Turkish Journal of Computer and Mathematics Education Vol.12 No.7 (2021), 549-554

Research Article

Blockchain Technology for IoT Security

Shameemul Haque[1] , Kailash Kumar[2] , Md Alimull Haque[3] , Md Faizanuddin[4] , Ejaz Shakeb[5], Amrendra Kumar Singh[6]

[1]Al Hafeez College,Veer Kunwar Singh University ,Ara – 802301, India ,shameem32123@gmail.com
[2]College of Computing & Informatics ,Saudi Electronic University, Riyadh-11673, ,Kingdom of Saudi Arabia k.kumar@seu.edu.sa
[3]Department of Computer Science,Veer Kunwar Singh University,Ara – 802301, India ,shadvksu@gmail.com
[4]Department of Commerce & Business Management, Veer Kunwar Singh University ,Ara – 802301, India
[5]Department of Computer Scince,Community College Riyadh ,Kingdom of Saudi Arabia ,eshakeb@gmail.com
[6]Jai Prakash College,Veer Kunwer Singh University
f_uddin2000@yahoo.com **,** akshakrawar@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 April 2021

Abstract – The Internet of Things (IoT) promoted a common operating picture (COP) through all modern applications. The COP is takes place only accomplished by the developments seen in wireless sensor network devices that have been able to connect through the network, sharing information, and conducting further analysis. In IoT, knowledge sharing and authentication of data through the central server and is hence vulnerable to security and privacy problems. System spoofing, false authentication, less data sharing reliability may take place. As part of IoT, Blockchain (BC) technology is integrated to solve these security and privacy issues by replacing the idea of the central server. This paper discusses the potential protection and privacy threats of IoT component activity and explores how it relates to distributed ledger-based blockchain (DL-BC) technologies. . Blockchain implementations have explicitly been studied here with regard to focused sectors and categories. This paper also discusses Blockchain technology, its contribution, and challenges specific to IoT.

Keywords: Internet of Things, IoT Security, Privacy, Blockchain, Distributed Ledger

I. INTRODUCTION

The Internet of Things (IoT) is an innovative technology that has grown and accrued enormous scope without human intervention to solve problems in science and engineering applications. It makes it possible to construct a machine-to-machine and human-to-machine interaction i.e. a smart workforce. The COP is accomplished by the improvements made in wireless sensor network devices that have been used to link and conduct distinct analysis through the network sharing data[1]. Therefore IoT is a mixture of various technologies that work to achieve smartness[2]. Communication technologies, information technology, Sensors, actuators and developments in computation and analytics are among these developments.

It may be challenging and daunting to discuss the integration of all those developments when operating from a broader and larger implementation point of view[3]. The major problem in wireless network is data security[4]. The complicated size of system connectivity, network
interconnection, and dispersed design of IoT stuff provides an understanding of the principle of the central server where all the authentication stuff or gadget is required to transmit on it. In this case, the interconnection of the devices will become questionable, causing false authentications or facilitating system spoofing that leads to an unreliable data flow. These projections forecast that twenty billion physical things will be connected to the internet and operate as a single network under the IoT by the end of 2020[5]. This assertion implies that by linking to a network of abundant things (NAT), allowing for digital connectivity, IoT could get even more complex shortly. In such situations, a massive amount of information from the inclosing boundaries or the applications or concentrate environment could be accessed by the NAT devices. These devices must connect with a computation and analytics infrastructure defined by the network and applications. This process is carried out completely over the internet and is moved to a central server storage point. This can lead to serious IoT protection and privacy problems that render it a struggle to encounter[6]. In order to resolve IoT protection and privacy concerns, by implementing the proposed blockchain technology, we will eradicate centralized maintenance of the NAT generated data. This paper reflects on the use of IoT blockchain technologies by evaluating data interruptions and security issues during interactions between IoT devices.

II. LITERATURE REVIEW

Alamri et al.[7] presented an analysis of IoT integration with blockchain by discussing benefits and limitations in detail, while Dukkipati et al. [8] proposed a blockchain-based access management model to address IoT protection and privacy problems, which is the biggest issue that IoT is facing today. Lao et al. [9] evaluated the core elements required to incorporate blockchain with IoT, which can help in securing data. Polyzos and Fotiou [10] The blockchain as an IoT service is introduced to illustrate how different aspects of blockchain technologies can be implemented as a service for multiple IoT implementations. Blockchain's ability

to address IoT security challenges has been checked. Atlam and Wills [11] Checked the convergence with the IoT system in distributed ledger systems. The current unified Iota architecture has different concerns, such as a single point of failure, reliability, protection, transparency, and data integrity. These barriers are a barrier to IoT applications' potential development. Shifting the IoT into one of the distributed ledger technologies might be the right solution to solve these issues. They have discussed the IoT system's blockchain and its core potential and obstacles. Karthikeyan et al. [12] A analysis of IoT security concerns was discussed, and then the blockchain was introduced as a suggested way to address these problems. Fotiou et al.[13] proposed a smart contract-based approach to overcome security and privacy issues of the IoT system and make it secure for the IoT device to be connected. This indicates a variety of frameworks in which blockchains are able to communicate with external systems and data sources from third parties.

III. CHALLENGES AND CONCERNS IN IOT

While the IoT has many advantages and can address a wide variety of problems in diverse fields, privacy and security challenges still exist. This section illustrates the different probable issues on IoT devices communications.

1. Challenges in IoT

IoT challenges are mainly associated to security and privacy issues. In addition to these, interoperability, the dearth of standards, regulatory issues, legal challenges, right issues, and developmental and economic issues of IoT is also a matter of great concern.

2. Security and Privacy Issues in IoT

IoT has brought tremendous advantages for users; some challenges, though, come with it. The key issues of the security experts and researchers cited are cybersecurity and privacy risks. For both private entities as well as governmental bodies, all of these are a big concern. IoT infrastructure vulnerabilities have been revealed by prevalent high-profile cryptography attacks. This vulnerability is simply because the Internet of Things network interconnectivity offers anonymous and untrusted internet mobility that needs new security solutions[14]. None of the issues are known to have a greater impact, such as protection and privacy, on IoT adaptation. It is tragic, though those consumers do not always have the requisite awareness of the safety consequences before a violation has occurred, causing massive harm, such as loss of vital data. With recent security vulnerabilities that have compromised the privacy of consumers, customers' appetite for sufficient protection is rising. In a recent research carried out on privacy and protection, the consumer-grade Internet of Things did not do well. There have been many difficulties with bugs in the new industrial automobile infrastructure. In addition to the above problems, unconscious use not updating passwords, and the absence of device upgrades have increased safety threats and access to the confidential data of the IoT systems to malicious applications. The risk of data leaks and other threats is raised by these improper security practices.

A. Security Issues

Perhaps the biggest challenge of the IoT is Authentication, confidentiality, and lack of optimal control on IoT device communication model to prevent threats from cyber-attacks and hijacking. There is also a lack of guidelines and benchmarks to describe IoT system protection. The absence of security laws or regulations of IoT devices or software development is also a concern. The IoT is distinct from conventional computers and computing systems, rendering it more vulnerable in numerous ways to security issues. Many systems are planned for application on a large scale, such as sensors and actuators on the Internet of Things. Usually, the implementation of the IoT consists of a set of similar devices with similar functionality. This connection amplifies the scope of any vulnerability that can change them all significantly. Similarly, several organizations have developed manuals for performing risk management. This move means that there is no precedent for the likely number of contacts linked to IoT devices. It is also evident that all of these devices can create contacts and irregularly communicate with other devices. These call for the consideration of IoT security-related open methods, strategies and tactics.

B. Privacy Issue

A major concern is not having proper protection against the data gathered by IoT devices and also there are still no specific guidelines for the details obtained by IoT devices.

C. Interoperability

Absence of documented standards for best design practices can have technical design risk protocols. If there is an interface of many IoT devices, then there is a lack of standard configuration. If the devices start behaving erratically, then also there is no standard documentation.

D. Legal and Regularity rights issues

Less progress has taken place in the areas of data sharing, trust policies, rules and regulations, making it impossible to combat data theft and crime.

E. *Development & Economic issues*

There is more strain on the internet, communications infrastructure, and very little has been done to strengthen the internet and communication infrastructure. There has been relatively little study to assess the technological and economic advantages of IoT in developed countries. With the continuing rise of the IoT, there

is so little understanding of policy plans. There is also an issue of insufficient funding in IoT research and development programs in developed as well as developing countries. The authors presented the different facets of security and privacy along with the IoT's interaction analysis[15]. The Things with Networked sensors and actuators (TNSA), Raw information and stored data storage (R-IP-DS), Analytical and computational engines (ACE) are three key components of the IoT. The relationship between these three components of the IoT was briefly analyzed to show the likelihood of issues with security and privacy occurring. A view of the schematic relationship between TNSA, R-IP-DS and ACE is depicted in figure1.From the interaction viewpoint, the data flow would come from the data collection unit i.e., networked sensors and actuators, to the information processing and storage unit. During the data flow process, there is a possibility of missing and mishandling the data. Data flowing across the internet with those protocols may deceive or misrepresent externally affected protocols. . The flow of data processes may be manipulated by hackers, for example. External users can hack or monitor the computing engines during the second interaction between R-IP-DS and ACE. In this case, there is a chance of observational interruptions. The third interaction is between the ACE and the TNSA, where it is essential to give feedback according to the computing algorithms and function accordingly. Chances of hacking and destructive influence of the feedback loop are also likely here. Apart from interactions between these three elements, there are also chances of missing the data in each component utilizing incorrect protocols. Therefore, the security and privacy problems in IoT have an immense reach, which may also be a major problem in the implementation of large-scale IoT.

IV. TYPES OF E-LEARNING

Fig.1. IoT component interaction [16]

IV. CAN BLOCKCHAIN TECHNOLOGY BE AN ANSWER TO THE ISSUES OF IOT?

Yes, one of the remedies to fix IoT security and privacy problem will be blockchain technology. This is because the blockchain technology replaces the IoT's central server principle and makes it possible for the data to flow through the decentralized blockchain ledger with each transaction with sufficient verification.

1. Blockchain Technology

Blockchain technology has grown with the rise and interest seen in the crypto-currencies called Bitcoin. Blockchain infrastructure is behind Bitcoin's growth and is the core factor. In a wide range of implementations, Blockchain is a tamper-proof ledger-based infrastructure that serves multiple use cases.

In general, considering increasing variables and data sample sets obtained, the BC represents a continuously processed and controlled database. The participant-created transactions and the recording blocks of those transactions are the main elements of BC. Here, the recorder block verifies whether transaction records have been kept in the right sequence or not. This does not allow the available data to be tampered. There is the need for a chain solution where the information recorded must be kept in chronological order. This stored transaction was shared with the network of nodes that were involved. This replaces the idea of the central server by using cryptography in the transaction exchange method to identify each node. This makes safe authentication possible[17].

2. IoT with Blockchain Architecture

It has become a must to combine blockchain with IoT to solve the challenges of the centralized IoT architecture and to exploit the myriad advantages of blockchain technology. It can be done in various ways to incorporate the blockchain with IoT. This segment includes a discussion on one of the techniques in a layered architecture to incorporate blockchain with the IoT. Four layers compose the basic layered blockchain with IoT architecture. The blockchain is added as a separate layer between the network and application layers in the IoT architecture, as seen in Fig. 3.

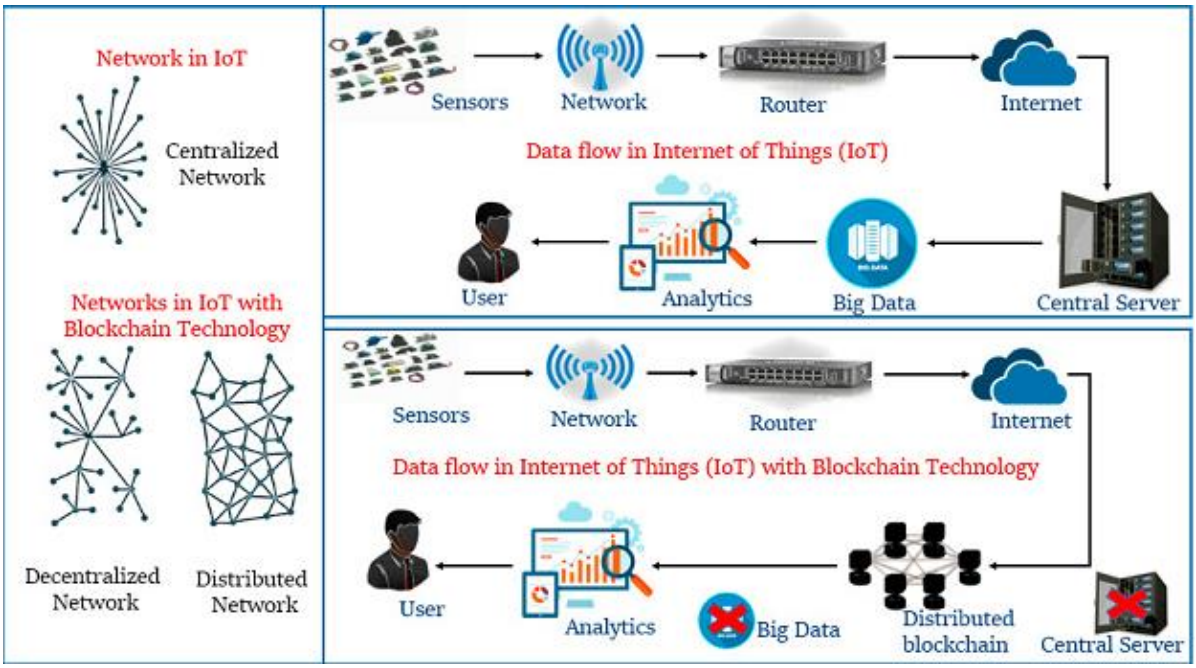

Fig.2. Network in IoT, flow of data in IoT, flow of data with blockchain in IoT [18]

3. Blockchain Technology Solutions to IoT

Blockchain applications can offer a better approach to the issues facing IoT networks. There are greater chances of getting an increased number of interacting devices in the growing scenarios of IoT networks. This increased number of devices will aim to connect via the internet using each of them as a tool. This can contribute too many issues because all of the information collected has been preserved in the central repositories. The flow of this method is clearly expressed in Fig.2. But the growing demands of IoT and its implementations have presented IoT as a large-scale device with sophisticated technology integration. The unified server would not be an optimal solution to such large-scale IoT systems [19]. The idea of a centralized server concept is the foundation of all of the IoT systems currently implemented. The sensor devices collect data from the targeted objects in IoT systems and allow data transmission through wired/wireless network refereeing to the central server as the internet. Analytics from the single framework was performed according to client expectations and ease. Similarly, if the research were to be carried out by a large-scale IoT system, the computing capacities of the modern internet are to redesign the internet infrastructure. One of the best solutions to solve this is to provide the functions "Peer-to-Peer Networking (PPN), Distributed File Storage (DFS) and Autonomous Machine Coordination (ADC)" for decentralized or distributed networks. These three functions can be performed via Blockchain, enabling IoT networks to monitor the vast number of linked devices and networks. BC helps the IoT systems in collaboration to handle transactions between the devices. BC would improve IoT systems' privacy and reliability and make them stable. BC enables peer-to-peer exchange in a faster manner with the aid of a distributed ledger. The IoT data flow system with BC technologies differs from the IoT process alone. The data sources are sensors-network-router-internet-distributed blockchain-analytics-user-in IoT with BC. The distributed ledger here is tamper-proof and would not misinterpret the findings of erroneous authentications. The Single Thread Contact (STC) in IoT is easily removed by BC, rendering the device stable. The data flow would be more reliable and secure with the implementation of the BC in the IoT [18].

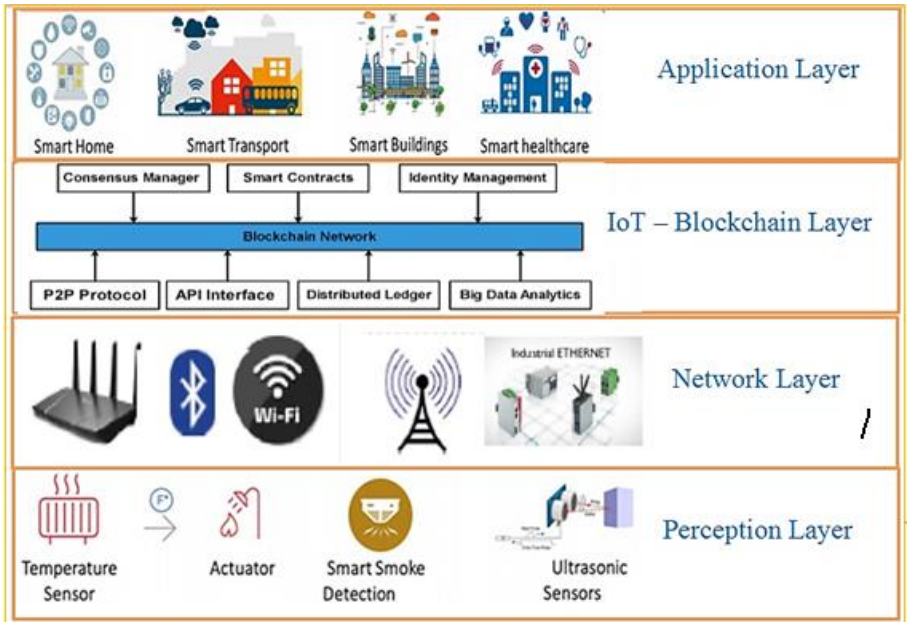

Fig.3. IoT Architecture with Blockchain

4. Blockchain technology has the following merits for large scale IoT systems.

- Blockchain can be used to manage and record measurements of sensor data while minimizing unwanted replication of malicious information.
- IoT system recognition, authentication and data transfer within distributed ledger architecture are all seamless.
- Instead of a third party controlling body; IoT devices can transfer data through a secure and trusted blockchain.
- Thanks to the native cryptographic procedures of blockchain, IoT devices are safe from data tampering.
- As there is no intermediary, initial implementation and running costs of IoT devices are reduced via blockchain.
- Inside the blockchain, IoT devices are directly addressable, offering a background of related devices and their details for troubleshooting and analytics purposes.

Blockchain technology also increases cost-efficiency in a system, in addition to security advantages. When a given requirement is met, Blockchain smart contracts will activate automatically, allowing system control and eliminating technological bottlenecks and inefficiencies, without the need for human interference.

5. Applications of Blockchain Technology

IoT blockchain implementations are infinite, undermining current systems across a number of sectors, including the banking market, commerce, retail, healthcare, automobile, manufacturing, mining, agriculture, and construction automation.

6. Challenges in Blockchain Technology Integrated IoT

Although when combined with IoT, blockchain technology could solve IoT's privacy and reliability concerns. BC technology, however, still has certain drawbacks that make it a challenge. Such challenges include the restriction of the ledger storage facility, restricted technical advances, shortage of qualified staff, lack of acceptable legal codes and requirements, processing speed and time improvements, computational capacities and difficulties with scalability.

V. CONCLUSIONS

With several concerns in the centralized IoT architecture, bringing the IoT into a distributed ledger systems may be the correct decision. The blockchain is among the different kinds of distributed ledger technology. It uses a decentralized approach that increases productivity and removes the single point of failure. Also blockchain, via tamper-proof and immutability functionality, provides improved authentication and data transparency. Incorporating the IoT blockchain can address IoT centralized structure challenges and offers the right way for future technologies. The goal of this paper, therefore, was to provide a detailed discussion on the integration of blockchain technology with the IoT system. After outlining the foundations of IoT, the paper presented a comprehensive discussion of integrating IoT with blockchain. The paper answered the topic of how blockchain would overcome IoT system problems. Also, recent developments are discussed, along with integrating the blockchain with IoT. Blockchain as an IoT utility is then addressed to illustrate how it is possible to apply different aspects of blockchain technology as a service for various IoT applications.

VI. FUTURE WORK

We also plan to incorporate blockchain properties for tracking, error detection, and automated fault repair in extremely sensitive IoT applications on the Internet. Also, simulation-based performance measurement can be carried out to show the scalability and reliability of blockchain-based technologies. Since IoT devices are in publicly available areas and potentially under an opponent's influence, it is possible to introduce a blockchain-based solution that can ensure the protection and secrecy of the information stored in the devices. It would also reduce the risk of an IoT computer's hardware and software being exploited if the device is open to anyone.

.

REFERENCES

1. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.
2. N. Manoj Kumar and A. Dash, "Internet of Things: An Opportunity for Transportation and Logistics," in Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017), 23rd to, 2017, pp. 194–197.
3. N. M. Kumar, A. Dash, and N. K. Singh, "Internet of Things (IoT): An Opportunity for Energy-Food-Water Nexus," in 2018 International Conference on Power Energy, Environment and Intelligent Control (PEEIC), 2018, pp. 68–72.
4. M. A. Haque, M. U. Bokhari, A. K. Sinha, and N. K. Singh, "Comparative study on Wireless threats and their Classification," in INDIACom-2017; IEEE Conference ID: 40353 2017 4th International Conference on "Computing for Sustainable Global Development", 01st - 03rd March, 2017 BVICAM, 2017, pp. 5057–5059.
5. B. Nguyen and L. Simkin, "The Internet of Things (IoT) and marketing: the state of play, future trends and the implications for marketing." Taylor & Francis, 2017.
6. A. Banafa, "IoT and blockchain convergence: benefits and challenges," IEEE Internet Things, 2017.
7. M. Alamri, N. Z. Jhanjhi, and M. Humayun, "Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review," Int. J. Comput. Sci. Netw. Secur, vol. 19, pp. 244–258, 2019.
8. C. Dukkipati, Y. Zhang, and L. C. Cheng, "Decentralized, blockchain based access control framework for the heterogeneous internet of things," in Proceedings of the Third ACM Workshop on Attribute-Based Access Control, 2018, pp. 61–69.
9. L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," ACM Comput. Surv., vol. 53, no. 1, pp. 1–32, 2020.
10. G. C. Polyzos and N. Fotiou, "Blockchain-assisted information distribution for the Internet of Things," in 2017 IEEE International Conference on Information Reuse and Integration (IRI), 2017, pp. 75–78.
11. H. F. Atlam and G. B. Wills, "Intersections between IoT and distributed ledger," in Advances in Computers, vol. 115, Elsevier, 2019, pp. 73–113.
12. P. Karthikeyyan and S. Velliangiri, "Review of Blockchain based IoT application and its security issues," in 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2019, vol. 1, pp. 6–11.
13. N. Fotiou, V. A. Siris, and G. C. Polyzos, "Interacting with the Internet of Things using smart contracts and blockchain technologies," in International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, 2018, pp. 443–452.
14. K. K. and N. K. S. Md Alimul Haque, Shameemul Haque, "A Comprehensive Study of Cyber Security Attacks, Classification and Countermeasures in the Internet of Things," in Digital Transformation and Challenges to Data Security and Privacy, IGI Global Publisher(Accepted), 2021.
15. K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," Internet Soc., vol. 80, pp. 1–50, 2015.
16. N. M. Kumar and P. K. Mallick, "The Internet of Things: Insights into the building blocks, component interactions, and architecture layers," Procedia Comput. Sci., vol. 132, pp. 109–117, 2018.
17. A. A. Aljabr, A. Sharma, and K. Kumar, "Mining Process in Cryptocurrency Using Blockchain Technology: Bitcoin as a Case Study," J. Comput. Theor. Nanosci., vol. 16, no. 10, pp. 4293–4298, 2019.
18. N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," Procedia Comput. Sci., vol. 132, pp. 1815–1823, 2018.
19. R. Maharajh, "Digital Liberty, the Knowledge Commons and some Challenges for the Governance of Information and Communication Technologies and the Internet for Brazil, Russia, India, China and South Africa," 2015.