Network security issues for the Internet of Things (IoT)

[Student Name]

[Institution Name]

[Date]

Network security issues for the Internet of Things (IoT)

Abstract-**Network security issues in the Internet of Things (IoT) are linked directly to extensive applications of its system. Starting from the current research trends and emerging threats of network security, this paper explores several network threats mitigation techniques of IoT devices and applications that exist in network layer structure and in other elements as well. The paper then comes up with future recommendations and technical challenges including public key infrastructure and perception of network design, algorithm security, digital certificates, as well as two-way authentication, etc.**

Keywords-Internet of things; malware, two-way authentication, PKI, DDoS attacks, threats

I. INTRODUCTION

Internet of Things (IoT) is viewed as one of the leading technologies and referred to as the future of the Internet. It enables devices and things an ability to perform self-configuring activities on the basis of interoperable communication protocols and standards for using intelligent interfaces through the potent globalized network infrastructure. The significant invention of IoT contributes to the novelty in smart environments including smart items, smart gadgets, smart home appliances or accessories, smart health, and etc.

The rapid expansion and utilization of IoT application, a great deal of network security issues have been abruptly raised. This is typically due to the interconnection between devices and systems in Internet Infrastructure, thereby such network issues need consideration. When everything is dependent and connected on Internet, such issues will tend to become evident; with the perpetual Internet, the global exposure often creates security vulnerabilities and security flaws that mainly lead towards exploitation by hackers, and they can also be distorted in an unmanageable environment with numerous IoT devices. Also, the IoT will further increase risks for attacks by hackers or cybercriminals (Aldowah, 2018).

Network security issues and challenges are typically identified through designers and developers who integrate potential security solutions in IoT applications and assist users to use IoT security features available in their devices. The major inspiration of this study is to provide an overview of the leading network security issues in IoT systems and applications and address major considerations on technical challenges with current research trends. The main contribution of this study is to present necessary insights into the type of attacks and mitigation techniques and how such actions can be facilitated by secure mechanisms or algorithms. This is believed to present future directions and opinions towards the use of potential solutions to mitigate network security issues based on the technical mitigation suggestions with attention to recommendations and effective conclusions.

II. Current Research Trends

In recent times, companies engaged in Information Technology has started giving significant consideration to network security issues due to the fact that the cases of cyber-attacks and cyber-offence have escalated. An investigation led by Shang, et al. (2016) further indicates that with the emergence of the "Internet of Things (IoT)," the issues concerning networking security issues have become much prominent. The result obtained from the following research further reveals that nearly 3 out of 10 people have experienced network security issues while using internet system. It has been noticed that the overall threat of network security occurs on social media websites due to poor encryption. However, it is also notable that the companies are also experiencing major issues due to network security problems as their sensitive information often get hacked and leaked by cybercriminals.

With the advancement in the field of "Internet of Things (IoT)," the cybercriminals and hackers have also become more advanced and thus they have made the network security system more vulnerable to hacking. In such a condition, the companies are determined to implement new approaches and techniques in order to strengthen the network security system. A study conducted by Kim, Wang, and He (2016) also reveals that that "Internet of Things (IoT)," has turned out to be controversial due to the security threats. Many problems have been experienced by different internet components. Regardless of all these growing concerns in "Internet of Things" related to the networking security issues, the enterprises in recent times are extending the utilization of "Internet of Things (IoT)." The following statement could be further approved by reviewing the study of Yang, et al. (2019) in which it has been explained that almost all retailing companies in 2019 have started to make use of e-commerce as a

platform to retail their products. The growth in a number of websites and web usage has given rise to the cases of cyber-attacks as well. It has been estimated that the overall cases related to cyber-attacks have increased by 30% from 2015 to 2019. Although the networking companies are investing billions of dollars in developing best security systems for “Internet of Things,” the problems interlinked with the networking security issues are growing at an exponential rate.

With network security a principal concern for undertakings, security will outweigh development if trust in "Internet of Things (IoT)" is to develop extreme security issues are to be maintained a strategic distance from. On the off chance that this should be possible, almost certainly, the selection will proceed at an exponential rate, more noteworthy solidification will drive designers to edge figuring and associated applications will open multipurpose robots, prompting far more prominent ability and usefulness (Yang, et al., 2019).

In recent times, it has been seen that the issue with IoT security is identified with the extraordinarily quick extension of keen home mechanization gadgets associating with the system. Since the IoT's developing torments have turned out to be especially excruciating with a few elements at play. For instance, gadgets are now associated with “Internet of Things (IoT)” incorporate “switches,” “printers,” “indoor regulators,” “webcams,” and “home mechanization centre points” fueled by man-made consciousness develops, for example, "Amazon" and "Google Assistant." There are likewise “savvy locks,” “smartwatches,” and a lot more devices that people use. In this manner, it could be stated that the demand for research concerning the prevention and mitigation of network security issues in “Internet of Things” has become a major necessity.

The network security mainly entails a list of practices and policies which monitor and regulate the unauthorized access, modification, denial of the computer network, and misuse of network-accessible resources. A study conducted by Wang, et al. (2019) indicates that the network security process also entails the process of authorizing access to data in the network system. Users are given with an ID and password through which a security level is maintained. However, it is also apparent that the traditional form of a network system which is merely based on ID and password has turned out to be obsolete as newer trends of security threats and mitigation strategies have been developed. For instance, the new researches on the networking security issues in “Internet of Things (IoT),” highlights that the increment in number of cyber-attacks on social media websites have enforced the companies involved in network security designing to come up with latest trends of security techniques which includes two-factor authentication along with firewall, secured pin code, etc (Wang, et al., 2019). As a result, it is recommended that the following techniques and systems must be implicated to reduce the threats concerning network security in “Internet of Things (IoT).”

III. Emerging cyber-threats

IoT emerged to attain novel momentum in recent era due to rapid growth and development of internet-connected devices. Nonetheless, security continues to be a crucial issue in IoT setting and also viewed as a foremost concern presented by stakeholders of IoT systems. Therefore, it is taken as a major concern to address the potential network security threats in IoT and its relatable security features that often create vulnerabilities in the privacy of network systems. IoT security rated as an area which strongly focuses on the security mechanisms to secure connected devices, networks, and protection of data stored in the Internet of Things. Several studies have indicated that embedded sensors and computing devices for machine-to-machine operations or bin home smart systems are main driving forces linked with IoT. Moreover, identification of network security threats in IoT systems makes IoT systems and applications out of security holes.

A. Network Layer security Problems

Customarily security issues refer to the general security issues occur in a communication network to threaten data integrity and confidentiality. Though the present communication network in IoT has comparatively strong measures for security and protection of systems, there are still several customary threats such as illegal access in networks, confidentiality harms, eavesdropping information, integrity damage, Man-in-the-Middle attack, DDoS attack, exploit attacks, virus invasions, etc (Wang, 2016). Besides customary issues, compatibility network issues are also part of network layer security where the Internet network security framework is implemented on the basis of the user’s requirement and not applied to the communication between network machines. With the use of some security mechanisms, the logic relationship between IoT machines can be split. Heterogeneity makes interoperability, security, and coordination of the network becoming worse. The cluster security issues involve DDoS attack, network congestion, authentication issues, and so on. IoT has a large number of devices so if its system uses the existing authentication mode in authenticate device where a

large number of data block the network. Also, the existing IP system does not use extensive nodes identification. The mutual authentication between numerous equipment cases causes wastage of key sources. Privacy disclosure is also an emerging threat with the increasing development of information retrieval setups or social engineering. This enables hackers to easily collect the user`s confidential information.

B. DDoS attacks

IoT is an emerging technology and has a lack of basic security controls. This enables software targets and cybercriminals to attack and add botnets to launch a DDoS attack. In this attack, attackers crippled the networks by hacking IoT applications and devices that are protected from hard or weak coded passwords. These attackers than incorporate such devices into botnets to carry out DDoS. These attacks disrupt networks for VoIP phones, smart video conference applications, and connected printers as well. They also damage IP connected network infrastructure and security systems. Additionally, a large number of IoT services with extensive data storage can be made easy for malicious activities to go unnoticed.

C. Poor Network Segmentation

Internet-connected operational technologies (OT) when used by misconfiguration, then it becomes the reason for failure to many firewalls for the detection of malicious activity by attackers to access OT systems.

D. Malware

The collection of multiple IoT devices such as wearable's, embedded technologies, and routers are known as IoT Botnet and are often attacked by malware. This attack enables hacker or attacker to gain control towards all connected devices in the network. IoT Botnets are different from customary devices as the infected IoT device can spread the malware, therefore targeting remain continuing to more and more Botnets. The malware attempts to start a connection from a shared set of devices and then perform a dictionary attack using a huge database until it passes the edge of connections by IoT device.

E. Weak password protection

Throughout the network development lifecycle, irrespective of security, the majority of the manufacturers requires their devices to set up easily. The login credentials are mainly required to set up new devices by manufacturers. This weak password or unchanged passwords are easy to detect by attackers and become the biggest threat to IoT network security.

F. Lack of encryption

In IoT systems, security is viewed as a basic factor in network establishment and so does the encryption in any IoT device. In many cases, Legacy Supervisory control and data acquisition (SCADA) controllers or several industrial protocols creates a lack of ability to encrypt the communication (Shahzad, 2017). Many attackers make use of sniffing software application to acquire login credentials (username and login passwords).

G. Cloud threats

The traces of digital war, the major potential threats to IoT devices are more likely to be cloud networks. These networks hold the biggest data to run and function IoT. The threats and risks of losing important data through hackers can create dangerous outcomes not only for organizations but also significantly affects the nation as well through cross-border attacks. These attacks and threats will propel nations to establish internet walls to limit the activity of IoT devices across particular regions. One of the biggest threats to IoT comes from the global system to share and exchange information on which IoT devices are highly dependent. According to the Global Risks Report of 2018, indicates the threat of network security threats and dangerous outcomes towards several interconnected organizations of IoT compromised due to internal vulnerabilities (Raban, 2018). Clouds would be the first to be easily compromised due to inappropriate network security regulations.

IV. ATTACK MITIGATION TECHNIQUES

A . Network Layer security measures

In the existing framework of IoT, the network layer is based on Internet or present communication network. IoT systems, nodes are arranged in random order with unreliable energy limitation and communication results in the dynamic topology of IoT system`s infrastructure. For diverse network architectures, it is pertinent to set up authentication based mechanisms, end-to-end key and authentication mechanism, Public Key Infrastructure for wireless network systems, intrusion detection, routing security, etc. Network availability should also be considered due to a large number of data. The use of network virtualization technology can greatly mitigate the intricacy of network management and chances of the wrong operation. Moreover, the developing trend of IPv6 based information security products provides secure utilization of next-generation networks (NGN) and transport carrier networks as well.

B. Design Security

Security of IoT devices based on different elements including the amount of confidential information assortment and mitigating cost plans of

security vulnerabilities. Alabady (2018), presented certain ideas that can address and mitigate key security issues that are often suggested by organizations to consider. These key points include, (1) carry out security risk valuation throughout the network design process; (2) assess device security measures; (3) focus on the protection of sensitive data in data transmission process; (4) oversee IoT devices, applications, and update software programs on regular basis.

C. Anti-malware and secure coding

IoT systems are vulnerable to attack and require the implementation of anti-malware protection, host-based firewall controls along with patch controlling policies to mitigate exposure. Telnet, ICMP, SSH, etc. reused to stop malware attacks and prevents malware to affect IoT devices (Alabady, 2018). On the other hand, IoT developers should create secure coding practices to apply on IoT devices during the software build process. The strong focus on quality assurance (QA) and threat identification or remediation should be adopted in IoT network development lifecycle. This will also help in streamlining security endeavours while mitigating threats simultaneously.

D. Two-way authentication technique

With the emerging trends in IoT, networks are rapidly expanding and also becoming powerful which requires the strong maintenance of data integrity and privacy. Two-way authentication technique for network security of Internet-of-things (IoT) is linked with the Internet standards, particularly with Data Transport Layer Security (DTLS) protocol (Schmitt, 2017). This protocol enables ease of security uptake by reusing engineering techniques, existing systems, and security infrastructure. The two-way authentication technique is designed to operate by following standard communication stacks to provide UDP/IPv6 networks. Moreover, due to the heterogeneous nature of IoT devices, two public-key cryptographic algorithms including Elliptic Curve Cryptography (ECC) and RSA (Rivest, Shamir and Adleman) plays important for network security in IoT devices.

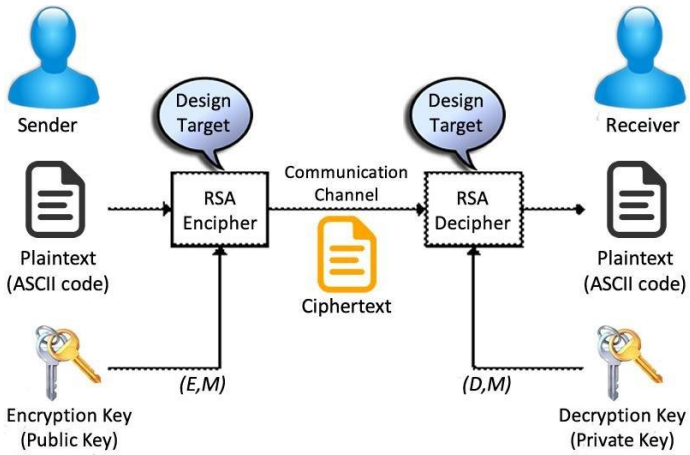

Figure 1RSA algorithm structure

E. Digital certificates

Digital certificates play a crucial role in the establishment of network authentication, data encryption and maintain integrity, device identity and confidential data. Public key infrastructure (PKI) uses digital certificates that can enable identity authentication for device-to-device and device-to-server security in IoT network systems. Digital certifications considered as the foundation of IoT network security, protection for its data, devices authentication, and establishing trust for all users who are interconnected with the network. PKI tackles network security challenges by using digital certificates with a network security protocol to secure and encrypt information in IoT network (Ammar, 2018).

F. Firewall implementation technique

The firewall technique to establish security and mitigate network security threats serves as abridge among IoT devices and internet connection. The firewall connects with the router through Ethernet cable to monitor and control vulnerabilities. The advancement in firewalls often uses artificial intelligence along with machine learning to address IoT device in network infrastructure and creates a baseline for stable activity. This enables devices to examine both internal and external network traffic and block abnormal traffic (Lee, 2017).

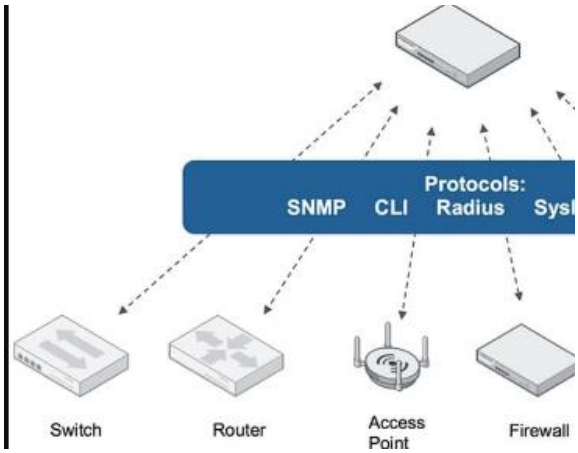

Figure 2Firewall working as a bridge`

V. Technical Challenges

It is a notable fact that regardless of all the crucial investment and research being done in the field of network security issues for protecting conversation, online payments, and other internet-based activities on "Internet of Things," the network security issues are growing constantly (Yaqoob, et al., 2017). In such condition, it has been noted that there are certain technical challenges which hinder the development of the new network security development process for the "Internet of Things (IoT)." Few of the most common types of technical challenges which makes it complicated for the networking engineers and IT experts to resolve the impending issues concerning network security are discussed below.

A. Poor and Ineffective Network Performance

In recent times, it is apparent that the network performance has been affected due to the poor management of traffic and networking elements such as encryption approaches. A study conducted by Zachariah, et al. (2015) states that "there is no question that poor network performance is a top challenge for network engineers, there is simply more total traffic; there is more traffic in all directions. In this manner, it becomes evident that the poor network performance is a major technical issue which restricts the improvement of the network security system. In addition to this, it is also a known fact that the growth in a number of users in the internet world has increased the traffic on social media websites and "Internet of Things (IoT)." As a result, the growth in a number of users have made it problematic and challenging for networking engineers to improve the network system.

In addition to this, without the availability of suitable equipment, it is completely impossible to provide a secure networking system to cater to the growing demand of users on "Internet of Things (IoT)". Hence, it becomes evident that the technical challenges caused by poor performance, lack of advanced equipment, and a growing number of users serve as a major technical challenge for improving the network security system in "Internet of Things (IoT)."

B. Ineffective and Obsolete Security Systems

It has been observed that there are extensive ranges of security system available to secure the overall transaction process, data sharing process, and communication process on "Internet of Things (Zachariah, et al., 2015)." In this way, it becomes evident that the security system has become ineffective and obsolete and thus it has become a major technical challenge for the network security system. One of the major factors affecting the network security system is that cyber-offenders and cyber-criminals are continually coming up with new technical designs and features to hack the enterprise's information system and acquire personal details of individuals. In this manner, the networking engineers are currently failing to maintain a strong and effective system for the protection of the network security system.

On the other hand, the paradigm of the present system is indistinct, blocking unapproved outside traffic from the inside system is not sufficient for securing information. Numerous dangers cause it into the system when representatives to react to a phishing email. Refusals of administration assaults just need to endeavour associations with succeed. Encryption secures traffic, however, encryption can likewise make it harder to screen the organized action (Sfar, et al., 2018). There are numerous devices that can be utilized to improve arrange security, however, guaranteeing they cooperate and give an exhaustive arrangement is troublesome. In this concern, it could be stated that obsolete systems should be upgraded and enhanced through encryption technique to make the networking system secured.

C. Configuration Management

It is a noticeable fact that the networking system is noted to be one of the most effective aspects of the network security system. However, it is also apparent that as the networking system is increasing in size, the network configuration system is turning out to be more complicated. The following statement could be further approved by reviewing the study of Lee and Lee (2015) in which it has been explained that the network configuration is now more difficult as it requires more encryption and extensive queries to cater the demand of

billions of internet users globally. The main factor which is making this technical challenge more complex is that the devices are now contradicting with each other. Therefore, it turns out to be more multifaceted for the networking engineers and IT experts to maintain the rules and procedures in the firewall. Furthermore, doing the configuration manually can also prove to be detrimental as the likelihood of errors increase and thus the networking system becomes more vulnerable to experience online security threats.

D. Cost Management

It has been noticed that the cost of operations in the field of Information Technology has increased. The cost of inflation has raised several technical challenges in the designing and development of contemporary network security system. It has been observed that the available budget is failing to meet the requirements for providing a secure networking system to users, particularly, when the network security system needs contemporary services such as telephony (VoIP) and face detection technology to secure the network system (Lee and Lee, 2015). In such a condition, it is assumed that the overall price of ***production should be reduced to facilitate the technical team in developing high-tech network security system for the Internet of Things***

E. Emergence of New Technologies

Yesterday's sensible choice methods indicate that the engineering is worked around the presumptions and abilities of yesterday's seller. Getting the best arrangements from the present merchants means making sense of how to interoperate, coordinate, and bolster numerous arrangements, or making sense of how to detach the majority of the old hardware without tearing down the whole system at the equivalent time. In such condition, a technical issue and challenges arise in the formation of a proper security system in the "Internet of Things (IoT)." The following statement could be further approved by reviewing the study of Conti, et al. (2018) in which it has been explained that the technology is getting advanced day-by-day. As a result, networking engineers are required to bring continual improvement and advancement in the network security system. Therefore, coping up with the technological changes results in giving rise to the complications to implicate effective security system in the "Internet of Things (IoT)."

VI. Opinions on Future Directions

The "Internet of Things (IoT)" is projected to come up with a new wave. It is a noticeable fact that in the future, more than 30 billion devices globally will be connected to the Internet. This increment in the number of devices will entice cybercriminals to get more access to user's data. In this concern, it has been assumed that the networking system interlinked with the "Internet of Things (IoT)" is required to be improved in the future (Kumar, Vealey, and Srivastava 2016). The advancement must be brought in the existing network security structure and thus the existing security features must be upgraded or replaced with newer ones. For instance, two-factor authentication may not prove to be advantageous in the future. In such condition, newer features must be implicated to secure the user's data, conversation, and data sharing process, and transaction as well.

It is believed that in the future, the entire process of technology will be based on Artificial Intelligence and thus the interaction of human with the gadgets will be done in an automated manner. The implication of Artificial Intelligence in gadgets and devices will be designed in a way that they will not give data accessibility to unauthorized persons. In addition to this, they will detect an insecure activity. As a result, the network security system in "Internet of Things (IoT)" will be advanced in the future and thus people will be able to share data, make online transactions, and store data in a well-protected environment.

VII. Conclusion

The objective of the study was to present the most crucial elements of IoT by focusing on the particular network security issues and challenges linked with IoT devices. A lot of network issues and challenges linked with the security of IoT applications are being experienced in many industries. The conducted research concerned with the potential security needs in the domain of IoT systems in heterogeneous environments to raise user awareness about secure network and devices utilization. This helps in the secure communication and sharing of information between networks or devices installed inside and outside organizations. Furthermore, this paper recommends certain solutions and mitigation techniques from several aspects, The solutions presented in this paper reflecting the architecture and framework of technical approaches and mechanisms by which the security and network quality will be increased in IoT environment. Also, data security and data protection are highly considered aspects that are addressed in the paper. The study gives key aspects for the organizations to address and increase security in IoT systems and applications. Such aspects include; network design security, data minimization, user guidelines for different

operations. As a conclusion, IoT requires continuous thinking and harmonization of its secure network systems. The study affirmed that network security of IoT based application and devices must be considered for its long-run process, through design to functional phases which includes: secure booting, access control, device authentication, IPS, patches and updates, and firewalling. The applications of IoT involves a complex set of technical contemplations among different types of stakeholders. The technical developments in the field of IoT enable the use of its system and applications or work with secure network settings. Efforts and security solution endeavours by government, technical industries, production sectors, and academic works for the provision of secure processes provide effective and secure use of IoT developments .

REFERENCES

Alabady, S. A., Al-Turjman, F., & Din, S. (2018). A novel security model for cooperative virtual networks in the IoT era. *International Journal of Parallel Programming*, 1-16.

Alabady, S.A., Al-Turjman, F. and Din, S., 2018. A novel security model for cooperative virtual networks in the IoT era. *International Journal of Parallel Programming*, pp.1-16

Aldowah, H., Rehman, S.U. and Umar, I., 2018, June. Security in internet of things: issues, challenges and solutions. In *International Conference of Reliable Information and Communication Technology* (pp. 396-405). Springer, Cham.

Ammar, M., Russello, G. and Crispo, B., 2018. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, pp.8-27.

Conti, M., Dehghantanha, A., Franke, K. and Watson, S., 2018. Internet of Things security and forensics: Challenges and opportunities.

Kim, S.M., Wang, S. and He, T., 2016, August. IoT networking: From coexistence to collaboration. In *2016 IEEE 22nd International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)* (pp. 212-217). IEEE.

Kumar, S.A., Vealey, T. and Srivastava, H., 2016, January. Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.

Lee, I. and Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), pp.431-440.

Lee, J.H. and Kim, H., 2017. Security and privacy challenges in the internet of things [security and privacy matters]. *IEEE Consumer Electronics Magazine*, *6*(3), pp.134-136.

Raban, Y. and Hauptman, A., 2018. Foresight of cyber security threat drivers and affecting technologies. *foresight*, *20*(4), pp.353-363.

Schmitt, C., Kothmayr, T., Hu, W. and Stiller, B., 2017. Two-way authentication for the internet-of-things. In *Internet of Things: Novel Advances and Envisioned Applications* (pp. 27-56). Springer, Cham.

Sfar, A.R., Natalizio, E., Challal, Y. and Chtourou, Z., 2018. A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), pp.118-137.

Shahzad, A., Kim, Y.G. and Elgamoudi, A., 2017, February. Secure IoT platform for industrial control systems. In *2017 International Conference on Platform Technology and Service (PlatCon)* (pp. 1-6). IEEE

Shang, W., Yu, Y., Droms, R. and Zhang, L., 2016. Challenges in IoT networking via TCP/IP architecture. *Technical Report NDN-0038. NDN Project*.

Wang, J., Pambudi, S., Wang, W. and Song, M., 2019. Resilience of IoT Systems Against Edge-induced Cascade-of-Failures: A Networking Perspective. *IEEE Internet of Things Journal*.

Wang, P., Chaudhry, S., Li, L., Li, S., Tryfonas, T. and Li, H., 2016. The Internet of Things: a security point of view. *Internet Research*.

Yang, K., Liu, S., Cai, L., Yilmaz, Y., Chen, P.Y. and Walid, A., 2019. Guest Editorial Special Issue on AI Enabled Cognitive Communication and Networking for IoT. *IEEE Internet of Things Journal*, *6*(2), pp.1906-1910.

Yaqoob, I., Ahmed, E., Hashem, I.A.T., Ahmed, A.I.A., Gani, A., Imran, M. and Guizani, M., 2017. Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE wireless communications*, *24*(3), pp.10-16.

Zachariah, T., Klugman, N., Campbell, B., Adkins, J., Jackson, N. and Dutta, P., 2015, February. The internet of things has a gateway problem. In *Proceedings of the 16th international workshop on mobile computing systems and applications* (pp. 27-32). ACM.