THE NEXTGEN CYBERSECURITY FOR U.S. AIRPORTS

GAMEABOVE
EASTERN MICHIGAN UNIVERSITY

Mosladdin Mohammad Shueb | mshueb@emich.edu | Ph.D. Student
Dr. Chuyang Yang & Dr. Xiangdong Che | Advisors
GameAbove College of Engineering and Technology, Eastern Michigan University, Ypsilanti, MI

Abstract

The integration of connected systems and optimization widen the attack surface for airport cyber-physical systems and could severely impact airport operations (Ukwandu et al., 2022). The purpose of this study was two folded. First, we identified the insufficiency of existing airport cybersecurity in relation to integrating emerging technologies with airport IT infrastructure. Second, we applied elements of blockchain to enhance the security and resiliency of airport IT systems by eliminating single points of failure, the impact of data breaches and ransomware, and unauthorized access. The proposed blockchain-powered cybersecurity ensures the security of IT assets while allowing smooth access to stakeholders such as travelers, vendors, airlines, and employees. In addition, the successful implementation of blockchain as a cybersecurity countermeasure would align airport cybersecurity initiatives with the requirements of TSA.

Background

- Day-to-day airport operation integrates advanced technologies and devices to achieve optimum performance, offer different services, and better management of IT infrastructure. The advancement of airport IT systems widens the cyber attack surface (Ukwandu et al., 2022).
- Cybersecurity incidents are on the rise. The average cost of a security breach is 7.35 million (Price et al., 2022).
- The existing airport information systems require more robust and resilient cybersecurity solutions to secure hardware-software, databases, wireless communication, Internet of Things (IoT), and open-source applications (Transportation Security Administration, 2023).
- The existing cybersecurity solutions are insufficient to protect against common attacks such as phishing, eavesdropping, Denial-of-Service (DoS), Man-in-the-middle (MITM), ransomware, and network.
- Other industries such as healthcare, automotive, and finance have already implemented blockchain to secure information systems (Nelaturu et al., 2022; BMW, n.d.).
- Elements of blockchain create a robust and resilient IT system by creating trust in a trustless environment and eliminating the negative impact of cybersecurity incidents (Ossamah, 2020).

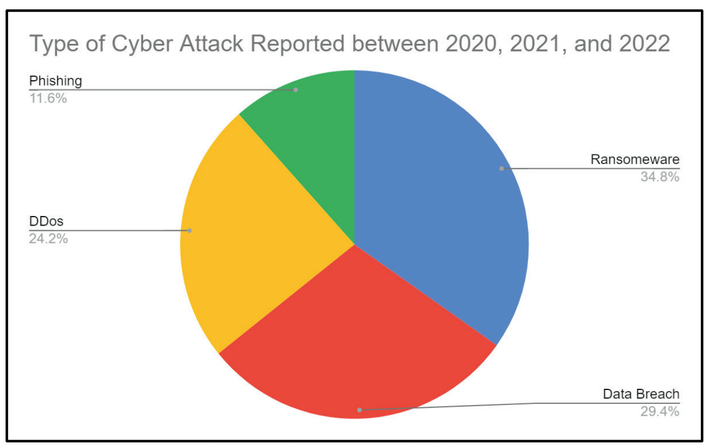

Figure 1: Reported Cyber Attack (Note: Inspired by XTI, 2022)

Research Questions

RQ1: Does the implementation of blockchain as a cybersecurity measure overcome the limitation of existing cybersecurity solutions and vulnerabilities of the airport?
RQ2: Do elements of blockchain support the integration of emerging technologies and devices at the airport?
RQ3: Will elements of blockchain create robust and resilient IT systems for airports?

Preliminary Findings

- Consensus between connected nodes verifies and validates the data in a block. Also, consensus can be used to authenticate users and their devices. Thus, a consensus mechanism could overcome the limitation of the traditional approach and prevent authorization misuse more efficiently (Ossamah, 2020).
- In a traditional network, all transactions are verified through a single node based on preset rules. In contrast, blockchain creates a Peer to Peer (P2P) decentralized network that verify all the transactions (data). Hence, a single compromised node cannot compromise the entire network. In a DoS attack, a single node containing blockchain can rebuild the entire network (Ossamah, 2020).

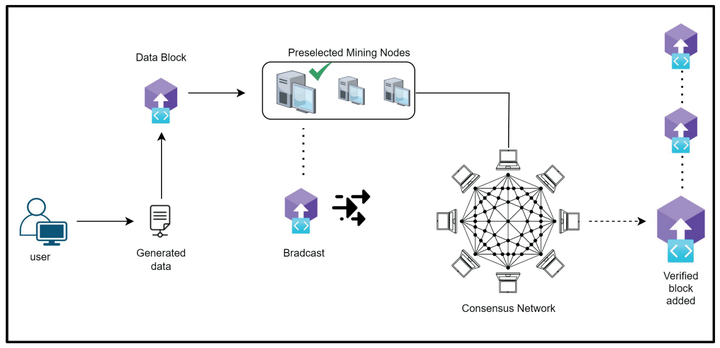

Figure 2: Consensus Algorithm to Validate Blocks.

- Blockchain uses a unique data structure with a header, block ID, and body. These blocks containing data connect to the existing blocks using a cryptographic link generated by SHA 256 hash functions. The transactions cannot be altered or deleted when recorded in a block (Ossamah, 2020). In addition, the data will be stored in multiple locations. Unlike a database where the data is stored in one location, the data within the blockchain is scattered within each node that is connected to the blockchain (Hyperledger Foundation, 2020). Hence, blockchain can protect sensitive information in a ransomware attack (49 CFR Part 1520, n.d.).

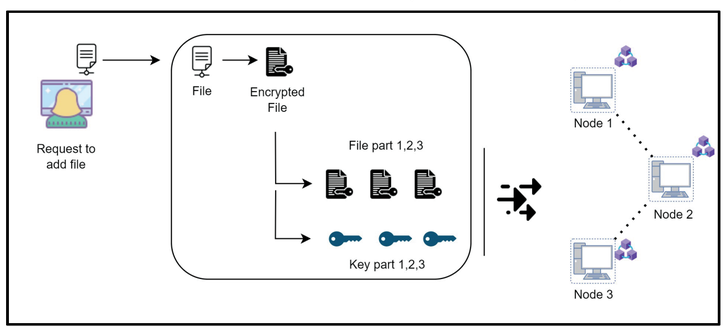

Figure 3: Data Storage System (Note: Inspired by Hyperledger Foundation, 2020).

Methodology

- Literature review and industry interaction included rising cybersecurity concerns at the airport, the need for robust and resilient solutions, securing information systems using blockchain, regulations, and attitude towards blockchain as a cybersecurity solution.
- An experimental research methodology will be used to determine the enhancement of airport cybersecurity with a pre-test and post-test control group.
- Data from the simulation of different attack scenarios will be collected before and after the implementation of the proposed blockchain-based cybersecurity solution.

Conclusion & Recommendations

- Advancement in information technology has changed cybersecurity requirements immensely over the last decades.
- The current landscape of U.S. Airport IT systems for a robust and resilient cybersecurity mechanism.
- Elements of blockchain can be integrated and utilized to eliminate the risks of a data breach, unauthorized access, and network failure at U.S. airports.
- The proposed solution provides high autonomy and resiliency by ensuring the airport IT operation's confidentiality, integrity, and availability.
- The findings of this study can be used to educate high-ranking airport personnel on the potential effectiveness of blockchain as a cybersecurity measure.
- Future research should explore the integration of blockchain considering evolving nature of technologies.

References

49 CFR Part 1520. (n.d.). 49 CFR Part 1520—Protection of Sensitive Security Information. Retrieved May 11, 2023, from https://www.ecfr.gov/current/title-49/subtitleB/chapter-XII/subchapter-B/part-1520

How blockchain is changing mobility | BMW.com. Retrieved April 28, 2023, from https://www.bmw.com/en/innovation/blockchain-automotive.html

Hyperledger Foundation (Director). (2020, March 9). Decentralizing Access Controls through Blockchain—Nitesh Emmadi, TCS. https://www.youtube.com/watch?v=l063PK70SOA

Nelaturu, K., Du, H., & Le, D.-P. (2022). A Review of Blockchain in Fintech: Taxonomy, Challenges, and Future Directions. Cryptography, 6(2), Article 2. https://doi.org/10.3390/cryptography6020018

Ossamah, A. (2020). Blockchain as a solution to Drone Cybersecurity. 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 1–9. https://doi.org/10.1109/WFIoT48130.2020.9221466

Price, J., C.M., & Forrest, J. (2022). 22 CM Module1_WEB.pdf. American Association of Airport Executives. https://aaae.org/AAAEMember2020/AAAEMember2020/Training-and-Certification-/CM_Program.aspx

Transportation Security Administration. (2023). TSA issues new cybersecurity requirements for airport and aircraft operators | Transportation Security Administration [Press Release]. https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-newcybersecurity-requirements-airport-and-aircraft

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. Information, 13(3), Article 3. https://doi.org/10.3390/info13030146

XTI, Socr. (2022, September 27). Top Cyber Threats Faced by the Aviation Industry—SOCRadar. SOCRadar® Cyber Intelligence Inc. https://socradar.io/top-cyber-threatsfaced-by-the-aviation-industry/