Security of Internet of Things (IoT) Devices and Systems

Emmanuel Ogundare
TECHiT

Security of Internet of Things (IoT) Devices and Systems

Introduction

The rapid increase in devices that are connected in recent decades has led to the emergence of the technology known as the Internet of Things (IoT). IoT gadgets include a number of objects which are submerged together with sensors and software that allows for the collection and the exchange of data via the internet (Kumar et al., 2019). These gadgets include game devices, home appliances and smart phones down to industrial machines. Thus, IoT systems is a representation of a large network of devices which are connected together, transmit and work together so as to perform an array of activities and services on their own without any form of supervision by human (Gazis, 2021).

When it comes to security, this is very important as regards IoT as it is very vital as a result of the sensitivity of the nature of the data that are not only transmitted, but also gathered via these devices. As these devices continue to make significant wave in different areas of lives and important infrastructures, security has become very important. IoT gadgets becomes susceptible to threats when enough security is not put in place. Data can be breached, unauthorized access by external people can be carried out and manipulation can be done. Also, IoT gadgets that has been breached can become a platform as entry points for cybercriminals embark on full scale attacks, which affects not just the privacy of people, but also national security and safety of the public.

Examination of concerns as regards IoT

The security issues as regards the IoT is multidimensional and this is as a result of the many susceptibilities that is inherent in IoT gadgets. For one, the absence of a viable standard is a major challenge to IoT gadgets. With a number of manufacturers developing IoT gadgets using various software and hardware, most times, interoperability issues emerge, thus making it challenging to embark on security measures that are consistent for these gadgets. Hence, the lack of a unified entity does not only complicate the security efforts, but instead further creates defects that cybercriminals can exploit on (Leloglu, 2017).

Also, a number of IoT gadgets lack enough authentication measures. This leaves them vulnerable to access from outside forces. Passwords that are weak, and the lack of multi factor security authentication are some of the major issues that’s it very easy for cyber attackers to hack into these

IoT devices. Once these devices have been infiltrated, it can be used as the point of entry into other networks, where damaging attacks can be carried out (Aldowah et al., 2018).

Another major concern when it comes to the security of IoT is the use of protocol encryption that are weak. Tawalbeh et al., (2020) argues that most IoT devices tend to transfer data that are sensitive via other networks while using encryption methods that are weak and outdated, thus making them vulnerable to compromise. Without a comprehensive encryption measure in place, the integrity and the confidentiality of data from IoT are endangered, which further poses great risks to security of the users. Also, when updates are not consistent, it enhances the security challenges that are in tandem with these devices. Unlike conventional computing gadgets that receive updates and patches frequently so as to tackle the vulnerabilities, most IoT devices tend to lack proper measures for updates. Often, most manufacturers tend to release security measures occasionally, and many times, device owners neglect to apply them as a result of their complex nature. Due to this, IoT devices will remain vulnerable to exploitation, leaving them to be exposed to attacks (Taherdoost, 2023).

The effects of these security compromises are profound. When data are breached, it leads to the exposure of data that are sensitive. Also, the violation of privacy tends to happen when IoT devices are accessed without authorization which allows for the access to another person's activities without their knowledge, this infringing upon their rights to privacy (Leloglu, 2017).

Also, security breaches cause large number of damages. For example, Aldowah et al., (2018) adds that IoT devices that has been compromised used in important infrastructures such as medical gadgets or grid devices can lead to the disruption of services and equipment's not functioning optimally which will lead to accidents with consequences on lives. Added to this, attacks that targets IoT devices that are linked to Industrial control systems tend to lead to disruptions in operations, damage n facilities and even potential environmental hazards.

Securing IoT Devices and Systems

The security of IoT systems and devices presents a number of issues which emerges from the intricate nature of IoT systems, the constraint of resources and the lack of knowledge and education among major stakeholders.

One of the major primary challenges in securing IoT devices is the complex nature of the IoT systems. IoT systems entails an array of devices, which span from small sensors to cutting devices. Each of these devices have various functions, operating systems and security requirements, thus making it quite challenging to implement security measures that are of standard across the ecosystem. Also, the huge volume and complexity of IoT gadgets have further complicated it as the security and management of large number of devices has become a major challenge (Aziz Al Kabir et al., 2023).

IoT devices, which are connected via an array of network, either wireless or wired forms the base of a major webs of communication. These networks which are connected develop a number of entry points for cyber attackers to exploit as a compromise of one major device can lead to the endangering of the entire IoT system. Also, the ever-dynamic nature of IoT networks, with various devices joining and leaving the network often further adds layers of complexity of securing and monitoring network traffic (Sadique et al., 2018).

Another major area of the complexity of IoT system is the diversified nature of communication methods which are used by various devices and systems. Mazhar et al., (2023) alludes that IoT devices adopts many communication approaches such as the use of WIFI and Bluetooth most especially, while depending on the applicability of their requirement and challenges. The management and security of communication, across various approaches further presents challenges that are interoperability in nature and further increases the attack surface for criminals who can exploit weakness. The constraint of resources further poses a major challenge to the security of IoT devices, especially when memory and processing power is limited. A number of IoT gadgets are designed with hardware resources to limit the size, costs and consumption of power. However, the limitations in resources often restrict the implementation of a comprehensive security feature, which include encryption and authentication which enhances detection. Due to this, the IoT devices, gives priority to the functionality over security, hence leaving them vulnerable to attacks (Kumar et al., 2019).

Additionally, power consumption concerns impact the security of IoT devices, especially those deployed in remote or battery-operated environments (Alkunidry et al., 2023). Security mechanisms such as encryption and authentication can consume significant computational resources and energy, leading to reduced battery life or operational efficiency. Balancing security requirements with power consumption considerations becomes a critical consideration in designing and deploying IoT devices, particularly in applications where energy efficiency is paramount. Furthermore, the lack of awareness and education among users, developers, and policymakers poses a significant challenge to IoT security (Canavese et al., 2024). Andreas et al., (2021) points out that many users may not fully understand the security risks associated with IoT devices and may inadvertently compromise security through poor configuration, weak passwords, or failure to apply security updates. Likewise, developers may lack awareness of security best practices or may prioritize functionality over security during the development lifecycle. Moreover, regulatory and compliance issues surrounding IoT security standards and certifications may further complicate the landscape, leading to inconsistencies in security practices and requirements across different jurisdictions (Canavese et al., 2024).

Addressing these challenges requires a concerted effort from all stakeholders involved in the IoT ecosystem. Manufacturers need to prioritize security in the design and development of IoT devices, considering factors such as interoperability, resource constraints, and usability. Additionally, policymakers should establish clear guidelines and regulations to promote security standards and incentivize compliance among manufacturers and users. Moreover, raising awareness and providing education on IoT security risks and best practices is crucial for empowering users and developers to make informed decisions and mitigate security threats effectively. Ultimately, addressing the challenges in securing IoT devices and systems requires a holistic approach that encompasses technical, regulatory, and educational initiatives to build resilient and trustworthy IoT ecosystems (Abed & Anupam, 2022).

Strategies for Enhancing IoT Security

The implementation of a comprehensive authentication mechanism is very important for ensuring the security of IoT systems and gadgets. Clark & Rajabion, (2023) adds that the 2FA also known as two0factor authentication is an important and significant approach to enhance access control to these devices beyond conventional password-based authentication. Through the requirements of users to provide another form of verification, which might include a social code sent to mobile phones or biometric, 2FA greatly reduces the risk of access that is not authorized, even when passwords are compromised. Added to this, the implementation of device identity management system for solutions allows organizations to develop and manage their peculiar identities for each of the IoT devices in their networks. This ensures the granular control of the devices and access so as to enhance the detection of compromised activities and access that are not authorized (Aljrees et al., 2023). Through the combination of a comprehensive authentication mechanism like 2FA with a robust device for identity management, organizations can greatly curb the risk of authorized access and further protect their IoT system from cyber criminals.

Enhancing encryption methods is an important approach for improving IoT security. Using encryption algorithms which well encrypted such as the use of Elliptic Curve Cryptography (ECC) or Advanced Encryption Standard (AES), enables the protection of data that are sensitive which are transferred between various IoT devices and backend systems form been intercepted or compromised by third parties (Rana et al., 2023). Through the encryption of data, Molina Zarca et al (2018) opined that organizations can ensure the integrity and confidentiality as well as privacy of their IoT communications, even when under cyber threats. Also, securing major key management practices are very important for the maintenance of the integrity of encryption schemes. An effective key generation, storage system and distribution challenge ensure that cryptographic keys are private and not accessible to cyber criminals. Added to this, the implementation of major renewal and rotational policies enables the mitigation of risk of major compromises which strengthens the encryptions security (Andreas et al., 2021). Through the adoption of strong encryption methods and the implementation of a comprehensive management practices, organizations can be able to safeguard the deployment of the IoT against any form of any third-party access and breaches.

Enhancing updates and patch management process is very important for the maintenance of the security of IoT systems and gadgets. Automated update systems that are streamlined enable the process of deployment of security patches and software updates to IoT system, which ensures that they can be well protected against weakness. These mechanisms are automated and enables the detection, installation and downloading, which reduces the burden on users to apply manually. By applying automation, organizations can ensure that IoT systems are regularly updated with the latest security features and thus in the process reduces any form of exposure to any form of cyber threats (Bhardwaj et al., 2024).

Evaluation of vulnerabilities as well as a regular audit of security are very important for effective update and practices of patch management. Embarking on a periodic audit enables organizations to recognize security weaknesses in their IoT systems. Through the regular assessment of the security posture of IoT devices and system, organizations can give priority to efforts towards remediation and further provide resources to ensure solving important security challenges. Assessment that are vulnerable help in the identification of weaknesses in IoT devices and software elements, which allows organizations to apply important patches and updates in a required manner (Almotairi et al., 2024). Also, regular security evaluation enhances a continuous improvement of update and management process by recognizing the areas for improvement and optimization.

Improving the IoT systems entails a multi-dimensional approach that addresses the underlying weaknesses and threats that are inherent in the deployment of IoT. Segmentation of networks is a n important approach for isolating IoT devices into various networks elements based on their functional roles. Through the segmentation of IoT networks, organizations can contain the effect of security breaches and further prevent any form of lateral movements by attackers within the network. Added to this, network segmentation allows organizations to implement security policies that are personalized and access control for various segments, thus reducing the risk of data been breached or authorized access.

Intrusion detection and prevention systems also known as –IDPS is very important in mitigating and detecting threats in IoT systems. These systems ten to monitor traffics of networks and behaviors o devices in real time so as to identify any form of activities that are suspicious and any form of anomalies that reveals any form of security interferences. Through the leveraging of machine learning algorithms and behavioral analysis approaches, IDPS is helping to detecting any form of attacks and accesses that are not authorized, enabling organizations to react swiftly and mitigate the impact of security incidents. Also, IDPS also complement automated update mechanisms through the provision of continuous monitoring and threat of detection capabilities and in the process improving the overall security posture of IoT deployment (Alkunidry et al., 2023).

Lastly, the incorporation of security by design tents is important for developing resilient and secure IoT solutions from the ground up. Through the integration of security considerations into the design and processes of development, organizations are able to tackle major security issues and weakness at all the stages of the lifecycle of the product. Security by design involves the implementing secure coding activities, threat modeling and security testing through the evolution of lifecycle to recognize and solve any form of security breaches (Alkunidry et al., 2023). Through the of security protocols and safeguarding IoT devices and systems from the beginning, organizations will help in the reduction of any form of breaches in security will ensuring that security remains the main aspect of the diplomat of IoT.

Future Directions and Emerging Technologies

Future directions in IoT security are set to leverage new technologies and creative ways in tackling new threats. Improvement in IoT security technologies is set to stress on improving the resilience as well as integrity of IoT systems via a combination of software and hardware-based solutions. This includes the evolution of secure hardware components, which include TEE known as trusted execution environment and hardware security modules HSM, which can provide tamper resistant storage and processing abilities for cryptographic keys and sensitive data. Added to this, new technologies in secure element integration, firmware integration and secure boot mechanism enables the mitigation of the risk of any form of tampering and attacks On IoT gadgets (Karie et al., 2020).

Also, the possibility of the effect of AI and Machine Leaning on the society of IoT is very crucial. Koirala et al., (2023) adds that AI driven security analytics and detection of anomaly can examine a large array of data in real time so as to identify behaviors that are unusual while at the same time detecting new threats while automating responsive actions. By leveraging ML methods, organizations are able to implore the detection of threats, improve response time to threats and adapt to new security controls. Also, AI powered predictive analytics will enable organizations to identify security issues and swiftly curb this weakness prior to them being exploited by malicious actors.

Blockchain technology and approaches that are decentralized are also emerging as promising solutions for improving IoT security. Blockchain is providing a denaturalization and immutable platform that can be adopted in the security of IoT engagement, this is by establishing trust between devices while ensuring the integrity of date. By using contracts that are blockchain and the distribution of consensus mechanism, organizations can implement a transparent and secure IoT ecosystem that resist any form of modifications that are unauthorized and any form of tampering. Also, decentralized identity management solutions which are based on blockchain allows for user authentication and the authorization of IoT devices, while reducing any form of risk of single points of failure and access that are not authorized (Fei et al., 2023).

Conclusion

Conclusively, the security of IoT devices is very significant in a world that getting connected. Hence, addressing the many challenges of IoT security entails a collaborative effort among all major stakeholders. They include the developers and manufacturers, the end users, policy makers and even retailers. Through the implementation of a mechanism that is robust in nature, improving the approaches of encryption and enhancing the process of patch management, organizations can improve security of IoT systems.

Also, the creating awareness and education is important for empowering users and developers so as to make decisions that re informed and take enough measures in protecting IoT devices. Government regulations are very important in the establishment of baseline security requirement while enhancing accountability in the IoT system.

References

Abed, A. K., & Anupam, A. (2022). Review of security issues in internet of things and Artificial Intelligence-Driven Solutions. *SECURITY AND PRIVACY*, *6*(3). https://doi.org/10.1002/spy2.285

Aldowah, H., Ul Rehman, S., & Umar, I. (2018). Security in internet of things: Issues, challenges and solutions. *Advances in Intelligent Systems and Computing*, 396–405. https://doi.org/10.1007/978-3-319-99007-1_38

Aljrees, T., Kumar, A., Singh, K. U., & Singh, T. (2023). Enhancing IOT security through a green and Sustainable Federated Learning Platform: Leveraging Efficient Encryption and the quondam signature algorithm. *Sensors*, *23*(19), 8090. https://doi.org/10.3390/s23198090

Alkunidry, D., Alhuwaysi, S., & Alharbi, R. (2023). Security threads and IOT security. *Journal of Computer and Communications*, *11*(09), 76–83. https://doi.org/10.4236/jcc.2023.119005

Andreas, A., Mavromoustakis, C. X., Mastorakis, G., Do, D.-T., Batalla, J. M., Pallis, E., & Markakis, E. K. (2021). Towards an optimized security approach to IOT devices with Confidential Healthcare Data Exchange. *Multimedia Tools and Applications*, *80*(20), 31435–31449. https://doi.org/10.1007/s11042-021-10827-x

Aziz Al Kabir, M., Elmedany, W., & Sharif, M. S. (2023). Securing IOT devices against emerging security threats: Challenges and mitigation techniques. *Journal of Cyber Security Technology*, *7*(4), 199–223. https://doi.org/10.1080/23742917.2023.2228053

Canavese, D., Mannella, L., Regano, L., & Basile, C. (2024). Security at the edge for resource-limited IOT devices. *Sensors*, *24*(2), 590. https://doi.org/10.3390/s24020590

Clark, M. J., & Rajabion, L. (2023). A strategic approach to IOT security by working towards a secure IOT Future. *International Journal of Hyperconnectivity and the Internet of Things*, *7*(1), 1–18. https://doi.org/10.4018/ijhiot.317088

Gazis, A. (2021). What is Iot? the internet of things explained. *Academia Letters*. https://doi.org/10.20935/al1003

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of things is a revolutionary approach for future technology enhancement: A Review. *Journal of Big Data*, *6*(1). https://doi.org/10.1186/s40537-019-0268-2

Leloglu, E. (2017). A review of security concerns in internet of things. *Journal of Computer and Communications*, *05*(01), 121–136. https://doi.org/10.4236/jcc.2017.51010

Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y. Y., Haq, I., Ullah, I., Ouahada, K., & Hamam, H. (2023). Analysis of IOT security challenges and its solutions using artificial intelligence. *Brain Sciences*, *13*(4), 683. https://doi.org/10.3390/brainsci13040683

Sadique, K. M., Rahmani, R., & Johannesson, P. (2018). Towards security on internet of things: Applications and challenges in Technology. *Procedia Computer Science*, *141*, 199–206. https://doi.org/10.1016/j.procs.2018.10.168

Taherdoost, H. (2023). Security and internet of things: Benefits, Challenges, and future perspectives. *Electronics*, *12*(8), 1901. https://doi.org/10.3390/electronics12081901

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IOT privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

Alkunidry, D., Alhuwaysi, S., & Alharbi, R. (2023). Security threads and IOT security. *Journal of Computer and Communications*, *11*(09), 76–83. https://doi.org/10.4236/jcc.2023.119005

Almotairi, A., Atawneh, S., Khashan, O. A., & Khafajah, N. M. (2024). Enhancing intrusion detection in IOT networks using machine learning-based feature selection and Ensemble models. *Systems Science &amp; Control Engineering*, *12*(1). https://doi.org/10.1080/21642583.2024.2321381

Bhardwaj, A., Bharany, S., Abulfaraj, A. W., Osman Ibrahim, A., & Nagmeldin, W. (2024). Fortifying home IOT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for Smart Cities. *Egyptian Informatics Journal*, *25*, 100443. https://doi.org/10.1016/j.eij.2024.100443

Fei, W., Ohno, H., & Sampalli, S. (2023). A systematic review of IOT Security: Research Potential, challenges, and future directions. *ACM Computing Surveys*, *56*(5), 1–40. https://doi.org/10.1145/3625094

Karie, N. M., Sahri, N. M., & Haskell-Dowland, P. (2020). IOT threat detection advances, challenges and future directions. *2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT)*. https://doi.org/10.1109/etseciot50046.2020.00009

Koirala, A., Bista, R., & Ferreira, J. C. (2023). Enhancing IOT device security through network attack data analysis using machine learning algorithms. *Future Internet*, *15*(6), 210. https://doi.org/10.3390/fi15060210

Molina Zarca, A., Bernal Bernabe, J., Farris, I., Khettab, Y., Taleb, T., & Skarmeta, A. (2018). Enhancing IOT security through network softwarization and Virtual Security Appliances. *International Journal of Network Management*, *28*(5). https://doi.org/10.1002/nem.2038

Rana, M., Mamun, Q., & Islam, R. (2023). Enhancing IOT security: An Innovative Key Management System for lightweight block ciphers. *Sensors*, *23*(18), 7678. https://doi.org/10.3390/s23187678