IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008093 |

Analysis of Blockchain Mechanism for Security issues and Challenges in IoT

Noothi Manisha[1], Dr. M. Jagadeeshwar[2]

Research Scholar, Department of Computer Science, Chaitanya (Deemed to be University), Hanamkonda, Warangal, India[1]

Professor, Department of Computer Science, Chaitanya (Deemed to be University) Hanamkonda, Warangal, India[2]

ABSTRACT: The internet of things (IoT) enabled a common operating picture (COP) across the various applications of modern day living. The COP is achieved through the advancements seen in wireless sensor network devices that were able to communicate through the network thereby exchanging information and performing various analysis.In IoT, the exchange of information and data authentication is only done through the central server there by leading to the security and privacy concerns. Chances of device spoofing, false authentication, less reliability in data sharing could happen. To address such security and privacy concerns, a central server concept is eliminated and blockchain (BC) technology is introduced as a part of IoT.

This paper elaborates the possible security and privacy issues considering the component interaction in IoT and studies how the distributed ledger based blockchain (DL-BC) technology contribute to it.Applications of BC with respect to focused sectors and category were clearly studied here. Various challenges specific to IoT and IoT with BC were also discussed to understand blockchain technology contribution.

KEYWORDS: The IoT, IoT Security; Challenges in IoT; Blockchain Technology, Applications of Blockchain Technology; IoT-BC; Central Server in IoT.

I. INTRODUCTION

The Internet of Things (IoT), an evolutionary technology that raised and gained huge scope in the science and engineering applications solving problems without the intervention of human-human work force. It enables mostly smart work force the internet of things (IoT) enabled a common operating picture (COP) across the various applications of modern day living[1].The COP is achieved through the advancements seen in wireless sensor network devices that were able to communicate through the network thereby exchanging information and performing various analysis. From this point one must clearly understand that IoT is not a single technology, it is a combination of multiple technologies that would work for the smartness achivement. . These technologies include communication technology, information technology, electronic sensor and actuator technology, and the trending advancements in computing and analytics. The integration of all such technologies could make it complex and difficulty in handling when working on wider and large application point of view. The complex scale of device integration, network interconnection, and distributed nature of the things in IoT gives a scope for central server concept where all the things or the devices would compulsory relay on it for authentication. In this case the interconnection between the devices would become unreliable allowing the data sharing with false authentications or allowing device spoofing leading to insecure data flow. The IoT could be become much more complex in the coming future by connecting to a Network of Plentiful Things (NPT) making a provision for digital access. In such cases, the NPT devices could obtain enormous amount of information from the inclosing boundaries or the application or focus environment. These devices must communicate with the network and software defined computing and analytics platform, and this process is completely done through internet and leading to a point of central server storage. This communication result in the rich interactions between the things and network it architecture, giving scope for huge data generation allowing reliable and trustworthy services over the wide area network of things through the Centralized Data Management Servers (CDMS). To address the security and privacy issues in IoT, we can eliminate centralized maintenance of the NPT produced data and thereby introducing the new Distributed Ledger-based technology called a blockchain technology. This paper focuses on the blockchain technology in IoT by analyzing the possible data interruptions and security concerns during the IoT component interaction.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008093 |

II. RELATED WORK

The web of Things (IoT) portray the system of physical items "things"- that are inserted with sensors, software's, and different advances for the reason and frameworks over the web. These gadgets go from customary family unit items to modern mechanical apparatuses. With in excess of 7 billion associated IoT gadgets today, experts are expecting this number to develop to 10 billion by 2020 and 22 billion by 2025. IoT has become the focal point of numerous disclosures to screen issues and moves identified with its plan and design.

Even though, IoT has several benefits and able to solve wide range of problems in various sectors, still the challenges exist. These challenges might be in the form of overcoming the security issues, privacy concerns etc. This section briefly explains the various possible issues by considering the study on the IoT component interaction. Mostly the challenges it are related to security and privacy concerns. Apart from these, few other challenges are interoperability, lack of standards, legal challenges, regulatory issues, rights issues, emerging it economy issues, and other developmental issues.
In IoT chances of arising issues in seven different ways were clearly stated in the following Table. The resulting challenges.

Issues	Challenges	Remarks
Security Issues	Design practices	Lack of resources in train future generations about secure out design.
	Cost vs. security trade offs	Lack of informed decisions over cost-benefit analysis of IoT.
	Standards & metrics	Lack of standards and metrics to identify the security IoT devices.
	Confidentiality, authentication and control	Lack of optimally controlled role in it device communication models to prevent the threat of hijacking and cyber attacks.
Privacy concerns	Fairness in data collection and use	Lack of strict rules against data collection and use.
	Transparency, expression and enforcement	Lack of multi-party models that enable transparency, expression and enforcement.
	Wide-ranging privacy expectations	Lack of privacy protection models for IoT and inability to recognize the privacy expectations of users.
	Identification	Lack of protection against the data collected by IoT devices.
Interoperability issues	Proprietary ecosystem and consumer wish	Lack of closed ecosystem concept in data collection format and reuse as per user choice. Individual security keys and protocols could be implemented.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008093 |

	Technical and cost constraints	Limitations to the technical resources and investments
	Schedule risk	Chances of outpacing the interoperability standards.
	Technical risk	Less awareness over the technical design risk protocols.
	Configuration	Lack of standard configurations for interfacing large number of IoT devices.
IoT standards issue	Proliferation of standards efforts	Fewer efforts in developing standards and protocols.
Legal, regulatory, rights issues	Data protection and cross border flow	Fewer developments in data sharing and trust policies, laws, and regulation.
	Discrimination in data	Lack of laws on using the IoT data in discriminatory way
	Device liability	Laws against the liability issues of IoT devices
Emerging economy issues	Investments	Limited investments in IoT research and developmental activities both in developed and developing countries.
Developmental issues	Infrastructure resources	More burden or pressure on the internet and communications infrastructure across the globe. Limited activities in strengthening the internet and communication infrastructure.
	Technical and industrial developments	Limited study to evaluate the technical and economic benefits of it in emerging economic countries.
	Policy and regulatory co-ordination	Less awareness on the policy plans with the continuous of growth of IoT

Here, to make it clearer on the various issues related to security and privacy aspects, the IoT component interaction study is considered. Three major components of IoT are the Things with Networked Sensors and Actuators (TNSA), Raw Information and Processed Data Storage (R-IP-DS), Analytical and Computing Engines (ACE). Fig. 1 shows the schematic interaction view between TNSA, R-IP-DS, and ACE.From the interaction point of view, data flow will start from the data collection unit i.e. Typically some things with networked sensors and actuators to information processing and storage unit, i.e. typically raw information Processing and data storage in the form of report states. During these process chances of losing, mishandling the Data occurs making the data flow process, not 100 %. This data must flow through the internet with some protocols and chances of misleading or misinterpret the protocols with the help of external influence are highly possible, for example, hackers can control the data process flow. During the second interaction between the R-IP-DS and ACE, he computing engines can be hacked or taken control by external users. In

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008093 |

this case chances of analysis interruptions exist. The third interaction is between the ACE to TNSA, here the feedback as per the computing algorithms must be sent and accordingly the things to should act. Here also chances of hacking and negative control over feedback loop are possible. Apart from interactions between these three components, in each individual component also chances of losing the data occur by means wrong protocols. Hence, there is huge scope for the security and privacy concerns in IoT, this even might be a serious problem in large scale IoT implementation.

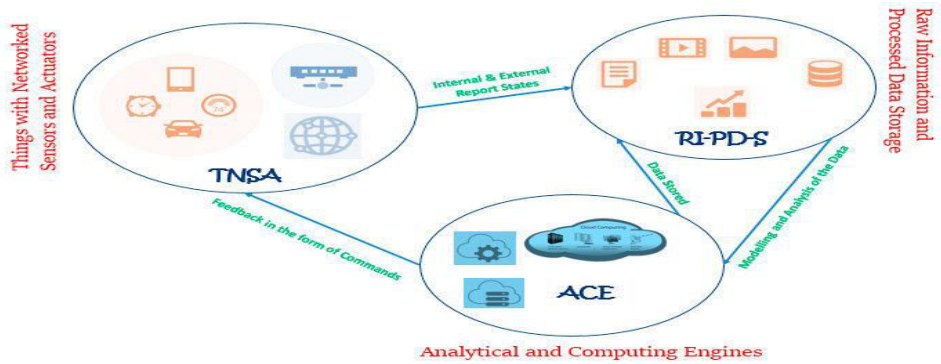


Fig. 1 IoT component interaction

III. METHODOLOGY

Yes. Blockchain technology would be one of the solution for addressing the security and privacy issues in it. This is because; the blockchain technology eliminates the central server concept of IoT and allows the data to flow through the blockchain distributed ledger for each transaction with appropriate authentication. Blockchain is ledger-based tamper proof technology that allows various use cases in wide range of applications. In general, the BC represents a continuously maintained and controlled database considering growing factors and collected data sample sets. The key elements of BC are participant created transactions, and the recorder blocks of such transactions. In general, the BC represents a continuously maintained and controlled database considering growing factors and collected data sample sets. The key elements of BC are participant created transactions, and the recorder blocks of such transactions.

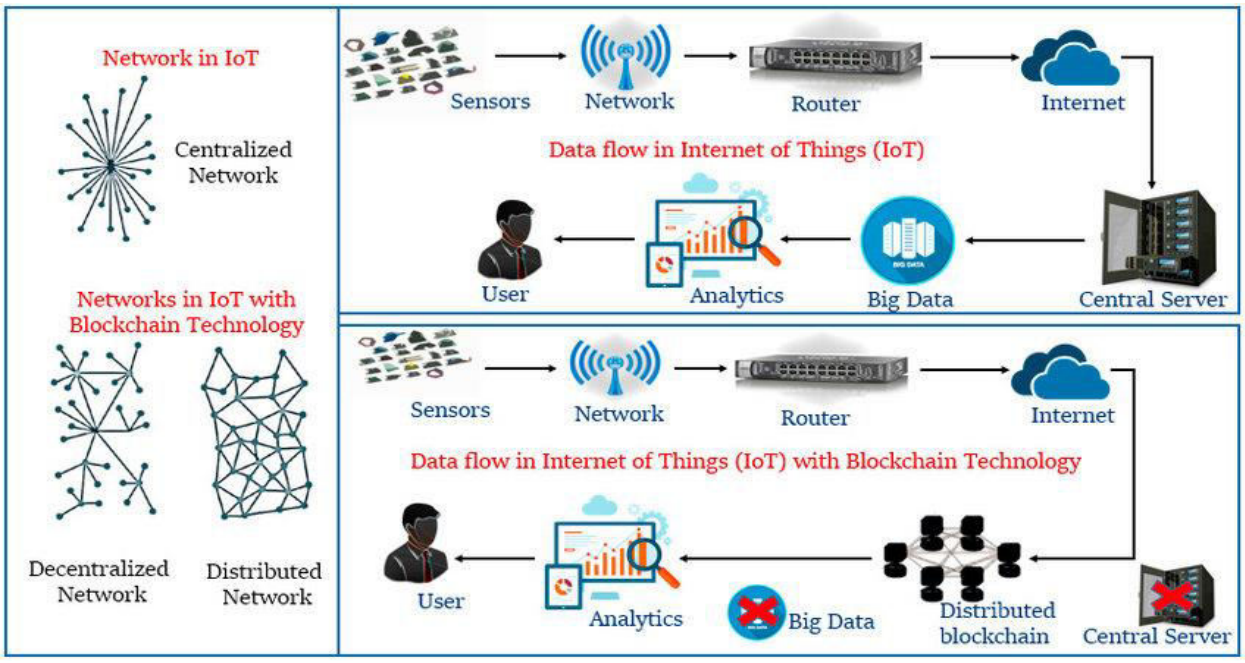


Fig. 2 IoT network types, data flow in IoT, data flow in IoT with blockchain technology

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008093 |

Blockchain technology would give better solution to the problems faced by IoT systems. In the growing scenarios of IoT systems, there are more chances for having increased number of interacting things or devices in it. . This would lead to many hurdles because, in IoT systems, mostly the collected data is maintained in the central servers. If the devices want to access the data they have to interact using the centralized network and the data flow will happen through the central server, this process flow is clearly depicted in Fig. 2. But the growing needs of it and its applications were portraying it as large-scale systems with integration of advanced technologies. In such large-scale IoT systems, the centralized server will not be an effective approach. Most of the IoT systems that are implemented as of now are relying on a centralized server concept. In IoT systems, the sensor devices collect the information from the focused things and allow the data transmission to the central server by means of a wired/wireless network refereeing as the internet. For handling the huge data processed in large scale IoT systems, there is a need for increasing the internet infrastructure. One best way to solve this is to have decentralized or distributed networks where "Peer-to-Peer Networking (PPN), Distributed File Sharing (DFS), and Autonomous Device Coordination (ADC)" functions could be capable. Blockchain can carry out these three functions allowing the IoT systems to track the huge number of connected and networked devices. BC allows the IoT systems to process transactions between the devices in co-ordination. BC will enhance the privacy and reliability of IoT systems making it to be robust. BC allows a peer to peer messaging in faster way with the help of distributed ledger as shown in Fig. 2. The data flow process in IoT with BC technology is different from only IoT system. In IoT with BC, the data flow is from sensors-network-router-internet-distributed blockchain-analytics-user. Here, the distributed ledger is tamper proof which does not allow in misinterpretation, wrong authentications in data. BC complexly eliminates the Single Thread Communication (STC) in IoT making the system more trust less. With the adoption of BC in IoT, the data flow will become more reliable and secure.

BC technology have the following advantages for large scale IoT systems, they are as follows
Tamper proof data.

- Trust less and peer to peer messaging possibility.
- Robust,
- Highly reliable
- More private data.
- Records the historic actions
- Records data of old transactions in smart devices.
- Permits the self-directed functioning.
- Distributed file sharing
- Elimination of single control authority
- Cost reduction in developing huge internet infrastructure

Challenges in Blockchain Technology Integrated IoT:

Even though block chain technology when integrated with IoT could overcome the privacy and reliability concerns of IoT. However, the BC technology is also having some limitations making it as a challenge. These challenges include the limitation with the ledger storage facility, limited developments in technology, lack of skilled workforce, lack of proper legal codes and standards, variations in processing speeds and time, computing capabilities, and scalability issues. These challenges were clearly represented and described in Table 2.

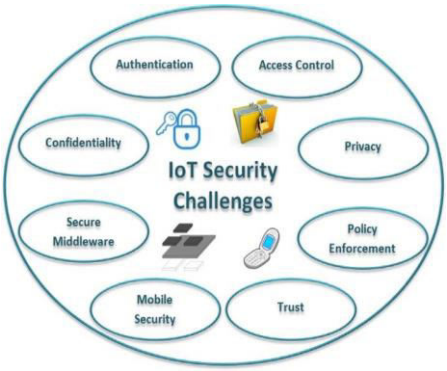
IV. EXPERIMENTAL RESULTS

In IoT with BC, the data flow is from sensors-network-router-internet-distributed blockchain-analytics-user. Here, the distributed ledger is tamper-proof which does not allow misinterpretation, wrong authentications in data. BC complexly eliminates the Single Thread Communication (STC) in IoT making the system more trust less. With the adoption of BC in IoT, the data flow will become more reliable and secure.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008093 |



V. CONCLUSION

This paper dealt with the various possible security and privacy issues in IoT. These were identified based on the observations in IoT component interaction. BC technology is identified as one of the solutions for addressing the issues and challenges in IoT. The scope for blockchain integration with IoT is explained in the paper. As a final, challenges in IoT with blockchain technology are also identified. Hope this paper would give basic idea to understanding the need for blockchain in IoT.

This technology can be applied to wide range of services in engineering fields. But the exact implications for each technology has to be studied clearly. Blockchain provides better flexibility in accessing the data. Authors would bring up the studies related to the potentials implication in various fields with appropriate demonstrative models.

Table 2. Challenges in blockchain technology integrated with IoT

Name of the challenge	Description
Limitation with storage facility	In the IoT ecosystem, the storage capacity required for sensors and actuators is very less when compared to the ledger-based blockchain technology. In IoT, single central server storage is facilitated, whereas, in BC, each ledger must be stored at the node on themselves. This increases the storage size with time when compared to the traditional storage seen in IoT devices.
Lack of skills in the field	Still the technology is new, many challenges are to be sought out to make it more convenient.
Legal issues	This technology does not have any legal codes to follow. This is one of the most challenging issues to be tackled.
Variation in computing capabilities	As it is a known fact that it systems are diverse and connected over vast networks, this becomes much more complex when blockchain technology is integrated with it. The need for running the encryption from all the things that are connected to blockchain-based out systems is essential. In such cases, all the algorithm for running the encryption may not have similar computing capabilities.
Processing time	When these computing capabilities are varying, the time required to perform the encryption would vary leading to the variations in processing time.
Scalability	This might lead to the centralization. If it becomes centralized the technic behind the cryptocurrency like Bitcoin would be revealed.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008093 |

REFERENCES

[1] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer System, 29 (7) (2013), pp. 1645-1660 https://doi.org/10.1016/j.future.2013.01.010.

[2] Nallapaneni Manoj Kumar, Archana Dash (2017) "The Internet of Things: An Opportunity for Transportation and Logistics." Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017), pp. 194-197, Coimbatore, Tamil Nadu, India.

[3] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," IEEE Wireless Communications, vol. 25, no. 6,pp. 12-18, Dec 2018.

[4] Ahmed Banafa (2017) "IoT and Blockchain Convergence: Benefits and Challenges." https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

[5] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug 2018.

[6] Ben Dickson, Decentralizing IoT networks through blockchain, (2016) https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/

[7] M. Samaniego and R. Deters (2016)"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, pp. 433-436. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102

[8] Nallapaneni Manoj Kumar, Karthik Atluri, SritejaPalaparthi (2018) "Internet of Things in Photovoltaic Systems." In Proceedings of IEEE National Power Engineering Conference (NPEC-2018), Madurai, Tamil Nadu, India.

[9] Maher Omar Alshammari, Abdulmohsen A. Almulhem and Noor Zaman, "Internet of Things (IoT): Charity Automation" International Journal of Advanced Computer Science and Applications (IJACSA), 8(2), 2017

[10] Ahmed Banafa (2017), "Three Major Challenges Facing IoT."IEEE Internet of things, newsletter, March 14, 2017 https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details