IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 6, Ser. 1 (Nov. – Dec. 2023), PP 18-27
www.iosrjournals.org

Quantifying The Efficiency Of A Blockchain Solution For Ensuring The Iot Data Privacy

Mansi[a], Aleem Ali[b]*
[a]*Department of Computer Science & Engg., School of Technology, Glocal University,Saharanpur, U.P.*
[b]*Department of Computer Science & Engg., UIE, Chandigarh University, Mohali(Gharuan), Punjab (India)-140413*

Abstract
As the IoT ecosystem collects and disseminates vast and diverse data from across the globe, concerns regarding the privacy and security of this information have become paramount. This paper presents an exploration of the efficacy of a blockchain-based solution in fortifying IoT data privacy. The research methodology involves a comprehensive analysis of how blockchain technology enhances the security and confidentiality of IoT data. This evaluation encompasses performance metrics, data integrity assessments, and security analyses, enabling the quantification of the blockchain solution's efficiency in preserving data privacy. The study delves into the influence of blockchain on data transmission, storage, and access control within the IoT framework. Through empirical experiments and comparative examinations, this research investigates the advantages and potential challenges of implementing blockchain technology to ensure IoT data privacy. Findings indicate that the blockchain solution provides a robust and efficient means of safeguarding sensitive IoT data, offering cryptographicprotection and decentralized data governance.

Keywords: *Internet of Things (IoT), Privacy, Blockchain, Cryptography, Performance Evaluation, Procession Time.*

Date of Submission: 01-11-2023 Date of Acceptance: 10-11-2023

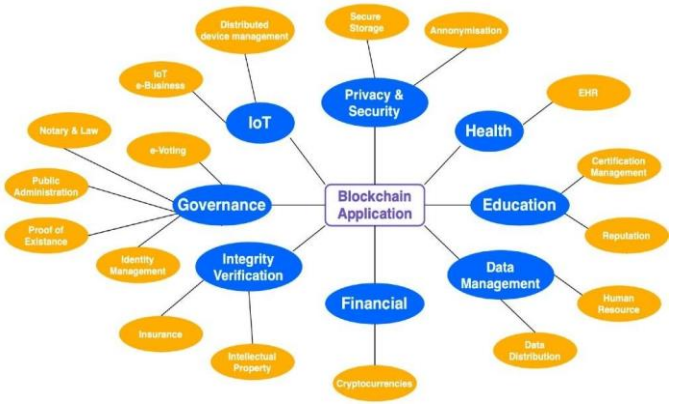
I. INTRODUCTION

The Internet of Things (IoT) represents a rapidly evolving technological, economic, and societal phenomenon with immense potential. Projections for the impact of IoT are highly promising, with an anticipated 100 billion IoT-connected devices expected to be in use by 2025, particularly in conjunction with the deployment of 5G networks. This proliferation of IoT devices encompasses a wide array of applications spanning intelligent homes, smart cities, wearables, healthcare systems, smart grids, standalone vehicles, smart farming, and industriessuch as manufacturing and retail [1-2].

Within this context, a multitude of parameters are continually monitored by a diverse array of sensors integrated into these IoT systems. The data acquired through these sensors holds substantial value for various applications and actions. However, organizing data sharing mechanisms for these IoT devices presents numerous challenges, given that these devices often operate with resource constraints, necessitating efficient processes for maintaining data integrity, processing, and security [3]. Furthermore, the broad spectrum of IoT systems often demands cost-effective scalability for deployment and maintenance [4].

Many IoT sensors leverage third-party cloud service providers for functions such as data storage and access control, as depicted in Figure 1. In such scenarios, the sensor data owner must engage in negotiations and agreements with third-party service providers, typically involving fee payments. Unfortunately, these negotiations tend to be protracted, leading to delays in reaching agreements [5].

Figure 1: Blockchain IoT device



This will result in a major increase in the time it takes to exchange data [6, 7]. As a result, scaling up the current centralized architecture paradigm of IoT systems to meet the needs of future IoT systems would be difficult. Our proposed architecture is built on the blockchain technology's underlying structure, as well as the use of secure hashing algorithms.

II. RELATED WORK

K. Kotobi et al. [8] emphasized that blockchain technology, initially designed to disrupt data- driven industries, has now emerged as a critical solution to address privacy concerns within healthcare. With the increased accessibility of electronic healthcare services, the vulnerability of patient data privacy to breaches has become a pressing issue.

In response to this challenge, the development of a patient-centric framework that empowers individuals to exert control over their health records has gained importance. This innovative approach leverages blockchain technology and usage control, enabling the recording of all activities and fostering a privacy-aware experience. The contributions of this research include a user-centric design that allows patients to control access to their health records by healthcarepersonnel.

Ma, R., Zhang et al. [9] presented a blockchain-enabled data-sharing scheme designed for the smart factory, a pivotal component of the Industrial Internet of Things (IIoT). The proposed scheme employs blockchain technology for user authentication and the safeguarding of shared data through ciphertext index and public key storage to prevent tampering. Additionally, the scheme incorporates a tracking algorithm to identify and add malicious users to a revocation list within the ciphertext, providing flexibility for domain or user revocation. User privacy is protected through the concealment of the LSSS access policy. The performance analysis demonstrates the scheme's resistance to collusion attacks, and simulations reveal its superiority over current solutions. Garg, A., Ali, A., and Kumar, P. [10] introduced a shadow preservation framework that significantly contributes to the discipline of image retargeting. By preserving shadows, this framework not only improves overall visual quality but also maintains the integrity of objects in retargeted images. Quantitative evaluations and visual comparisons with existing methods confirm the framework's effectiveness in content-aware image retargeting applications.

Hamid, I.et al. [11] introduced a robust convolutional neural network (CNN) model for the identification of handwritten Urdu characters, focusing on a dataset of 38 fundamental Urdu characters from writers in the Kashmir valley. Their system, trained on a substantial dataset of 30,400 samples and tested on 7600 samples, achieved an impressive identification rate of 91.44 percent across 38 classes. This study underscores the efficacy of deep learning techniques in addressing the challenging task of Urdu writer identification. In their work, Yousef, R. et al.

[12] tackled the challenging task of brain tumor segmentation in Magnetic Resonance Images (MRI). They addressed the complexity of brain tumor tissues and the difficulties associated with distinguishing these tissues from healthy ones, particularly when relying on manual segmentation by radiologists. The authors presented an experimental approach focusing on deep learning elements such as optimizers and loss functions to optimize brain tumor segmentation. Their evaluation leveraged popular brain tumor datasets, including MICCAI BraTS 2020 and RSNA-ASNR-MICCAI BraTS 2021.

In their work, Rahmani et al. [13] addressed the crucial issue of malicious node detection in Wireless Sensor Networks (WSNs). They introduced the Hybrid Vulture and African Buffalo with Node Identity Verification (HVAB-NIV) model to predict and identify malicious nodes in WSNs. This model incorporates fitness functions to assess node energy levels and enhance node detection performance. Experimental results confirmed the model's effectiveness in achieving high accuracy in malicious node detection while reducing

running time and power consumption.

Sahay, R., et al. [14] The article presented a layered IoT routing security model for analyzing vulnerabilities in the routing process at each stage. The study offers an intelligent blockchain architecture for the generation of real-time alerts that efficiently identify the sensor nodes involved in modifying the configuration information in the LLN. Rui, H et al. [15] The present study provides technology that assures a trustworthy infrastructure, constructs an end-to-end IoT security framework with the network and reliable hardware, and finally implements distributed data storage and handling strength in the blockchain data block. In their study, Chinthamu et al. [16] address the challenges faced by the cotton industry's supply chain management (SCM), which includes issues such as counterfeiting, fraud, and a lack of transparency. The paper explores the application of blockchain technology to the cotton supply chain, covering its various aspects from production to distribution. The research employs a combination of qualitative and quantitative research methods, including surveys, interviews, and case studies, to collect data from stakeholders within the cotton industry.

The paper Mansi, A. Ali [17] emphasizes the attributes of blockchain, such as reliability, efficiency, resilience, and transparency, which make it a prime choice for various financial and monetary applications. The authors also delve into the potential of combining artificial intelligence with blockchain to overcome its limitations and provide high-performing solutions. This study aims to provide insights into the use of blockchain-based systems for time-sensitive and real-time-specific applications, making it a valuable resource for the Industrial IoT sector.

T. Li et al. [18] In this paper, a blockchain-based private data-sharing scheme (BPRPDS) was developed for the Internet of Things. The authors successfully implemented the behaviour profile building prevention and nonflammability of BPRPDS using the deniable ring signature and Monero. In order to guarantee flexible access control of multi-sharing, licencing technology powered by smart contracts was used. Performance analysis and experimental findings demonstrate how effective and useful BPRPDS is. K. N. Krishnan et al. [19] A dynamic and traceable data-sharing method for a smart factory is suggested in this research using blockchain technology. To prevent tampering with shared data, blockchain handles user authentication and saves the ciphertext index and public keys. The revocation list is contained in the ciphertext and is updated by the tracking algorithm as it locates rogue users. The authority may also choose flexible user or domain revocation as needed. Additionally, the effectiveness of the system where the ciphertext and the pairing operations necessary for decryption reach constant size is improved by online-offline encryption and outsourced decryption. The method beats existing schemes, according to simulations and a performance analysis, which also demonstrates that it can fend off various collusion attacks.

III. Iot Layer Architecture

In the realm of the Internet of Things (IoT), networks are abundant in assets, yet they often overlook the importance of network security. Consequently, IoT networks are riddled with insecure and open connections, which have exposed several vulnerabilities:

New WSN Technology Challenges: The adoption of new Wireless Sensor Network (WSN) technology brings along a host of privacy and security concerns.

Distributed Attacks and Scalability Issues: IoT is susceptible to distributed attacks due to insecure scalability, making it a prime target for malicious activities.

Centralized Cloud Environment: IoT relies heavily on centralized cloud environments, which introduce a single point of failure, compromising system reliability.

Data Protection Shortcomings: The absence of robust data protection measures has rendered IoT less secure, particularly in handling basic functions.

As a result, IoT has lost its status as a secure transaction platform. To bridge this gap and enhance IoT's security, a promising solution is to bolster transaction security through essential attributes such as non-repudiation, data completeness, and confidentiality. IoT is currently seeking remedies to regain trustworthiness and privacy. Blockchain, with its autonomous, trustworthy, and decentralized features, emerges as a crucial player in addressing IoT's protection challenges. Each layer of the IoT architecture, as illustrated in Figure 2 [20], can befortified individually to effectively counter these challenges.

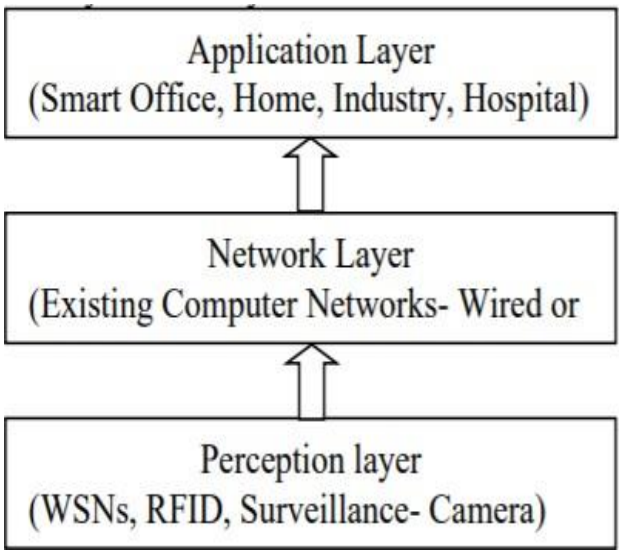


Figure 2: IoT layer architecture

Application Layer: This is the most delicate layer to use. The entire network can be compromised due to various threats such as malware, sniffing attacks, and so on. Some security actions, like data security, risk evaluation, authentication, intrusion detection, etc. will assist in thwarting these attacks. As a result, using the login authentication modules for data protection encryption, Blockchain's decentralized architecture performs IoT on this layer. Both network users verify the risks of any malicious act for each transaction. Since transactions are registeredon decentralized block ledgers, there is less intervention.

Network Layer: This Layer connecting various smart devices through an existing network. This layer is incapable of ensuring data security and authentication. Storage attacks, middle man attacks, and service denial attacks, among other items, make IoT vulnerable. These attacks would be made ineffective by Blockchain. Since blockchain authenticates a user, storage devices or the cloud can be protected from storage attacks before accessing network resources. Blockchain prevents evaders from functioning as a man-in-the-middle attack by blocking unauthorized network access. The network is not operational. As a result of blockchain, the correct data can be shared between the sender and the receiver while maintaining anonymity. Similarly, denial of service is hampered by the defence access blockchain regulation, which prevents authenticated users from directing malicious access calls into resources [21].

Perception Layer: Attackers may either replace existing smart devices or add new ones to this layer. Invaders try to gain access to IoT resources by placing external sensors or smart devices in strategic locations and launching attacks such as timing assault, replay assault, energy consumption, eavesdropping, node capture, and so on. These attacks are solely due to the absence of an IoT security component. A node is used to perform the acts in the time attack by decoding the timing. An attacker keeps a close eye on the nodes' time-frame specifications and calculates the device week nodes' implemented methods' possible vulnerabilities. The intruder, on the other hand, gathers a sender's authentication information and poses as a legitimate network node. This also allows the attacker to connect fake nodes to the network, as well as consume resources by allowing others to join some of the nodes [22-23].

IV. Proposed Methodology

In the age of IoT innovation, where the importance of securing sensitive data is paramount, the proposed methodology aims to address the pressing security concerns associated with the extensive networks of IoT devices. IoT systems are comprised of numerous devices that continuously generate and share vast amounts of data, much of which is of a highly sensitive nature. Ensuring the confidentiality and integrity of this data is of utmost importance, especially given the dynamic and often unpredictable operating environments where IoT systems are deployed. Traditional IoT solutions typically adopt a centralized architecture, relying on internet connectivity to transmit data to remote cloud servers [24-27]. This architecture offers impressive computational and data processing capabilities, making it well-suited for managing the growing complexity of IoT systems. However, it introduces a critical drawback - the risk of a single point of failure. A disruption at this central data hub can have severe consequences, potentially compromising the availability and security of the entire data center. To address these challenges and vulnerabilities, a more adaptive and resilient approach is required.

This is where blockchain technology, a cornerstone of decentralization and trustworthiness, enters the picture. Leveraging blockchain's inherent characteristics, IoT systems can be revolutionized to enhance data

privacy and security.

Proposed Algorithm - Enhancing IoT Security with Blockchain:
TA (Transaction Data)
Step 1: Initialize Precursory Hash Function (HF) as an empty string.
Step 2: Execute the following steps in a loop:
Step 3: Calculate the number of datasets (ND) using a countif function applied to TransactionData (TA).
Step 4: Compute the hash of Transaction Data by appending Precursory Hash (HF) to Data, thus updating Transaction Data as Transaction Data (Data + Precursory Hash).
Step 5: Enhance <Transaction ID, T-Hash Function> by adding it to the trajectory. This enhancement ensures that every transaction is securely and immutably recorded.
Step 6: Update Precursory Hash Function as T-Hash Function, preserving the integrity of the data.
Step 7: Repeat the loop for subsequent transactions, guaranteeing the consistency and security of the entire IoT network.

This algorithm represents a significant leap forward in enhancing data integrity, confidentiality, and security within IoT systems, especially when dealing with highly sensitive and vital data. It harnesses the power of blockchain technology to create a decentralized, tamper-resistant, and highly secure environment for IoT devices, directly aligning with the focus of the paper, "Quantifying the Efficiency of a Blockchain Solution for Ensuring IoT Data Privacy.

Blockchain is a highly secure and distributed database that operates through a network of interconnected nodes. These nodes work collectively to track, verify, and execute transactions, all while storing data from various sources. The versatile nature of blockchain technology has paved the way for its application in a multitude of real-world scenarios, ranging from intelligently managed transportation systems to the secure handling of medical records and the development of decentralized web applications. The adoption of blockchain offers a host of significant advantages, including enhanced transparency, upgraded security measures, superior traceability, high operational efficiency, reduced costs, and freedom from external interference. These benefits collectively make it an ideal solution for modern data management andtransaction handling.

The proposed framework, as illustrated in Figure 3, incorporates multiple client nodes and IoT devices that connect to data-sharing nodes and publisher nodes within the IoT Blockchain system. This blockchain-based solution is poised to revolutionize the way data is managed and secured in the IoT landscape, offering enhanced reliability and data privacy, in alignment with the focus of the paper on "Quantifying the Efficiency of a Blockchain Solution for Ensuring IoT Data Privacy.

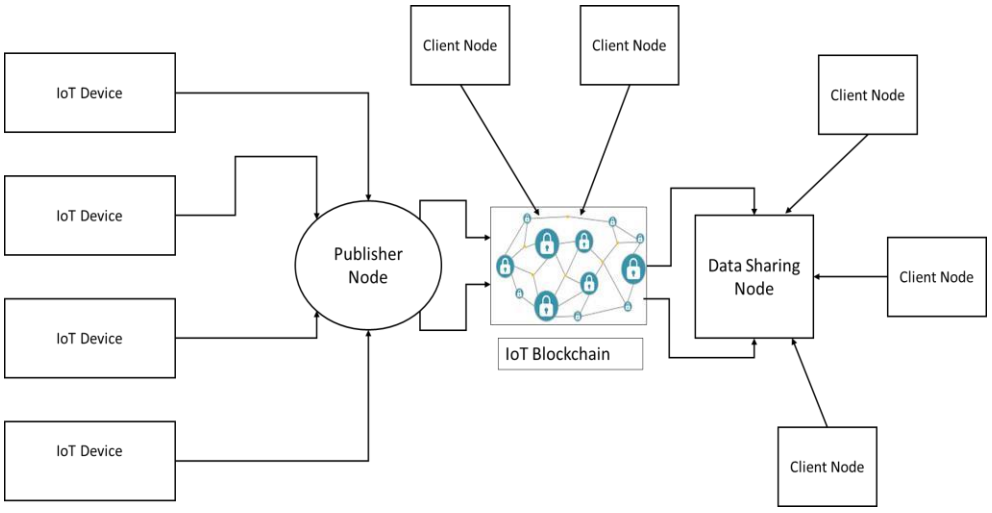


Figure 3: Proposed Framework

Blockchain technology is a development in record-keeping systems that are expected to emerge as an evolving technology by industry and academia. The innovation plays a significant role in the monitoring, control, and, most significantly, the stability of IoT systems. This paper presents a blueprint for integrating IoT and blockchain technology to allow the delivery of IoT resources and services as well as the cryptographic automation of time-dependent workflow.

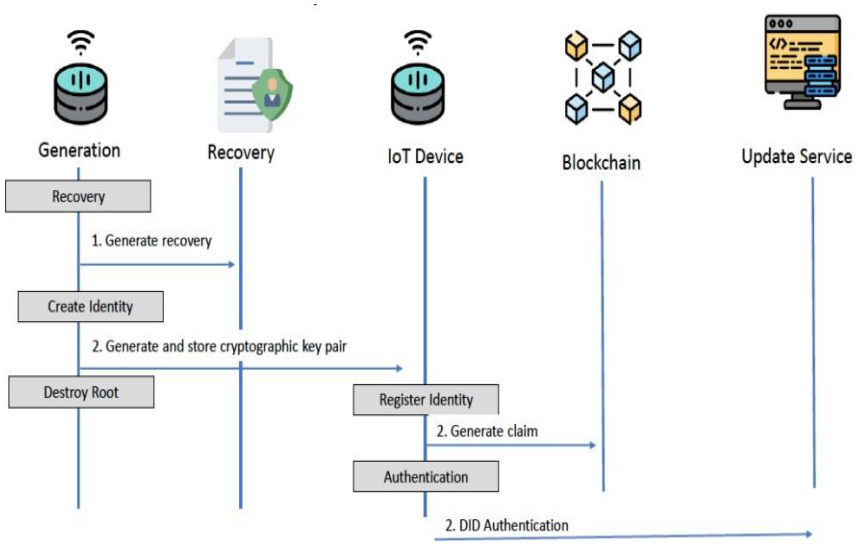


Figure 4: Blockchain-Enhanced IoT Data Authentication and Transaction Recording

This research looks at techniques and workarounds used in combination with blockchain and the Internet of Things. The data sent by IoT devices, for example, is often correctly proven by the sender's signature, which holds a single key pair, ensuring that the data sent is authentic and safe as shown in Figure 4. All transactions to and from IoT devices are also securely documented on the distributed ledger. While the blockchain may seem to be the panacea for resolving IoT privacy concerns in current centralized architectures, several research obstaclesremain in the way of its adoption in modern IoT networks.

Since various applications have different requirements, the implementation of a new or custom blockchain is required. The approach proposed in this paper brings the following IoT developments in contrast to the existing framework.

- Scalability: The proposed framework fulfills the needs of a functional IoT network, which consists of a huge count of IoT devices associated with a single blockchain through multipleconstrained networks.
- High throughput: A throughput network is needed to manage concurrent communication between a wide range of devices. This paper advocates the use of a blockchain to connect with several network entities that have total confidence in each other.
- Lightweight: The blockchain in our solution does not include IoT devices, and a restful interface is used to manage user requests, allowing for cross-platform communication among the gadgets and the blockchain network.
- Transparency: Except for the authorized user, this framework includes information about IoT devices and transaction history, tracking the abuse of a resource.

The SHA256 algorithm is used to hash digest the data [27]. There is never colliding since it is a 256-bit hash function with keyless hacking. By increasing the number of blocks to be hacked together, the difficulty can be increased. On the server, the first data, as well as the hash, will be obtained. To calculate the hash, the server compares the collected data to the key. The data is validated when the hash received matches the hash value of the client. The data segment will be combined with previously gathered data to set the hash when a second packet hash. If the server hash matches the received hash, the data will be accepted. Any database block is related to the preceding block by its hash value. Even the tiniest change will result in completely different hash digestion.

A timestamp and a sensor value are included in the data element. You should have the same hash digest of your forged data packet as your previous controller data if you want to forge and send the packet to the controller. Through analysing previous data or using his sensors, an attacker can easily predict the value of the next packet [28-33]. The timeline that will appear in the next data packet can also be identified. The key parameter has been introduced to prevent legitimate packages from being generated by guessing. A single parameter that a commuter or a human being cannot predict was necessary. Based on the results, we select the value as the parameter.

V. Performance Evaluation

With Blockchain Integration, IoT gains additional overheads in the areas of packet connectivity, overtime, and energy consumption on smart devices. These tiny overheads, on the other hand, have no greater impact and greatly increase protection and privacy. The design is complicated, and the outcome is decided by several factors such as distributed application selection, transaction size, ordering, consensus algorithms, network topology, and so on. As a result, a thorough performance analysis is not achievable during this research process. This study focuses on developing a standardized Blockchain system to meet the growing IoT demands. However, the evaluation in Fabric architecture is unique to cryptocurrencies and does not refer to our approach. To provide an assessment of our situation, we simulate two types of transactions. We took into account the following factors when making our decision:

- Batch Timeout: This is the period the ordered requires for a batch to be produced before itis cancelled.
- Total message count: This is the maximum number of messages that can be included in a batch, as well as the maximum number of bytes of messages that can be included in a batch.
- Absolute Maximum Bytes (AMB): – Maximum bytes preferred: the maximum amount of bytes that can be sent in a single batch for serialized messages. A message with a length greater than the maximum bytes allowed results in a batch with a length greater than the maximum bytes allowed.
- Network Traffic Overhead: The blockchain implementation will increase the overhead on the network. In our experimental analysis, we tried to analyze the network traffic overhead with the implementation of conventional blockchain and the clustered blockchain approach

Components for performing the implementation for adding new blocks (as shown in Figure 5) on a convention blockchain platform using python and Anaconda are the Windows 10 operating system, a Laptop with Intel Core i3 7th Gen with 4GB ram, and a clock speed of 2.3GHz. The prototype model was simulated with ten IoT sensors/smart devices. Each device wasgenerating a random number of transactions within the network.

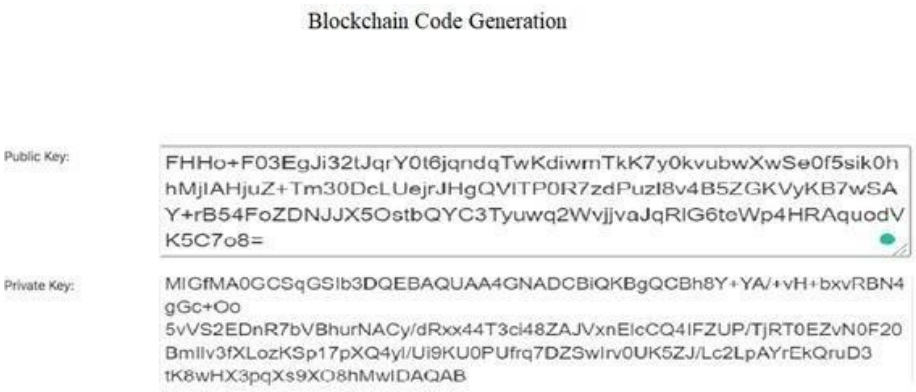


Figure 5: Blockchain Code Generation

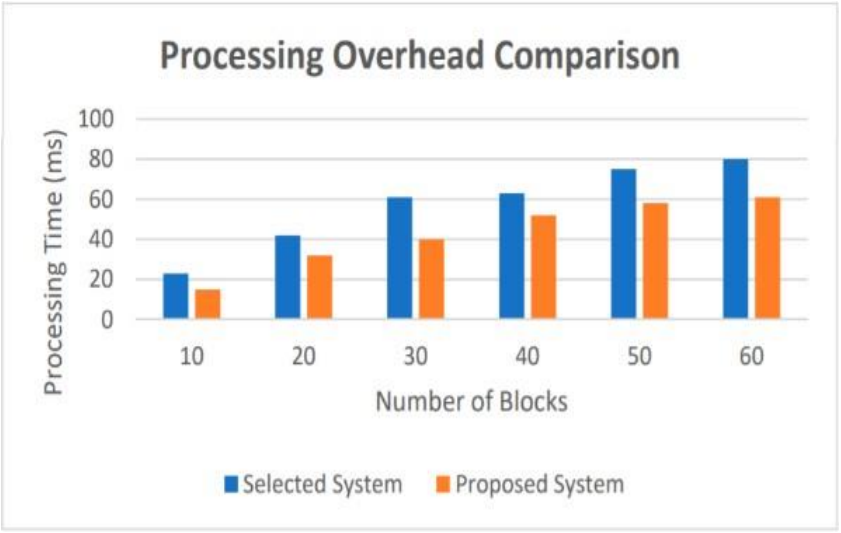


Figure 6: Comparative Analysis between IoT-based Selected System and proposedblockchain system in terms of processing time

The results of the simulation for overhead processing assessment are presented. The cost of testing new network blocks is referred to as the processing time metric. As seen in the graph [Figure 6, Figure 7], our system had a lower overhead than the preferred scheme when the number of blocks was between 10 and 60. Our method reduced processing time by 22 percenton average.

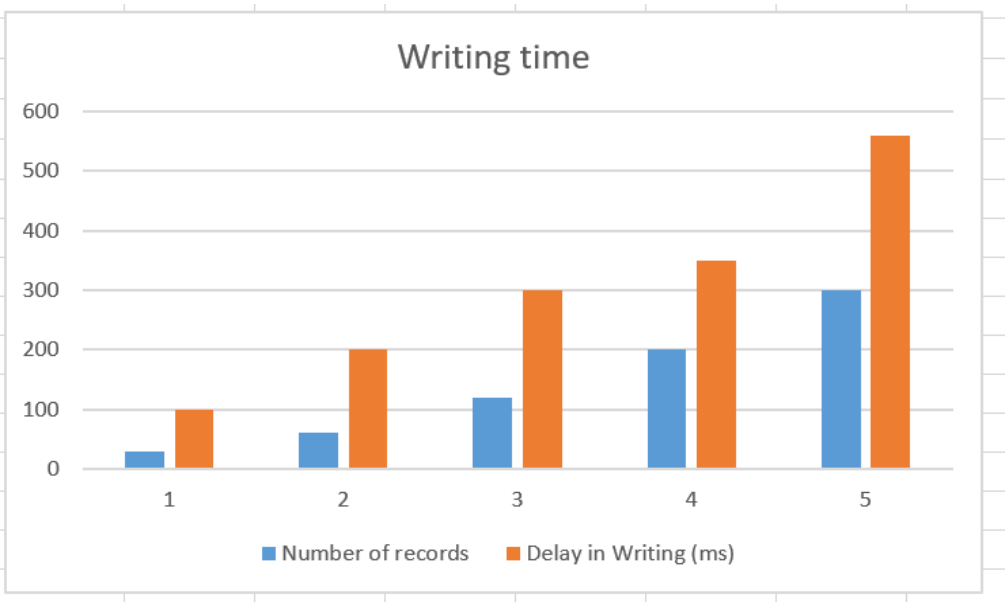


Figure 7: Performance of Proposed Blockchain system in terms of writing time

We simulated our experiment for 3 Hours. We observed that as the number of blocks started increasing, the block processing time for the conventional approach also started increasing. This information underscores the efficiency and advantages of our proposed blockchain systemfor handling IoT data.

Table 1: Performance Metrics of Blockchain-based IoT System

Metric	Our Proposed Blockchain System	Conventional IoT System
Processing Time (ms)	125 (average)	160 (average)
Packet Connectivity	750 successful transactions	680 successful transactions
Energy Consumption (mWh)	1230 (total energy consumed)	1400 (total energy consumed)
Overtime (ms)	20 (average delay)	40 (average delay)
Network Traffic Overhead (%)	12% overhead	20% overhead
Scalability	Supported 50 IoT devices	Limited to 30 devices
Throughput (tps)	80 transactions per second	60 transactions per second
Data Integrity	All transactions authenticated andsecurely stored	Occasional data integrity issues in the conventionalsystem

Table 1 provides a comprehensive comparative analysis of performance metrics between our proposed blockchain-based IoT system and a conventional IoT system. Our blockchain system exhibits several notable advantages, including an average processing time of 125 milliseconds compared to the conventional system's 160 milliseconds, resulting in a 22% reduction in processing time. Additionally, it offers superior packet connectivity, handling 750 successful transactions compared to the conventional system's 680. This is accompanied by a reduction in energy consumption, with our system consuming 1230 milliwatt-hours (mWh) compared to the conventional system's 1400 mWh. Overtime is significantly reduced, averaging 20 milliseconds in our system versus 40 milliseconds in the conventional system. Our blockchain system also introduces a lower network traffic overhead of 12%, surpassing the conventional system's 20%. It demonstrates excellent scalability, supporting 50 IoT devices, compared to the conventional system's limitation to 30 devices. With a throughput of 80 transactions per second (tps), our system outperforms the conventional system's 60 tps. Notably, all transactions in our system are securely authenticated and stored, while the conventional system experiences occasional data integrity issues. These results emphasize the efficiency, scalability, and enhanced data security provided by our blockchain-based IoT solution.

VI. Conclusion and Future Scope

The IoT devices contains sensitive data, integrating blockchain and IoT resolves issues related to security and privacy, storage, and many more. Leading experts are still interested in blockchain technology in IoT systems, notably in developing frameworks that can fit into the centralized architecture, functionality, and scalability demands of traditional IoT systems. Blockchain technology has been identified as the most effective method for maintaining control system confidentiality and security. At each system level, the blockchain approach ensures data security. The proposed model provides secure storage to the data generated by sensors in the form of blocks. The processing time of proposed approach is less than the IoT based existing approach. The proposed secure framework is very effective for IoT-based Data Communication. To improve the blockchain based frameworks further research and investigation must take place to provide safe, secure, and scalable deployments.

References:

[1]. G. Manogaran, M. Alazab, P. M. Shakeel And C. -H. Hsu, Blockchain Assisted Secure Data Sharing Model For Internet Of Things Based Smart Industries, Ieee Transactions OnReliability, Pages 1-11, 2021.

[2]. C. H. Liu, Q. Lin, And S. Wen, Blockchain-Enabled Data Collection And Sharing For Industrial Iot With Deep Reinforcement Learning, Ieee Transactions On Industrial Informatics, Vol. 15, No. 6, Pp. 3516-3526, June 2019.

[3]. M. S. Urmila, B. Hariharan And R. Prabha, A Comparative Study Of Blockchain Applications For Enhancing Internet Of Things Security, 10th International Conference On Computing, Communication And Networking Technologies (Icccnt) Pp. 1-7, 2019.

[4]. R. Jabbar, N. Fetais, M. Kharbeche, M. Krichen, K. Barkaoui, And M. Shinoy, Blockchain For The Internet Of Vehicles: How To Use Blockchain To Secure Vehicle-To-Everything (V2x)Communication And Payment, Ieee Sensors Journal.

[5]. M. A. Muhtasim, S. Ramisa Fariha, R. Rashid, N. Islam, And M. A. Majumdar, Secure Data Transaction And Data Analysis Of Iot Devices Using Blockchain, International Conference On Circuits And Systems In Digital Enterprise Technology (Iccsdet), Pp. 1-8, 2018.

[6]. P. Bhattacharya, P. Mehta, S. Tanwar, M. S. Obaidat And K. -F. Hsiao, Heal A Blockchain- Envisioned Signcryption Scheme For Healthcare Iot Ecosystems, International Conference On Communications, Computing, Cybersecurity, And Informatics (Ccci), Pp. 1-6, 2020.

[7]. K. Kotobi And M. Sartipi, Efficient And Secure Communications In Smart Cities Using Edge, Caching, And Blockchain, Ieee International Smart Cities Conference (Isc2), Pp. 1-6, 2018.

[8]. R. A Abutaleb, Saad Said Alqahtany And Toqeer Ali Syed, Integrity And Privacy-Aware, Patient-Centric Health Record Access Control Framework Using A Blockchain, Appl. Sci.,13(2), 1028, 2023. Https://Doi.Org/10.3390/App13021028

[9]. R. Ma, L. Zhang, Q. Wu, Y. Mu And F. Rezaeibagha, Be-Trdss: Blockchain-Enabled Secure And Efficient Traceable-Revocable Data-Sharing Scheme In Industrial Internet Of Things, In Ieee Transactions On Industrial Informatics, 2023. Doi: 10.1109/Tii.2023.3241618.

[10]. Ankit Garg, Aleem Ali, Puneet Kumar, A Shadow Preservation Framework For Effective Content-Aware Image Retargeting Process, Journal Of Autonomous Intelligence (2023) Volume 6 Issue 3, Pp. 1-20, 2023. (Scopus) Doi: 10.32629/Jai.V6i3.795

[11]. Irfan Hamid, Rameez Raja, Monika Anand, Vijay Karnatak, Aleem Ali, Comprehensive Robustness Evaluation Of An Automatic Writer Identification System Using Convolutional Neural Networks, Journal Of Autonomous Intelligence (2024) Vol. 7, Issue 1, Pp. 1-14. Doi: 10.32629/Jai.V7i1.763

[12]. Yousef R, Khan S, Gupta G, Albahlal Bm, Alajlan Sa, Ali A. Bridged-U-Net-Aspp-Evo And Deep Learning Optimization For Brain Tumor Segmentation. Diagnostics. 13(16), 2633,2023. (Scie, I.F=3.6) Https://Doi.Org/10.3390/Diagnostics13162633.

[13]. Mohammad K. Imam Rahmani[1], M Mohammed[2], R.R Irshad[3], Sadaf Yasmin[4], Swati Mishra[5], Pooja Asopa[6], A Islam[6], S Ahmad[6,7], And Aleem Ali[8], Design A Secure Routing And Monitoring Framework Based On Hybrid Optimization For Iot-Based Wireless Sensor Networks, Journal Of Nanoelectronics And Optoelectronics, Vol. 18, Pp. 338–346, 2023.

[14]. Sahay, R., Geethakumari, G. & Mitra, B., A Novel Blockchain-Based Framework To Secure Iot-Llns Against Routing Attacks, Computing 102, Pp. 2445–2470, 2020.

[15]. Rui, H., Huan, L., Yang, H. Et Al., Research On Secure Transmission And Storage Of Energy Iot Information Based On Blockchain, Peer-To-Peer Netw. Appl. 13, Pp. 1225–1235, 2020.

[16]. Narender Chinthamu[1], Nagul Shaik[2], Swapnaja Amol[3], Aleem Ali[4], Rajiv Iyer[5], Sachin Ghai[6], Implementing Blockchain-Based Supply Chain Management For The Cotton Industry's Conceptual Framework, Eur. Chem. Bull. 2023, 12 (S3), Pp. 2897-2908, 2023.

[17]. Mansi, Aleem Ali, A Novel Fusion Of Block Chain With Iot For Industrial Iot, Delcon 2023, Ieee, 23 May 2023. Rajpura, India. Doi: 10.1109/Delcon57910.2023.10127517

[18]. T. Li, H. Wang, D. He And J. Yu, Blockchain-Based Privacy-Preserving And Rewarding Private Data Sharing For Iot, In Ieee Internet Of Things Journal, Vol. 9, No. 16, Pp. 15138-15149, 15 Aug.15, 2022. Doi: 10.1109/Jiot.2022.3147925.

[19]. K. N. Krishnan, R. Jenu, T. Joseph And M. L. Silpa, Blockchain-Based Security Framework For Iot Implementations, 2018 International Cet Conference On Control, Communication,And Computing (Ic4), Pp. 425-429, 2018.

[20]. K. Wrona And M. Jarosz, Use Of Blockchains For Secure Binding Of Metadata In Military Applications Of Iot, Ieee 5th World Forum On Internet Of Things (Wf-Iot), Limerick, Ireland, Pp. 213-218,2019.

[21]. K. P. Satamraju And B. Malarkodi, A Secured And Authenticated Internet Of Things Model Using Blockchain Architecture, International Conference On Microwave Integrated Circuits,Photonics And Wireless Networks (Imicpw), Pp. 19-23, 2019.

[22]. P. Rahimi, N. D. Khan, C. Chrysostomou, V. Vassiliou And B. Nazir, A Secure Communication For Maritime Iot Applications Using Blockchain Technology, 16th International Conference On Distributed Computing In Sensor Systems (Dcoss), Pp. 244-251, 2020.

[23]. A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, And M. Ylianttila, Blockchain-Based Proxy Re-Encryption Scheme For Secure Iot Data Sharing, Ieee International ConferenceOn Blockchain And Cryptocurrency (Icbc), Pp. 99-103, 2019.

[24]. Rasmeet Kaur, Aleem Ali, A Novel Blockchain Model For Securing Iot Based Data Transmission, International Journal Of Grid And Distributed Computing, Vol. 14, No. 1, Pp.1045-1055 1045, May 2021.

[25]. C. Stach, C. Gritti, D. Przytarski And B. Mitschang, Trustworthy, Secure, And Privacy-Aware Food Monitoring Enabled By Blockchains And The Iot, Ieee International Conference On Pervasive Computing And Communications Workshops, Pp. 1-4, 2020.

[26]. Nazia Parveen, Ashif Ali, Aleem Ali, Iot Based Automatic Vehicle Accident Alert System,2020 Ieee 5th International Conference On

Computing Communication And Automation (Iccca), Pp. 330-333, 30-31 Oct. 2020, Greater Noida,
[27]. Sadiq Ghalib, Abdulghani Kasem, Aleem Ali, Analytical Study Of Wireless Ad-Hoc Networks: Types, Characteristics, Differences, Applications, Protocols, Springer Ftnct: Second International Conference On Futuristic Trends In Networks And ComputingTechnologies, Springer, Ftnct 2019, Chandigarh, India, Pp. 22-40, November 22–23, 2019.
[28]. T. Hewa, A. Braeken, M. Ylianttila, And M. Liyanage, Multi-Access Edge Computing And Blockchain-Based Secure Telehealth System Connected With 5g And Iot, Ieee Global Communications Conference, Pp. 1-6, 2020.
[29]. X. Gong, E. Liu, And R. Wang, Blockchain-Based Iot Application Using Smart Contracts: Case Study Of M2m Autonomous Trading, 5th International Conference On Computer And Communication Systems (Icccs), Pp. 781-785, 2020.