IOT security framework for IOT healthcare devices

Gan Zhen Wen, Nicholas
School of Computing
Asia Pacific University of Technology & Innovation (APU)
Kuala Lumpur, Malaysia
TP059739@mail.apu.edu.my

Chandra Reka Ramachandran
School of Computing
Asia Pacific University of Technology & Innovation (APU)
Kuala Lumpur, Malaysia
Chandra.reka@staffmail.apu.edu.my

Dr. Vinesha Selvarajah
School of Computing
Asia Pacific University of Technology & Innovation (APU)
Kuala Lumpur, Malaysia
vinesha@apu.edu.my

***Abstract*—Over the years, advancement of technology has led to an increase in research and development of IoT devices. The healthcare sector is one of the most affected by IoT devices. IoT healthcare devices presents a new option to treat patients. IoT healthcare devices range from pacemakers to remote patient monitoring and wearable devices. However, IoT devices are connected to the Internet. This means that IoT devices may be in risk of cyber-attacks that can steal sensitive patient data and medical records. In this paper, potential technologies and techniques that can improve the overall security posture of IoT devices will be reviewed. Previous security frameworks by past researchers will also be highlighted for their effectiveness in improving IoT security.**

Keywords—IoT, framework, security, blockchain, machine learning, healthcare

I. INTRODUCTION

In the recent years, advancement of technology has led to an increase in research and development of IoT devices [1-8]. This is especially true for the healthcare sector. IoT healthcare devices such as remote patient monitoring and wearable healthcare devices has improved healthcare quality by remote monitoring [9]. However, as IoT devices are connected to the Internet, these devices will be exposed to cyber-attacks. Sensitive patient data and medical records may be stolen because of such attacks. Therefore, it is critical and important that the IoT healthcare devices are protected with sufficient security mechanisms and early detection methods to prevent cyber-attacks. This paper will highlight on the potential technologies and techniques that may improve the security of IoT healthcare devices. It will also include security frameworks proposed by past researchers and highlight their effectiveness.

II. ATTACKS ON IOT

According to Tabassum and Lebda in [10], there are three layers of IoT architecture that are commonly targeted for cyber-attacks. This includes Perception Layer, Transport Layer and Network Layer. The perception layer consists of the physical sensors and actuators of the IoT devices. The research stated that jammingis a common attack in this layer. Jamming involves in using high radio frequency signals to jam the communication of the IoT device. This enables the cybercriminals to disable the Intrusion Detection System (IDS) of the device.

The transport layer controls the end-to-end links of IoT devices. Commons attacks are the remote-control attack and man in the middle attack (MITM). Remote control attacks intercept the communication between devices using botnets or MITM attacks to gain control of the device. This can lead to full disruption of the device and lost of control. Man in the middle attack involves in the cybercriminal intercepting, tampering and deleting information in the data communication channel. This may lead to denial of service and injection attacks as information is altered to make the device more vulnerable and more easily exploited by the cybercriminal.

The network layer involves in the usage of technologies such as Radio Frequency Identification (RFID) and WiFi. Common attacks are eavesdropping and denial of service attacks. Eavesdropping involves in the cybercriminal listening in and altering the data. Denial of service attacks floods the network of the device with requests to crash its service, rendering the device unusable for a time duration.

III. BLOCKCHAIN IN IOT

According to Minoli and Occhiogrosso in [1], blockchain is a linked list of blocks created by nodes and are cryptographically secured. Each block contains a header, a payload (protected transaction data) and security metadata. Blockchains are basically a distributed database that stores a list of records while prevents tampering of the records concurrently. It provides global accessibility, integrity and ability to save and transfer stored data in a secure manner.

In a study carried out by Minoli and Occhiogrosso in [1], they found that IoT devices are vulnerable in the face of cyber-attacks. This requires end-to-end security to reduce the risk of such attacks and the loss of sensitive data stored in IoT device. The study shows how blockchain can be applied to the IoT devices as layered security mechanisms. They provided detailed description and application of each layer: End-to-end layer, Analytics/Storage-level, Gateway-level, Fog Networking layer, Site-level layer and Device-level layer. The researchers conclude that blockchain can be used to secure the integrity of data being transferred over the network in an IoT device.

In addition, Rathee et al in [11] had established that the management of huge amount of data in IoT healthcare leads to increase of human efforts and potential security risks. The researchers proposed a security framework that uses blockchain technology for IoT healthcare systems. The framework uses blockchain to establish a secure multimedia communication system for data transfer. This provides secrecy and transparency among the users. The study emphasizes that blockchain in healthcare is required to

intermediates activity, patient records and medicine information from provider to customer and any illegal activity in the communication process that are conducted can be traced easily.

Dwivedi et al in [9] found that IoT wearable technology such as remote patient monitoring devices poses grave privacy risks and security concerns, especially on data transfer and logging of data transactions. The researchers proposed a security framework using modified blockchain models for IoT devices. The framework contains five parts: Cloud storage, Overlay network, Healthcare providers, Smart Contracts and Patient Equipped with healthcare wearable IoT devices. In addition, a combination of symmetric and asymmetric encryption algorithm (ARX, Diffie-Hellman Key Exchange, Ring Signature) were applied to increase the security of the system. The study concluded that the model provides a solution to security issues in an IoT device while considering the resource limited factors of IoT devices.

Moreover, Srivastava, Crichigno and Dhar in [12] researched that IoT healthcare devices tend to have issues in secure and efficient transmission of medical data. The proposed model was an integration of blockchain technology in IoT healthcare systems. Similarly to the previous study, the provided system uses a combination of blockchain models and encryption algorithms to provide a secure data transmission system for IoT health care devices.

Mistry et al in [13] highlighted that IoT in the industrial sector faces major security and privacy preservation concerns. The study provided an overview of the usage of blockchain in 5G enabled IoT in several sectors such as smart homes, smart cities, healthcare, industry 4.0, supply chain, agriculture, autonomous vehicle, unmanned aerial vehicle, multimedia and digital rights management. The researchers provide an in-depth look into the issues and challenges in implementing blockchain in 5G-enabled IoT devices. The study concluded that several issues and challenges must be addressed for blockchain to be successfully implemented in 5G-enabled devices.

In summary, blockchain technology is becoming increasingly popular as the go-to option for providing secure data transmission and storage. This is especially important in IoT healthcare devices as the data it stores and transmit are sensitive data.

IV. MACHINE LEARNING IN IOT

According to Al-Garadi et al in [14], the goal of machine learning is to improve accuracy and performance in completing a task through the learning from experience and by training. By training the machine, it helps in improving its accuracy when completing its tasks. Machine learning algorithms can be classified into three categories: Supervised learning, Unsupervised learning and Reinforcement learning.

Supervised learning uses training datasets to train on the classification and prediction model. It provides the example input and output. It uses the example as a basis on predicting and classifying new data [14].

Unsupervised learning uses unlabeled data in its training process. It provides the input but not the output for training. It is to train how the machine categorize input data into distinct feature groups by categorizing their similarities [14].

Reinforcement learning is essentially a trial-and-error learning method. The training involves in giving an indication if the selected action is right or wrong and it learns from its mistakes [14].

Pirbhulal et al in [15] highlighted that patient data is important and critical, therefore it is paramount that secure transmission is prioritized in the smart healthcare sector. The study proposed a framework that uses machine learning based biometric security by extracting electrocardiogram (ECG) for training phase. The framework involves in several phases including: QRS-Detection Process, Feature Extraction, Feature concatenation, Polynomial Approximation, Unique Biometric Entity Identifier, Machine Learning Training and User Authentication phase. The researchers concluded that the proposed framework solves resource efficiency issues and provides an efficient and secure user authentication for smart IoT devices.

In a study carried out by Punithavathi et al in [16], it is found that IoT applications presents a big challenge in terms of securing data transmission and its network. Similarly to the previous study, they proposed a cloud-based lightweight cancelable biometrics authentication system for IoT devices. The cancelable biometric system features several stages such as Biometric Input, Feature Extraction, Feature Transformation and Machine Learning Training. The study results show that the accuracy of the biometrics system is accurate by measuring the equal error rate and time complexity. The researchers concluded that the system successfully produces accurate and secure results for IoT applications.

Al-Garadi et al in [14] has established that the implementation of security measures for IoT devices are ineffective, therefore, improvements must be made for the IoT devices to be secure and reliable. The study shows an in-depth survey of machine learning techniques and deep learning techniques that may potentially be used to improve the overall security of the IoT systems. The researchers also highlight on the issues and challenges faced when implementing machine learning and deep learning techniques for IoT security. The study provides a guide to enhance the security of IoT systems by using machine learning and deep learning techniques.

Xiao et al in [17] found that IoT devices that integrate a variety of devices into its networks may be exposed to potential cyber threats such as spoofing and eavesdropping attacks. The study provides an overview of the machine learning based IoT security techniques. This includes machine learning based authentication and machine learning based access control and IoT malware detection. The researchers identified the issues and requirements of IoT devices to implement machine learning techniques to improve the IoT devices overall security posture.

In summary, machine learning algorithms provides a potential solution for IoT devices to detect and prevent cyber threats as well as improve the device's overall security posture. This is especially important in IoT healthcare devices as they contain sensitive data.

V. PREVIOUS FRAMEWORKS FOR IOT

Security frameworks presents a guideline to improve the security of a system. There are several security frameworks

proposed by past researchers on improving the overall security of IoT devices.

Tabassum and Lebda in [10] discovered that the increasing number of smart IoT devices and the complexity of the networks involved in IoT devices made it difficult to safely secure data during communication between the devices. The study showed that modern conventional security controls proved insufficient to prevent the ever-changing types of cyber attacks against IoT devices. The researchers proposed a security framework for IoT devices as well as a list of security enhancement techniques. The framework includes an Intrusion Detection System, Machine Learning Monitoring and Classification, Secure Authorization, Authentication and Access Control and Encryption Algorithms. The researchers concluded that the implementation proved efficient and recommends placing IDS at every application layers of IoT architecture for better threat detection.

According to Pirbhulal et al in [18], IoT healthcare systems faces massive resource constraints. This causes implementation of security and privacy controls a big challenge and a major concern. The study proposed a biometric-based security framework for IoT healthcare systems. It uses a physiologically based key generation mechanism and an efficient resource optimization model to manage resources used accordingly.

In a study carried out by Badr, Gomaa and Abd-Elrahman in [19], it is found that blockchain is becoming a popular security option for replacing outsourced trusting solutions in the IoT healthcare sector. The researchers proposed a security framework that uses blockchain on the healthcare communication entities in an e-health platform. The proposed consists of multiple tiers: Tier 1: Constrained and Unconstrained nodes (devices-sensors) and Patient (Gateway-Aggregator), Tier 2: N Authorities (Hospitals, Medical facilities), Tier 3: The EHRs cloud providers (Could Storage Servers for EHRs Records).

Rathee et al in [20] found that accessing network services in fog computing gave rise to the increase risk of cyber-attacks in the fog layer. The researchers proposed a secure routed handoff mechanism to avoid threats by applying trust value and rating of each IoT and fog devices based on their communication behavior. It revolves around having a trust manager established between the IoT layer and fog layer that records all nodes in its table and detects malicious nodes. The researchers concluded that the framework proved accurate with up to 85% accuracy of detection of malicious behavior.

According to Zhang et al in [21], data confidentiality and integrity are critical importance for IoT devices as they carry private and sensitive data. When IoT devices are connected to the Internet, they may be exposed to potential cyber-attacks. The study proposed a physical layer-based security framework for IoT devices on using authentication and key generation. The framework involves in using Radio Frequency Fingerprinting Identification and key generation for authenticity. The researchers conclude that the low complexity of the techniques is suitable for the resource limited IoT devices.

Elhoseny et al in [22] established that the advancement of IoT in the medical sector poses a big challenge for its medical data in terms of security and integrity. The study proposed a hybrid security framework for securing the diagnostics contents of data in medical images. The framework involves in four continuous processes: Hybrid Encryption (RSA, AES), Data Concealment (2D-DWT-1L, 2D-DWT-2L), Extraction of Embedded Data and Decryption of Extracted Data. The researchers concluded that the implementation of framework successfully hides the patient data into a transmitted cover image.

In summary, past frameworks provide an in-depth overview on how various technology can be integrated into IoT devices to improve the overall security posture. This is especially important when reviewing and selecting technologies to integrate into IoT devices.

VI. CONCLUSION

In conclusion, IoT devices in healthcare faces many challenges in terms of implementing effective security and privacy controls. Several studies show that blockchain presents a good option for securing integrity of the data during transmission and storage. Researchers also agreed that machine learning algorithms provides a way to improve threat detection to prevent potentially harmful cyber-attacks against the IoT devices. Several proposed security frameworks by past researchers also may potentially improve the IoT devices security posture. However, there is a lack of combination of framework that includes blockchain, machine learning detection and advanced encryption methods that may potentially improve security of the IoT device. This may be due to the resource-constraint factors of IoT devices.

REFERENCES

[1] W. M. Rasheed, R. Abdulla, L. Y. San., "Manhole cover monitoring system over IOT" *Journal of Applied Technology and Innovation*, vol. 5, no. 3, pp. 1-6, 2021.

[2] H. Singh, R. Abdulla, S. K. Selvaperumal., "Carbon Monoxide Detection Based IoT" *Journal of Applied Technology and Innovation*, vol. 5, no. 3, pp. 7-12, 2021.

[3] Tj. V. Moussa, C. Nataraj, A. Seeralan., "IoT based smart irrigation system" *Journal of Applied Technology and Innovation*, vol. 5, no. 3, pp. 48-54, 2021.

[4] T. Eldemerdash, et al., "IoT Based Smart Helmet for Mining Industry Application," *International Journal of Advanced Science and Technology*, vol. 29, no. 1, pp. 373-387, 2020.

[5] R. Lakshmanan, et al., "Automated smart hydroponics system using internet of things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6389-6398, 2020.

[6] F. S. Hon, R. Abdulla, S. K. Selvaperumal., "Wheel Chair-Person Fall Detection with Internet of Things," *Solid State Technology 63.1s* (2020): 911-922, 2020.

[7] A. M. Samson, R. Dhakshyani, R. Abdulla., "IOT Based Sustainable Wallet Tracking System," *International Journal of Advanced Science and Technology*, 29(1), pp. 1301 – 1310, 2020.

[8] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," Internet of Things, vol. 1, pp. 1–13, 2018.

[9] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," Sensors, vol. 19, no. 2, p. 326, 2019.

[10] A. Tabassum and W. Lebda, "Security Framework for IoT Devices against Cyber-attacks," arXiv preprint arXiv:1912.01712, 2019.

[11] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," Multimedia Tools and Applications, pp. 1–23, 2019.

[12] G. Srivastava, J. Crichigno, and S. Dhar, "A light and secure healthcare blockchain for iot medical devices," 2019, pp. 1–5.

[13] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," Mechanical Systems and Signal Processing, vol. 135, p. 106382, 2020.

[14] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," IEEE Communications Surveys & Tutorials, 2020.

[15] S. Pirbhulal, N. Pombo, V. Felizardo, N. Garcia, A. H. Sodhro, and S. C. Mukhopadhyay, "Towards Machine Learning Enabled Security Framework for IoT-based Healthcare," 2019, pp. 1–6.

[16] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K.-K. R. Choo, "A lightweight machine learning-based authentication framework for smart IoT devices," Information Sciences, vol. 484, pp. 255–268, 2019.

[17] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?," IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, 2018.

[18] S. Pirbhulal, O. W. Samuel, W. Wu, A. K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," Future Generation Computer Systems, vol. 95, pp. 382–391, 2019.

[19] S. Badr, I. Gomaa, and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT-EHRs systems," Procedia Computer Science, vol. 141, pp. 159–166, 2018.

[20] G. Rathee, R. Sandhu, H. Saini, M. Sivaram, and V. Dhasarathan, "A trust computed framework for IoT devices and fog computing environment," Wireless Networks, vol. 26, no. 4, pp. 2339–2351, 2020.

[21] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," IEEE Wireless Communications, vol. 26, no. 5, pp. 92–98, 2019.

[22] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," Ieee Access, vol. 6, pp. 20596–20608, 2018.