Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Comprehensive Study of Lightweight Block-Chain Model for Data Sharing in Internet of Things for Smart Applications

S.Muthulakshmi [#1], Dr.A.Kannammal [*2]

[1]Assistant Professor, Sri Krishna College of Technology, Coimbatore, India

[2]Professor & Head, Coimbatore Institute of Technology, Coimbatore, India.

muthunjanu@gmail.com, kannaphd@gmail.com

Article Info
Page Number: 6660-6671
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 March 2022
Revised: 30 April 2022
Accepted: 15 June 2022
Publication: 19 August 2022

Abstract
Blockchain Technology, the fundamental technology that underpins Bitcoin, has gotten a lot of attention since its creation. Music, financial services, the Internet of Things (IoT), smart grid, edge computing, cyber security, and healthcare have all shown interest in its possibilities. Lightweight Blockchain is a technical advancement that allows society to alter how it trades and links information. This reputation may be inferred particularly from its characteristics of allowing mutually distrusting entities to share information and associate without relying on a trusted third party. The fundamental standards and characteristics of the Block chain were assessed in this study, and the exhibition and application circumstances of different sectors were examined. Data storage and sharing are two major blockchain-based healthcare use cases that being investigated. We also offered professional advice on choosing suitable industries, as well as an overview of the challenges and potential developments of blockchain technology.

Keywords: Internet of things, Blockchain, Data storage, Data sharing

INTRODUCTION

In recent years, the rapid development of Internet of things market, BLE, Zigbee, NFC, WiFi, LoRa, NB-IoT, 5 G rapid development of Internet communication technologies such as Cloud services are universal services, mature big data and artificial intelligence technology, to be used for comprehensive data collection, transfer, storage, analysis and security [1-3]. Technological advances also mean new defiance. The huge amount of data connected to the real world of the Internet intrudes on the user's personal privacy, necessitating a significant increase in security input. The data collected by the different networks is often limited to their specific domain, making data exchange difficult, as well as the problem of data islands. Even when businesses have agreed to share data within the legal framework, they frequently need to set up a dependable central repository. Institutions with a common mission [4,5]. Conversely, the administration, data storage and transmission of the equipment must fully cover the costs of creating and maintaining a centralized organization; if it fails, the whole system will be paralyzed. Furthermore, the centralized organization is inaccessible to participants, has too much power, and data can be compromised due to hostile activities from within or without [6].

As a result of the development and popularization of COINS, the use of black chain technology and research became popular and attracted the attention of governments, technology companies,

and educational institutions [7]. Black chain technology is now used in a variety of areas including finance, commerce, investigation, Internet of Things, asset protection, entertainment and medical health. Due to the technical characteristics of decentralization, reliable database, loss of trust, anonymity of transactions, social maintenance and open source programming, the blockchain will allow users to achieve mutual trust and achieve a reliable transfer of wealth without centralized companies. This advantage is useful for minimizing individual failure points, system security and other problems in the current management of the Internet of Things [9, 10].

With the introduction of blockchain technology, a new idea in IoT key management has emerged. Second, because of the high number of heterogeneous devices, the IoT network contains many weak nodes. Intruders may be able to quickly get access to these vulnerable nodes and utilize them for nefarious purposes. Intrusions in the Internet of Things may be quickly detected utilizing blockchain-based intrusion detection technology, which is an important security precaution in the Internet of Things [11-13]. Third, since IoT has a large number of users, especially when combined with edge computing, the network level is very complex, and controlling system access rights is a problem in IoT. Traditional access control has the drawbacks of being sluggish and vulnerable in real time. Using blockchain with access control improves the name and functionality of Internet of Things (IoT) access control, a hot topic in the industry [14,31]. Finally, with the Internet of Things, data leakage has always been a major security issue. The privacy of users is compromised at the IoT's perception, transmission, and processing layers [15,]. The combination of blockchains with privacy protection provides a more anonymous and real-time security solution for IoT privacy protection. The rest of the work is divided into the parts below: Section 2: Review of Literature and Related Topics Section 2.1 summarizes the results of the survey. Section 3 concludes with future research suggestions.

LITERATURE SURVEY

A number of academics have developed a secure and efficient data system using soft computing methods. Blockchain-enabled data collection and sharing for industrial IoT systems is one of them, and it's the subject of this article. It has quickly expanded to a variety of areas of life. The industrial sector is one of the most frequent uses of IoT technology.

Zhang*, et al*. [16] proposed an Internet of Things (IIoT) light industrial data agreement technique based on blockchain technology to provide secure data transfer in the IIoT for smart city applications. A distribution ledger is used on many gate edges. The lightweight data block structure was an improvement over traditional blockchain technology. According to the simulation results, the proposed light data consent technique reduces the average hop count on data transmission, reducing the risk of data theft. The accuracy of the data was verified, as well as the low power consumption and delay.

Liang *et al*. [17] demonstrated a Secure a fabric blockchain-based data transfer algorithm for industrial IoT. This approach uses a blockchain-based dynamic secret segmentation mechanism. A trustworthy trading center was built using the Power Blockchain sharing idea,

which can also share power trading books. The Power Data Consensus technique and linked dynamic storage were designed to protect the transfer of energy data.

Liu *et al*. [18] suggested a Distributed access control system based on blockchain technology to protect IoT data. The proposed approach was developed using a fog computer concept and a chain of alliances. This method uses mixed linear and nonlinear spatiotemporal chaotic systems (MLNCML) and the least significant bit (LSB) on edge and then the encrypted data is uploaded to the cloud.

Shi *et al*. [19] presentedBacS for IoT Distribution, a blockchain-based access control system. To use BacS to access DMS, first create an identifier with a blockchain node account address, and then change the access control permissions for the device data and save it to the blockchain. Create authentication, revocation, access control and audit processes in BacS. Finally, it uses a lightweight symmetric encryption technique for the IoT Distribution System that protects privacy.

Ge *et al*. [20] created a decentralized safe approach based on blockchain technology to store the vital data generated by the IoT system. This approach solves the issues of data reliability, security, and privacy that may emerge in a conventional IoT-cloud system. The RSA accumulator is used in this article to provide an Unspent Transaction Output (UTXO) verification technique that maintains the computational cost of light nodes to generate and validate the UTXO evidence constant.

To meet the needs of the Internet of Things, **Mohanty*et al*. [21]** developed an efficient Lightweight integrated Blockchain (ELIB) model. The suggested approach was tested in a smart home environment as an important illustration of its application in many IoT scenarios. A centralized manager generates shared keys to transmit data and handles all incoming and outgoing requests for a smart home's resource-constrained resources.

Thakker, *et al*. [22] have created a blockchain-based data management system that enables them to generate certificates for IoT devices and access data from anywhere. Certified IoT devices benefit from our blockchain-based IoT certificate management solution, which ensures user privacy and data integrity while facilitating data storage and retrieval. The data generated by IoT devices is kept on the blockchain thanks to the certificates that the devices are issued. By creating and verifying certificates depending on the amount of data saved, evaluate the Ethereum system for calculating transaction costs and speeds.

Chi *et al*. [23] developed a safe data-sharing architecture based on identity authentication and Hyperledger Fabric to ensure data sharing security. Present a community identification algorithm that separates clients into different data-sharing groups based on the similarity of label data. The scope of data sharing was established using the findings of community detection as assessed by the degree of sharing, successfully narrowing the scope of query shared data and increasing data sharing efficiency.

Liu,*et al*. [24] developed a blockchain-enabled efficient data collection and safe sharing scheme that integrates Ethereumblockchain with deep reinforcement learning (DRL) to provide a reliable and secure environment. In order to collect as much data as possible, DRL was employed, and blockchain technology was used to ensure data sharing security and reliability.

Lu *et al*. [25] were the first to create a multi-party blockchain-enabled secure data exchange system. Turn the data sharing issue into a machine learning challenge using privacy-preserving federated learning. The privacy of the data is maintained by providing the data model rather than the actual data. Finally, include federated learning into the permission blockchain consensus process so that the consensus computing work may be put to use for federated training as well.

Unal, *et al*. [26] investigated a practical approach for integrating Blockchain with FL to provide privacy-preserving and secure large data analytics. We recommend utilizing fuzzy hashing to detect variances and anomalies in FL-trained models to protect user data and trained models against poisoning efforts. Modeling attack types was used to evaluate the proposed method in a quasi-simulated setting.

Singh, *et al*. [27] showed how to build a centralized cloud-based cross-domain data exchange platform by combining multiple security gateways. The data is kept in a centralized cloud through security gateways utilizing blockchain technology. Once the application detects a hazardous activity, the centralized cloud verifies the issue from the blockchain. In addition, anybody who participates in detrimental conduct in the security gateways will be sanctioned. The algorithms are used to authenticate and transmit data. On a global scale, the proposed architecture provides for secure data transmission across domains.

Gongs *et al*. [28] presented a privacy-protection solution for the Internet of Things that combines blockchain technology with ring signature and proxy reencryption. With this method, the data permitted for sharing in the IoT was transmitted in the system as ciphertext, the data sender's identity information was protected, and the distributed ledger alleviated the pressure of mass data storage on a centralized server. The accuracy and safety of the proposed system are also evaluated.

For consumer IoT devices, **Hu *et al*. [29]** developed a distributed, efficient, and secure data exchange system. The four layers that make up this architecture are the IoT devices layer, edge storage layer, blockchain network layer, and application services layer. Smart contracts based on attributed based access control (ABAC) and the searchable encryption algorithm include Device Retrieval Contract (DRC), Policy Management Contract (PMC), and Authorization Verification Contract (AVC). Using simulated trials, demonstrate that our proposed architecture can manage large-scale data access demands while retaining an acceptable level of communication overhead.

Si, *et al*. [30] have created a lightweight IoT information exchange security architecture based on blockchain. The system employs a two-chain architecture, with distributed storage and tamper-proof data in the data blockchain and an improved practical Byzantine fault-tolerant

(PBFT) mechanism consensus method in the transaction blockchain. Data registration efficiency; resource and data transactions in the transaction blockchain were improved transaction efficiency and privacy protection thanks to upgraded algorithms based on partial blind signature algorithms. A dynamic game strategy of node cooperation is proposed to prevent detrimental local dominance behavior. The unknown node's status is determined by reporting its institutional reputation value; the high-trust reference report is then used to correct the malicious node's weight in the overall report and node merging, resulting in Bayesian equilibrium.

Table 1: Overall analysis of survey

Authors	**Title**	**Proposed Algorithms / Techniques**	**Objective**	**Limitations**	**Journal Name**
Zhang, *et al.*[16]	Ldc: A lightweight data consensus algorithm based on the blockchain for the industrial internet of things for smart city applications	Dada consensus algorithm	Defending against data theft	Concerns about privacy and security flaws	Future Generation Computer Systems
Liang, *et al*. [17]	A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things	Data Transmission Technique	Improving the transfer rate and the pace at which money is received in the pocket	The block cannot be stored on the blockchain due to data capacity and storage limitations.	IEEE Transactions on Industrial Informatics
Liu, *et al*. [18]	Privacy protection for fog computing and the internet of things data based on blockchain	Least significant bit method algorithms	Resolve the issue of an access control point of failure.	It is insecure and exposes personal information.	Cluster Computing
Shi, *et al*. [19]	BacS: A blockchain-based access control scheme in distributed internet of things	Lightweight symmetric encryption algorithm	This formalizes the IoT distributed architecture with the conventional centralized access control approach.	Protecting privacy will take time.	Peer-to-peer networking and applications

Ge ,*et al*. [20]	A blockchain based decentralized data security mechanism for the Internet of Things	Probabilistic polynomial time (PPT) algorithm	In a typical IoT-Cloud system, there are problems with dependability, security, and privacy.	The light node constant's verification computational complexity	Journal of Parallel and Distributed Computing
Mohanty, *et al*. [21]	An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy	Lightweight consensusalgo rithm	To address the needs of security and privacy in IoT, an ELIB model was created.	Complexity of computation, bandwidth, latency, and overhead	Future Generation Computer Systems
Thakker, *et al*. [22]	Secure Data Management in Internet-of-ThingsBased on Blockchain	Ethereum's consensusalgo rithm	Data recovery is also carried out using an effective and secure data management system.	Testing architecture has to be improved for a bigger and more varied collection of IoT devices.	IEEE International Conference on Consumer Electronics
Chi,*et al*. [23]	A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things	Community Detection Algorithm	The community detection server receives and analyzes all client label data.	Some concerns about security and privacy	Journal of Network and Computer Applications
Liu, *et al*. [24]	Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning	Blockchain-enabled secure data sharing among MTs	The blockchain technology is utilized to guarantee data sharing security and dependability.	Other services include communicatio n, which is provided via a mobile communicatio n base.	IEEE Transactions on Industrial Informatics
Lu,*et al*. [25]	Blockchain and Federated Learning for Privacy-preserved Data Sharing in Industrial IoT	Differential private federated learning	Using privacy-preserving federated learning, turn the data sharing issue into a machine learning problem.	Effectively ensuring data privacy is still a work in progress.	IEEE Transactions on Industrial Informatics

Unal, *et al*. [26]	Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things	FL algorithms	Gives a step-by-step guide on combining Blockchain with FL to offer data analysis services.	To offer industry-quality insights, a large number of real-world industrial case studies are required.	Computers & Security
Singh, *et al*. [27]	Cross-Domain Secure Data Sharing using Blockchain for Industrial IoT	Digital Signature Algorithm	They utilize blockchain technology to store data on the cloud.	The possibility to search encrypted data has yet to be explored.	Journal of Parallel and Distributed Computing
Gong,*et al*. [28]	A data privacy protection scheme for Internet of things based on blockchain	cryptographic algorithm	With blockchain, ring signature technology, and proxy reencryption, IoT privacy is protected.	Noise issues, complex calculations, and poor computation efficiency are all issues that need to be addressed.	Transactions on Emerging Telecommunications Technologies
Hu, *et al*. [29]	Blockchain Enabled Data Sharing Scheme for Consumer IoT Applications	Searchable encryption algorithm	Satisfy large-scale data access demands while keeping communication overhead to a minimum.	The network layer's incentive mechanisms must be taken into account further.	IEEE Consumer Electronics Magazine.
Si, *et al*. [30]	IoT information sharing security mechanism based on blockchaintechnology	Practical Byzantine fault-tolerant (PBFT) mechanism consensus algorithm	Solve the problem of IoT data sharing security.	Performance must be improved, and the danger of data leaking must be eliminated.	Future Generation Computer Systems

2.1 SUMMARY OF THE SURVEY

In all, 30 articles are examined in this study. In each article, a distinct algorithm and procedure were employed. We investigated which method they employed, how much system they

secured, what limitations they achieved, and assessment metrics in this survey. Some techniques are provided security vulnerabilities, privacy leakage problems, computation complexity, scalability, latency, and poor calculation efficiency while evaluating the current research articles, which are included in table 1. Some techniques are ineffective in terms of data security. However, there is room for growth in terms of deep learning speed.

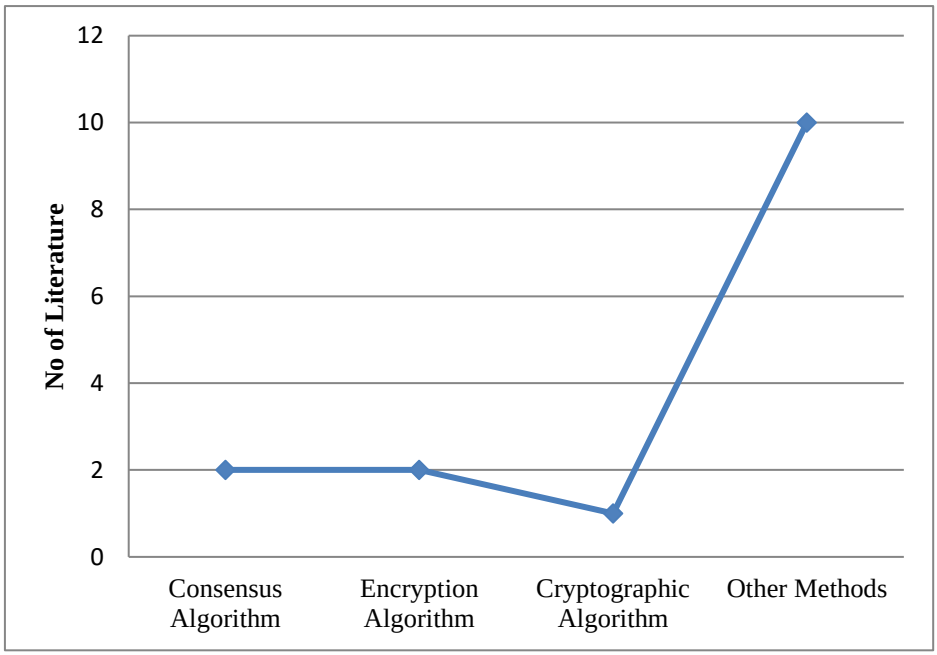

Fig 1: Survey related to Algorithms

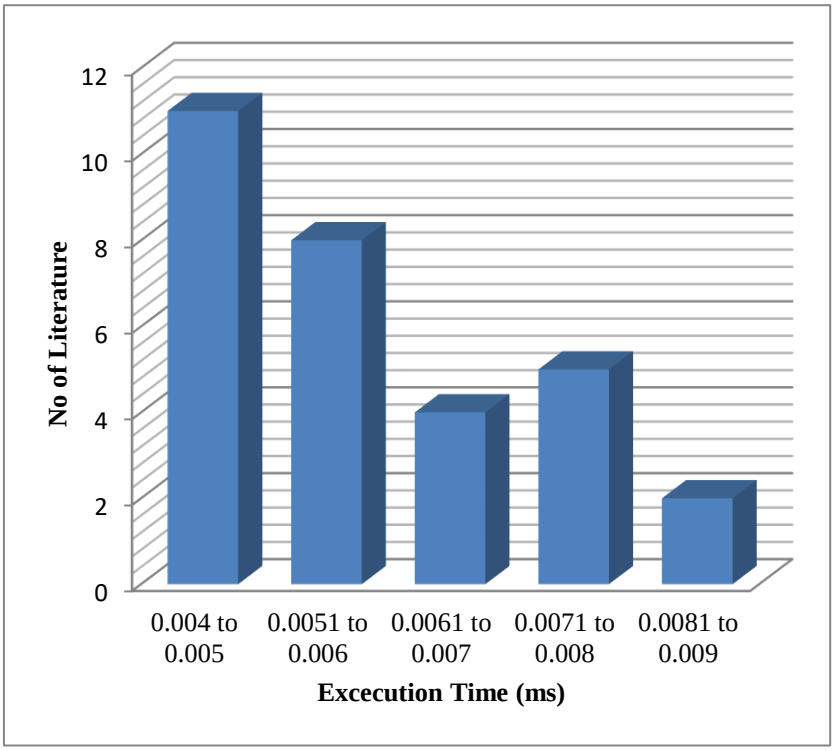

Fig 2: Survey based on an Execution Time

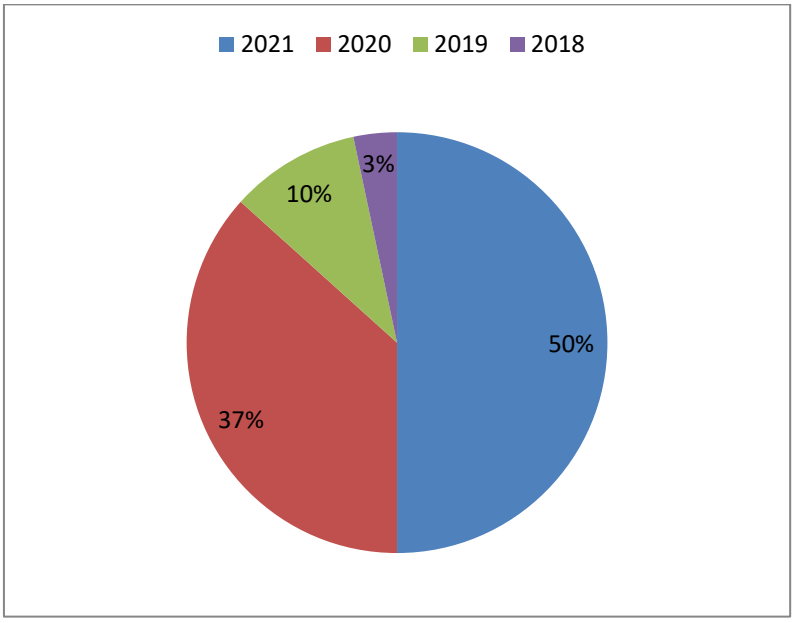

Fig 3: Survey based on Literature papers

The algorithm detection is shown in Fig 1. Consensus Algorithm, Encryption Algorithm, Cryptographic Algorithm, and other Methods are among the algorithms employed here. Two of the 30 literatures are classified as Consensus Algorithm, two as Encryption Algorithm, one as Cryptographic Algorithm, and ten as Other Methods. Fig 2 shows a review of the literature based on execution time. 11 literatures with execution times of 0.004 to 0.005ms, 8 literatures with execution times of 0.0051 to 0.006 ms, 4 literatures with execution times of 0.0061 to 0.007 ms, 5 literatures with execution times of 0.0071 to 0.008 ms, and 2 literatures with execution times of 0.0081 to 0.009 ms were studied. Fig 3 uses the survey report to examine the years. In this study, 50 percent of articles by 2021, 37 percent of articles by 2020, 10% of articles by 2019 and 3% of articles by 2018 were examined.

CONCLUSION

This study seeks to provide an overview of the literature on blockchain and the Internet of Things, with a focus on problems related to an IoT environment. With the development of high-speed networks and intelligent network devices, the Internet of Things (IoT) is the next emerging technology. IoT devices, however, are increasingly vulnerable to assaults and unable to defend themselves. We emphasized the fundamental ideas in block chain in this article, which has necessitated its application in the area of IoT. We also illustrated the significance of smart contracts in block chain technology using diagrams that depicted the ideas. The absence of a thorough literature review for the development of bid systems prompted this study.

REFERENCES

[1] Manogaran, Gunasekaran, MamounAlazab, P. Mohamed Shakeel, and Ching-Hsien Hsu. “Blockchain assisted secure data sharing model for Internet of Things based smart industries”. IEEE Transactions on Reliability, 2021.

[2] Xu, H., He, Q., Li, X., Jiang, B. and Qin, K., Bdss-fa: A blockchain-based data security sharing platform with fine-grained access control. IEEE Access, vol.8, pp.87552-87561,2020.

[3] Zhang, Q., Li, Y., Wang, R., Liu, L., Tan, Y.A. and Hu, J., Data security sharing model based on privacy protection for blockchain-enabled industrial Internet of Things. International Journal of Intelligent Systems, 36(1), pp.94-111, 2021

[4] Wei, X., Yan, Y., Guo, S., Qiu, X. and Qi, F., Secure Data Sharing: Blockchain enabled Data Access Control Framework for IoT. IEEE Internet of Things Journal 2021.

[5] Manzoor, A., Braeken, A., Kanhere, S.S., Ylianttila, M. and Liyanage, M., Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. Journal of Network and Computer Applications, vol. 176, pp.102917, 2021.

[6] Yuvaraju, M. and Mansingh, P.B., A Secure Data Sharing Scheme Based on Blockchain for Industrial Internet of Things Using Consensus Algorithm. In Industry 4.0 Interoperability, Analytics, Security, and Case Studies (pp. 119-132). CRC Press, 2021.

[7] Wang, D. and Zhang, X., Secure data sharing and customized services for intelligent transportation based on a consortium blockchain. IEEE Access, vol. 8, pp.56045-56059,2020.

[8] Goyat, R., Kumar, G., Saha, R., Conti, M., Rai, M.K., Thomas, R., Alazab, M. and Hoon-Kim, T., Blockchain-based data storage with privacy and authentication in Internet-of-things. IEEE Internet of Things Journal,2020.

[9] Qin, Xuanmei, et al. "LBAC: A lightweight blockchain-based access control scheme for the internet of things." Information Sciences vol. 554,pp. 222-235, 2021.

[10] Rathee, G., Ahmad, F., Sandhu, R., Kerrache, C.A. and Azad, M.A., On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. Information Processing & Management, vol. 58(3), p.102526, 2021.

[11] Sharma, S., Chaudhry, R. and Bhardwaj, D., Blockchain for Secure Internet of Things. In High Performance Vision Intelligence , Springer, Singapore,pp. 33-54,2020

[12] Ma, X., Wang, C. and Chen, X., Trusted data sharing with flexible access control based on blockchain. Computer Standards & Interfaces, vol. 78, pp.103543, 2021.

[13] Banotra, A., Gupta, S., Gupta, S.K. and Rashid, M., Asset Security in Data of Internet of Things Using Blockchain Technology. In Multimedia Security ,Springer, Singapore,pp. 269-281, 2021.

[14] Anjelin, D.P. and Kumar, S.G., Blockchain Technology for Data Sharing in Decentralized Storage System. In Intelligent Computing and Applications Springer, Singapore,pp. 369-382, 2021

[15] Huang, H., Zhu, P., Xiao, F., Sun, X. and Huang, Q., A blockchain-based scheme for privacy-preserving and secure sharing of medical data. Computers & Security, 99, p.102010, 2020.

[16] Zhang, Wenbo, Zonglin Wu, Guangjie Han, Yongxin Feng, and Lei Shu. "Ldc: A lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications." Future Generation Computer Systems, vol.108 pp.574-582, 2020.

[17] Liang, Wei, Mingdong Tang, Jing Long, Xin Peng, Jianlong Xu, and Kuan-Ching Li. "A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things." IEEE Transactions on Industrial Informatics,vol.15, pp.6 3582-3592, 2019.

[18] Liu, Y., Zhang, J. and Zhan, J., Privacy protection for fog computing and the internet of things data based on blockchain. Cluster Computing, 24(2), pp.1331-1345, 2021.

[19] Shi, Na, Liang Tan, Ciaxia Yang, Chen He, Junli Xu, Yang Lu, and Hao Xu. "BacS: A blockchain-based access control scheme in distributed internet of things." Peer-to-peer networking and applications pp.1-15, 2020.

[20] Ge, C., Liu, Z. and Fang, L., A blockchain based decentralized data security mechanism for the Internet of Things. Journal of Parallel and Distributed Computing, vol.141, pp.1-9, 2020.

[21] Mohanty, SachiNandan, K. C. Ramya, S. Sheeba Rani, Deepak Gupta, K. Shankar, S. K. Lakshmanaprabu, and Ashish Khanna. "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy." Future Generation Computer Systems vol.102, pp.1027-1037, 2020.

[22] Thakker, J., Chang, I. and Park, Y., Secure data management in Internet-of-Things based on blockchain. In IEEE International Conference on Consumer Electronics (ICCE), pp. 1-5,2020.

[23] Chi, J., Li, Y., Huang, J., Liu, J., Jin, Y., Chen, C. and Qiu, T., A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things. Journal of Network and Computer Applications, vol. 167, pp.102710, 2020

[24] Liu, C.H., Lin, Q. and Wen, S., Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning. IEEE Transactions on Industrial Informatics, vol. 15(6), pp.3516-3526,2018.

[25] Lu, Yunlong, Xiaohong Huang, Yueyue Dai, SabitaMaharjan, and Yan Zhang. "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT." IEEE Transactions on Industrial Informatics vol. 16, no. 6, pp. 4177-4186, 2019

[26] Unal, Devrim, Mohammad Hammoudeh, Muhammad Asif Khan, AbdelrahmanAbuarqoub, Gregory Epiphaniou, and RidhaHamila. "Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things." Computers & Security vol. 109,pp.102393, 2021.

[27] Singh, Parminder, MehediMasud, M. Shamim Hossain, and Avinash Kaur. "Cross-Domain Secure Data Sharing using Blockchain for Industrial IoT." Journal of Parallel and Distributed Computing 2021

[28] Gong, J., Mei, Y., Xiang, F., Hong, H., Sun, Y. and Sun, Z., A data privacy protection scheme for Internet of things based on blockchain. Transactions on Emerging Telecommunications Technologies, vol. 32(5), pp.e4010, 2021.

[29] Hu, B., Chen, Y., Yu, H., Meng, L. and Duan, Z., Blockchain Enabled Data Sharing Scheme for Consumer IoT Applications. IEEE Consumer Electronics Magazine,2021.

[30] Si, H., Sun, C., Li, Y., Qiao, H. and Shi, L., IoT information sharing security mechanism based on blockchain technology. Future Generation Computer Systems, vol. 101, pp.1028-1040, 2019.

[31] Muthulakshmi, S., Kannammal, A., Padma Priya, M., Pramila, V., & Shobiadevi, G. (2022). Improvising micro transactions using IOTA tangle on smart refrigerator applications. International Journal of Health Sciences, 6(S4),4955-4965.

[32] Sangeetha, T. and Mohanapriya, M., 2022. A Novel Exploration of Plant Disease and Pest Detection Using Machine Learning and Deep Learning Algorithms. Mathematical Statistician and Engineering Applications, 71(4), pp.1399-1418.

[33] Sangeetha T, Kumaraguru M, Akshay S, Kanishka M. Biometric based Fingerprint Verification System for ATM machines. InJournal of Physics: Conference Series 2021 May 1 (Vol. 1916, No. 1). IOP Publishing.

[34] Sangeetha, T., Mohanapriya, M., Pavithra, S., Ragamira, S. and Sneha, S., 2022. A Novel Deep Learning Approach for Alzheimer's Disease Segmentation and Classification Using RCNN. Mathematical Statistician and Engineering Applications,71(3), pp.1159-1172.45.

[35] K.Mythili ,S.Muthulakshmi, Dr.T.Rajesh Kumar, T.Sangeetha "Similarity Disease Prediction System for Efficient Medicare"-Publication date 2020/4 Test Engineering & Management Volume 83 Issue ISSN:0193-4120 Pages 3s 350 -3354 Publisher the Mattingley Publishing Co., Inc.

[36] T Sangeetha, G Lavanya, D Jeyabharathi, T Rajesh Kumar, K.Mythili, "Detection of Pest and Disease in Banana Leaf Using Convolution Random Forest" Test Engineering and Management, Volume 83, Page Number: 3727 -3735,March -April 2020.

[37] Muthulakshmi S , Dhivya dharshini B , Hema Priya S , Jaya priya RR, " Receiver System Based Student Tracking System using IoT" , Journal of Physics: Conference Series, Volume 1916.

[38] R.Kanmani, S.Muthulakshmi, R. Radhapoorani, N. Suganya, K. Sri subitcha, M. Sriranjani, "Prediction of Covid Disease using Advanced IoT and Support Vector Machine", IEEE Xplore, 2021.

[39] S.Subhakala, S.Muthulakshmi, A.Geetha, K.Dhanya, "Design of Smart Village Using Internet of Things and Cloud Computing", Pakistan Journal of Biotechnology,2017.