Faculty of Natural and Applied Sciences Journal of Computing and Applications
Print ISSN: 3026-8133
www.fnasjournals.com
Volume 2; Issue 1; September 2024; Page No. 100-104.

Cybersecurity in the Internet of Things: Securing the Connected World

Yakubu, A. L.
Federal Polytechnic Kaltungo

Corresponding author email: lidaniyakubu@gmail.com

Abstract
IoT introduces a new dawn of device interconnectivity, changing the way in which devices communicate and share information with each other. This sort of technological advancement often comes with a significant rise of cybersecurity threats, bringing major problems to the reliability of the IoT bionetwork as a whole. The study's aim is to propose a solution which will help in mitigating the risk of cybersecurity threats in IoT, classifying those types of threats into physical manipulation/malware and data breaches. In other to curve these threats, it is necessary to take a multi-layered security approach, effective management practice, and device-level security. The security measures discussed include authentication and management policy. However, constant challenges of some primary authentication processes such as weak passwords, inadequate secure communications protocols, interoperability issues, and lack of secure data storage have brought the need for this research. Artificial intelligence, blockchain, and cloud computing provide a promising opportunity to reinforce security in IoT. In the quest for a safer IoT future, this study underlines the significance of collective teamwork and partnership. The study also highlights the criticality of more robust security measures in IoT bionetwork. A call to action echoes through the study by urging researchers and stakeholders to come together in other to address those threats by embracing the evolving nature of technological advancement in other to ensure the secure progression of the IoT future. Collaborating together through shared knowledge in other to bring a more secure network as well as to straighten the future of the IoT network foundation for the continuation and the growth of the IoT bio connectivity.

Keywords: Internet of Things, Cybersecurity, Measures, Threats, Security

Introduction

The Internet of Things refers to the network of physical devices such as vehicles, home appliances, as well as other items implanted with sensors and software, by allowing those devices to collect and transmit data with other interrelated devices within the bionetwork. Those devices which are known as smart devices can collect, store and share data with their ilk, by enabling those interoperable devices to interact with each other via certain protocols. IoT is an intricate network of interconnected devices and sensors which facilitate the continuous data exchange between devices. The connection within the bionetwork goes beyond legacy computing devices, by interconnecting a diversified variety of devices such as domestic appliances, industrial mechanisms, hospital equipment and wearable apparatus shares real-time data. The connection of those devices has lead a new era of seamless connectivity among networked devices due to its flexibility. Now a days, more devices both new and legacy are being connected to each other on a daily basis. Now, the benefits of increased collaborations among expert in the field of cybersecurity and IoT is highly needed. Cyber security refers to the act of protecting a computer network and its data from unauthorized access and threats by using certain safety measures and protocols. My idea is to propose the use of collaborative applications which will enhance the security level in the IoT bionetwork so as to protect data from getting accessed or intercepted by an unwarranted user. The Internet of Things has transformed the way we live and work, our daily activities such as routine, routes, schedules and more have been recorded and learned by the IoT devices, the adoption of IoT not only makes our lives more convenient and easy, but it also introduces a significant rate of cyber threats. The IoT network environment is crawling with constant increases in cyber-security threats which seriously requires fast and speedy attention to provide solutions to those threats. The broad nature of the IoT network gives an opening in the surface for malicious actors always searching to exploit the known and unknown vulnerabilities within the system. My aim is to propose a solution which will curve and address the constant security threats within the IoT ecosystem. It is believed that carefully examining the present threats in the network will help scholars in the field

Cite this article as:
Yakubu, A.L. (2024). Cybersecurity in the Internet of Things: Securing the connected world. *FNAS Journal of Computing and Applications, 2*(1), 100-104

understand how to counter them. Through a collaborative effort not only will we ensure data integrity, user confidence will also be restored as well. The proposal in this paper is to use a combination (hybrid) of multiple security applications which will not only strengthen the current IoT foundation but also produce a safe environment where data are more secure and devices can function properly in the absence of frequent safety compromises and threats. This study will also mention various types of cyber-security threats and their functions within the IoT network, it will also address the future direction of where the IoT network & its industry should be heading, by making an informed recommendation in other to fortify the IoT bionetwork against more emerging threats in the future.

Cybersecurity in the area of IoT

Cybersecurity in IoT refers to the aspect of security practice which deals with the safety and integrity of the network and its devices. Starting from the network configuration, protective measures, and data transmission protocols of the network ecosystem. IoT introduces exceptional connectivity between devices and convenience to users but often introduces a number of cyber threats which often require serious attention. This study will propose a suggestive measure to cybersecurity threats within the IoT bionetwork, which each one is conveyed by its unique set of benefits.

Types of IoT Threats

The most concern in IoT ecosystem is the constant compromise of sensitive data, which often lead to data exploitation and vulnerability within the IoT device & network. There are various types of IoT threats which include the following.

1- Data breaches. This refers to the act of stealing sensitive information transmitted through the bionetwork or stored on the IoT devices.
2- Distributed denial of service (DDoS) attack. This is the process of overwhelming the IoT devices with traffic in other to render the data/device unusable.
3- Malware and ransomware. This is the act of infecting the IoT devices with malicious software to compromise or extort data. In 2019, a ransomware attack targeted a healthcare facility's IoT devices, including patient monitor and medical imaging equipment, disrupting services and compromising patient data (Davis, 2019).
4- Man-in-the-middle (MitM) attacks. This is the act of intercepting a transmitting data and altering it between the IoT device and the server.
5- Social engineering. This is the act which include tricking users into revealing sensitive information or gaining access to IoT device physically.
6- Firmware attack. This is the practice of targeting the software that controls IoT devices to gain control or to disrupt operation.

The integrity of the IoT network & devices is of outmost concern, as they are always vulnerable to compromise which will lead to sensitive information compromise. An insecure communication procedures as well as cryptographic weakness within the bionetwork mechanism often exposes the devices and the network to eavesdropping and malware attack. Malicious actors and malwares can easily abuse the network with the aim to render it vulnerable to attack from any angle e.g. intercept or manipulate private information or even inject a virus/botnet to take over the network or its devices in other to cause harm.

IoT Security challenges

A compromised IoT device may pose a critical safety risk to individuals, organizations or the bionetwork infrastructure. For instance, in the aspect of smart hospitals, a little compromise can lead other people's lives to threats e.g. in the hospital ICU or those having a pacemaker attached to their hearts. The vulnerability within the network can basically lead to data breaches personal safety and financial loss. Inadequate data handling can result in unauthorized disclosure of sensitive information (Weber, 2020). Exposure to private information always leads to very high consequences for the owner. Repeated threats always undermine the public interest and trust in IoT technology. The intuitive nature of those IoT threats demands a broad approach to efficient measures. Understanding those types of threats and their depth in the network is the backbone to designing effective countermeasures to drawback the risk and provide safeguard and integrity to the IoT bionetwork.

Countermeasures and practices against IoT threats

As the wide spread of IoT devices continues, it is even more vital to fortify those devices as well as the network from an often evolving threats to safety and security. This study outlines the protective measures in management and operational practice, device-level security, and network-level security. Commencing the booting in a more secure and regulated way by ensuring firmware and updates have time to process and are up-to-date to properly synchronize and address the patches and preventing malware attack. Developing a strong 3 MFA authentication techniques and apparatus e.g. a combination of authentication methods like (OTP, DNA, iris, fingerprint, or voice) recognition

Cite this article as:
Yakubu, A.L. (2024). Cybersecurity in the Internet of Things: Securing the connected world. *FNAS Journal of Computing and Applications, 2*(1), 100-104

biometrics will help curve the data breaches and ensure that only authorized personnel have access to those devices or networks. Data should be encrypted in two different aspect, the first aspect is encrypting data during storage. Storing data either online or offline is always at the risk of compromise, end-to-end encryption protocol should be employed and structured in the network in other to safeguard transmitting data from being intercepted by a third party. Adhering to a more secure database, coding structure during the development phase/manufacturing stage with a regular automated ON THE AIR (OTA) software update, hardware chip embedded in it to identify and patch vulnerability should help create a resilient IoT software package. Dividing the network into segments with additional access control measures can help to minimize malicious attacks. Liang et al., (2020) suggest the implementation of a fine-grained network segmentation to isolate IoT devices from other network resources. Embedding an AI intrusion detection system in the IoT bionetwork to help identify and thwart malicious activities to improve the general system. Constant monitoring of the IoT bionetwork combined with anomaly detection apparatus will enable the tracking and identification of suspicious activity in the early stage of an attack.

Management and operational practices

The first stage of security is during the software development and manufacturing stage. Enlightening the end users and the developers about the paramount of best security practices by reducing the likelihood of unintentional vulnerability in the system by granting users access to only where they can perform their duties effectively. Implementation of risk assessment and efficient system vulnerability management protocols enables organizations to identify potential security weakness in the systems. Implementing comprehensive system breach & responds/recovery protocols to ensure a swift and effective response to security incident which can minimize potential damage. Employing easily adaptive security measures through the entire IoT network and in the devices to prevent network breaches and provide data integrity. A well designed security protocol is mandated after a device has been decommissioned so that it will not be re-commissioned by a malicious party and put back into service again. Adhering to a more established regulatory framework and industrial-grade apparatus will help provide a well-structured protective approach to safeguarding the IoT bionetwork.

The future direction of cybersecurity in IoT

The future of IoT has been gazing towards a particular direction, where in combination both the network and data are secure from threats. The Internet of Things is designed to facilitate the connectivity of a large number of devices within a network over a long distance, IoT security is often marked by constant challenges & threats which is often mitigated by technological advancement in certain areas. The safe haven for IoT and its devices where certain protocols and advanced mechanisms are to be employed in other to secure the ecosystem from attacks and threats are as follows.

Blockchain

Exploring blockchain technology as a means to enhance IoT security. The decentralised nature of blockchain leverages the ledger in other to ensure data integrity and secure communication between IoT-interrelated devices. Blockchain technology has permitted the use of smart biometric authentication methods to ensure network integrity. Blockchain also enables programmed transactions amongst IoT devices which in turn facilitate machine-to-machine (M2M) communication. It also facilitates interoperability between IoT devices in other to support cybersecurity mechanisms across multiple sectors such as health care, finance and government sectors. The main point is how to enhance the IoT system security architecture to protect external manipulation activities which can be solved through effective network security and collaboration, inherent to blockchain security architecture because of its scalability and encrypted nature which contribute to the privacy and security of the IoT ecosystem via the large amount of data generated from a variety of sensor and devices, furthermore the IoT ecosystem security can be enhanced with the introduction of blockchain technology into its mechanism, the blockchain provides an added advantage because of its resistance to manipulation, when a transmission has been made it can never be altered. Also, blockchain technology can be used in parallel with cloud computing. So, by leveraging the features of blockchain technology, IoT devices can ensure secure, reliable, and efficient operation and protection against various cyber threats and vulnerabilities.

Cloud computing

Cloud computing is very collaborative with blockhain technology, particularly in the aspect of averting cyber-attack e.g. internet of things firmware, and wireless protocols. The interconnection of interrelated intelligent devices and the constant use of public network makes the devices vulnerable to malicious attacks, and this is a major concern in IoT security, such as smart health, smart city, energy management etc. Cloud computing provides several security features including access control, data encryption, DDoS protection, scalability and data backup/recovery, threat detection and

response. Cloud computing security provides a robust and proactive approach to protecting data and cloud-based applications. There is an utmost need for a system that can identify and counter potential threats in the IoT ecosystem. Cloud computing also introduces certain advantages somehow similar to that of blockchain which makes them collaborative in nature. Other features such as real-time processing and machine learning abilities in cloud computing enable the AI and ML algorithm to analyze data from the devices in other to discover knowledge and predict future attack. Taking cloud computing, blockchain and merging its features with that of IoT can help unlock the full potential of the network and its devices, driving innovation, preventing false positive outcomes, and transforming lives.

Artificial Intelligence

The field of artificial intelligence provides an endless possibility for learning and advancement, particularly in the area of machine learning. Amouri et al. (2021) proposed the use of an algorithm that learns normal behaviour and identifies deviation, where a machine can be trained using a related set of supervised or unsupervised data fed into the machine in other to predict or discover certain patterns or knowledge which is called knowledge discovery through data (KDD). It gives IoT and those 'things' a cerebrum to think which is called embedded intelligence by a few researchers (Guo et al., 2013). The application of AI can be used to discover glitches, bugs, vulnerabilities and the frequency of malicious attacks by feeding the machine with relevant data that was previously recorded using SIEM. The benefits of AI particularly in threat detection & machine learning algorithms excel in many forms, the incorporation of AI & IoT brings numerous benefits which comprise enhanced automation, predictive maintenance, increased scalability and decision making. By incorporating blockchain, fog computing, and AI technologies with IoT, we aim to create a more proficient, automated, and secure IoT network and devices which will transform industries as well as improve our daily lives and secure our apparatus from cyber-attacks. Kaplan., (2016) stated that the growing interest in the study and development of AI are pushing the product vendor to introduce AI into almost every strategy they make.

Recommendation for IoT cybersecurity

Secure communication protocol.

Based on my understanding, using a hypertext transfer protocol system (HTTPS), Transport layer security (TLS) can enhance security to protect data in transit. HTTPS is basically the extension of HTTP which adds an extra layer of security by encrypting the data transmission exchange between a website and its user which ensures that data remains intact and secure during transmission. Https uses secure socket layer/transmission layer security SSL/TLS protocols to provide secure communication among web browser and web servers which most IoT devices support that. HTTPS also use encryption algorithms like Advance encryption standard (AES) to protect data. More on that HTTPS also uses Digital signatures to verify authenticity. TLS uses the cryptographic protocol to provide secure communication between devices and network, typically between client and server which is used to authenticate client involvement and ensure data integrity during the exchange, TLS uses two main protocols which are Handshake protocol to establish a secure connection, and Record protocol to encrypt and decrypt data exchange. I believe by employing this protocol to IoT bionetwork we can ensure a secure web browser and server.

Security Information and Event Management system (SIEM).

Building on my own research, this particular system is developed in other to analyze and monitor security-related incidents from different sources in other to protect data and provide reasonable improvement to data security and incident response. This feature combines data collected from various sources such as the Logs, network, and endpoints, to monitor and prevent unauthorized access. SIEM also used analytics in the context of machine learning to analyze security-related data flow and proper management of the related data. SEIM is essential to organization to monitor and analyze security-related data in real-time, to respond quickly and effectively to secure incidents and to improve overall security response. Adopting SIEM and using its advantages based on how it mine data from various sources can help improve the IoT network threat response time improve security.

Standardization and Interoperability

I also came to understand by manufacturing a top tier apparatus with cutting edge security features, and ensuring interoperability among those devices can significantly enhance all the security infrastructure of the IoT ecosystem. Inter-operability is the foremost definition of IoT, making sure that those devices are completely synchronized not just in connection but in security features as well.

Implementing dynamic security policies

In my own understanding, adopting specific policies with respect to how those devices and network are to be operated for many years to come, such as policies which can also evolve with the constant challenges of cyber-security threats

Cite this article as:
Yakubu, A.L. (2024). Cybersecurity in the Internet of Things: Securing the connected world. *FNAS Journal of Computing and Applications, 2*(1), 100-104

in IoT is crucial. This policy includes automated software patches, as well as a preemptive intelligence threats prevention and assessment team. A team which will be responsible for regular assessment and evaluation of past security threats encounter in other to mitigate or curve any future threats. With the constant evolving threats to IoT security. A regular MFA biometric update can help provide a more secure access control to IoT networks and devices. Implementing those policies will help guide user on how to properly secure their devices and network from threats.

Cross collaboration

My aim is to encourage partnership amongst IoT developers, cybersecurity experts, and academic researcher during the development and implementation phase. This will help bring a methodical approach and solution to IoT insecurity. Security mechanisms can only be achieved through research collaboration and merging technology, methods and techniques into one single entity. Integrating the system with a more diverse protective mechanism like DNA or behavioral biometric or OTP authentication can lead to the implementation of more reliable and robust protective measures. Navigating the highly complex structure of IoT security threats can help in understanding & addressing those challenges, and by also embracing emerging technology like the aforementioned techniques which are promising to ensure the continued growth of cybersecurity in IoT.

Conclusion

The foundation of the IoT bionetwork represents a vast chance for innovation and improvement but the network is always hunted with a large number of security threats that require vigilant action. This study identified the most common types of threats within the IoT bionetwork and the ways to mitigate those threats. Each of the aforementioned proposed protective measures is designed to fortify the system from breaches, as well as the continuous challenges that often cast shadows on its integrity. Data breaches, privacy infringement and the looming threats of botnet, DDoS and malware attacks will be curved to their minimum. The repercussions from these threats which involve safety risk and financial loss highlight the vitality of robust security measures. Security boot process, encryption protocol and other management practices are fundamental to forming resilient protection from all sorts of evolving IoT threats. It has become evident that safeguarding individual business and entire community is of vital importance. IoT security is not simply a technological concern but also a collective responsibility. As we witness the widespread influence of IoT apparatus, it is now important to continue to develop and implement positive measures in other to secure the IoT network and its devices. Curving security threats, particularly in the area of IoT often requires collective knowledge and academic research from multiple perspectives. Securing the IoT bionetwork requires a collective responsibility born purely from the needs to enhance security in IoT. On this aspect sharing insight and resources is the best way to start. Collectively we can curve the threats to insecurity in IoT, assuring that the device and its security mechanism are fully sustainable and safe to use. As we are at the dawn of IoT growth, it is imperative to ensure the scrutiny and the safety of our IoT ecosystem to enable us to a smooth and smart operations.

References

Amouri, A., Hamouda, D., & Derhab, A. (2021). Anomaly-based intrusion detection for IoT networks through fog computing: A deep learning approach. *Journal of Information Security and Applications, 58,* 102804. https://doi.org/10.1016/j.jisa.2020.102804

Davis, J. (2019). Ransomware attack on Alabama hospital forces emergency room closure. Health IT Security. Retrieved from https://healthitsecurity.com

Guo, B., Zhang, D., & Yu, Z. (2013). From the Internet of Things to embedded intelligence. *World Wide Web, 16*(4), 399–420.

Kaplan, J. (2016). *Artificial intelligence: What everyone needs to know*. Oxford University Press.

Liang, X., Shetty, S., Tosh, D., & Kamhoua, C. (2020). ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. *Future Generation Computer Systems, 78,* 1125-1137. https://doi.org/10.1016/j.future.2016.11.031

Weber, R. H. (2020). Internet of Things: Privacy issues revisited. *Computer Law & Security Review, 31*(5), 618-627. https://doi.org/10.1016/j.clsr.2015.07.002

Cite this article as:
Yakubu, A.L. (2024). Cybersecurity in the Internet of Things: Securing the connected world. *FNAS Journal of Computing and Applications, 2*(1), 100-104