**IPV6 and IoT Security Issues**

Research Paper

IPV6 and IoT Security Issues

In the recent past decades, technology has greatly advanced. The conventional technology systems and devices are being replaced by advanced technology innovations that are perceived to provide better security, convenience, and privacy. Internet Protocol Version 6 (IPv6) and Internet of Things (IoT) are two key innovations that are changing the technology landscape globally. IPV6 refers to an advanced internet protocol version 6 which is soon expected to replace IPV4 protocol. On the other hand, Internet of things (IoT) refer to the interconnection of many computing devices like smart watches, thermostats, RFID tags and many more to provide an integrated way of interaction. IPv6 and IoT are strongly related due as they work together to provide a secure and efficient way for computing devices to communicate and interact across a network (Matharu, Upadhyay & Chaudhary, 2014).

Petrov (2019), suggests that the industry is estimated to have a market value of over $1.7 trillion, and by 2025 there will be over 64 billion IoT. IPv6 infrastructure has been proposed and recommended by several researchers as a key upgrade and a ‘game changer’ in the growing and complex internet industry. IPv6 can accommodate 340 undecillion IP addresses with its 128-bit address capacity while IPv4 has only 32-bit address capacity (Caicedo et al., 2009). The purpose of this paper is to review the literature on the security issues of internet of things and IPv6, describe the current issues, and identify the possible recommendations by the authors for future studies.

# Problem Description

Studies have shown numerous IPv6 and IoT security issues through analyzing different dynamics and risk factors associated with the technologies. Valera & Lee (2016) studied on the problem of security on the mobility of wireless security networks, which was a key concern in the implementation of IPv6. Caicedo, Joshi & Tuladhar (2009) looked at the security issues in deploying and shifting to IPv6. The study noted that due to the increasing number of internet of things devices, management challenges and scalability were key concerns that could compromise the security of devices. Two studies Razzaq, Gill, Qureshi, & Ullah (2017) and Shen, Zhang & Gu, (2012) looked at the IoT technology security issues, such as the problem associated with the increasing number of devices and the decreasing number of IP addresses affected the effectiveness of communication across home environments and exposed them to different types of malicious attacks. Similarly, Shah & Parvez (2015) studied on the security issues on the next IP migration, particularly focused on comparing the attacks that are common in IPv4 and how they would change or arise during the migration to IPv6. Studies show that there is need to address the existing gaps prior to fully migrating from IPV4 to IPV6 across IoT networks (Lamaazi et al., 2014). For the network to be effective, network engineers should have a clear framework to implement IPV6 while not exposing IoT devices to security and privacy threats (Frustaci, Pace, Aloi & Fortino, 2017). Taking these literature studies into account, it is evident that IoT and IPv6 technologies face serious security issues that have the potential to compromise their effectiveness and expose businesses and people to serious risks, such as malicious attacks and data breaches.

# Methodologies

To explore this topic, researchers have used both quantitative and qualitative methods to collect and analyze data. Valera & Lee (2016) research used a document analysis approach towards gathering the data which was sourced from the published and existing secondary sources. Caicedo, Joshi & Tuladhar, 2009, studies were selected using triangulation strategies, which involved searching for multiple data sources, authors, statistics, and theoretical frameworks. Frustaci, Pace, Aloi & Fortino (2017) gathered sources which included journals, case studies, books and data surveys related to the topic. The sources were selected based on their relevance on discussing the issues of IPV6 and IoT, as well as their analysis on the current and future trends. Shah & Parvez (2015), study involved a critical analysis and a discussion created through interpretation and integrating different ideas from different researchers.

# Significant Findings

The key findings from the studies showed that IPV6 network structure will have numerous challenges when it comes to its use in the internet of things (Caicedo, Joshi & Tuladhar, 2009). The studies also showed that there are underlying issues in the network architecture, distribution, costs, device management, and security of IoT networks to operate in IPV4 protocols. Lamaazi et al. (2014) also had similar findings on the security issues due to complexity in management of IoT devices in IPv4 environment. Valera & Lee (2016) found that the security issue on the mobility of wireless security networks was a key concern in the implementation of IPv6. The authors found mobile and wireless networks were vulnerable to different attacks due to the modes of data packet forwarding in between mobile nodes and other nodes. Shen, Zhang & Gu (2012) and Razzaq, Gill, Qureshi, & Ullah (2017) studied IoT technology security issues, and noted that due to the increasing number of devices the decreasing IP addresses affected the effectiveness of communication across home environments and exposed them to different types of malicious attacks. Shah & Parvez (2015) noted that in order to address the drawbacks of IPv6, it is vital to have an exhaustive consideration of the security aspects.

# Discussion, Implications, and Future Research

The major challenge of IoT is to effectively integrate IPV6. The enormous network environment and considerations such as software and hardware compatibility raises concerns of “interoperability, homogeneity, openness, security, flexibility, and heritage” (Lamaazi et al., 2014). The research shows that more evaluations and preparations need to be done to address the challenges that might affect the effectiveness of IPV6 in IoT networks (Shah & Parvez, 2015). To accomplish this, scholars recommend further research to explore the constraints and the complexity of IoT network management. Without adequate measures, the IPV6 might be counterproductive, exposing the IoT networks to more complex security threats and vulnerabilities. The studies evaluated in this research confirmed that there is need for advanced measures to manage the dynamics of IoT and IPv6 technologies and comprehensive mitigation techniques that can be used to prevent the risks that are associated with network migration and IoT environments.

# Conclusion

This paper evaluated the IPV6 and IoT issues. Despite the capabilities of IoT and IPv4 technologies, experts have raised major concerns about their security due to their dynamics that could expose them to enormous security threats if inadequate measures are not taken to achieve a smooth transition.

References

Caicedo, C. E., Joshi, J. B., & Tuladhar, S. R. (2009). IPv6 security challenges. *Computer*, *42*(2), 36-42.

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal*, *5*(4), 2483-2495.

Lamaazi, H., Benamar, N., Jara, A. J., Ladid, L., & El Ouadghiri, D. (2014, July). Challenges of the internet of things: IPv6 and network management. In *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (pp. 328-333). IEEE.

Matharu, G. S., Upadhyay, P., & Chaudhary, L. (2014, December). The internet of things: Challenges & security issues. In *2014 International Conference on Emerging Technologies (ICET)* (pp. 54-59). IEEE.

Petrov C., (2019). Internet of Things Statistics 2019 [The Rise Of IoT]. Techjury.com. Available online: <https://techjury.net/stats-about/internet-of-things-statistics/>

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications*, *8*(6), 383.

Shah, J. L., & Parvez, J. (2015). Security Issues in Next Generation IP and Migration Networks. *IOSR Journal of Computer Engineering*, *17*(1), 13-18.

Shen, L., Zhang, Y., & Gu, J. (2012). Development Trend of IPv6-based Information Security Products in Network Layer of IOT [J]. *Netinfo Security*, *8*.

Valera, P., & Lee, S. (2016). Security measures in overcoming mobile ipv6 security issues. *International Journal of Databases Theory and Application*, *9*(7), 297-304.\