Blockchain Technology for the Security of Internet of Things: Challenges, Solutions, and Future Trends

By Mohammed Uzair Khan

***Abstract*— The Internet of Things (IoT) is a rapidly growing area of technology that has brought with it a range of security challenges. These challenges include device vulnerabilities, data breaches, and privacy concerns, among others. This report contains an assessment of current literature on how blockchains are used to tackle IoT challenges. It also contains a critical analysis on the challenges faced by IoT security and how blockchain technology can be leveraged to address these challenges. Additionally, it also reviews existing blockchain-based solutions for IoT security and evaluates their effectiveness. Finally, emerging trends in blockchain for IoT security are discussed.**

Keywords*— *Blockchain, Internet of Things, Security, Privacy, Data Breaches

I. Introduction

The Internet of Things (IoT) has come about as a transformative technology that has completely changed the way we interact with our devices and the world. With a wide range of applications, including healthcare, transportation, manufacturing, and home automation, among others, IoT devices have become increasingly pervasive [1][2]. IoT devices have many benefits, however they also come with a range of security challenges. Some of these challenges are device vulnerabilities, data breaches, and privacy concerns, and more. These challenges are further complicated by the fact that many IoT devices are often unsecured, have limited processing power, and lack the ability to be updated regularly. Recently, blockchain technology has been used to address some of the security challenges faced in IoT. This report provides a critical assessment of the current literature on how blockchain is used for IoT security. It also contains an analysis of the challenges faced in IoT security and examines how blockchain technology can address these challenges. Additionally, it also reviews existing blockchain-based solutions for IoT security and evaluates their effectiveness. Finally, emerging trends in blockchain for IoT security are discussed.

II. Challenges in IoT Security

With the increased adoption of IoT devices across many fields, there is also an increase in the number of malicious actors trying to gain access to and manipulate the data collected. As more devices are connected to a network, the attack surface also increases. This correlation is why without robust security measure in place, IoT devices run the risk of leaking sensitive data or becoming an access point to a private network. Some of the reasons why IoT devices pose a large threat to their connected network are discussed in [3]. These devices are built with only the necessary computational power to complete their task. As a result, they often do not have the necessary computational resources to implement the best security measures to ensure data protection[4]. Another issue is that these devices often use a variety of transmission technologies. This makes it difficult to standardise communication, therefore increasing the number of security precautions needed to affect all the different technologies. A gap in communication monitoring can be remotely exploited and monitored [5]. This problem is further exacerbated by the lack of computational resources as stated earlier. In addition, many of the basic components that make up an IoT device are left with untreated vulnerabilities. This could affect many millions of already deployed devices [27]. This issue is further exacerbated by the fact that these devices are difficult to update and don't receive regular updates, therefore leaving them vulnerable for a long time between updates. Lastly, many users are unaware of security issues that could affect them due to their adoption of IoT devices. This leads to them not taking the necessary steps to protect themselves and leaving them exposed to vulnerabilities.

Although legislation cannot guarantee the secure use of IoT data, it can mitigate some of the damage caused by data misuse. Currently, there is no standardized legislation or secure data policy in place to address these concerns. Despite this, various countries have made efforts to safeguard user data, such as the General Data Protection Regulation (GDPR) [6] and the Health Insurance Portability and Accountability Act (HIPAA) [7]. IoT device manufacturers and app developers must provide GDPR compliant security to ensure the safety of user data, particularly when accessing personal health information like heart rate, weight, blood pressure, and other health insights.

In order to tackle the various security challenges faced by IoT devices, a comprehensive approach must be adopted that takes into account the CIA triad. This approach prioritizes the confidentiality, integrity, and availability of data to authorized users. To achieve this, it is important to establish clear security policies and regulations, and develop effective security solutions that are tailored to the unique requirements of IoT devices [28]. One of the main challenges faced in the industry is a lack of standardisation. By standardising the approach to device and information security using the CIA triad, organizations can better protect themselves against the potential threats posed by the use of IoT technology.

A. CIA Triad for Information Security

To effectively address the security challenges faced by IoT devices, it is important to adopt a methodology that considers the CIA triad for information security. This methodology is

widely used in the cybersecurity industry and can be applied to most security challenges faced by IoT devices. The CIA triad provides a framework for classifying security challenges into three main considerations: confidentiality, integrity, and availability [8]. By analysing issues through the lens of the CIA triad, more targeted and effective security solution can be developed to better align with the unique needs of IoT devices.

1) Confidentiality

Ensuring confidentiality is a critical aspect of IoT security. This covers two key concepts; privacy and data confidentiality. Privacy refers to the controlling and managing of information of legitimate users or devices. Data confidentiality refers to the protection of data from passive attacks during transmission[9]. Implementing robust confidentiality measures can prevent unauthorized access to sensitive information and protect the privacy of users and their data.

2) Integrity

Integrity is a critical component of the CIA triad that refers to the protection of data from modification in order to maintain accuracy and consistency from end-point to end-point[10]. Any unauthorized modification to the data during transmission can compromise the entire system's security, leading to significant risks to the IoT devices and the network as a whole [29]. Therefore, it is crucial to have measures in place to verify integrity against malicious actors.

3) Availability

Availability refers to the ability of authorized users to access data when needed and prevent unauthorized denial of service. In other words, it ensures that the resources required for the proper functioning of IoT devices are available when needed. This can be threatened by various types of attacks such as distributed denial of service (DDoS) attacks, which can flood the network with traffic, making it difficult or impossible for legitimate traffic to reach its destination. By taking measures to ensure availability, the CIA triad helps to safeguard the operation of IoT devices.

B. Types of attacks

The types of attacks an IoT system might face can be analysed layer by layer, as discussed in [11]. The physical layer, network layer, and application layer of the OSI model are all potential areas of attack. In response, blockchain technology can be used as a security solution. For instance, an example of a physical layer attack is eavesdropping, which falls under the confidentiality aspect of the CIA triad because an unauthorized party has access to private information. Another example of attack is DoS attacks, which are a network layer attack that can affect the availability aspect of the CIA triad by preventing devices from accessing the server. Finally, an example of an application layer attack is attacking authentication, which can compromise the integrity aspect of the CIA triad. Most IoT devices lack proper authentication, such as weak AKA authentication [12], making them vulnerable to attack. Once authentication is compromised, an attacker can modify any data in transit without the users being aware [13].

III. Blockchain Technology and its Benefits for IoT Security

Blockchain technology has emerged as a potential solution for addressing the security challenges faced by IoT. Blockchain technology is a distributed ledger technology that is characterized by its transparency, immutability, and security. These features make it well-suited for addressing the security challenges faced by IoT.

A blockchain is a distributed ledger technology that comprises blocks that are chained together. Reference [11] details the exact structure of a block in the blockchain, including the header which contains the nonce, previous hash, timestamp, and data, as well as defining the Merkle Root Hash. The blockchain is maintained by nodes in the peer-to-peer network, where any node can choose to be a miner[14]. A miner is responsible for adding new blocks to the blockchain through mining. Mining involves solving a resource-intensive cryptographic puzzle called Proof of Work (POW) [15], where miners compete to solve the puzzle and be the first to add a new block to the chain. This system is commonly used in crypto currencies such as Bitcoin and Ethereum [16][17]. There are many other consensus algorithms used with blockchain technology, such as Proof of Stake (POS), Proof of Burn (POB), Paxos, etc. In [18] they provide a detailed and thorough description of distributed consensus algorithms.

Additionally, when a new transaction occurs, it is broadcast to the entire network. The transaction is then verified by each miner who receives it by validating the signatures contained within the transaction. Each block in the blockchain has a distinctive hash. This allows other nodes to use it to verify the integrity of the block [30]. The verified transaction is then appended to the miner's own pending block of transactions that are waiting to be mined. The security of the blockchain is ensured by the fact that multiple miners process a single transaction, making it difficult for a malicious actor to modify the data in the chain. This distributed consensus mechanism enables the blockchain to achieve high levels of security and immutability.

Blockchain technology offers several benefits for IoT security when viewed through the lens of the CIA triad.

1) Confidentiality

One-way blockchain provides confidentiality for IoT devices is by using public-key cryptography [19] to secure transactions. This is where each user or device has a public key and a private key. When a transaction is initiated, it is signed with the private key, and the public key is then used to verify the authenticity of the transaction. This means that only authorized users or devices with the correct private key can access the data.

Moreover, blockchain can provide an additional layer of confidentiality by enabling the creation of private blockchains or permissioned blockchains, which limit access to certain users or devices. This is achieved by controlling access to the blockchain network and implementing encryption techniques to protect the data. A model utilising this method is suggested in [20] where devices in a smart home are linked to a resource capable device, circumventing the resource constraint stated earlier, in clusters called Local Blockchains. These are connected using an overlay network with nodes designating cluster heads to decrease network overhead. This allows the user to designate which devices can communicate with each other using a shared key generated using the Diffie-Hellman algorithm. The main difference between this and the traditional Bitcoin blockchain is when a transaction is added to a block, it is treated as a true transaction without POW or other resource intensive puzzles [31]. Altogether, this covers

the two key aspects of confidentiality (data protection and privacy) through hashing algorithms and key sharing.

Although a concession had to be made due to the limited resources of IoT devices, this method leaves the user too vulnerable because it opens up the blockchain to manipulation from malicious actors. Actors would have an easier time making changes because their alterations would be treated as true because there is no verification through POW or POS or otherwise. This vulnerability is a glaring issue in the implementation of the suggested blockchain-based IoT security solution.

2) Integrity

The second Blockchain technology enhances the integrity of IoT data by providing a tamper-proof and transparent record of all transactions, ensuring that data remains accurate and consistent. In a blockchain, every transaction is recorded in a block that is verified by multiple nodes in the network, ensuring that any change to the data must be approved by the majority of the nodes. This makes it extremely difficult for an attacker to modify data without being detected. Additionally, all blockchains use a hashing algorithm to encrypt their data. For example, Bitcoin uses the SHA256 hashing algorithm and Ethereum uses their own Ethash[21]. This means that an attacker does not have access to the plain-text information and would have to rely on other resource intensive and currently impractical methods to break the hash.

As stated earlier, one method of compromising integrity is to perform an authentication attack. Blockchains verify the authenticity of a message by using digital signatures. When a user sends a message or transaction, they use their private key to generate a digital signature which is attached to the message. When a node on the network receives a message, it can verify its authenticity by using the sender's public key. The node can use the public key to decrypt the digital signature and compare it to the message [32]. If the digital signature matches the message, it means that the message is authentic and has not been modified in transit. This process ensures that messages on the blockchain are authenticated and secure, and that they cannot be tampered with or altered by unauthorized parties[22].

The DecAuth decentralised authentication scheme is suggested in [23]. This suggests that only the authentication and authorisation of messages needs to be done on the blockchain. This has the benefits of being relatively light on computation resources, which makes it specifically suitable for IoT devices, since there are fewer things to calculate. Additionally, it enables the user to allow only trusted actors to access and can validate a message. The reduction in computational complexity also means that it costs less energy to run and wont impact message the speed of communication.

3) Availability

Blockchain can also enhance the availability aspect of the CIA triad by ensuring that data is accessible to authorized users even during times of network disruptions or attacks.

In a traditional centralized system, a single point of failure or attack can lead to the denial of service and loss of data accessibility (DoS/DDoS). However, blockchain uses a decentralised system which means that data is replicated and distributed across multiple nodes in the network, ensuring that there is no single point of failure. As a result, even if some nodes are compromised or offline, the data can still be accessed from other nodes in the network. Additionally, because blockchain is an immutable ledger (i.e., remain unchanged, unaltered, and indelible), it can provide a clear audit trail of data access and modification, making it easier to identify and prevent unauthorized denial of service attacks. Overall, blockchain's ability to enhance availability through decentralized distribution and immutability makes it a valuable tool for enhancing the security of IoT devices.

Due to the lack of standardisation across the IoT industry, smart devices are more vulnerable to single points of failure than any other device. More research is needed to develop standards and mechanisms to ensure those standards. This is especially relevant as IoT devices become incorporated into critical infrastructure across many industries.

By leveraging these benefits, blockchain-based solutions can improve the security of IoT devices and help address the many challenges facing this rapidly evolving field. These solutions range from secure device provisioning and firmware updates to the protection of sensitive data, such as personal health information and financial data [33]. Overall, blockchain can play a significant role in improving the security of IoT devices and ensuring that they remain safe and trustworthy in the face of emerging threats.

IV. Future of Blockchain-Based IoT Security

Blockchain based IoT security is an area of active research and development. There are several emerging trends that are likely to shape the future of the industry.

A. Integration with AI and other Security Technologies

We can expect to see the integration of blockchain other emerging technologies such as AI and machine learning. AIs solve the problem of analysing the massive volume of data produced by IoT devices [24] and can help identift abnormal data usage by analysing blockchain’s immutable ledger.

Additionally, the incorporation of smart contracts can improve the response time to inceidents as smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code [34]. These contracts can help automate the enforcement of security policies for IoT devices, which would address the integrity and availability aspects of the CIA triad

B. Blockchain-based identity management systems

Blockchain-based identity management systems can provide secure and tamper-proof identity verification for IoT devices, which would address the confidentiality aspect of the CIA triad. The research in [23] already points in this direction and continued development in blockchain for identity authentication is a possibility.

C. Hybrid Blockchain Models

Hybrid blockchain models are a combination of public and private blockchains. They would combine the security and transparency of public blockchains with the controlled access and privacy of private blockchains.

Hybrid blockchains are already being trialled in supply chain management [24]. This allows participants to access and update the blockchain whilst keeping their transactions hidden. This addresses the integrity aspect of the CIA triad by ensuring the accuracy and consistency of data.

V. Conclusion

In conclusion, blockchain technology offers significant benefits for IoT security when viewed through the lens of the CIA triad. Confidentiality is enhanced through encryption, access control, and identity management. Integrity is ensured through a tamper-proof and transparent record of transactions. Availability is improved by reducing the risk of DDoS attacks and ensuring system uptime. Hybrid blockchain models and the integration of other technologies, such as AI and machine learning, are likely to be the future trends for the security of IoT devices. The use of blockchain technology provides a promising solution for securing the vast network of interconnected devices and data generated by the IoT.

References

[1] Kashani, M.H., Madanipour, M., Nikravan, M., Asghari, P. and Mahdipour, E., 2021. A systematic review of IoT in healthcare: Applications, techniques, and trends. Journal of Network and Computer Applications, 192, p.103164.

[2] Kalsoom, T., Ahmed, S., Rafi-ul-Shan, P.M., Azmat, M., Akhtar, P., Pervez, Z., Imran, M.A. and Ur-Rehman, M., 2021. Impact of IOT on Manufacturing Industry 4.0: A new triangular systematic review. Sustainability, 13(22), p.12506.

[3] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, "Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis," Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.

[4] Smart Yet Flawed: IoT Device Vulnerabilities Explained. Available online: https://www.trendmicro.com/vinfo/us/security/ news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained (accessed on 17 April 2023).

[5] M. Lefoane, I. Ghafir, S. Kabir and I. U. Awan, "Multi-stage Attack Detection: Emerging Challenges for Wireless Networks," International Conference on Smart Applications, Communications and Networking, Palapye, Botswana, 2022.

[6] Zonouz, S., Rrushi, J. and McLaughlin, S., 2014. Detecting industrial control malware using automated PLC code analytics. IEEE Security & Privacy, 12(6), pp.40-47.

[7] Hernandez, G., Arias, O., Buentello, D. and Jin, Y., 2014. Smart nest thermostat: A smart spy in your home. Black Hat USA, (2015).

[8] Team, I.G.P., 2020. EU general data protection regulation (gdpr)–an implementation and compliance guide. IT Governance Ltd.

[9] Shuaib, M., Alam, S., Alam, M.S. and Nasir, M.S., 2021. Compliance with HIPAA and GDPR in blockchain-based electronic health record. Materials Today: Proceedings.

[10] A. Abdulhamid, S. Kabir, I. Ghafir and C. Lei, "Dependability of the Internet of Things: Current Status and Challenges," International Conference on Electrical, Computer, Communications and Mechatronics Engineering, Maldives, Maldives, 2022.

[11] Shave, L., 2018. The CIA of security and access. IQ: The RIMPA Quarterly Magazine, 34(2), pp.18-22.

[12] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches." International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.

[13] Humayun, M., Hamid, B., Jhanjhi, N.Z., Suseendran, G. and Talib, M.N., 2021, August. 5G network security issues, challenges, opportunities and future directions: A survey. In Journal of Physics: Conference Series (Vol. 1979, No. 1, p. 012037). IOP Publishing.

[14] Samonas, S. and Coss, D., 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3).

[15] Mohanta, B.K., Jena, D., Ramasubbareddy, S., Daneshmand, M. and Gandomi, A.H., 2020. Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal, 8(2), pp.881-888.

[16] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access, vol. 6, pp. 1-12, 2018.

[17] Cas Cremers and Martin Dehnel-Wild. "Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion". In: Network and Distributed Systems Security (NDSS) Symposium 2019 (2019). doi: 10.14722/ndss.2019.23394

[18] Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B. and Bangash, Y.A., 2020. An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. IEEE Internet of Things Journal, 7(10), pp.10250-10276.

[19] Mendoza, J.J. and Nunez, F., 2019. Blockchain-driven on-demand control loops over IoT environments. IEEE Access, 7, pp.157524-157534.

[20] Sharma, D.K., Pant, S., Sharma, M. and Brahmachari, S., 2020. Cryptocurrency mechanisms for blockchains: models, characteristics, challenges, and applications. Handbook of research on blockchain technology, pp.323-348.

[21] Valdeolmillos, D., Mezquita, Y., González-Briones, A., Prieto, J. and Corchado, J.M., 2020. Blockchain technology: a review of the current challenges of cryptocurrency. In Blockchain and Applications: International Congress (pp. 153-160). Springer International Publishing.

[22] M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, "Machine Learning for Botnet Detection: An Optimized Feature Selection Approach". International Conference on Future Networks & Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.

[23] Kim, Y.J. and Skibniewski, M.J., 2022. Building information modeling on blockchain: basic principles, development tools, an application scenario, and future directions. In Research Companion to Building Information Modeling (pp. 615-634). Edward Elgar Publishing.

[24] Panda, S.S., Mohanta, B.K., Satapathy, U., Jena, D., Gountia, D. and Patra, T.K., 2019, October. Study of blockchain based decentralized consensus algorithms. In TENCON 2019-2019 IEEE Region 10 Conference (TENCON) (pp. 908-913). IEEE.

[25] Pal, O., Alam, B., Thakur, V. and Singh, S., 2021. Key management for blockchain technology. ICT express, 7(1), pp.76-80.

[26] Dorri, A., Kanhere, S.S. and Jurdak, R., 2016. Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.

[27] Ghimire, S. and Selvaraj, H., 2018, December. A survey on bitcoin cryptocurrency and its mining. In 2018 26th International Conference on Systems Engineering (ICSEng) (pp. 1-6). IEEE.

[28] Karame, G.O. and Androulaki, E., 2016. Bitcoin and blockchain security. Artech House.

[29] S. Eltanani and I. Ghafir. "Coverage Optimisation for Aerial Wireless Networks." 2020 14th International Conference on Innovations in Information Technology (IIT). IEEE, 2020.

[30] Mohanta, B.K., Sahoo, A., Patel, S., Panda, S.S., Jena, D. and Gountia, D., 2019, October. Decauth: Decentralized authentication scheme for iot device using ethereum blockchain. In TENCON 2019-2019 IEEE Region 10 Conference (TENCON) (pp. 558-563). IEEE.

[31] M. Hammoudeh, I. Ghafir, A.Bounceur and T. Rawlinson, "Continuous Monitoring in Mission-Critical Applications Using the Internet of Things and Blockchain," International Conference on Future Networks and Distributed Systems. Paris, France, 2019.

[32] Atlam, H.F., Azad, M.A., Alzahrani, A.G. and Wills, G., 2020. A Review of Blockchain in Internet of Things and AI. Big Data and Cognitive Computing, 4(4),p.28.

[33] Atlam, H.F. and Wills, G.B., 2019. Intersections between IoT and distributed ledger. In Advances in Computers (Vol. 115, pp. 73-113). Elsevier.

[34] Liu, J., Yan, L. and Wang, D., 2021. A hybrid blockchain model for trusted data of supply chain finance. Wireless personal communications, pp.1-25.