Efficient Design for Smart Environment Using Raspberry Pi with Blockchain and IoT (BRIoT)

Sunil K. Ponugumati[1], Kamran Ali[1], Aboubaker Lasebae[1], Zaid Zahoor[1]
Anum T. Kiyani[2], Ali Khoshkholghi [1], Maddu Latha[3]
[1]Faculty of Science and Technology, Middlesex University London, UK
[2] York St John University, London
[3] Acharya Nagarjuna Univeristy, Andhra Pradesh

***Abstract*—Internet of Things (IoT) is reshaping digital world day by day by integrating several technologies to provide smart services. However, intrinsic features of IoT resulting in a number of challenges, such as decentralization, poor interoperability, privacy, confidentiality, and security vulnerabilities. Several security techniques like encryption, third-party software's are in use currently to protect users data. Blockchain was initially established for digital crypto currencies with a Proof of Work (PoW) consensus process and the advantage of smart contracts, which enabled distributed trust without the involvement of a third party. Its distributed trust concept paved the way for many other developments, such as the development of new consensus mechanisms such as Proof of Stake (PoS) and Proof of Authority (PoA), which aided in the adoption of Blockchain with low computation machines into sectors such as smart industry and smart transportation. Blockchain implementation in IoT can address the security issue, here we proposed a design using Raspberry Pi as edge node (BRIoT).**

***Index Terms*—Internet of Things (IoT), Blockchain, Edge Computing, Raspberry Pi.**

I. Introduction

Internet has became the standard for communication since 1980 when World Wide Web (WWW) and the TCIP/IP protocol were introduced, these helped the world a lot in speeding up the communication and for lot more innovations. Gradual improvement in technology made multiple researcher's and organizations to focus on automating the regular on going communications which improves performance. When communication world experiencing automation, Kevin Ashton coined the phrase "Internet of Things" in 1999 using wireless technologies like RFID and wireless sensor networks (WSN).

The Internet of Things (IoT), became more popular as the proposed system works by combing physical things like sensors and actuators with latest technologies. This system is also capable of acting without human involvement depending on the supplied data, going beyond automating tasks with specified fixed attributes. IoT devices collects data from physical devices like sensors, scanners process and transmits it to cloud servers. Numerous everyday items that are connected to the internet in some form under an IoT paradigm produce enormous amounts of data that must be processed, saved, and presented in a smooth, user-friendly, and effective manner [1]

Cloud computing is an evolution of cluster and grid computing, which were designed to pool resources in one location and use them for high-performance computation [2].The on-demand availability of computer system resources, particularly with computational power and data storage, is known as cloud computing. This idea of on demand availability was initially introduced by the CEO of Google at the search engine conference (SES Sane Jose) in August 2006.

Prior to the development of edge computing, conventional cloud computing centralised the computational and storage issues by transferring all data to the cloud computing centre through the network. Edge computing is a new paradigm for computing that carries out computation at the network's edge. At the network's edge, it performs computations and offers services, with data creation as its primary goal. In order to meet the critical needs of the IT industry in terms of agile linking, real-time business, data optimization, application intelligence, security, and privacy, edge computing involves moving the cloud's network, computing, storage capabilities, and resources to the edge of the network. It also provides intelligent services at the edge to satisfy the needs of low latency and high bandwidth on the network. The Internet of Things will experience a significant stress from cloud computing if all of the massive amounts of data produced by linked devices are sent to cloud servers. At this time, edge computing is necessary to manage work within its area and share the burden of the cloud, another major benefit is that Cloud-based data is not lost when there is an issue with edge computing. Some Internet services, such as in-depth data analysis of data mining and sharing, need the collaboration of cloud computing and edge computing, requiring some data to be handled by edge computing and then sent back to the cloud for processing [3]

Blockchain is a technology that was first developed to make it easier for people to conduct commercial transactions (trades) using a new cryptocurrency called Bitcoin that is not backed by any banks or governments [4]. The Blockchain's major goal is to free people from any form of trust that we are now expected to invest in intermediaries who "manage" and "control". Initially it is designed for cryptocurrencies like Bitcoin. Nakamato developed the idea of Blockchain in 2008, which is a distributed append-only public ledger system, and it has gained a lot of interest as a new peer-to-peer (P2P) technology for distributed computing and de-

centralised data exchange.It is protected against attacks that aim to take over the system. Ethereum, a transaction-based state-machine, was later introduced in 2013 to program the Blockchain technology. It is interesting to note that, outside of cryptocurrencies, Blockchain is being used in a variety of industries due to its distinctive and alluring features, such as transactional privacy, security, the immutability of data, auditability, integrity, authorization, system transparency, and fault tolerance. These include identity management, intelligent transportation, supply chain management, mobile crowd sensing, agribusiness, Industry 4.0, the Internet of Energy (IoE), and security in mission-critical systems [5]

This study employs Blockchain Technology in a smart environment with IoT devices as an effective means of communication, quicker real time data processing, and enhanced security.

The paper is structured as follows. Section II provides an overview of the Internet of Things, covering its characteristics and vulnerabilities, as well as the significance of decentralised security. Section III covers Blockchain and its types. Section IV presents our proposed architecture, including design and execution. Section V brings the paper to a close and discusses future work.

II. Overview

A. Internet of Things

The Internet of Things (IoT) paradigm was first characterised as a new dimension added to the world of Information and Communication Technologies (ICTs) that enables for the creation of new dynamic networks of networks by connecting everyone and everything, anytime and everywhere. IoT is no longer a new phenomenon. It has emerged as one of the most significant technologies of the twenty-first century, having applications in a wide range of sectors including transportation, energy, civil infrastructure, smart buildings, environmental monitoring, healthcare, military, manufacturing, and production. [6]. IoT has made it possible for new discoveries, innovations, and interactions between things and people. The capabilities that IoT offers are the fundamental reason for the significant attention that the area has attracted in recent years from both the academic and industrial sectors. It also ensures the creation of a future in which all intelligent things and technology are linked to the internet and capable of communicating with one another with the least amount of human intervention.The main goal of IoT is to improve people's lives by enabling all of the smart items that surround us to understand our needs, wants, and preferences and act in accordance with those preferences without receiving explicit instructions. [7].

B. Concept of IoT

The Internet of Things ecosystem includes billions of smart objects in its architecture that enable data transmission, processing, and storage. Several layered architectures has been proposed by researchers till today. Wu et al. suggested a five-layer Internet of Things design [8]. The four-layer IoT design has been proposed by several researchers, Gokhale et al. and Muhammad et al. [9] [10]. Here we look into a four layered architecture

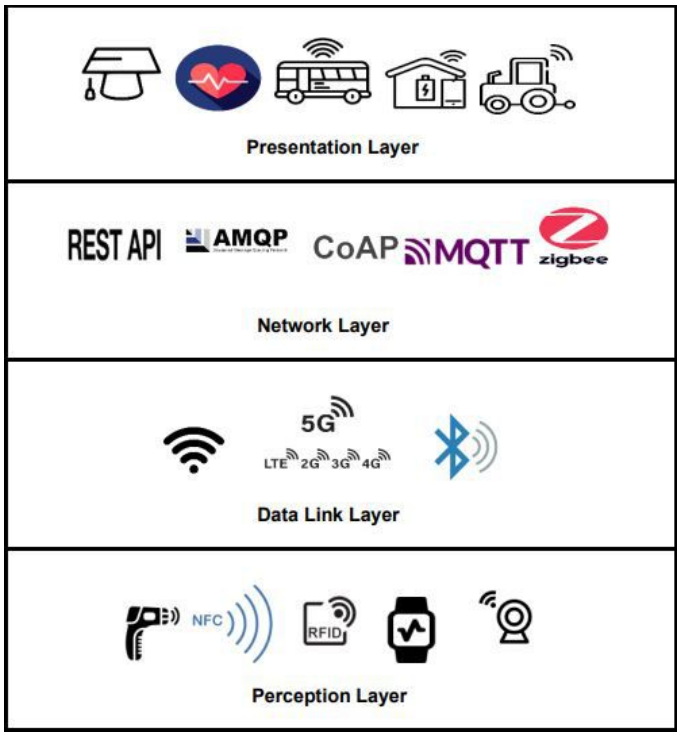

Fig. 1. IoT Layered Architecture

Perception Layer: In IoT, looking the design from bottom-up approach perception layer is the first layer that collects all the data surrounded in our environment. It collects information using a variety of technologies, including Wireless Sensor Networks (WSN), and Radio Frequency Identification (RFID) many more and employs actuators to operate items. Main components in this layer are bar code readers, radio frequency identification (RFID) tag readers, cameras, and other types of sensors. The collected data in this layer is termed as raw data [7].

Data Link Layer: The network layer is in charge of providing data with routing channels so that it may be transferred in packet form across the network region. This creates logical connections, manages routing, and makes routing choices for data transport. This layer also includes network gear such as switches, firewalls, bridges, and routers that enable communication using 3G, 4G, 5G, Wi-Fi, infrared technologies [7].

Network Layer: The data link layer includes communication protocols, which primarily provide network layer functional services. Bluetooth, ZigBee, RFID, low power wide-area networks, Z-wave, and cellular are among the standard technologies and protocols mentioned by organisations for data communication protocols [11].

Presentation Layer: User interface Layer is the top layer of the Internet of Things architecture, and it is responsible for providing customers with shrewd and perceptive apps and services based on their requirements. Examples of these

applications include smart transportation, smart housing, and smart cities [12].

C. Vulnerabilities of IoT

Multiple IoT device vulnerabilities make it simpler for attackers to take over the target device. The OWASP (Open Web Application Security Project) identified IoT vulnerabilities and proposed counter measures in 2018 report. [13]

- Inadequate physical protection: The vast majority of Internet of Things devices can operate on their own in complex, heterogeneous situations without supervision. With relatively little effort, this uncontrolled operating might allow an adversary to get illicit physical access to such devices, giving them control of them. As a result, the attacker would harm the devices physically, maybe disclosing the cryptographic methods that were being utilised, copying their firmware via a rogue node, or just erasing their control or their cyber data.
- Insufficient energy harvesting: IoT devices are frequently built with limited energy, and they might not always have the tools or procedures in place to automatically renew it. A hacker might deplete the energy supplies by broadcasting a barrage of corrupted signals, rendering the devices inoperable for authorised users or activities.
- Insufficient authentication: The constraints imposed by the IoT paradigm may make it challenging to build complex authentication methods. Limited energy and computing power are some of these restrictions. This restriction of ineffective authentication measures might be leveraged by an attacker to implant false, malicious nodes or compromise data integrity, interfering with IoT devices and network interactions. Such circumstances might bring adverse misplacement, destruction, or damage of the authentication keys that are used and transferred, giving a sensation of perpetual risk. All other sensitive information that could be included is likewise subject to this. Even the most sophisticated authentication techniques (or those that are ordinarily effective) become useless in these situations, because the keys are not being stored or transferred securely.
- Improper ciphering: The security of one's data is crucial when it comes to the Internet of Things (IoT), especially for systems that run in critical CPS. It is well knowledge that encryption is a useful technique for keeping data safe while it is being sent and stored so that only authorised users may access it. Resource limitations brought on by the internet of things (IoT) may affect the resilience, efficiency, and efficacy of cryptographic algorithms since the security of cryptosystems depends on the algorithms built into them.
- Unused open ports: The development of technology and the network for devices provided multiple ports taking into account future usage where an adversary can connect to unused and open ports and exploit a number of flaws in a number of Internet of Things (IoT) devices because these devices have ports that are left open when they don't need to be and because they run susceptible services.
- Inadequate access management: Unauthorized access to the data and linked devices of the internet of things should be prevented by a well-managed credential system (IoT). The majority of Internet of Things devices, in addition to the cloud management platforms they employ, are known to not require a password with a strong enough level of complexity. In addition, many devices do not prompt the user to change the default user credentials after installation. Additionally, administrator privileges have been given to the majority of users. As a result, a threat actor may gain illegal access to the system, endangering both the data on it and the whole Internet.
- Improper security patch management: In order to keep fewer attack avenues and improve their functional capabilities, operating systems for IoT devices as well as embedded firmware and software should be patched appropriately. Despite this, a considerable number of occurrences suggest that many manufacturers either fail to regularly maintain security updates or fail to implement automatic patch-update methods. Furthermore, there are no integrity guarantees for even the currently existing update mechanisms, which makes them vulnerable to malicious alterations and the wide dissemination of such changes.
- Poor programming procedures: Strong programming methods and the introduction of security components may boost the Internet of Things resilience, however several researchers have noted that a great deal of firmware is issued with known security flaws. These flaws include backdoors, the use of root users as main access points, and a lack of Secure Sockets Layer (SSL). As a result, it would be simple for a threat actor to exploit well-known security flaws in order to produce buffer overflows, make unauthorised modifications to the data, or gain unauthorised access to the device.
- Not enough audit methods: It is simpler to conceal undesired acts caused by IoT since many Internet of Things devices lack thorough recording mechanisms.

D. Characteristics of IoT

- Confidentiality: Preventing data packet interception and inspection as well as host intrusion such that data, passwords, information, or configuration settings might be taken over by a hacker.
- Integrity: Integrity is the assurance that the packets saved or received via a network haven't been altered without authorization.
- High Availability: Ensuring that equipment cannot be compromised in any way that would cause them to cease functioning correctly or serving their intended purpose.
- Authorization (Data and Device): The procedure used to determine if a resource may be accessed. For instance, to execute programs, run actuators, or read or write data. Authorization also entails restricting or rescinding

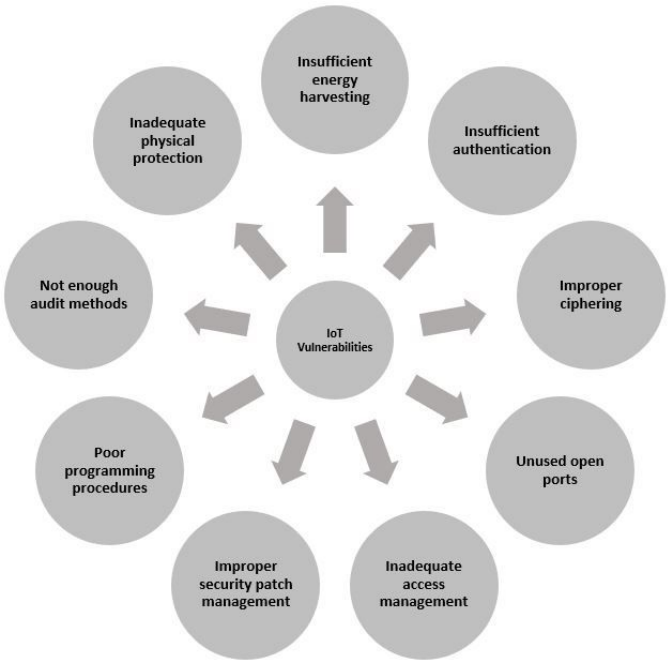

Fig. 2. IoT Vulnerabilities

access in order to safeguard against anybody or anything negative.

[14]

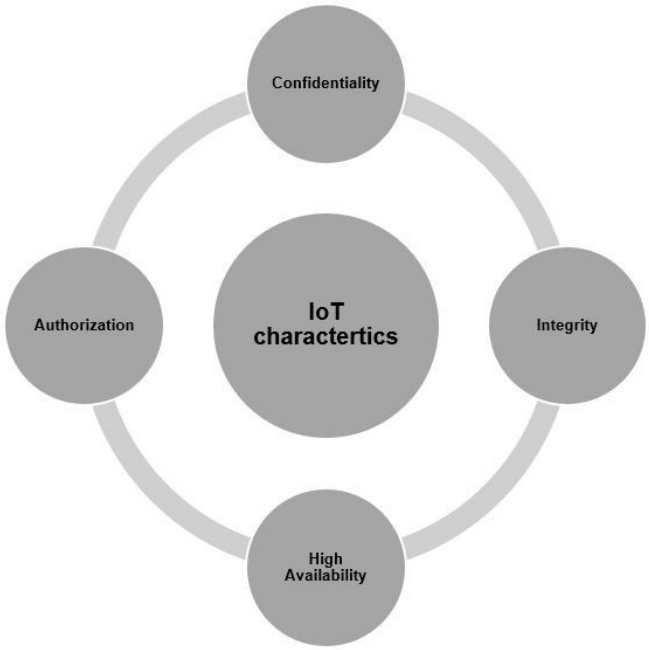

Fig. 3. IoT Characteristics

E. Importance of Decentralized Security in IoT

Technology's expansion and advancement are reaching ever-new, loftier levels. The most innovative items are still being released daily as a result of competition between businesses. This fosters competition among the businesses and could force a product to be rushed into production in order to meet consumer demand, which increases the risk that the product will contain risks due to the hurried nature of the manufacture. We should all place a high priority on safeguarding our privacy and personal information. Our privacy is something that we take very seriously since we do not want any of our personal information to fall into the wrong hands.Identity theft could happen if the data is acquired by someone with malicious intent. Many companies consider the necessity to safeguard customers' privacy and safety while creating new products. On the internet of things, data and privacy protection is a crucial concern. In relation to the breadth of the topic at hand, the amount of information offered here is relatively sparse. You expose threats and new applications to attackers who may quickly notice a mistake in the code and miss use as these apps grow bigger and bigger and as smart devices become smarter and smarter. IoT solutions must therefore offer Confidentiality, Authenticity, High Availability, Data Privacy, and Authorization [15]. A centralised system in which devices are managed, identified, and approved centrally is the Internet of Things (IoT) ecosystem. Blockchain offers a decentralised administration and authentication mechanism that can uphold users' rights to safety and privacy. In contrast to centralised approaches, Blockchain offers security, authentication, and trust management in both distributed and decentralised IoT environments [14].

III. Blockchain

A. Blockchain Types

Public Blockchain: Public Blockchain is decentralised; there isn't a single organisation in control of the whole Blockchain network. As a result, once newly uploaded data has been confirmed on the Blockchain, it cannot be changed. The primary advantage of an open Blockchain is that users may freely enter and access data since the ledger is distributed rather than centralised. It is also safe because of the 51 percent rule, which asserts that "no one can achieve dominating power on this network." [16]

Private Blockchain: A Blockchain that is controlled by an individual or a company is referred to as a "Private Blockchain." In contrast to a Public Blockchain, there is a fee in this world to allow limited access to read if you engage in activities like reading or writing. The choice of whether to provide mining rights to anyone is made by the manager of the central office. [17]

B. Blockchain consensus

A consensus is a method or technique used in distributed processes or systems to establish mutual confidence amongst the participating nodes. Because IoT is a network of heterogeneous items using a variety of technologies, it is difficult to build trust amongst all the participating nodes. Blockchain's consensus process provides a robust validation method for the

IoT. The process of the consensus protocol verifies whether the information should be introduced to the network or not.

One of the key advantages of Blockchain technology is its capacity to verify a block's trustworthiness in a decentralised, trustless setting without the need for a dependable third-party authority. Trustworthiness in a decentralised environment may be verified via consensus algorithms. Realistic Byzantine fault tolerance (BFT), proof-of-work, and proof-of-stake are some of the consensus techniques used in Blockchain technology. [18]

C. Blockchain smart contract

In the 1990s, a computerised transaction protocol known as "smart contracts" was created to carry out an agreement's contractual duties. When a given condition is satisfied, the predefined terms of smart contracts take instant effect. Smart contracts are a significant leap in Blockchain technology. Smart contracts are made feasible by Blockchains. In essence, Blockchains serve as the foundation for smart contracts. The acceptable contract provisions are converted into a computer programme that may be executed. [18]

The goal of a Blockchain smart contract consensus protocol is to offer a mechanism for recording and verifying conversations that occur throughout the whole distributed network. An IoT device engaging with the network can carry out a smart contract by simply sending an exchange to its location, without the need for third-party intervention. This Blockchain smart contract idea aids in the verification and validation of transactions before they are committed in IoT. [19]

IV. Proposed Design

Several authors are using blockchain as a way to overcome security gaps in IoT deployments by taking advantage of decentralised management. [20] presented a WiFi-based long distance network concept (WILD) integrating with blockchain. [21] addressed using RaspberryPi to create a blockchain network that may be used in the pharmaceutical sector.

The proposed design is cost efficient for smart environments like smart homes, smart green house, smart warehouses. This Design uses low-cost computing devices such as Raspberry Pi which acts as an edge node which can work with provided power supply and uses WiFi, Bluetooth to connect to surrounding devices and network. It's external storage capability helps to deploy Blockchain to achieve secrecy, integrity, and high availability.

A. Raspberry Pi

Raspberry Pi was created in the United Kingdom by the RASPBERRY PI foundation to encourage smart learning and teaching basic computer science to the younger generation. In 2012, they began creating minicomputer boards in partnership with the tech society Broadcom. In the same year, the first Pi model was released. This credit card-sized small board computer is capable of doing many activities that a regular desktop or computer can, without the size. Raspberry Pi is a bare-bones personal computer that is very affordable. It focuses on encouraging people to learn, and its low cost makes it more accessible to individuals on a low income or living in a disadvantaged residential area. [22]

B. Ethereum Blockchain

The Blockchain is a type of data structure that primarily comprises of data in a linked list-like sequential format. All of the participants will receive copies of the data, which is kept in the form of a ledger. Since encryption is used to ensure that information cannot be changed or faked, decentralised ledger based on the data structure may be maintained safely and securely. Every two transactions are sequentially tied to one another, and the block enables users to view every transaction's history. This level of transparency is offered to a large extent. [23]

The most recent block is made up of a timestamp, some data, and the cryptographic hash value of the previous block appended sequentially. No one entity has control over the ledger because of the distributed nature of Blockchain; instead, the participating peers confirm the accuracy of each block. Since the Blockchain operates without the involvement of a central authority, it is desirable for all of the network's nodes to resolve disagreements, prevent security breaches, monitor currency flow, and provide an indisputable exchange in order to stop fraudulent operations.The consensus method is the process by which every node determines that a piece of shared material is correct and that the message added to the block is correct. [23]

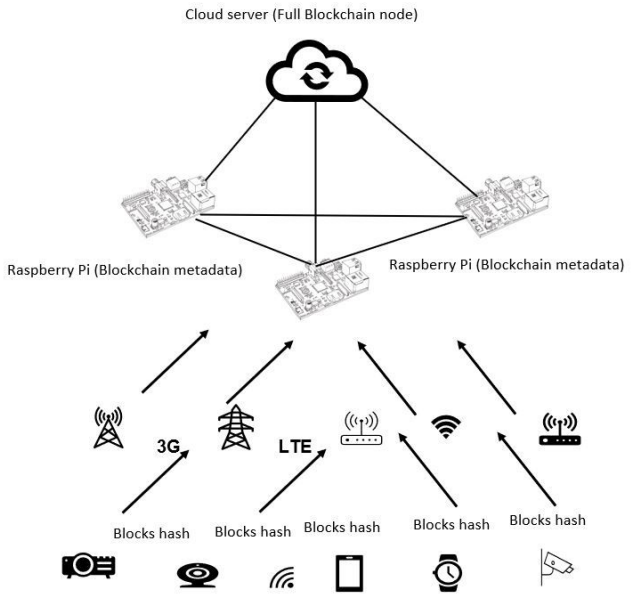

Fig. 4. BRIoT Architecture

Storage of the whole Blockchain at IoT devices is difficult due to multiple limitations. To overcome the storage and computation limitation the possible options are storing Blockchain nodes data in three levels

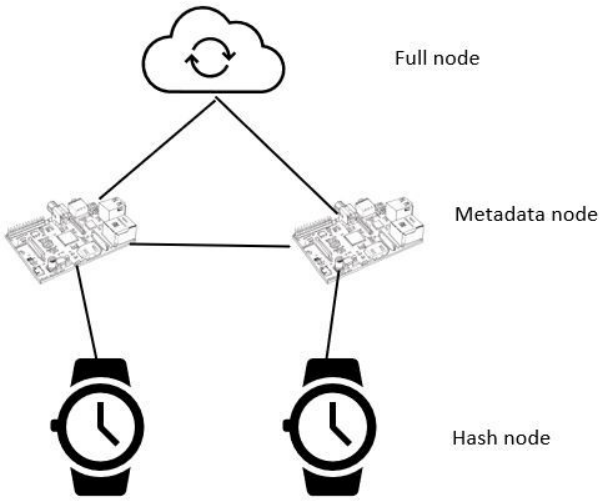

Fig. 5. BRIoT Storage

- A complete or full node or entire Blockchain information, which is a node that stores the whole Blockchain in the cloud server which possess enough storage and computational power.
- Semi node or metadata node, in which metadata (only the timestamp and hash value of each block's metadata) is stored which contains only blocks information on Raspberry Pi.
- Storage of Block chain hash information on IoT objects.

V. Conclusion

Blockchain aspires to change the next generation of IoT. The proposed design overcomes existing IoT vulnerabilities like storage, power supply and processing capability also this paper has offered an analysis of the interplay between Blockchain technology and the Internet of Things. Articles on the Internet of Things, IoT security utilising Blockchain, Blockchain scalability in IoT, and new problems and potential in IoT have been covered here. For a successful Blockchain and IoT integration, an investigation of the major difficulties of Blockchain and IoT integration should be conducted, taking into account the concerns stated in this study. In the future, we plan to examine how Blockchain and IoT may complement one other in their integration utilising edge computing, as well as how Blockchain technology can address edge computing's various security and data integrity challenges.

References

1 Bryant, B. and Saiedian, H., "Key challenges in security of iot devices and securing them with the blockchain technology," *Security and Privacy*, vol. 5, no. 5, p. e251, 2022.

2 Kumar, V., Laghari, A. A., Karim, S., Shakir, M., and Brohi, A. A., "Comparison of fog computing & cloud computing," *Int. J. Math. Sci. Comput*, vol. 1, pp. 31–41, 2019.

3 Cao, K., Liu, Y., Meng, G., and Sun, Q., "An overview on edge computing research," *IEEE access*, vol. 8, pp. 85 714–85 728, 2020.

4 Panarello, A., Tapas, N., Merlino, G., Longo, F., and Puliafito, A., "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

5 Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., and Janicke, H., "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

6 Sanislav, T., Mois, G. D., Zeadally, S., and Folea, S. C., "Energy harvesting techniques for internet of things (iot)," *IEEE Access*, vol. 9, pp. 39 530–39 549, 2021.

7 Kassab, W. and Darabkh, K. A., "A–z survey of internet of things: Architectures, protocols, applications, recent advances, future directions and recommendations," *Journal of Network and Computer Applications*, vol. 163, p. 102663, 2020.

8 Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., and Du, H.-Y., "Research on the architecture of internet of things," in *2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, vol. 5. IEEE, 2010, pp. V5–484.

9 Gokhale, P., Bhat, O., and Bhat, S., "Introduction to iot," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, no. 1, pp. 41–44, 2018.

10 Muhammad, F., Anjum, W., and Mazhar, K. S., "A critical analysis on the security concerns of internet of things (iot)," *International Journal of Computer Applications*, vol. 111, no. 7, pp. 1–6, 2015.

11 Bekkai, B., Bendjenna, H., and Kitouni, I., "Internet of things: A recent survey," in *2021 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI)*. IEEE, 2021, pp. 1–9.

12 Ikrissi, G. and Mazri, T., "Iot-based smart environments: State of the art, security threats and solutions." *ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences*, 2021.

13 Jiang, X., Lora, M., and Chattopadhyay, S., "An experimental analysis of security vulnerabilities in industrial iot devices," *ACM Transactions on Internet Technology (TOIT)*, vol. 20, no. 2, pp. 1–24, 2020.

14 Roy, S., Ashaduzzaman, M., Hassan, M., and Chowdhury, A. R., "Blockchain for iot security and management: Current prospects, challenges and future directions," in *2018 5th International Conference on Networking, Systems and Security (NSysS)*. IEEE, 2018, pp. 1–9.

15 Detres, W., Chowdhury, M. M., and Rifat, N., "Iot security and privacy," in *2022 IEEE International Conference on Electro Information Technology (eIT)*. IEEE, 2022, pp. 498–503.

16 Subramanyam, M. S. and Jyothi, C., "A review on iot security with blockchain."

17 Shah, R., "A systematic review on blockchain in iot," in *2022 4th International Conference on Energy, Power and Environment (ICEPE)*. IEEE, 2022, pp. 1–6.

18 Dai, H., Zheng, Z., and Zhang, Y., "Blockchain for internet of things: a survey. ieee internet things j 6 (5): 8076–8094," 2019.

19 Cp, V., Kalaivanan, S., Karthik, R., and Sanjana, A., "Blockchain-based iot device security," in *2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP)*. IEEE, 2022, pp. 1–6.

20 Kaushik, I. and Prakash, N., "Applicability of iot for smart agriculture: Challenges future research direction," in *2021 IEEE World AI IoT Congress (AIIoT)*, 2021, pp. 0462–0467.

21 Fernando, E., Meyliana, and Surjandy, "Blockchain technology implementation in raspberry pi for private network," in *2019 International Conference on Sustainable Information Engineering and Technology (SIET)*, 2019, pp. 154–158.

22 Mahmood, S., Palaniappan, S., Hasan, R., Sarker, K. U., Abass, A., and Rajegowda, P. M., "Raspberry pi and role of iot in education," in *2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)*, 2019, pp. 1–6.

23 Ranganthan, V. P., Dantu, R., Paul, A., Mears, P., and Morozov, K., "A decentralized marketplace application on the ethereum blockchain," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2018, pp. 90–97.