information between invisibly embedded different uniquely identifiable real-world devices around us (Khan et al., 2012).

In 2018, there were 23.14 billion connected devices installed, and by 2022, Statista predicts that there will be an astounding 42.62 billion installed devices (Qamar & Zardari, 2022). Additionally, they forecast that by 2025, there will be almost 75 billion IoT devices, growing at a rate of leaps and bounds. By 2020, there will be 30 billion linked items with roughly 200 billion connections, producing revenue of about 700 billion euros, according to an evaluation by Chen et al. (2014). There are currently nine billion devices in China, and by 2020, there should be 24 billion. The IoT will fundamentally alter our societal norms and economic structures in the future. Every other product we use daily, including TVs, refrigerators, burglar alarms, smoke detectors, and vehicles, now has internet access, expanding the concept of the internet of things.

The IoT revolution began as soon as it was developed, and it has since spread to many different fields of technology. Nowadays, it's difficult to find a household without at least one Internet of Things-enabled device (Singh & Singh Tomar, 2019). The bulk of these products and programmes, regrettably, are not built to withstand security and privacy attacks, which leads to a surge in IoT network security and privacy problems including confidentiality, authentication, the integrity of data, access control, and secrecy, amongst others (Hossain et al., 2015). IoT devices are regularly targeted by criminals and trespassers. According to one assessment, 70% of IoT devices are relatively simple to hack. Therefore, it is crucial to have a reliable system in place to protect internet-connected devices from crackers.

The other sections of the article are structured as follows: Section 2 explores IoT applications architecture, and Section 3 discusses security concerns in IoT. Section 4 analyses several attacks, section 5 suggests potential countermeasures, while Section 6 wraps up the article.

2. IOT APPLICATIONS ARCHITECTURE

By 2020, it's anticipated that over 25 billion things will be connected (Kober, 2015). This is a big quantity, hence the 1980-adopted TCP/IP protocols that make up the current Internet architecture (H & Tejaswini, 2018), cannot effectively manage a network the size of the Internet of Things (IoT), hence a new open architecture was needed that could address several privacy and Quality of Service (QoS) issues, as well as support the current network applications using open protocols (Li & Gan, 2013). Without a suitable assurance of privacy, many people are unlikely to utilise IoT (Li & Gan, 2013). Therefore, two of the biggest IoT challenges are data protection and user privacy (ITU, 2005). The following is a description of each IoT layer:

2.1 Application Layer

This layer activates IoT applications for all industries based on the information that has been analysed. Applications facilitate the development of the Internet of Things, hence this layer is crucial for the network's overall expansion (Villamil et al., 2020). Smart cities, smart automobiles, and smart planets are just a few examples of Internet of Things applications.

2.2 Network Layer

Data transmission to various IoT hubs & devices is handled by the Internet of Things protocol stack. To deliver heterogeneous network services, Switches and routers devices among others function by utilising some of the most modern technologies, including WiFi, LTE, Bluetooth, 3G, and Zigbee. By gathering, filtering, and transferring data to and from various sensors, network gateways act as an intermediary between different IoT nodes (Leo et al., 2014).

2.3 Perception Layer

This is the IoT device layer, which gives each thing a physical meaning. It is composed of data sensors capable of detecting the temperature, humidity, speed, position, and other aspects of the products, such as RFID tags, and infrared sensors (Sen, 2014). This layer gathers relevant data about the items from the sensor systems that are attached to them and converts them into digital signals, which are then transferred to the network layer for more processing.

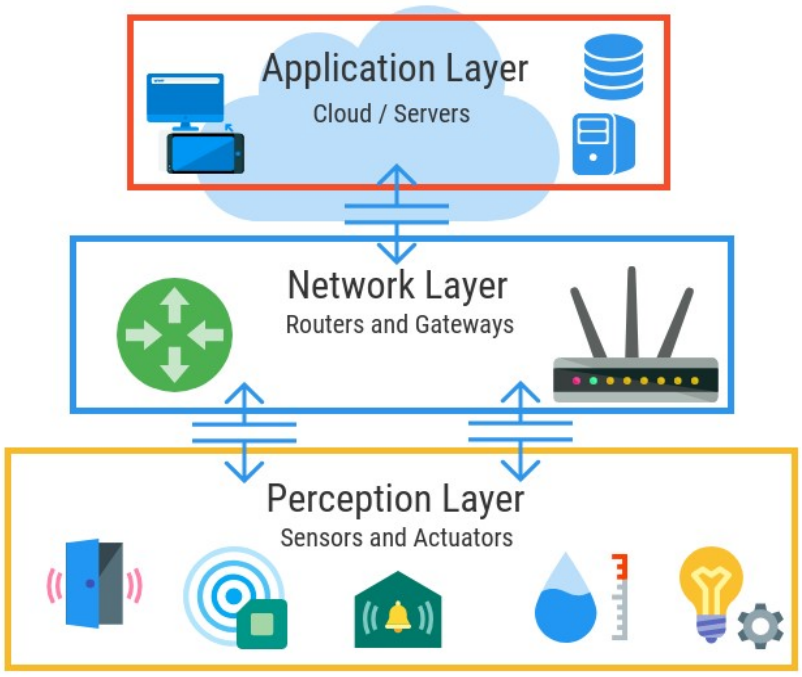

Figure 1: IoT architecture with three layers
Source: myPhython

3. SECURITY CONCERNS

IoT enables everything and everyone locatable and addressable, which will significantly improve the quality of our lives. However, it is less likely to be widely embraced if users lack confidence in the security and privacy of their data (Nimodiya & Ajankar, 2022). For IoT to be widely adopted, it needs a solid security architecture. Here are a few potential IoT-related problems:

3.1 Unauthorised RFID Access

Accessing tags without permission that include identifying data is a significant IoT problem that must be resolved since it can reveal any type of user-specific personal information. An unauthorised reader can read the tag, but they can also change it or even harm it. In this regard, Nimodiya and Ajankar (2022) provided a summary of some of the real-world vulnerabilities posed by RFID, including the RFID Virus, the Side Channel Attack utilising a cell phone, and the SpeedPass Hack.

3.2 Abuse of Cloud Computing

A large network of convergent servers that supports resource sharing is known as the cloud. These shared resources may be vulnerable to numerous security risks, including phishing and man-in-the-middle attacks. The clouding platform must be fully secured, hence precautions must be taken (Taghizadeh, 2020). The Cloud Security Alliance (CSA) listed several potential concerns, including the malicious attacker, data loss, account takeover, and obscene usage of shared computers, among others (Aamir et al., 2012), which are described as follows:

a) The hazard of a malicious insider is that someone with access to the user's data may be engaged in data manipulation.
b) Data Loss is a risk where any nefarious user who has unauthorized access to the system can change or remove the current data.
c) A type of account hijacking threat known as "man-in-the-middle" (MITM) allows the attacker to change or intercept messages sent between two parties.
d) Cloud computing could be utilised in horrifying ways because, if an attacker is successful in uploading malicious software to the server, such as through the employment of a zombie army (botnet), they could gain control over a large number of additional connected devices.

3.3 Breach in Sensor-Nodes Security

As described in Section 4.2, sensor nodes are a part of bi-directional sensor nodes where data acquisition is also feasible in addition to transmission, WSNs are susceptible to a variety of assaults. The following is a summary of some of the potential assaults that Wang (2006) discussed, including jamming, tampering, Sybil, flooding, and several other types of attacks:

1. By tampering with the frequencies used by sensor nodes, jamming blocks the entire network.
2. Tampering is a type of attack where the attacker can extract or change the node data to create a controlled node.
3. Sybil attack asserts numerous fictitious identities for a node, giving it significant power.
4. Flooding is a type of DOS attack that is brought on by excessive traffic and causes memory fatigue.

4. ATTACKS

Attacks on devices with internet access are nothing new. The newest issue is the security of IoT devices, which are being manufactured on a big scale but have little to no security. Every other product we use daily, including TVs, refrigerators, alarm systems, smoke alarms, and vehicles, now has internet access, expanding the concept of the internet of things. If the right precautions are not followed, these gadgets, while valuable, will only increase the number of vulnerable devices already in use. The following section discusses attacks that currently exist:

4.1 Denial of Service (DoS) Attack

The inability of a service or infrastructure owing to capacity saturation is referred to as a denial of service (DoS) (Kolias & Kambourakis, 2017) assault. DoS attacks differ a little bit in nature from other kinds of attacks. It doesn't include information theft or security breaches; rather, it damages the reputation and accessibility of services, which may result in a decline in customer loyalty and financial strength. Distributed Denial of Service (DDoS) attacks are a common type of DoS in which numerous malicious systems assault a single target or service.

More than 80 prominent websites, like Netflix, Twitter, Reddit, the Guardian, and CNN, were brought down by the Mirai DDoS attacks (Kolias & Kambourakis, 2017) on the Dyn network, which was the largest ever recorded. This was brought on by an Internet of Things botnet that the malware Mirai generated. Once infected with Mirai, devices continue to scour the internet for vulnerable IoT devices before infecting them with malware by logging in using well-known default usernames and passwords. Another notable instance is the 2016 attack on the BBC domain. The BBC's website was the target of a DDoS assault in 2016 that brought down the whole domain, including their on-demand television and radio player, keeping them unavailable for more than three hours. A DDoS assault that targeted at least 5 Russian banks in November 2016 caused their services to be unavailable for about 2 days.

These kinds of attacks are typically carried out using a botnet, which consists of a large number of devices that have been programmed and controlled to send connection requests to a service at a specified time, all of which are unknown to the owner. Due to the millions of connected IoT devices, if any of them were to become compromised, they could unleash massive DDoS assault waves. The main causes of this kind of vulnerability are outdated security firmware, an insecure web interface, insufficient authentication, and insufficient security configurability.

4.2 Man in The Middle (MiTM) Attack

Man-in-the-middle occurs when an intruder or attacker attempts to enter communication lines between numerous users or systems (Ahmed et al., 2020). Such attackers may intercept and modify messages from one or both ends without the victims being aware that they are being monitored. As the initial communication passes via the attacker, the recipient may feel they are still receiving a message from the true recipient. Home router attacks can capture personal information as well as user passwords for internet accounts and business networks (Ahmed et al., 2020). Attackers typically target the TCP connection created between the server and client during any HTTP conversation for this type of assault to occur. The attacker has a variety of tools at their disposal, including breaking the actual TCP connection into two separate connections, one of which connects the attacker to the client and the other to the server (Ahmed et al., 2020). The interceptor may begin functioning as a proxy server as soon as the TCP connection is severed.

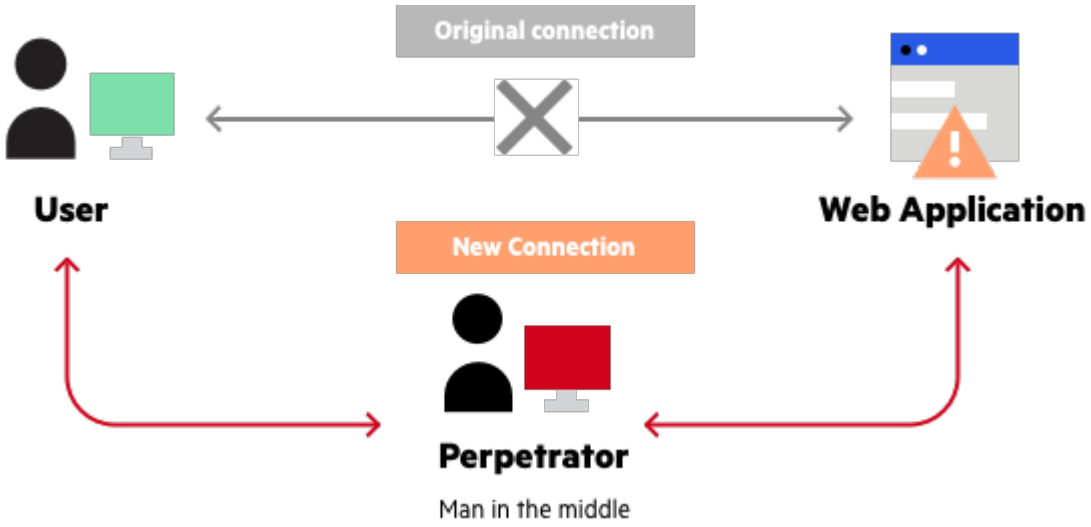

Fig 2: Man in the Middle Attack
Source: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

This gives the attacker access to read and alter the data, by adding another option. These assaults in IoT are brought on by unencrypted transport and insecure network services.

4.3 Identity and data theft

The primary method of committing identity theft is data collection. In this social media age, several data sources can give a comprehensive snapshot of a person. The sources can include data from IoT devices like smartwatches or fitness trackers, as well as information from social media (Abomhara & Køien, 2015). A user becomes more vulnerable to attacks and is more likely to become a target as a result of having access to more data.

Even though IoT devices are highly helpful, they also gather a lot of data that, in the wrong hands, might lead to disasters. For these devices, there needs to be a proper protocol about the kind of data they gather and the data they provide to the cloud servers. Data leaks result from a lack of protocol and sufficient standards, and a vast volume of disorganised data can be exploited and used against consumers.

5. COUNTERMEASURES FOR IoT SECURITY

As the number of IoT gadgets increases, more people are exposed to threats through them (Homes, 2018). However, security must be assured during the design and execution phases of a system, and IoT must be made more secure with a universally recognized and strong structure (Communications et al., 2011). The major forms of attacks are mentioned in the preceding section, and they must also be addressed while attempting to secure IoT. The following are some countermeasures against these threats:

5.1 Security Awareness

Human user awareness and concern in the IoT network is another critical safety mechanism for the success and evolution of the IoT framework. Patton et al. (2014) used real-world data to demonstrate the dangers of failing to secure the Internet of Things. They accessed publicly available IoT equipment (SCADA devices, webcams, traffic control devices, and printers) with no password or the default password. The results were fascinating, revealing that many of these devices were truly accessible. If people continue to be negligent with security and use the bare minimum of security, such as the default password that comes with the product, the Internet of Things will cause more harm than good. If a device in the network is insecure, crackers will have more opportunities to launch attacks against the entire network.

5.2 Establishing Trust

To provide a smooth transfer of the IoT device in terms of access control and authorisation, trust between the two owners must be established because IoT devices may be physically passed from one owner to another. By creating a framework for item-level access control Xie and Wang (2014) proposes the concept of reciprocal trust for inter-system security in IoT. It establishes confidence across the IoT development, operation, and transmission phases. Two processes establish trust: the creation key and the token. An entitlement system assigns a creation key to any new entity that is created. The manufacturer of the item must apply for this key. The token is created by the maker, and it is paired with the device's RFID identity.

This method ensures that permissions are modified by the device itself if it is assigned a new owner or is handled in various departments within the same organisation, removing the new owner's overhead. These tokens can be changed by the owners of the previous token, so superseding the earlier token's rights and access control. This process is analogous to replacing an old key when purchasing a new residence.

5.3 Confederate Architecture

It is difficult to manage the safety of algorithms in the IoT since there are no international standards or policies to control how they are created and used. The Internet of Things must have a decentralised design that promotes internal autonomy or a centralised unit to overcome the heterogeneity of numerous devices, programmes, and protocols. Based on the notion of federated IoT presented by Anggorojati et al. (2012) an access control delegation model is proposed. The model offered takes into account the scalability and flexibility that are critical components of IoT systems. Castrucci et al. (2012) attempted to create an architecture for critical infrastructures called Secure Mediation GateWay (SMGW).

This approach is an IoT abstraction because it can be applied to any sort of distributed infrastructure, irrespective of how different it is in nature and operation from IoT. SMGW can locate all the relevant distributed information from multiple nodes, conquer the heterogeneity of heterogeneous nodes, and transfer all the information and messages over the unsecured Internet network, regardless of whether it is a telephony, power, or water distribution node. With the aid of this study, Leo et al. (2014) federated technique might be expanded upon and used to provide the architecture for a smart home centered on the SMGW.

Security cannot be ensured solely by policies and standards; enforcement methods are also necessary. In their work Neisse et al. (2014) used the SecKit security tools in conjunction with the MQ Telemetry Transport (MQTT) protocol to solve this issue. The current policies might not work because IoT is dynamic. Although the proposed policy model may considerably increase the security of the IoT, it also prolonged the process.

6. CONCLUSION

Every layer of the IoT infrastructure is vulnerable to assaults. As a result, there are several security issues and needs that must be resolved. While the current state of IoT research is centered on authentication and access control protocols, it is imperative to include new networking protocols like IPv6 and 5G to accomplish the dynamic mashup of IoT topology given the rapid growth of technology. IoT has undergone significant small-scale developments, notably within businesses and in a few select industries. The IoT framework needs to scale from one firm to a cohort of diverse systems, which raises several security issues. How we currently live could be drastically changed by the Internet of Things. However, the fundamental challenge in creating completely intelligent frameworks is security. If security concerns like confidentiality, privacy, authentication, access control, trust management, end-to-end security, global norms, and standards are effectively handled, IoT has the potential to quickly revolutionise everything. Wireless, software, new identification, and hardware innovations are needed to meet the open research challenges in IoT, such as standards for embedded devices, implementation of specific control and identity set up systems, and trust management hubs.

REFERENCES

1. Aamir, M., Hong, P. X., Ali, A., & Tahir, M. (2012). *Cloud Computing Security Challenges and Their Compromised Attributes*.
2. Abomhara, M., & Køien, G. M. (2015). *Cyber Security and the Internet of Things : Vulnerabilities , Threats , Intruders*. *4*, 65–88. https://doi.org/10.13052/jcsm2245-1439.414
3. Ahmed, E., Islam, A., Ashraf, M., Chowdhury, A. I., & Rahman, M. M. (2020). Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider. *2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020*, *July*. https://doi.org/10.1109/ICCCNT49239.2020.9225283
4. Anggorojati, B., Mahalle, P. N., Prasad, N. R., & Prasad, R. (2012). *Capability-based Access Control Delegation Model on the Federated IoT Network*.
5. Castrucci, M., Neri, A., Caldeira, F., Aubert, J., Khadraoui, D., Aubigny, M., Harpes, C., Simões, P., Suraci, V., & Capodieci, P. (2012). *Design and implementation of a mediation system enabling secure communication among Critical Infrastructures*. *5*, 86–97. https://doi.org/10.1016/j.ijcip.2012.04.001
6. Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with China Perspective. *IEEE Internet of Things Journal*, *1*(4), 349–359. https://doi.org/10.1109/JIOT.2014.2337336
7. Communications, W. P., Bandyopadhyay, D., & Sen, J. (2011). *Internet of Things - Applications and Challenges in Technology and Standardization*.

8. Ding, J., Nemati, M., Ranaweera, C., & Choi, J. (2020). IoT connectivity technologies and applications: A survey. *IEEE Access*, *8*, 67646–67673. https://doi.org/10.1109/ACCESS.2020.2985932
9. H, U. K., & Tejaswini. (2018). Internet of Things (IoT) A Gateway for Smarter Life. *International Journal of Engineering Research & Technology (IJERT)*, *6*(13), 1–7. www.ijert.org
10. Homes, I. S. (2018). *Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes*. 1–17. https://doi.org/10.3390/s18030817
11. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015*, *July*, 21–28. https://doi.org/10.1109/SERVICES.2015.12
12. Iera, A., Floerkemeier, C., Mitsugi, J., & Morabito, G. (2010). The Internet of things. *IEEE Wireless Communications*, *17*(6), 8–9. https://doi.org/10.1109/MWC.2010.5675772
13. ITU. (2005). ITU Internet Reports. The Internet of Things. *International Telecommunication Union*, 212.
14. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*, 257–260. https://doi.org/10.1109/FIT.2012.53
15. Kober, C. (2015). The internet of things. *Economist (United Kingdom)*, *411*(8964), 89–96.
16. Kolias, C., & Kambourakis, G. (2017). *DDoS in the IoT : October*. https://doi.org/10.1109/MC.2017.201
17. Leo, M., Battisti, F., Carli, M., & Neri, A. (2014). A federated architecture approach for Internet of Things security. *2014 Euro Med Telco Conference - From Network Infrastructures to Network Fabric: Revolution at the Edges, EMTC 2014*, *November*. https://doi.org/10.1109/EMTC.2014.6996632
18. Li, Y., & Gan, X. L. (2013). Study on the architecture and key technology for internet of things. *Advanced Materials Research*, *710*, 660–664. https://doi.org/10.4028/www.scientific.net/AMR.710.660
19. Neisse, R., Steri, G., & Baldini, G. (2014). *Enforcement of Security Policy Rules for the Internet of Things*. 165–172.
20. Nimodiya, A. R., & Ajankar, S. S. (2022). A Review on Internet of Things. *International Journal of Advanced Research in Science, Communication and Technology*, *113*(1), 135–144. https://doi.org/10.48175/ijarsct-2251
21. Qamar, R., & Zardari, B. A. (2022). A Study of Blockchain-Based Internet of Things. *Iraqi Journal for Computer Science and Mathematics*, 15–23. https://doi.org/10.52866/ijcsm.2023.01.01.003
22. Sen, J. (2014). *Internet of Things: Applications and Challenges in Technology and Standardization*. *May*. https://doi.org/10.1007/s11277-011-0288-5
23. Singh, K., & Singh Tomar, D. D. (2019). Architecture, enabling technologies, security and privacy, and applications of internet of things: A survey. *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018*, 642–646. https://doi.org/10.1109/I-SMAC.2018.8653708
24. Taghizadeh, S. (2020). *Security Threats and Countermeasures in*. *August*.

25. Villamil, S., Hernández, C., & Tarazona, G. (2020). An overview of internet of things. *Telkomnika (Telecommunication Computing Electronics and Control)*, *18*(5), 2320–2327. https://doi.org/10.12928/TELKOMNIKA.v18i5.15911
26. Wang, Y. (2006). *A Survey of Security Issues In Wireless Sensor Networks*.
27. Williams, R., Mcmahon, E., Samtani, S., Patton, M., & Chen, H. (2017). *Identifying Vulnerabilities of Consumer Internet of Things (IoT) Devices : A Scalable Approach*. *July*. https://doi.org/10.1109/ISI.2017.8004904