Apply Blockchain Technology for Security of IoT Devices

[1]Yahye Adam Omar, [1]S B Goyal and [2]Vijayakumar Varadarajan

[1]City University, Petaling Jaya, Malaysia
[2]University of South Wales, Sydney Australia
E-mail : yahyeadam33@gmail.com, drsbgoyal@gmail.com, Vijayakumar.varadarajan@gmail.com

2021 Emerging Trends in Industry 4.0 (ETI 4.0) | 978-1-6654-2237-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/ETI4.051663.2021.9619295

Abstract :- **The world is only beginning to see the value and potential impact of the internet of things (IoT). Until recently, access to the internet was bounded via desktop, tablet, or smartphone. With the (IoT), practically all devices and objects can be connected to the internet and monitored remotely. IoT devices simplify our lives and make organizations more efficient; however, there are still challenges to address, particularly in the security context. As we continue to embed these connected objects and a wider variety of wireless devices, it is mandatory to provide confidence in this vast incoming information source. Blockchain has emerged as a disruptive technology that will transform the way we store, share information, and impose restrictions to know the authentications. The data distribution and robust level of encryption will remove the need for trust among the involved parties and add another security layer for IoT data. IoT devices generate too much data using sensors and stored, processed, accessed the same using cloud computing and achieve security some extend using big-data. Big-data security mechanism is not sufficient to meet the security requirements of IoT devices. We have proposed the Blockchain encryption mechanism using different layers architecture for the IoT devices to achieve the desired security level. In this paper, we have focused on how Blockchain could possibly improve IoT security. We also survey the most relevant work to investigate challenges associate with IoT Blockchain convergence. This proposed mechanism will achieve the security mechanism in IoT devices some extend.**

Keywords—IoT, privacy, blockchain, internet security threat, distributed ledger technology, peer-to-peer

I. INTRODUCTION

From smart cars, smart homes to smart cities, the internet of things (IoT) is becoming an essential part of our daily lives. IoT is a giant network with connected devices; these devices gather and share data about how they are used and the environment in which they are operated [1]. Early forms of communication with an IoT often involved machine to machine (M2M) [2]. Today, IoT has expanded beyond M2M and enclosed systems towards sensors of all kinds that can communicate with each other from anywhere in the world. With the IoT, we can apply more value to our products. With billions of connected devices, heterogeneity is a major challenge facing the development of IoT ecosystems [3]. However, aside from heterogeneity and data integration present in IoT, generated data's trustworthiness is also an important issue [4]. For example, untrusted organizations can modify information according to their interests, so the reports they provide might not be completely reliable; this promotes the necessity to verify that the information has never been altered. One way to ensure that the data remains immutable is through Blockchain technology [5]. This paper proposes a generic model to integrate IoT and Blockchain technology, and the potential advantages of their combination will be analyzed. The layout of the paper as follows: section II focused on the IoT Security and Privacy challenges, followed by section *A* IoT Vulnerabilities issues, section *B* Potential Attacks and Glitches, section III Blockchain Concepts overview, section *IV* proposed the Model to Integration of Blockchain for IoT Devices**,** section *V* expected results summary, section *VI* discussion and finally covered the conclusion & future work.

II. IOT SECURITY AND PRIVACY CHALLENGES

The internet of things is an emerging technology that is expanding quickly with considerable security gaps and is plagued with vulnerabilities, malware, and the potential to disrupt infrastructure [6]. Consumers, businesses, and governments use IoT devices that range from simple to complex and from small to large [7]. During the last few years, the use of IoT devices has grown rapidly. There are over 7 billion active IoT devices globally, and they have been widely used in smart manufacturing, smart wear, smart homes, etc. [8]. This increase in IoT device implementation will meet with an increase in the regulatory effort too. Cybersecurity is a top concern in today's increasingly digital world for businesses, government entities, and individuals. As millions of IoT devices become connected, hackers find new vulnerabilities to exploit using sophisticated attacks make it far more difficult for systems to identify, protect, and react to these threats. Beyond stealing intelligently or disrupting business activities, hackers now have more entry points that allow them to damage our physical world and post serious safety risks with the presence of IoT technology. Many organizations and individuals embrace the IoT, yet; very few understand how to secure the devices. In addition to providing thermostat control for our homes, monitoring our fitness, and turning our lights on at night. The IoT is influential to critical infrastructures such as utility grids and communication systems. A cyberattack on

those systems will have major consequences. The potential for cyberattacks and compromising privacy is increasing due to serious vulnerabilities in IoT devices [9]. IoT devices lack basic security defenses and can fall victim to malware and attacks [10]. With the IoT, consumers are beginning to have privacy concerns [11]. In addition, companies are worried about a severe breach with IoT devices. The reality is that every day more and more devices are passively collecting petabytes of data without our knowledge, which can fall into the wrong hands affecting our privacy. Businesses can lose sales, have increased legal costs, and lose investor confidence. Consumers face equally as serious risks as they might telemarketing, junk mails, spam, and identity theft. Billions of devices make up the internet of things, from RFID to refrigerators; they talk to each other, interact with the environment, and produce petabytes of data. However, the IoT will affect our privacy due to serious vulnerabilities in the devices.

A. IoT Vulnerabilities Issues

A vulnerability is a flaw in a system that allows hackers to exploit and gain access to an unauthorized asset or cause a security breach [12]. The potential for cyberattacks and compromising privacy is increasing due to vast vulnerabilities in IoT devices. Researchers found that over half a million IoT devices are vulnerable to medium or high severity attacks, which can pose serious security risks. Researchers also found that 98 percent of all IoT device traffic is unencrypted, exposing personal and confidential data on the network [13] [14]. Connected devices are becoming a major target for cyber-attacks.

Table I. Common IoT vulnerabilities

S.No	***Vulnerability***	***Description***
1	Weak, Guessable, or Hardcoded Password	Publically available or easily brute-forced credentials used by IoT device manufacturers
2	Insecure Data transfer	Lack of encryption or access control
3	Lack of secure update mechanism	Lack of ability to securely update the device firmware.
4	Insufficient privacy protection	User's personal information stored on the device
5	Lack of device management	Luck of support, monitoring, and response capabilities to the anomalies

There are various ways to exploit a vulnerability in IoT devices; a hacker can explore the entire network and commands a controller from rogue devices to carry out some physical actions such as revoking a faulty security system to allow someone to gain access into a building. When an architect begins to design a building, there is a set of codes and standards in which they follow to provide safety for the client. However, IoT manufacturers are flying blind, as there are no standards or common language [15]. Governments and regulatory bodies recognize the problem of poor or no security standards for devices connecting to the internet. They are proposing minimum-security measures for device manufacturers and labeling to raise users' awareness about how secure their devices are. These can be enforced as laws or industry standards and regulations. With next-generation internet capabilities 5G, dramatic increase in data speed and throughput, IoT devices will be key players in the cybersecurity threat landscape [16].

With the rapid expansion of IoT, vendors and manufacturers have not even discovered the vulnerabilities extent. Developers are working on incorporating security modules that include user and password management, and secure storage, along with anti-counterfeiting and authentication solutions [17]. However, the problem is, IoT devices are often vulnerable than servers and network devices connected to the internet because they do not have enough computing power to support basic protections such as antimalware and firewalls.

B. Potential Attacks and Glitches

According to the Symantec internet security threat report (ISTR), routers and connected cameras are the most IoT devices infected by malware, and the primary sources of IoT attacks, accounting for over 90% of the malicious activity [18]. Smartphones, tablets, wearable technology, and smart home devices are now being adapted into everyday lives and appear on enterprise networks. As we keep up to develop these interconnected devices and extensive wireless devices, the IoT can be the source of a significant cybersecurity threat, including data leakage, distributed denial-of-service attacks (DDoS), and any attack that can be controlled from botnets.

Cybercriminals use unique malware, usually a Trojan horse, to breach the security of computer users. Often, cybercriminals will seek to infect and control thousands of IoT devices so they can act as the master of an extensive zombie network or bot network [19]. The botnets can deliver many types of cyber-crimes such as DDoS attacks, spreading malware, online fraud, and wide-scale spam or phishing campaigns. One of the dramatic cases of the threat of unsecured IoT devices is the Mirai botnet [20]. The attackers built their botnet army by running a simple script against devices on the internet that attempted to log in with 61 known IoT default passwords. If they successfully logged in, the IoT device was infected with malware that directed them to follow the instructions of a central command. The attack was very effective, and it is estimated that there were nearly half a million Mirai-infected IoT devices mainly composed of closed-circuit, TV cameras, DVRs, and routers.

III. BLOCKCHAIN CONCEPTS OVERVIEW

Block-chain technology is a peer-to-peer (P2P) distributed ledger technology (DLT) where all participants can access the distributed ledger [21]. Blockchain network facilitates a new decentralized distributed way of managing information across parties who do not necessarily trust each other but have a common interest. Block-chain allows us to make transactions more directly and lower the use of intermediaries example, companies or banks. The Blockchain came to life as the technology backend of cryptocurrency (Bitcoin) in 2009 [22]. Bitcoin requires a validated and secure database for the transactions; these transactions must be resistant to modification and related to their owners. For example, if you currently possess five Bitcoins after several succession currency purchases or trades, each of those transactions must be strapped to you to resolve your account total. Blockchain database stores the transactions in sequence blocks (chain) where each new block is dependent on the previous block [23]. In the first few years after the emergence of Bitcoin, blockchain technology was relatively unknown.

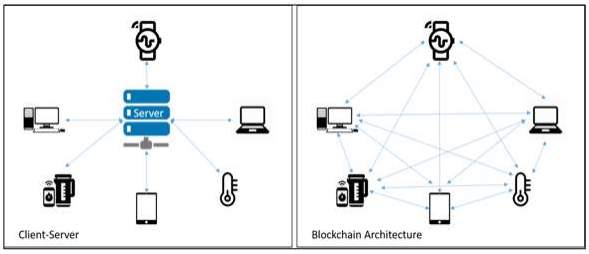

Fig. 1. Client-Server Vs. Blockchain Architecture

However, there were properties of Blockchain technology that made it appealing outside the domain of cryptocurrency. Innovators discovered that the same qualities of (DLT) that made it perfect for ensuring the integrity of Bitcoin could also be a way to store all types of data in a more secure and validated manner [24]. While traditional structured and unstructured databases have served us well for several decades, they have some fundamental security weaknesses [25]. These issues include; account administration and ensuring only the right people have access to specific data. Innovators have worked hard to plug these gaps, but challenges persist until (DLT) has not been elegantly addressed.

Unlike traditional databases that use authentication to permit specific rights, DLT uses a consensus mechanism to enable permissions. This consensus mechanism ensures that only transactions allowed by predetermined rules can take place. It also assures that a transaction is associated with a specific person [26]. DLT can ensure that a digital-based real estate transaction is authentic and retains its integrity. DLT can ensure that a vote over the internet is accurate and correlated with a specific individual. Blockchain technology is an inherent design that makes fraud and transaction manipulation something familiar in traditional databases remarkably tough and nearly impossible.

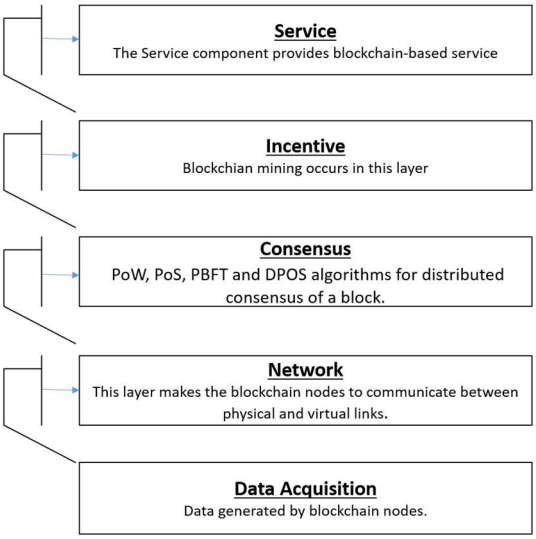

Fig. 2. Blockchain Layers

IV. MODEL TO INTEGRATION OF BLOCKCHAIN IN IOT DEVICES

Fig.3 illustrates the process that merges the use of IoT and Blockchain. It is a fully decentralized system where every device is directly writing data to the Blockchain network. Blockchain will serve as middleware between IoT and applications [27]. Every node has a unique identity, which the Blockchain handles, providing a reliable way to identify a specific source of any leakages and take quick remedial action [28]. The smart contract, which is the agreement between two parties in the Blockchain, ensures the Blockchain network's proper working mechanism, making data immutable [29]. The IoT Blockchain layer has all the modules to provide various Blockchain technology features, including peer-to-peer (P2P) communication, identity management, and consensus.

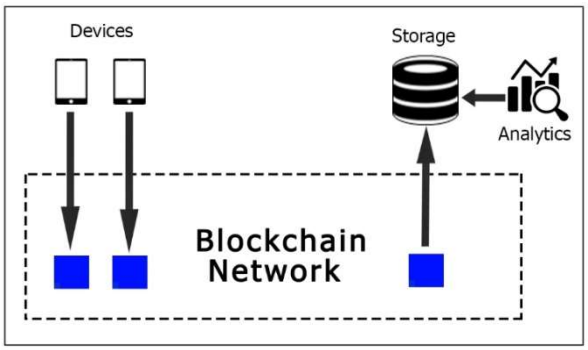

Fig. 3. Blockchain and IoT Integration Model

In order for a transaction to be executed (write or read data from the ledger), every packet that the IoT device induces will be represented as a transaction. The data is wrapped in the acquisition layer and encrypted with a digital signature.

The network layer creates nodes connectivity in the underlying communication network. In the Blockchain, we have various consensus algorithms such as proof of work (PoW), proof of stake (PoS), and delegated proof of stake (DPoS), which are essential to agree on one particular Blockchain state. Although the incentives layer is not mandatory to reword the validation process when everything is a part of the internal organization process, the coating is established for the future where a reward is needed for validation. The service component gives users Blockchain-based services for different industrial sectors.

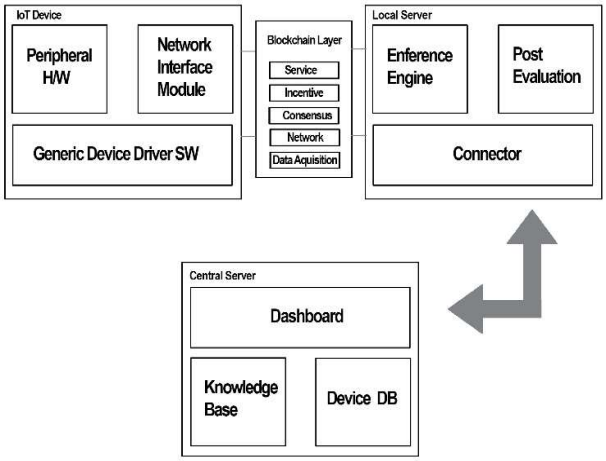

Fig. 4 Blockchain Layer and Its component for Integration to IoT

The proposed architecture shown in fig. 4 creates a Blockchain baseline that connects all the IoT devices in the network, bringing embedded Blockchain security mechanism. There is a (P2P) network for data distribution, and mostly the information is the same in every node and encrypted. The network devices are digitally identified, giving each device a unique identity, which refers to the identity of things (IDoT) [30]. The Blockchain layer can precisely and immutably identify devices as individual entities by hashing or using non-fungible smart contracts. Because of each block's sequential cryptographic hashing, it is computationally infeasible to rewrite Blockchain history, and that is crucial for storing data or analytics purpose.

V. Results

Overall, the results presented below show that; decentralization aspect of DLT means that hacking or altering any records will be significantly more challenging than with a centralized system. Fig. 5 shows the Blockchain node design, where a complex network of connected physical systems can process information and communicate peer-to-peer to enable common service. By converging IoT and Blockchain technology, we can effectively build a decentralized platform to mitigate IoT security obstacles effectively. In addition, every IoT device in the Blockchain network has an encrypted, unique, and immutable identity to ensure better privacy and security. Disrupting the system by getting the authentication data of a single party is particularly impossible even if one network participant's security is compromised.

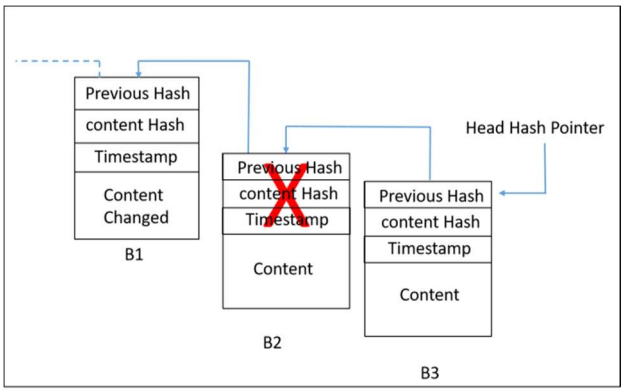

Fig. 6 Block tampering representation of Blockchain

Blockchain data is encrypted and tamper-proof [31]. With cryptography and timestamp, each block proceeds strictly in chronological order; such irreversibility in time ensures that any tamper with blockchain data will be easily traceable. The consensus mechanism safeguards the data codes and verifies their authenticity even if there are errors or tampering with an individual node. The legitimacy of the entire blockchain ledger can be guaranteed, given that the majority of nodes carry the same information. This feature resolves the current IoT ecosystem that depends on a centralized platform and prevents altering the data.

VI. Discussion

One of the main goals of this study was to evaluate the need for Blockchain technology in IoT security. The concept behind IoT is about connecting merely everything to the internet for data-gathering into our work and personal lives. Blockchain is based on cryptography and P2P network for data-distribution, which is an essential part of understanding why IoT will need the Blockchain rather than the open internet.

The results indicate that DLT can mitigate potential privacy and security challenges in IoT devices. The integration of the Blockchain layer in an organization's architecture allows it to be transformed so that security, cost, and trust issues existing in the current IoT systems are guaranteed. Works that deal with the subject [32] [33] [34] proposed various approaches for the integration of IoT and Blockchain technology; however, no clear solution has been addressed in terms of scalability and availability in a large-scale IoT environment. Various companies in the market are already working on use cases for uniting these two technologies. To adopt Blockchain in large-scale IoT, we need to overcome technical and security concerns.

VII. Conclusion and future work

This paper explores the security and privacy issues in IoT-based centralized systems and solutions provided by IoT with Blockchain. DLT is recognized as one of the solutions for addressing the issues and challenges in IoT. Based on the proposed model for integrating IoT and Blockchain, we were able to contribute an easy and manageable environment to unite the two technologies. As a final, challenges in IoT with blockchain technology are also addressed. However, we need further studies in order to overcome core issues in terms of throughput in a large-scale IoT context, as well as need to focus on the IoT devices' privacy also. We need to evaluate the results in the multidomain industries like healthcare, logistics, and manufacturing, etc.

References

[1] Rouse, Margaret. "Internet of things (IoT)". IOT Agenda. Retrieved 14 August 2019.

[2] Lueth, K. L. (2020, May 25). Why the Internet of Things is called Internet of Things: Definition, history, disambiguation. IoT Analytics GmbH. https://iot-analytics.com/internet-of-things-definition/

[3] Z. K. Zhang, M. C. Yi Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230-234, Nov 2014

[4] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191-1221, Secondquarter 2020, doi: 10.1109/COMST.2019.2962586.

[5] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227. https://doi.org/10.1016/j.iot.2020.100227

[6] Tawalbeh, L.'. Muheidat, F., Tawalbeh, M., & Quwaider, M., IoT Privacy and Security: Challenges and Solutions. Applied Sciences, 10(12), 2020, 4102. https://doi.org/10.3390/app10124102

[7] Theobald, M.: The Importance of Security by Design for IoT Devices (2018). https://www.redalertlabs.com/blog/the-importance-of-security-by-design-for-iot-devices. Accessed 20 Aug 2018

[8] Lueth, K.L. State of the IoT 2018: Number of IoT Devices Now at 7B—Market Accelerating. Available online: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (accessed on 6 December 2019).

[9] Abdur, M., Habib, S., Ali, M., Ullah, S.: Security issues in the internet of things (IoT): a comprehensive study. Int. J. Adv. Comput. Sci. Appl. **8**(6) (2017)

[10] Alladi, T., Chamola, V., Sikdar, B., Choo, K.R.: Consumer IoT: security vulnerability case studies and solutions. IEEE Consum. Electron. Mag. 9(2), 17–25 (2020).

[11] Alhirabi, N., Rana, O., & Perera, C., Security and Privacy Requirements for the Internet of Things. ACM Transactions on Internet of Things, 2(1), 2021, 1–37. https://doi.org/10.1145/3437537.

[12] Vulnerability Management Life Cycle | NPCR | CDC". www.cdc.gov. 2019-03-12. Retrieved 2020-07-04.

[13] O'Donnell, L. (2020, April 22). More Than Half of IoT Devices Vulnerable to Severe Attacks. Threatpost.ttps://threatpost.com/half-iot-devices-vulnerable-severe attacks/153609/

[14] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand and A. H. Gandomi, "Addressing Security and Privacy Issues of IoT Using Blockchain Technology," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 881-888, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3008906.

[15] H. Fang, A. Qi and X. Wang, "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement," in *IEEE Network*, vol. 34, no. 3, pp. 24-29, May/June 2020, doi: 10.1109/MNET.011.1900276.

[16] D. Fang and Y. Qian, "5G Wireless Security and Privacy: Architecture and Flexible Mechanisms," in IEEE Vehicular Technology Magazine, vol. 15, no. 2, pp. 58-64, June 2020, doi: 10.1109/MVT.2020.2979261.

[17] Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. (2020). A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. Future Internet, 12(2), 27. https://doi.org/10.3390/fi12020027

[18] Dange S., Chatterjee M. (2020) IoT Botnet: The Largest Threat to the IoT Network. In: Jain L., Tsihrintzis G., Balas V., Sharma D. (eds) Data Communication and Networks. Advances in Intelligent Systems and Computing, vol 1049. Springer, Singapore. https://doi.org/10.1007/978-981-15-0132-6_10

[19] 2. N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," in *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559-3570, April 2020, doi: 10.1109/JIOT.2020.2973176.

[20] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, 2017, pp. 1-5, doi: 10.1109/CCWC.2017.7868464.

[21] Chen, G., Xu, B., Lu, M. et al. Exploring blockchain technology and its potential applications for education. Smart Learn. Environ. 5, 1 (2018). https://doi.org/10.1186/s40561-017-0050-

[22] Chen, G., Xu, B., Lu, M. et al. Exploring blockchain technology and its potential applications for education. Smart Learn. Environ. 5, 1 (2018). https://doi.org/10.1186/s40561-017-0050-

[23] Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. Internet of Things, 1–2, 1–13. https://doi.org/10.1016/j.iot.2018.05.002

[24] Adeyemi, A., Yan, M., Shahidehpour, M., Botero, C., Guerra, A. V., Gurung, N., Zhang, L. C., & Paaso, A. (2020). Blockchain technology applications in power distribution systems. The Electricity Journal, 33(8), 106817. https://doi.org/10.1016/j.tej.2020.106817

[25] Patrício, L.D. and Ferreira, J.J., "Blockchain security research: theorizing through bibliographic-coupling analysis", Journal of Advances in Management Research, Vol. 18 No. 1, 2020, pp. 1-35. https://doi.org/10.1108/JAMR-04-2020-0051

[26] Minoli, D., & Occhiogrosso, B., Blockchain mechanisms for IoT security. Internet of Things, 1–2, 2018, 1–13. https://doi.org/10.1016/j.iot.2018.05.002

[27] Hang, L., & Kim, D.-H., Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. Sensors, 19(10), 2019, 2228. https://doi.org/10.3390/s19102228.

[28] Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.

[29] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M., On Blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 2018, 173–190. https://doi.org/10.1016/j.future.2018.05.046

[30] A. H. M. Amin, N. Abdelmajid and F. N. Kiwanuka, "Identity-of-Things Model using Composite Identity on Permissioned Blockchain Network," *2020 Seventh International Conference on Software Defined Systems (SDS)*, Paris, France, 2020, pp. 171-176, doi: 10.1109/SDS49854.2020.9143887

[31] M. Samaniego, U. Jamsrandorj and R. Deters, "Blockchain as a Service for IoT," *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and*

Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 2016, pp. 433-436, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.

[32] Minoli, D., & Occhiogrosso, B., Blockchain mechanisms for IoT security. Internet of Things, 1–2, 2018, 1–13. https://doi.org/10.1016/j.iot.2018.05.002

[33] Aditya Tandon, Challenges of Integrating Blockchain with Internet of Things., International Journal of Innovative Technology and Exploring Engineering, ISSN 2278-3075 (online), 8(9S3), 2019, 1476–1489. https://doi.org/10.35940/ijitee.i3311.0789s319.

[34] Villegas-Ch, W., Palacios-Pacheco, X., & Román-Cañizares, M., Integration of IoT and Blockchain to in the Processes of a University Campus. Sustainability, 12(12), 2020, 4970. https://doi.org/10.3390/su12124970