Journal of Advances and Scholarly Researches in Allied Education
Vol. 20, Issue No. 4, October-2023, ISSN 2230-7540

An Analysis the Iot-Based Intelligent Communication system driven by Blockchain Technology

Rajendra Kumar Malviya[1]*, Ravindra Tiwari[2]

[1] Research Scholar, LNCT, Bhopal, MP, India

Email: phdwork.sanjay@gmail.com

[2] Guide, LNCT, Bhopal, MP, India

Abstract- ***The prospect of improved communication system security, transparency, & efficiency through the combination of blockchain technology & IoT has attracted a lot of attention. In order to tackle the ever-changing problems with data integrity, privacy, & trust in the IoT ecosystem, this study thoroughly examines an intelligent communication system that is built on the IoT and uses blockchain technology. This research delves into the ways in which blockchain's core feature, smart contracts, can automate & enforce secure communication protocols, protecting the authenticity of data transmitted between Internet of Things devices. The paper's stated goal is to provide readers with an understanding of Blockchain's architecture & operation; furthermore, the research examines how this invention contributes to the attainment of security in the IoT. Research shows that compared to an IoT framework that doesn't use blockchain technology, one that does offer a far higher degree of security.***

Keywords- Internet of Things, Communication Systems, Blockchain, Technology

----------X----------

INTRODUCTION

The widespread use of IoT devices has brought about a new age of unparalleled connectedness, completely altering our interaction with the world around us. Given the increasing importance of these interconnected devices in our everyday lives, it is crucial to prioritise the security, integrity, & efficiency of the communication infrastructure. Blockchain technology is being seen by many as a revolutionary answer to the problems caused by the distributed and data-intensive character of IoT networks. An intelligent communication system based on the IoT and strengthened by the novel incorporation of blockchain technology is the subject of this study's extensive investigation. Concerns about data integrity, privacy, & trust in the ever-changing and expansive network of networked devices could be alleviated through the complementary integration of the IoT with blockchain technology. The introduction of blockchain technology, which creates a distributed or immutable record, has the ability to revolutionise the way IoT devices securely exchange data, communicate, or transact with one another. Aiming to solve the weaknesses of centralised systems, this solution intends to bring about a paradigm shift by establishing the communication infrastructure on blockchain principles. This will guarantee a transparent & verifiable record of interactions. Examining how well different consensus algorithms function inside the blockchain framework to keep a distributed ledger in check within the context of Internet of Things applications, the paper delves into the potential consequences of doing so. The research goes beyond blockchain to explore the convergence of AI & IoT. The goal is to create a smart communication system that can learn from its surroundings & adjust its performance accordingly. Incorporating AI algorithms makes the system smarter, more secure, & able to manage data efficiently and do predictive analytics.

Blockchain

Many different sectors can benefit from blockchain technology, which is a secure & flexible ledger system. Satoshi Nakamoto proposed the concept of blockchain technology in 2008. An immutable distributed ledger that records transactions and keeps tabs on assets in a corporate network is known as a blockchain. The hash addresses connect the blocks, making them immutable. A network-broadcast request initiates the transaction procedure. After that, the transaction is confirmed using the consensus mechanism in accordance with the blockchain's data. A fresh block is built & uploaded to the blockchain once the verification is complete. Full nodes keep an exact replica of the blockchain, which improves its reliability. Blockchain technology guarantees user privacy & security while introducing trust to P2P networks.

Because it addresses the most significant problems with the IoT, blockchain technology is finding

increasing use in IoT applications. Using blockchain technology for Internet of Things applications not only improves security, privacy, & transparency, but also opens the door to new features and economic models (Dai HN, Zheng Zet al. 2019).

Verifying the legitimacy of transactions & keeping track of ownership changes are two major advantages. Using blockchain technology, supply chain managers can identify the origins of IoT device security flaws and create an unchangeable ledger of product details like processing method, origin, or transportation route (Rejeb A, Keogh JG et al. 2019).

Figure 1 shows a basic blockchain schema, with the first block of the blockchain being referred to as the genesis block. For the IoT case study, this block will be used to launch the smart contract. Blockchain blocks contain the hash code for the following block. Since additional blocks cannot be added to the blockchain at this time, the transaction history could be safely preserved.

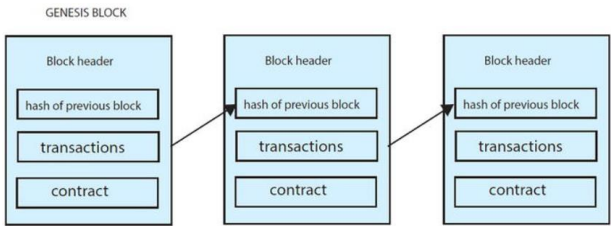

Figure 1. A blockchain illustrated.

Blockchain & Internet of Things integration

The majority of IoT solutions nowadays run on server-based infrastructures. Data from the IoT needs to be stored, maintained, & retrieved by these server systems. By utilising robust data analytics technologies, organisations are able to analyse, utilise machine learning techniques, and visualise massive amounts of data. Multiple protocols for data management, communication, and security are essential to the upkeep & protection of these centralised systems. Nevertheless, according to Zhang Y, Kasahara et al. (2008), centralised systems encounter problems with scalability, latency, and the possibility of a single point of failure. As a result, the viability of IoT systems is compromised.

To get over those problems, you could adopt blockchain technology. It has many of benefits. Here are a few benefits:

- **Decentralization**: Many nodes work together to validate & confirm transactions in a decentralised network. Because of this, there is no longer any requirement for a central server, and the hazards connected with having just one server are significantly diminished. One typical security risk in centralised systems is the well-known denial-of-service (DoS) attack.

- **Immutability & transparency:** Information recorded on a blockchain is immutable and permanent. Applications where the data on the blockchain needs to be trusted by different entities will find this functionality particularly beneficial. Centralised systems, on the other hand, are run by only one person or group, which makes them opaque and problematic in contexts where user privacy & data ownership are paramount.

- **Enhanced security:** Blockchain systems commonly use public key cryptography. By using digital signatures, which guarantee the authenticity of data, it strengthens data security. In addition, several parties use consensus processes to confirm the transaction's legitimacy. The system's robustness against unauthorised data manipulation is greatly enhanced by this intrinsic property.

- **Smart contracts:** The data interchange in IoT systems that are built on the blockchain is based on smart contracts. Deployed on the blockchain, these agreements execute themselves according to predetermined rules. They remove the need for middlemen and facilitate interactions between Internet of Things devices, paving the way for autonomous, secure transactions. Using smart contracts, procedures inside IoT networks can be streamlined and trust can be better established.

- **Scalability**: For blockchain, scalability is a high throughput of transactions per second. When network traffic increases, traditional blockchains might not be able to handle it. One of the many approaches that have been suggested to address these issues is the off-chain solution, sometimes called a layer-2 solution. These solutions enable the processing of transactions outside of the main blockchain, which frees up space and decreases the likelihood of congestion. This is especially helpful in the IoT space when the quantity of connected devices and data increases. On top of that, these layer-2 solutions offer extra privacy & security advantages.

LITERATURE REVIEW

Amrita Dahiya et al. (2022) Blockchain, powered by Distributed Ledger Technology (DLT), is a cutting-edge technological innovation that shows great promise for many different kinds of industries. One solution to the problems of online privacy & trustworthiness is the distributed ledger, which is really just a database that is both distributed and encrypted. Indeed, the range of blockchain's potential uses is growing daily. There are strong reasons in favour of using blockchain technology in many different contexts because to its unique

properties, such as secure and transparent data exchange. Our article provides an all-encompassing overview of blockchain technology and associated ideas. Despite the abundance of research in these areas, several challenges related to data dependability, storage, & scalability persist. The decentralised, transparent, immutable, and auditable nature of blockchain technology has made it an indispensable tool for solving these problems. Domains such as the IoT, the cloud, or social media can greatly benefit from the latest technology advancements, which allow for the construction of trust in dispersed systems without the requirement for authority. Some may see the IoT & cloud computing as two of the least important technologies that could benefit from blockchain technology. Domains such as content creation and sharing, trademarking, and rights management stand to benefit greatly from the combination of social media and blockchain technology. We show how blockchain may work with the IoT, cloud computing, & social media, as well as the problems and difficulties that come with it, in this article. We also highlight some of the most important studies conducted in each field.

Dr Sheetalrani R Kawale et al. (2022) There are numerous security holes in the IoT, which is a network that connects many physically different items. By virtue of having distinct identifiers, IoT allows for the complex interconnection of disparate pieces of computing & communication hardware. In order to achieve the application's objective, IoT integrates many technologies, such as mobile devices, industrial machinery, animals, humans, and other physical-digital entities. This fosters an atmosphere of teamwork. Data theft (also known as data breaches), botnet attacks—in which several systems try to take over the victim's system & steal their private data—and denial-of-service (DoS) attacks are just a few of the security problems. One may classify the many security-based techniques that have emerged recently as either cryptographic-based or non-cryptographic-based, depending on whether they aim to bolster security or not. Both have both advantages and disadvantages, although cryptographic methods are more commonly used. When it comes to protecting the Internet of Things, the research says that blockchain technology is vital.

Abdulsalam S. Albulayh et al. (2022) These days, many industries are witnessing the meteoric rise of the IoT. Because of this, managing IoT data communications becomes more complicated. There would be security & privacy issues if this problem were to be addressed utilising a centralised paradigm. One possible solution to the problem of how to manage the widespread & trustless exchange of data from the Internet of Things is technologies like blockchain. To tackle the issue of efficient management of IoT data communication, this article proposes a new, lightweight IoT architecture that is blockchain-centric. Built on top of an event-driven smart contract, it allows for simple publish/subscribe data transmission between IoT devices in a way that is both manageable & trustless. A single smart contract is crucial to the proposed system's design in order to keep system complexity & overhead to a minimal. The smart contract specifies all the system procedures that allow the various system participants to communicate data effectively over the IoT. The lack of direct connection between blockchain, IoT devices, and the system makes it more suitable for large-scale IoT deployments that include devices with limited computing & energy capabilities. The ability to mimic various IoT configurations was built into a practical Ethereum-based implementation of the system. The outcomes of the evaluation proved that the suggested design was both practical and efficient. Taking into account experimental settings with different scales & densities, we were able to provide secure data connections with minimal latency & resource usage.

Geetanjali Rathee et al. (2019) Smart technology development has recently shifted to a new paradigm with the advent of the Communicating Things Network (CTN). CTNs are made up of physical devices that can collect and exchange digital data. In contrast to any structure or network that relies on human intervention, CTN aspires to create smart appliances that increase productivity & deliver real-time data more quickly. Physical items in the network are able to communicate with one another, gather data about their environments, and use that information to make smart decisions. Today, CTNs are becoming more important in people's lives since they help cut expenses, make things more transparent, or boost efficiency across the board. Here, we take a look at the IoT, a major use case for CTNs, and offer a Blockchain-based secure Hybrid Industrial IoT architecture. In a hybrid industrial architecture, when a company's many branches are situated in multiple countries, we have implemented this strategy. Despite the fact that IoT devices help many organisations cut costs & improve quality, there are a number of hazards that can develop in these devices caused by different types of invaders. Hackers can gain access to IoT devices and use them for harmful purposes. Employees might do things like nap during work hours or steal products from the company. Blockchain technology is thought to be the most effective method for preventing these problems because it safeguards the control system in real-time while also providing confidentiality. In order to keep things transparent amongst users in different locations, we have utilised a Blockchain mechanism to retrieve data from IoT devices and put

it on the Blockchain in this paper. In addition, the suggested framework has been tested against Blockchain's internal communication in a scenario where many attackers have compromised IoT devices. In comparison to the traditional method, the findings from using Blockchain technology in simulations show an 89% success rate in user request time, falsification attack, black hole attack, or probabilistic authentication situations.

Göran Pulkkis et al. (2018) While the IoT opens up numerous possibilities for digitalization, it also makes IoT systems prime targets for cybercriminals. With more and more gadgets connecting to the Internet, the chances of harmful behaviours are growing. Security solutions that work with limited IoT devices are necessary. An answer may lie in tailored blockchain-based Internet of Things security. Distributed ledger technology (blockchain) relies on a constantly expanding linked list of data structures (blocks) that are replicated in every node of a network of computers acting as peers. A blockchain is a distributed ledger that stores records of transactions that users have initiated. Ensuring that all operations on IoT data are recorded as transaction records in blockchain blocks will help prevent unauthorised operations on this data. Discussing blockchain's potential for safeguarding IoT systems, this chapter provides an introduction to the technology and its security aspects. In this chapter, we will look at a few real-world applications of blockchain-based solutions in different IoT settings.

Yong Yu et al. (2018) IoT is spearheading a digital upheaval in enterprise & education. IoT simplifies people's lives, but it also raises concerns about privacy and security. The distributed ledger technology known as blockchain has great promise for the security of the IoT, which might have far-reaching effects in industries as diverse as manufacturing, banking, and trade. In the IoT, the blockchain architecture offers a fascinating replacement for the conventional centralised paradigm, which is failing to satisfy certain requirements. This article delves into the common privacy or security concerns with the IoT or builds a framework to include blockchain technology into the IoT. This integration can offer a number of benefits, such as improved scalability, authentication, decentralised payment, and data assurance for the IoT. As an additional demonstration of blockchain's value to the IoT, we offer some recommendations for addressing privacy and security concerns pertaining to the protocol.

METHODOLOGY

Blockchain technology creates an immutable ledger of all transactions between users. When a larger number of customers actively participate in regulating any given commerce, decentralisation becomes a real possibility. Internet of Things (IoT) blockchain ecosystem design is presented in response to security concerns. The essentials and optimum conditions of blockchain improvement are covered in this study. New blockchain user accounts populated with community & answer details are required for use of the Stuff Server Web. In its database, the Material internet server keeps the address & transmits it to the community app. The code is loaded onto the webserver by the model sensor while it is operating over a file protocol. By confirming their inclusion in the blockchain's address on the dataset, users can choose the appropriate location to store data or build blocks. The transaction requires the creation of a block after collecting the information from the sensor. According to Emanuel Ferreira Jesus et al. (2018), once the data has been communicated from the sensor, it will be saved on the blockchain server unless it has already been deleted before the block is formed.

A user can accept the contents contained in an implementation block by going to the IoT Registry as a participant id. If the blockchain information matches the database, the details will be shown on the user's application. No changes will be possible.

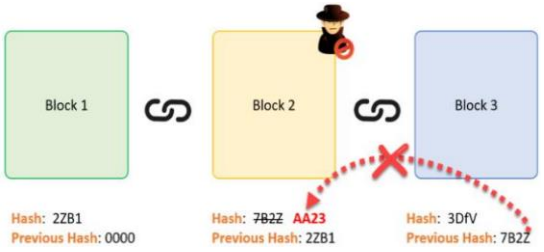

Figure 2: Block Formation

Although the data will be removed by changing the archive's status, it will not be wiped. The division of functions guarantees that all duties are carried out, eliminating the possibility of a single point of failure. In order to track down the data, we will create the trustworthy root of the data. We implemented the suggested model on the application server & database server. Everyone can still access the data using the name and password, but data protection is in place to ensure that no one can view such data. We also make sure that your data is protected and kept private. Since our methods for viewing and storing data have already been defined, there will be an abundance of common practices.

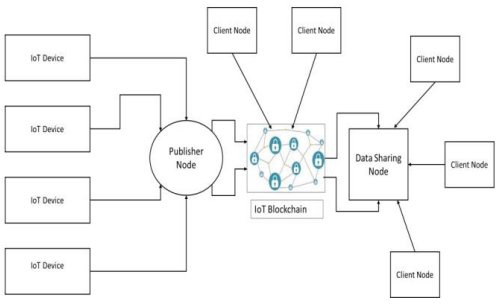

Figure 3: The proposed method's flow diagram

In their 2018 study, Emanuel Ferreira Jesus et al. discussed hash functions: You might think of these mathematical operations as fingerprint details that give a description. The likelihood of producing a unique output from a single dataset is extremely low. Among the many popular uses of hash, data integrity verification stands out. No matter the input size, the hash output size must be constant; nevertheless, the exact size is algorithm dependent. There are multiple hash algorithm definitions in the SHA-256 algorithm. Here are some characteristics that hash algorithms should possess:

(i) One way: Using the hash values to deduce the input must be a formidable challenge.

(ii) Compression: The ideal size of a hash is that of a small subset of the data.

(iii) Ease calculation: A cheap hash algorithm should be able to evaluate the hash value.

(iv) Diffusion: To prevent algorithm re-engineering, the hash output can be varied from a few bits to about half if just one bit of input is changed.

(v) Collision: If two inputs provide the same hash, then it should be challenging to compute them.

Pseudo Code is the given algorithm

```
Input

Input hashing

Plain Data = "input the plan data";

Read the data using the function of WL("Raw data: {0}", plainData);

Hashed Data = Calculate Sha256Hash(plainData);

WL("Hash {0}", hashed Data);

WL(ComputeSha256Hash("input the plan data")

Applying the function for reading the line using RL ();

Compute Sha256Hash(rawData)

Compute the Using (SHA256 sha256Hash = SHA256. Create())

Bytes = sha256Hash. ComputeHash (Encoding.UTF8.GetBytes(rawData));

Applying the loop

for (inti = 0; i<bytes.Length; i++)

applying the for appending the string (bytes[i].ToString("x2"));

return

returning the stringing
```

RESULTS

The blockchain is a decentralised database that stores all of a transaction's details in a series of interconnected blocks. Every block header undergoes a SHA256 cryptographic hash to generate a hash value.

```
[ Private Key ]
  9fa62f812155899293d9b1c6d55e8489584ee32567aad4fe4904a3a908bc3fa6
[ Public Key ]
  a8216d247e3beba9a7fc3067ab06cda193cfca75
[ Address ]
  1AzZCTc9igEjVKbYPXTLvArLjToebXBL6T
```

Figure 4: Key Generation

Output streamed with the last 5,000 lines trimmed

],

"previous_block":
"000055464755e4b75dbfdcc5305b205ded7fef438a6ee67481ed29b7f0ce10dc",

"nouce": 23654,

"hash": "0000f6f2a05a7ec72856b974a1328f5ea24708b4795e7f2baedef6cd82da9c57"

}

[Miner new block]

{

"index": 5528,

"timestamp": 1591053274,

"tx": [

"9e153d0a7919eb3b8cf916ebf5bc1787acb72d322cd8bcab1a2804c4c4851a37"

],

"previous_block":
"0000f6f2a05a7ec72856b974a1328f5ea24708b4795e7f2baedef6cd82da9c57",

"nouce": 39981,

"hash": "0000ce7011296752f914efc38fdcd272812bab081ffae1e69e55a4e092f3bdcc"

}

Block hash computation is very similar to Bitcoin's. The hash before this block has only four zeros because our difficulty setting is rather low. We simply added it to the array of transaction hashes for convenience. Anaconda, a blockchain platform supporting a complicated number of transactions, is used to conduct the simulation in Python with a block size of 4 bytes. Ubuntu 16.04 LTS(Linux) OS, Intel(R) Core (TM)-i5-10210U CPU @ 160GHz-2.11GHz, 26 8.00GB RAM, 1TB ROM, and 512GB SSD are the minimum system requirements for the simulation.

Every block header undergoes a SHA256 cryptographic hash to generate a hash value. Block hash computation is very similar to Bitcoin's. The hash before this block has only four zeros because our difficulty setting is rather low. Typically, this may be made in a matter of seconds, and it's designed to make digging easier to grasp the concept. The transaction hash is also a part of a Merkle tree, and the tx field in Bitcoin stands in for that. We simply added it to the array of transaction hashes for convenience. The Bitcoin mining algorithm uses SHA56, which is based on the string +Nouce, which is a number, in the block header. Although the header information is simplified by a simple blockchain, the mechanism & Bitcoin remain constant. A local file containing the blockchain in JSON format is maintained.

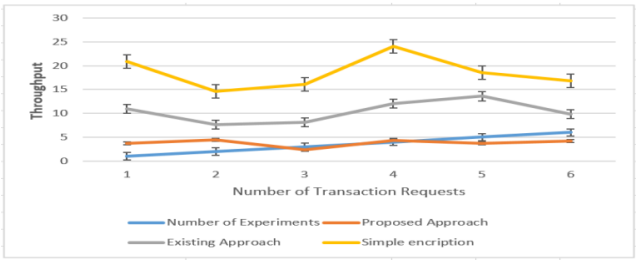

Figure 5: Measurement of Transaction Request Throughput

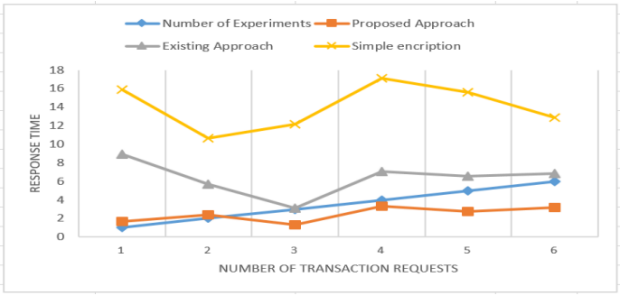

Figure 6: Time Required to Respond to a Certain Amount of Transaction Requests

The process of creating a block is connected to the data about transactions, so when the block is saved, the data about the block is also saved. The initial transaction in the blockchain will be the mining reward, and there will be prizes for mining. The created block itself is the reward for mining. The total amount entered for every transaction in the block is also given to the miner. For the certification of transactions, there will be certain sorting rules, such as sorting by blockage, transaction fee, transaction amount, etc. We limited the implementation to just rewards in order to make it simpler. The present procedure will be the one to receive the prize. We can always make a new process if the old one doesn't exist. P2P stands for "Peer-to-Peer," which describes the network architecture of the blockchain. We execute the code using the Python programming language and the Anaconda framework. While guaranteeing the maximum chain, the new node will synchronise all data from the other node's blockchain.

CONCLUSION

An innovative communication system powered by blockchain technology has been integrated with the IoT, which represents an enormous step forward in digital connectivity & data management. In our ever more linked world, the synergistic convergence of various technologies has opened up a world of possibilities, revolutionising device communication and interaction. By facilitating frictionless interaction amongst various systems, devices, or sensors, the intelligent communication system built on the IoT provides efficiency never before seen. Integrating blockchain technology into the IoT increases its trustworthiness, transparency, & security. Blockchain guarantees the integrity of data shared between devices due to its decentralised & tamper-resistant nature. This article presents a recent article on the blockchain in the IoT. We clearly outline five essential components, along with their needs & difficulties, for the creation of IoT blockchain architecture. Additionally, we find gaps that prevent a strong IoT blockchain architecture from developing. The potential use of a blockchain to protect the transmission of sensitive information in the IoT is discussed in this article.

REFERENCES

1. Albulayhi, A. S., & Alsukayti, I. S. (2023). A Blockchain-Centric IoT Architecture for Effective Smart Contract-Based Management of IoT Data Communications. *Electronics*, *12*(12), 2564.

2. Dahiya, A., Gupta, B. B., Alhalabi, W., & Ulrichd, K. (2022). A comprehensive analysis of blockchain and its applications in intelligent systems based on IoT, cloud and social media. *International Journal of Intelligent Systems*, *37*(12), 11037-11077.

3. Dai HN, Zheng Z, Zhang Y. Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal. 2019;6(5):8076-8094

4. Dogo, E. M., Salami, A. F., Nwulu, N. I., & Aigbavboa, C. O. (2019). Blockchain and internet of things-based technologies for intelligent water management system. *Artificial intelligence in IoT*, 129-150.

5. Emanuel Ferreira Jesus, Vanessa R. L. Chicarino, Célio V. N. de Albuquerque, Antônio A. de A. Rocha, A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack, Security and Communication Networks, vol. 2018, Article ID 9675050, 27 pages, 2018.

6. Kawale, S. R., Srilatha, B., Ganesh, N. G., Girish, M., Sahu, D. N., & Sade, A. S. (2022). Block Chain Driven Intelligent Communication System for IoT. *NeuroQuantology*, *20*(9), 2770.

7. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review. 2008

8. Pulkkis, G., Karlsson, J., & Westerlund, M. (2018). Blockchain-Based Security Solutions for IoT Systems. *Internet of Things A to Z: Technologies and Applications*, 255-274.

9. Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Networks*, *94*, 101933.

10. Rejeb A, Keogh JG, Treiblmaier H. Leveraging the Internet of Things and blockchain technology in supply chain management. Future Internet. 2019;11(7):161

11. Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-based solutions to security and privacy issues in the internet of things. *IEEE Wireless Communications*, *25*(6), 12-18.

12. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J. Smart contract-based access control for the Internet of Things. IEEE Internet of Things Journal. 2018;6(2):1594-1605

Corresponding Author

Rajendra Kumar Malviya*

Research Scholar, LNCT, Bhopal, MP, India

Email: phdwork.sanjay@gmail.com