Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 6.886|
Vol. 16 Issue 12, Dec- 2021
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Enhancing IoT Data Privacy with Blockchain Technology

Mansi*[1], Aleem Ali[2]
[1]Research Scholar, Department of Computer Science &Engg., School of Technology, Glocal University, Saharanpur, U.P.
[2]Associate Professor, Department of Computer Science & Engg., School of Technology, Glocal University, Saharanpur, U.P.
mansi@gmail.com, aleem@theglocaluniversity.in
**Corresponding Author:Mansi, Research Scholar*

Abstract

In the ever-expanding Internet of Things (IoT) landscape, ensuring the privacy and security of data has become increasingly critical. This paper investigates the effectiveness of leveraging blockchain technology to bolster the privacy of IoT data. Through a comprehensive analysis, we explore how blockchain enhances data security and confidentiality in IoT environments. Our evaluation includes performance metrics, data integrity assessments, and security analyses, providing insights into the efficiency of blockchain solutions for preserving data privacy in IoT networks. The study examines the impact of blockchain on data transmission, storage, and access control within IoT frameworks, offering empirical evidence and comparative examinations to identify advantages and potential challenges.

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

1. INTRODUCTION

The Internet of Things (IoT) is rapidly evolving, with an estimated 100 billion connected devices by 2025. From smart homes to industrial sensors, IoT technology permeates various aspects of our lives, promising increased efficiency, convenience, and insights. In this context, blockchain technology has emerged as a potential solution to address the inherent vulnerabilities of centralized IoT architectures [1]. By offering a decentralized and immutable ledger, blockchain provides a secure framework for managing and securing IoT data, thereby mitigating risks associated with data breaches, tampering, and unauthorized access [2].

This paper delves into the challenges of managing data sharing mechanisms in IoT ecosystems, particularly focusing on the security and privacy concerns inherent in centralized architectures [3-4]. We propose leveraging blockchain technology to address these challenges, offering a decentralized and secure solution.

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].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.

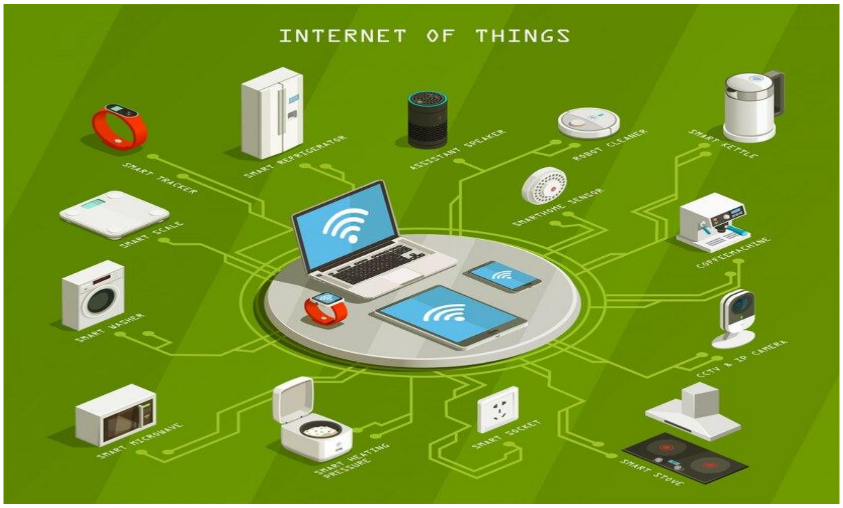

Figure 1: Internet of Things Typical Architecture

2. Background study

Prior research has explored the integration of blockchain in various domains, including healthcare, smart factories, and image retargeting. These studies highlight the potential use of blockchain to enhance security, privacy, and efficiency in diverse applications.

Ma, R., Zhang et al. introduced a blockchain-enabled data-sharing scheme tailored for smart factories, a critical component of the Industrial Internet of Things (IIoT) [8-9]. Their scheme employs blockchain technology for user authentication and data safeguarding, incorporating features such as ciphertext indexing and public key storage to prevent tampering. Additionally, the scheme incorporates a tracking algorithm to identify and blacklist malicious users, thereby enhancing security and privacy in IIoT environments.

Sahay, R., et al. 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.presents study providestechnology 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. addressed 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.

T. Li et al. presented 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. Krishnanet al. presented 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.

These studies underscore the diverse applications and benefits of integrating blockchain technology with IoT systems, ranging from healthcare data management to image processing and industrial automation. By leveraging blockchain's decentralized and tamper-resistant nature, researchers aim to address critical security and privacy challenges inherent in IoT ecosystems, paving the way for more secure and trustworthy IoT deployments.

3. 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:

Lack of Security Focus: Many IoT deployments prioritize functionality and connectivity over security measures. Consequently, security considerations often take a backseat, leading to the proliferation of insecure connections within IoT networks.

Inadequate Authentication Mechanisms: IoT devices may lack robust authentication mechanisms, making them susceptible to unauthorized access and exploitation. Weak or default credentials, coupled with lax authentication protocols, create opportunities for malicious actors to infiltrate IoT networks [11-14].

Insufficient Encryption: Data transmitted across IoT networks may be inadequately encrypted, exposing sensitive information to interception and tampering. Without robust encryption protocols in place, IoT devices are vulnerable to eavesdropping and data manipulation attacks.

Poorly Configured Devices: Misconfigured IoT devices pose a significant security risk, as they may inadvertently expose critical network assets to unauthorized access or compromise. Inadequate security configurations, such as open ports or default settings, increase the attack surface and facilitate unauthorized entry into IoT networks.

Limited Update Mechanisms: Many IoT devices lack robust mechanisms for receiving and applying security updates, leaving them vulnerable to known exploits and vulnerabilities. Without timely updates and patches, IoT devices remain exposed to evolving security threats, compromising the overall security posture of IoT networks.

Addressing these vulnerabilities requires a concerted effort to prioritize security in IoT deployments, implementing robust authentication, encryption, and access control mechanisms. Additionally, ongoing monitoring, maintenance, and regular security updates are essential to safeguard IoT networks against emerging threats and vulnerabilities [15-17]. By proactively addressing security concerns and adopting a defense-in-depth approach, organizations can enhance the resilience and security of IoT ecosystems.

4. Proposed Methodology

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 [19-21].

Proposed Algorithm - Enhancing IoT Security with Blockchain:

Initialize: Start by initializing a Precursory Hash Function (HF) as an empty string.

Calculate Hash: In a loop, calculate the hash of the Transaction Data by appending the Precursory Hash (HF) to the Data. This action updates the Transaction Data as Transaction Data (Data + Precursory Hash).

Enhance Transaction ID: Enhance each Transaction ID by incorporating the calculated hash function (T-Hash Function) into the trajectory. This step ensures that every transaction is securely and immutably recorded.

Update Hash Function: Update the Precursory Hash Function as the T-Hash Function to maintain the integrity of the data.

Repeat for Subsequent Transactions: Repeat the above steps for subsequent transactions, ensuring the consistency and security of the entire IoT network.

This algorithm represents a significant advancement in enhancing data integrity, confidentiality, and security within IoT systems, particularly for handling highly sensitive and vital data. By leveraging blockchain technology, it establishes a decentralized, tamper-resistant, and highly secure environment for IoT devices, aligning directly with the focus of the paper.

By incorporating blockchain technology into IoT systems, this framework aims to address critical challenges related to data integrity, security, and privacy. It introduces a decentralized approach to data management, where transactions are securely recorded and validated across a distributed network of nodes. This not only enhances the security of IoT data but also ensures its immutability and transparency.Organization of Blockchain: Nakamoto has portrayed the means to run the network of blockchain in Nakamoto [Nakamoto (2008)].

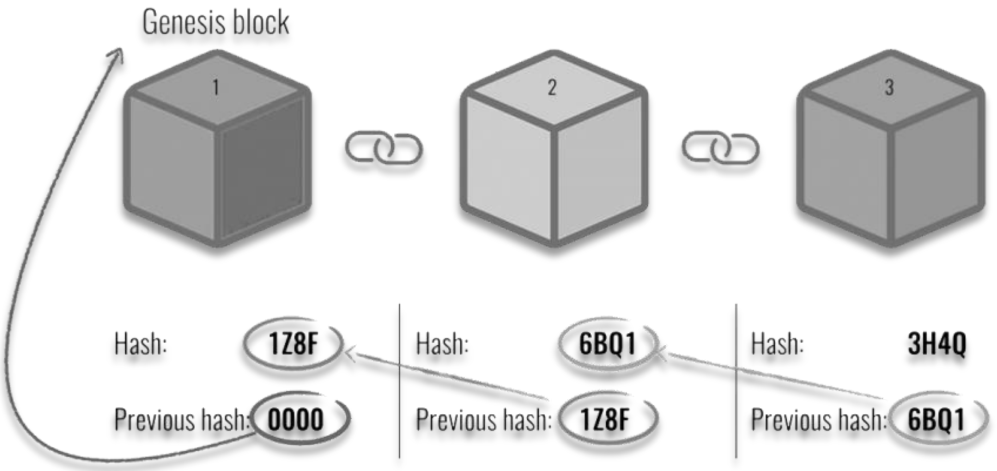

Figure 2: Organization of Blockchain[Nakamoto (2008)][26]

Furthermore, the framework facilitates secure data sharing and communication among IoT devices, enabling seamless integration and interoperability within IoT networks. By leveraging blockchain's cryptographic features and consensus mechanisms, it establishes a trustless environment where data exchanges are verifiable and tamper-proof.

The proposed framework, depicted in Figure 3, integrates numerous client nodes and IoT devices, linking them to data-sharing nodes and publisher nodes within the IoT Blockchain system. This innovative blockchain-based solution is positioned to transform the management and security of data within the IoT landscape, providing heightened reliability and data privacy. It aligns perfectly with the core focus of the paper, which is to assess the effectiveness of a Blockchain Solution in safeguarding the privacy of IoT data.

Overall, the proposed framework represents a significant step towards enhancing the efficiency and security of IoT data transmission and storage. Through its implementation, it is poised to revolutionize the way IoT data is managed, ensuring privacy, reliability, and integrity across the entire network [16-22].

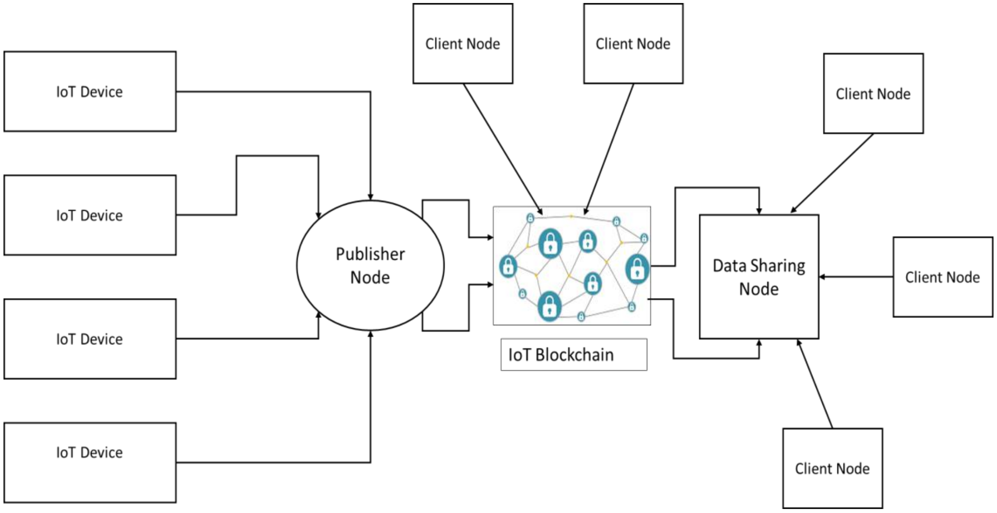

Figure 3: Proposed Framework

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.

The use of the SHA256 algorithm ensures the secure hashing of data, with its 256-bit hash function making collisions virtually impossible. Increasing the difficulty by hashing more blocks together strengthens security. When a server obtains the initial data and hash, it compares them to ensure validation. If the received hash matches the client's hash value, the data is accepted. Any alteration to a database block results in a different hash, ensuring data integrity. Timestamps and sensor values are included in data elements, making it challenging for attackers to forge packets without predicting future values. Introducing a key parameter prevents unauthorized packet generation, enhancing overall security [23-27].

5. Performance Evaluation

Integration of blockchain into IoT introduces additional overhead in packet connectivity, overtime, and energy consumption on smart devices, albeit with negligible impact compared to the enhanced protection and privacy it offers.

The complexity of the design is influenced by various factors such as distributed application selection, transaction size, consensus algorithms, and network topology, making thorough performance analysis challenging. This study aims to develop a standardized blockchain system to meet the increasing demands of IoT, although the evaluation in Fabric architecture primarily pertains to cryptocurrencies rather than our approach.

To assess our situation, we simulated two types of transactions, considering factors like batch timeout, total message count, absolute maximum bytes, and network traffic overhead. The implementation involved utilizing components like the Windows 10 operating system, a laptop with Intel Core i3 7th Gen processor, and ten IoT sensors/smart devices generating random transactions within the network.

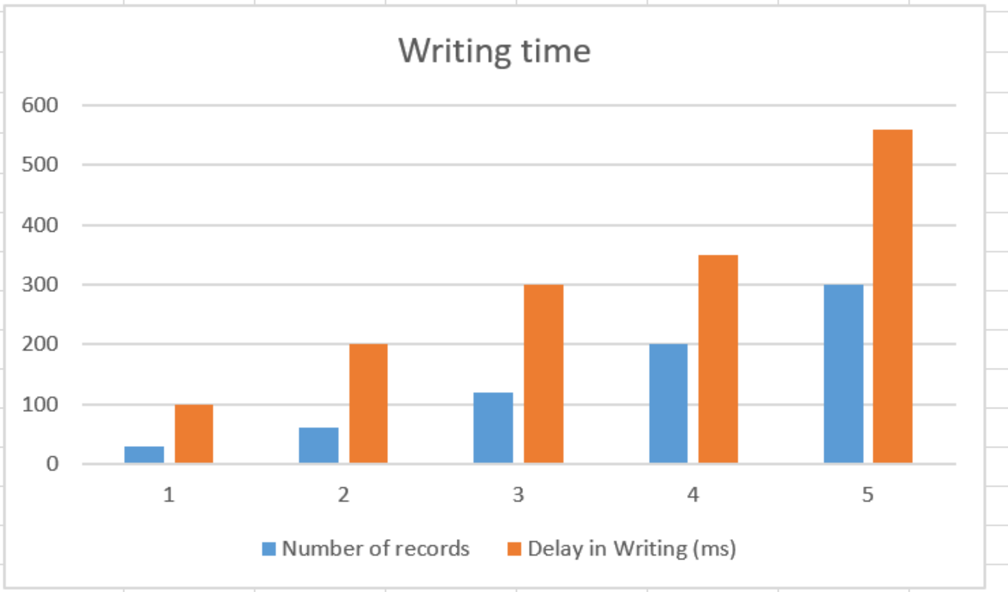

Figure 4: Performance of Proposed Blockchain system in terms of writing time

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 system for handling IoT data [28-31].

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 and securely stored	Occasional data integrity issues in the conventional system

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 [31-34]. These results emphasize the efficiency, scalability, and enhanced data security provided by our blockchain-based IoT solution.

6. Conclusionand 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. 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.
2. 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
3. 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

4. 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.
5. 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.
6. Sahay, R., Geethakumari, G. & Mitra, B., A novel Blockchain-based framework to secure IoT-LLNs against routing attacks, Computing 102, pp. 2445–2470, 2020.
7. 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.
8. 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.
9. 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
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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 Conference on Blockchain and Cryptocurrency (ICBC), pp. 99-103, 2019.
16. 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.

17. 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.
18. 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,
19. 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 Computing Technologies, Springer, FTNCT 2019, Chandigarh, India, pp. 22-40, November 22–23, 2019.
20. 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.
21. 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.
22. R. Kaur, A. 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, 2021.
23. S.Sachdeva, A.Ali, A Hybrid approach using digital Forensics for attack detection in a cloud network environment,International Journal of Future Generation Communication and Networking, Vol. 14, No. 1, pp. 1536-1546,2021.
24. N. Parveen, A. Ali, A. Ali, IOT Based Automatic Vehicle Accident Alert System, IEEE 5th International Conference on Computing Communication and Automation, PP. 330-333, 2020.
25. Bakhtawar Aslam et al., Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic, Pers Ubiquitous Comput., pp. 1–17, 2021, doi: https://dx.doi.org/10.1007%2Fs00779-021-01596-3.
26. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system, 2008.
27. 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 on Reliability, pages 1-11, 2021.
28. 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.
29. 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.

30. 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.
31. 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.
32. 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.
33. 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.
34. 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