Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

A Secure and Efficient Method for Sharing Data Between Edge-Enabled internet of things Devices using ECC

[1]Mr.K.Uday Kiran, [2]Kancharla Sai

#1 Assistant Professor, #2 Pursuing M.C.A Department of Master of Computer Applications

QIS COLLEGE OF ENGINEERING & TECHNOLOGY

Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272

Abstract: The project proposes an Edge-based Blockchain Secure Data Sharing Scheme (EB-SDSS) to enhance the efficiency and security of data transmission between IoT devices, edge servers, and cloud servers, addressing latency and security concerns inherent in traditional cloud systems. By utilizing edge servers that receive data directly from IoT devices, the scheme significantly reduces data transfer times, offering better performance in comparison to centralized cloud models. The integration of Blockchain technology ensures data integrity and security by storing tamper-proof records through hash-based transactions, aligning with blockchain-based secure data sharing models in IoT environments. To protect data, AES symmetric encryption is employed, while Local Sensitive Hashing (LSH) facilitates efficient and rapid searches across Blockchain-stored IoT data, ensuring quick access without compromising security. Furthermore, a certificate-less signature scheme is introduced to verify the authenticity of IoT devices and the data they share, reducing the need for complex certificate management. Shamir's secret sharing scheme is used to enhance the security of cryptographic keys, ensuring that sensitive data is securely shared and stored, which aligns with previous work on data security and privacy in IoT systems. As an extension, the project introduces two enhancements: the use of Elliptic Curve Cryptography (ECC) for more efficient encryption, ensuring stronger security with smaller key sizes, and the implementation of cache memory to accelerate LSH search operations, reducing the need for repeated searches for identical queries. This innovative approach not only improves the overall efficiency and security of IoT data sharing but also paves the way for more resilient and responsive IoT applications across various domains such as industrial IoT, healthcare, and smart cities.

Index Terms *- Edge-based Blockchain, Secure Data Sharing, IoT Devices, AES Encryption, Local Sensitive Hashing (LSH), Certificate-less Signature, Shamir's Secret Sharing, Elliptic Curve Cryptography (ECC), Cache Memory, Data Integrity, Tamper-proof Records, IoT Applications, Efficiency, Security.*

1. INTRODUCTION

The Internet of Things (IoT) encompasses a diverse range of applications, including smart cities, transportation, healthcare, and energy management, significantly enhancing user experiences and services [6][10]. Forecasts indicate that the IoT market will witness exponential growth, with investments reaching $4.3 trillion and over 30 billion connected devices by 2024, generating vast amounts of data requiring effective management and sharing [10]. Efficient data sharing among IoT devices enhances contextual understanding, enabling coordinated actions and intelligent decision-making [3][5]. However, challenges such as lack of trust, data tampering, unauthorized access, and privacy concerns hinder effective data sharing, resulting in data silos that impede IoT development [7][8]. The integration of blockchain technology into IoT data sharing frameworks offers a tamper-proof and transparent structure, ensuring data integrity and authenticity while fostering trust among participants in the IoT ecosystem [2][6]. Blockchain-based approaches have been proposed to address issues of data security and privacy in industrial IoT systems, thereby enhancing the reliability of IoT networks [4][18]. This project proposes an Edge-based Blockchain Secure Data Sharing Scheme (EB-SDSS), which combines edge computing and blockchain technologies to address latency, privacy, and performance challenges, enabling secure and efficient data sharing within IoT environments [1][14][15].

2. RELATED WORK

The intersection of IoT, edge computing, and blockchain has garnered significant attention due to its potential to address the challenges of data privacy, security, and efficient sharing. Several studies have explored various solutions to improve IoT data management and sharing, with a focus on utilizing blockchain to enhance security and integrity.

In the context of IoT, the adoption of blockchain technology has been widely discussed as a means to ensure tamper-proof data sharing and transparency. Cui et al. [1] proposed a blockchain-based solution for secure data sharing among vehicles, leveraging consortium blockchain to provide trust and integrity in vehicular networks. Manogaran et al. [2] extended this concept to smart industries, developing a blockchain-assisted secure data sharing model for IoT-based systems. This work highlighted the potential of blockchain to ensure the security and authenticity of data in industrial settings.

Yu et al. [3] further explored blockchain-enhanced data sharing in industrial IoT systems, introducing a mechanism for traceable and direct revocation, which ensures that sensitive information is protected from unauthorized access. In a similar vein, Zheng and Cai [5] proposed a privacy-preserved data sharing model for multiple parties in industrial IoT networks, addressing the challenge of ensuring secure and private data exchanges among various stakeholders.

On the edge computing front, several studies have demonstrated its effectiveness in reducing latency and improving the performance of IoT systems. Xie et al. [6] conducted a survey on blockchain technology applied to smart cities, recognizing edge computing as a critical component for achieving low-latency data processing in such environments. Chen et al. [8] explored the use of edge computing in healthcare applications, enabling fast and secure data sharing for electronic health records. Additionally, Shamir’s secret sharing scheme, as employed in several works [4][12], has been identified as a useful cryptographic method to enhance the security of key management in distributed IoT networks.

Recent advancements have also introduced the combination of edge computing with blockchain to address the scalability and performance limitations of traditional cloud-based models. Xu et al. [16] proposed a blockchain protocol for wireless networks under adversarial conditions, demonstrating the feasibility of combining edge and blockchain for secure communication. The integration of elliptic curve cryptography (ECC) has also been suggested as a more efficient encryption method, ensuring strong security while reducing computational overhead [4][19].

In the area of data sharing, privacy-preserving techniques have been widely researched. For example, Lu et al. [4] investigated the use of federated learning alongside blockchain to enable privacy-preserved data sharing in industrial IoT. Similarly, local sensitive hashing (LSH) techniques have been explored for efficient search operations over blockchain-stored data, providing quick access to large-scale IoT datasets while maintaining privacy [16][17].

This body of work highlights the evolving landscape of IoT data sharing, where the integration of blockchain and edge computing provides a promising solution to the challenges of privacy, security, and performance. The proposed Edge-based Blockchain Secure Data Sharing Scheme (EB-SDSS) builds on these advances, leveraging blockchain’s tamper-proof features and the performance benefits of edge computing to provide an efficient and secure framework for IoT data sharing.

3. MATERIALS AND METHODS

The proposed Edge-based Blockchain Secure Data Sharing Scheme (EB-SDSS) integrates edge computing and blockchain technology to enable secure and efficient data sharing across IoT devices, edge servers, and cloud servers. Blockchain, as a decentralized and distributed ledger, ensures data integrity and transparency through tamper-proof, hash-based transactions, addressing the need for secure data exchange in IoT systems [1], [7], [14]. AES symmetric encryption is employed for securing data during transmission, ensuring confidentiality and data protection [4], [5]. To enhance data retrieval efficiency, Local Sensitive Hashing (LSH) is utilized, supporting scalable and fast access to shared information [11], [13]. Furthermore, Shamir’s secret sharing scheme is adopted to safeguard cryptographic keys, mitigating risks associated with key management and ensuring robust protection of sensitive data [12], [3]. This approach combines blockchain's decentralized security with edge computing's low-latency capabilities, offering a comprehensive solution for secure data sharing in IoT and industrial environments [2], [19].

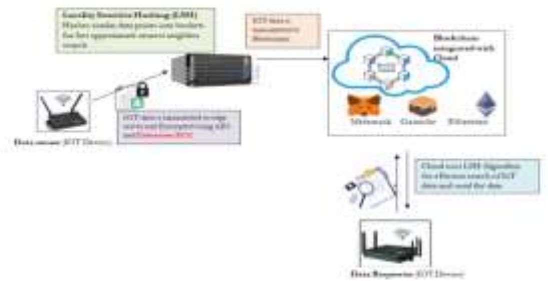


Fig.1 Proposed Architecture

This image (Fig.1) illustration showcases a secure IoT data-sharing system integrates blockchain and Locality Sensitive Hashing (LSH) for efficient and secure data exchange. IoT devices (data owners) encrypt collected data using AES and Extended ECC before sending it to an edge server [4], [5]. The encrypted data is then uploaded to a blockchain, utilizing tools like Metamask, Ganache, and Ethereum for secure storage and transaction management [7], [19]. LSH enhances data retrieval by hashing similar data into buckets for efficient approximate nearest neighbor searches [11], [13]. Data requesters query the cloud, where LSH enables fast retrieval while ensuring privacy and data integrity [3], [14].

i) Implementation:

The implementation of the described system integrates blockchain, IoT, and advanced cryptographic techniques for secure data handling and efficient search. The User Signup and Login modules utilize blockchain to ensure secure registration and authentication, preserving data integrity [7], [14]. In the File Upload module, files are encrypted with AES and ECC algorithms, and signed using a bilinear hash code, guaranteeing data confidentiality and integrity, with hash codes stored on the blockchain for traceability [4], [5], [12]. The LSH Search module leverages Local Sensitive Hashing (LSH) for efficient data retrieval, caching search results on the edge server to speed up subsequent queries [11], [13]. Efficiency Graphs showcase the execution times for signing, encryption, and search processes. The use of ECC enhances encryption efficiency for IoT devices, while Cache Memory stores previously searched queries, reducing computational load and improving search performance [3], [6], [19].

ii) System Modules:

a) User Signup: This module enables new users to register with the application. User details are securely stored on the blockchain, ensuring the integrity and authenticity of the information [7], [14].

b) **Cloud IoT User Login:** Registered users log in to the system by verifying their credentials against the blockchain, ensuring secure access to the platform and protecting against unauthorized entry [6], [7].

c) Data Owner File IoT Upload: Users can upload files, and a Bilinear hash code is generated for signing and verifying file integrity using the blockchain. Files are encrypted with the AES symmetric algorithm and ECC, while a Local Sensitive Hashing (LSH) vector is created from the file contents. The file is stored in the cloud, and the LSH vector and signing hash code are saved in the Edge Blockchain server [4], [5], [11], [12].

d) LSH Data User Search: Users perform keyword searches, with the Edge server using the LSH algorithm to find relevant files based on similarity. This module leverages cache memory to store previous search results, improving retrieval times for repeated queries and reducing the load for LSH vector searches [11], [13].

e) Proposed Efficiency Graph: This module generates graphs to illustrate the execution times of various processes, including signing algorithm key setup, signing messages, verifying messages, and encryption times for AES and ECC algorithms. It highlights the performance advantages of ECC in terms of speed and efficiency for IoT systems [3], [4], [12].

f) Extension Efficiency Graph: This module visualizes search operation execution times using the proposed LSH method with cache memory. It compares search times, demonstrating the enhanced retrieval speed enabled by the cache memory extension [11], [13].

iii) Extension:

The extension of the project aims to optimize both the encryption process and data retrieval by introducing two key enhancements:

a) Elliptic Curve Cryptography (ECC): ECC replaces traditional AES encryption with a more efficient cryptographic technique. ECC provides equivalent security to AES but with smaller key sizes and lower computational overhead, making it more suitable for resource-constrained IoT devices [4], [12]. This shift enhances the performance of encryption and decryption processes in IoT environments.

b) Cache Memory: Cache memory is introduced on edge servers to store previously searched queries and their results. This reduces the need for repetitive searches in the Local Sensitive Hashing (LSH) vector, significantly improving data retrieval speed by preventing redundant computations [11], [13]. The cache ensures faster retrieval for repeated queries, enhancing the overall efficiency of the system.

iv) Technical Implementation:

The Ethereum platform, utilizing Smart Contracts written in Solidity, is employed to securely store property and lease details on the blockchain. The following steps outline the implementation process:

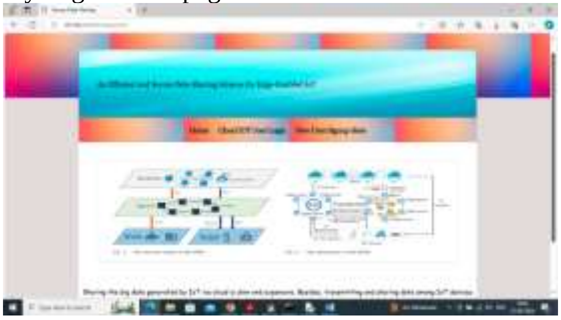
- Initiating Ethereum Tool: Navigate to the hello-eth/node-modules/bin folder and double-click the runBlockchain.bat file to start the Ethereum tool [6], [7].
- Deploying the Smart Contract: Deploy the Smart Contract by running the migrate command. This generates a contract address, which is used in Python to interact with the blockchain [1], [4].
- Interfacing with the Blockchain via Python: Use Python to call the Smart Contract using its address for saving and retrieving data. Comments in the Python script specify how the contract is integrated with the system [5], [3].

This blockchain-based implementation offers a robust and secure framework for managing lease and mortgage processes, reducing fraud and ensuring transparency in property transactions [2], [14].

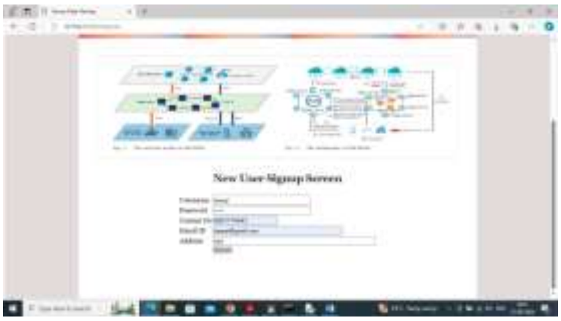
4. RESULTS & DISCUSSION

To run project double click on 'run.bat' file to start python server and get below page

In above screen python server started and now open browser and enter URL as http://127.0.0.1:8000/index.html and press enter key to get below page

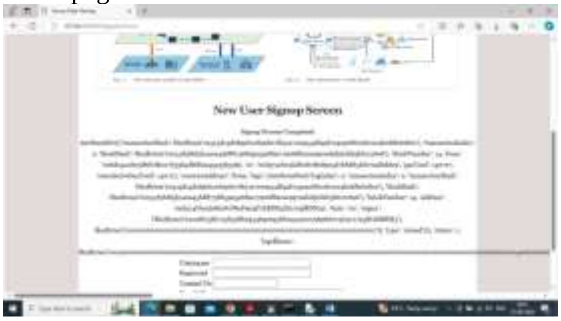


In above screen click on 'New User Signup' link to get below page



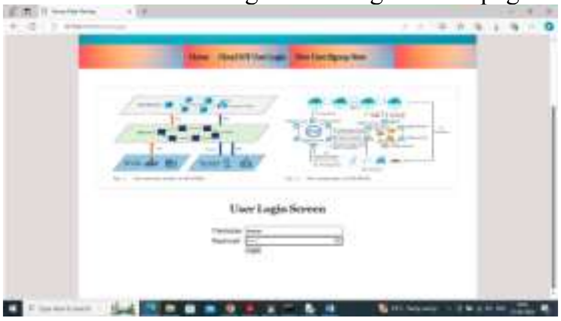
New User Signup Screen

In above screen user is login and after login will get below page



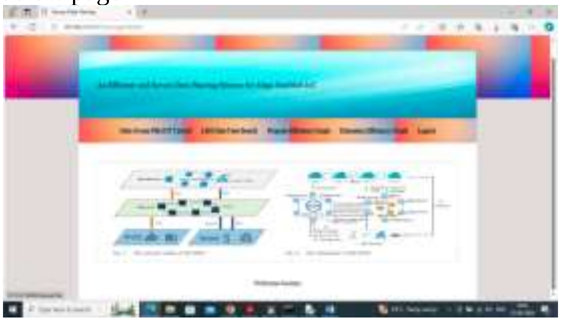
New User Signup Screen

In above screen user detailed saved in Blockchain and then I am displaying all log details obtained from Blockchain which contains details like Block no, transaction no, hash code and many other details. By showing above details you can say to your guide that details are saving in Blockchain. Now click on 'User Login' link to get below page

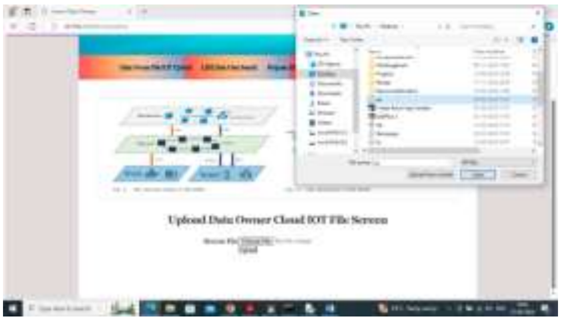


User Login Screen

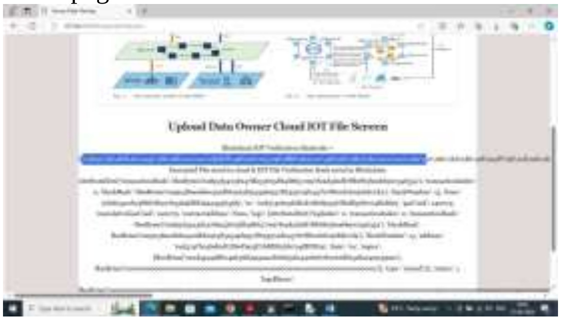
In above screen user is login and after login will get below page



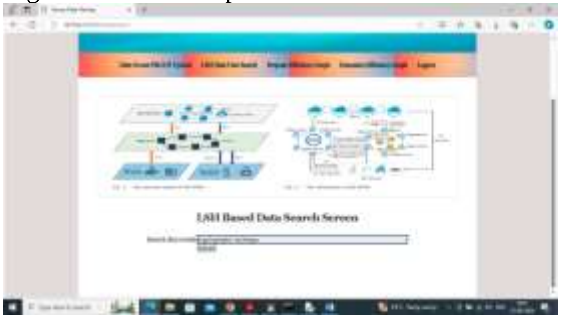
In above screen user can click on 'Data Owner File IOT Upload' link to upload file to Edge and cloud server



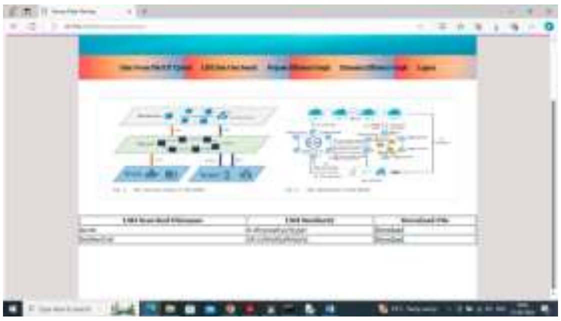
In above screen selecting and uploading file and then click on 'Open and 'Upload' button to save file in Edge Blockchain and cloud and then will get below page



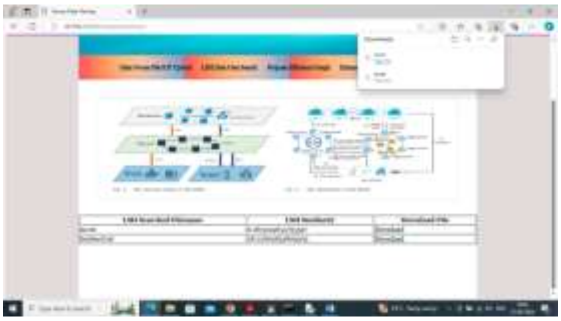
In above screen in blue colour text can see SIGNING hash code generated from uploaded file and then details are saved in Blockchain and showing all log details obtained from Blockchain after storage. Similarly you can upload any number of files. Now click on 'LSH Data User Search' link to get below search option



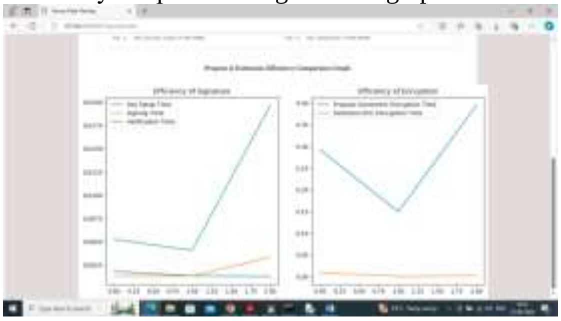
In above screen entered some keywords to search and then press button to get details from Blockchain LSH search



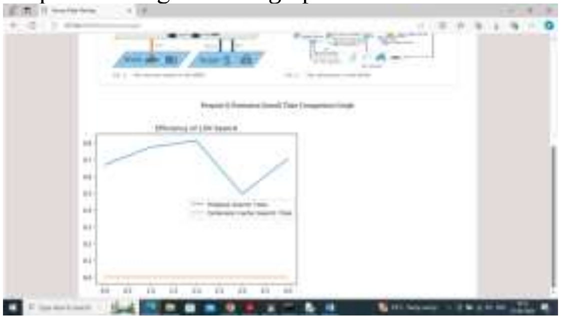
In above screen got search result from LSH along with file names, similarity score and 'Download' option. By clicking on Download link we can download file in decrypted format



In above screen in browser address bar can see file downloaded and similarly you can search for any number of queries. Now click on 'Propose Efficiency Graph' link to get below graph



In above screen in first graph displaying 'Efficiency of signature' where x-axis represents number of file uploaded and y-axis represents execution time and each line represents different task such as Key Setup time, signing and verifying time. In second graph showing encryption time for Propose AES and extension ECC algorithm and in both algorithms can see 'Extension ECC' tool less execution time and its faster than propose algorithm. Now click on 'Extension Efficiency Graph' link to get below graph



In above graph displaying efficiency of search time with propose and extension cache technique. In above graph x-axis represents 'Number of Query Search' and y-axis represents 'Search Time' and then blue line represents propose LSH search time and orange line represents Cache search time.

Similarly by following above screens you can run complete code

5. CONCLUSION

The integration of blockchain technology ensures tamper-proof storage and verification of data, fostering trust and integrity in information shared among IoT devices. By leveraging edge servers positioned closer to IoT devices, the system reduces data transfer time to cloud servers, significantly enhancing responsiveness and overall performance. The use of Local Sensitive Hashing (LSH) and caching techniques optimizes data retrieval, enabling quick access to relevant information while reducing computational load. Additionally, the implementation of certificate-less signature schemes within the blockchain framework strengthens device authentication, ensuring secure and reliable data sharing across the network. To balance strong encryption and performance efficiency, the system employs AES symmetric encryption alongside lightweight Elliptic Curve Cryptography (ECC), which reduces execution time while maintaining robust security. This combination ensures an efficient and secure framework for data sharing in edge-enabled IoT environments.

Future Scope: could focus on scaling the system to handle the increasing number of IoT devices and users, ensuring efficient data sharing as the IoT ecosystem expands. The integration of Artificial Intelligence (AI) and Machine Learning (ML) can enhance data analysis, predictive maintenance, and decision-making, ultimately improving user experience and operational efficiency. Additionally, enabling interoperability with other blockchain networks could facilitate seamless data sharing and collaboration across heterogeneous IoT systems, fostering a more connected and efficient ecosystem. Future iterations may also prioritize improving real-time data processing capabilities, which is critical for applications in smart cities, healthcare, and industrial automation, where immediate responses are essential.

REFERENCES

[1] J. Cui, F. Ouyang, Z. Ying, L. Wei and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain", IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 8857-8867, Jul. 2022.

[2] 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 Trans. Rel., vol. 71, no. 1, pp. 348-358, Mar. 2022.

[3] K. Yu, L. Tan, M. Aloqaily, H. Yang and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT", IEEE Trans. Ind. Informat., vol. 17, no. 11, pp. 7669-7678, Nov. 2021.

[4] Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT", IEEE Trans. Ind. Informat., vol. 16, no. 6, pp. 4177-4186, Jun. 2020.

[5] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs", IEEE J. Sel. Areas Commun., vol. 38, no. 5, pp. 968-979, May 2020.

[6] J. Xie et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges", IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2794-2830, 2019.

[7] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar and K.-K. R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system", Comput. Secur., vol. 85, pp. 288-299, Aug. 2019.

[8] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing", Future Gener. Comput. Syst., vol. 95, pp. 420-429, Jun. 2019.

[9] A. Jindal, G. S. Aujla and N. Kumar, "Survivor: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment", Comput. Netw., vol. 153, pp. 36-48, Apr. 2019.

[10] V. Liu, "Business benefits of the Internet of Things: A Gartner trend insightreport", Gartner, 2019, [online] Available: https://www.gartner.com/en/doc/3806366-business-benefits-of-the-internet-of-things-a-gartner-trend-insight-report.

[11] B. Cui, Z. Liu and L. Wang, "Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage", IEEE Trans. Comput., vol. 65, no. 8, pp. 2374-2385, Aug. 2016.

[12] N. Chen, J. Li, Y. Zhang and Y. Guo, "Efficient CP-ABE scheme with shared decryption in cloud storage", IEEE Trans. Comput., vol. 71, no. 1, pp. 175-184, Jan. 2022.

[13] T. Wang, Y. Lu, J. Wang, H.-N. Dai, X. Zheng and W. Jia, "EIHDP: Edge-intelligent hierarchical dynamic pricing based on cloud-edge-client collaboration for IoT systems", IEEE Trans. Comput., vol. 70, no. 8, pp. 1285-1298, Aug. 2021.

[14] R. Yang, F. R. Yu, P. Si, Z. Yang and Y. Zhang, "Integrated blockchain and edge computing systems: A survey some research issues and challenges", IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1508-1532, 2019.

[15] R. Li, T. Song, B. Mei, H. Li, X. Cheng and L. Sun, "Blockchain for large-scale Internet of Things data storage and protection", IEEE Trans. Services Comput., vol. 12, no. 5, pp. 762-771, Sep./Oct. 2019.

[16] M. Xu, F. Zhao, Y. Zou, C. Liu, X. Cheng and F. Dressler, "BLOWN: A blockchain protocol for single-hop wireless networks under adversarial SINR", IEEE Trans. Mobile Comput., vol. 22, no. 8, pp. 4530-4547, Aug. 2023

[17] M. Xu, C. Liu, Y. Zou, F. Zhao, J. Yu and X. Cheng, "wChain: A fast fault-tolerant blockchain protocol for multihop wireless networks", IEEE Trans. Wireless Commun., vol. 20, no. 10, pp. 6915-6926, Oct. 2021.

[18] M. Xu, Z. Zou, Y. Cheng, Q. Hu, D. Yu and X. Cheng, "SPDL: A blockchain-enabled secure and privacy-preserving decentralized learning system", IEEE Trans. Comput., vol. 72, no. 2, pp. 548-558, Feb. 2023.

[19] M. Xu, S. Liu, D. Yu, X. Cheng, S. Guo and J. Yu, "CloudChain: A cloud blockchain using shared memory consensus and RDMA", IEEE Trans. Comput., vol. 71, no. 12, pp. 3242-3253, Dec. 2022.

[20] K.-K. R. Choo, S. Gritzalis and J. H. Park, "Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities", IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3567-3569, Aug. 2018.

AUTHOR PROFILE

Mr. K. Uday Kiran is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Bapatla Engineering College, Bapatla. His research interests include Machine Learning, Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Mr. Kancharla Sai [2]has received his MCA (Masters of Computer Applications) from QIS college of Engineering and Technology Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh-523272 affiliated to JNTUK in 2023-2025