Lightweight Cryptographic Framework for Trustworthy Data Exchange in Edge-Assisted IoT Networks

Durga A[1], T Anil Kumar [2*], K Yatheendra [3], G Viswanath [4]

[1] P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
E-mail: ad6893696@gmail.com ; ORCID-ID: 0009-0008-9421-3600

[2] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology,Puttur,
E-mail: anil.thumburu@gmail.com ; ORCID-ID: 0009-0003-3312-3031

[3] Assistant Professor, Department of AI &ML, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: k.yatheendra84@gmail.com ; ORCID-ID: 0009-0003-1382-8587

[4] Associate Professor, Dept. of AI & ML, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: viswag111@gmail.com ; ORCID-ID: 0009-0001-7822-4739

Area/Section: Engineering and Technology
Type of the Paper: Regular Paper
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.15726056
Google Scholar Citation: IJMTS

How to Cite this Paper:
Durga, A., Kumar, T. A., Yatheendra, K. & Viswanath, G. (2025). Lightweight Cryptographic Framework for Trustworthy Data Exchange in Edge-Assisted IoT Networks. *International Journal of Management, Technology, and Social Sciences (IJMTS), 10*(1), 319-333. DOI: https://doi.org/10.5281/zenodo.15726056

International Journal of Management, Technology, and Social Sciences (IJMTS)
A Refereed International Journal of Srinivas University, India.

CrossRef DOI: https://doi.org/10.47992/IJMTS.2581.6012.0389

Received on: 18/04/2025
Published on: 24/06/2025

© With Authors.

This work is licensed under a Creative Commons Attribution-Non-Commercial 4.0 International License subject to proper citation to the publication source of the work.
Disclaimer: The scholarly papers as reviewed and published by Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the SP. The SP disclaims of any harm or loss caused due to the published content to any party.

Lightweight Cryptographic Framework for Trustworthy Data Exchange in Edge-Assisted IoT Networks

Durga A[1], T Anil Kumar [2*], K Yatheendra [3], G Viswanath [4]

[1] P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,

E-mail: ad6893696@gmail.com ; ORCID-ID: 0009-0008-9421-3600

[2] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology,Puttur,

E-mail: anil.thumburu@gmail.com ; ORCID-ID: 0009-0003-3312-3031

[3] Assistant Professor, Department of AI &ML, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: k.yatheendra84@gmail.com ; ORCID-ID: 0009-0003-1382-8587

[4] Associate Professor, Dept. of AI & ML, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: viswag111@gmail.com ; ORCID-ID: 0009-0001-7822-4739

ABSTRACT

To address the latency and security challenges inherent in traditional cloud-based systems, this project introduces a Lightweight Cryptographic Framework designed for secure and efficient data exchange in edge-assisted IoT networks. The core of the system is an Edge-Based Blockchain Secure Data Sharing Scheme (EB-SDSS), which decentralizes data processing by enabling edge servers to interact directly with IoT devices. This significantly reduces data transfer delays and enhances performance compared to conventional cloud-centric models. The integration of blockchain technology ensures tamper-proof and transparent data storage through hash-based transaction records. This guarantees data integrity and trust in the system. To protect sensitive IoT data, AES symmetric encryption is employed for robust and lightweight encryption, while Locality-Sensitive Hashing (LSH) facilitates fast and efficient data retrieval across the blockchain. To eliminate the overhead of certificate management, a certificate-less signature scheme is implemented to authenticate IoT devices and verify data legitimacy. In addition, Shamir's Secret Sharing method is utilized to protect cryptographic keys, enhancing the secure exchange and storage of sensitive information. As an extension, the project incorporates Elliptic Curve Cryptography (ECC) to offer strong encryption with smaller key sizes, optimizing resource usage on constrained IoT devices. Furthermore, cache memory is leveraged to accelerate LSH operations, reducing the computational burden for repeated queries. By combining these cryptographic techniques and edge-computing principles, the framework enhances the security, efficiency, and responsiveness of IoT data sharing. It is especially suitable for sectors such as industrial automation, healthcare systems, and smart cities, where real-time data integrity and confidentiality are critical. This innovative approach lays the groundwork for scalable and trustworthy IoT ecosystems, supporting more agile and secure applications in next-generation smart environments.

Keywords: Edge-based Blockchain, Secure Data Sharing, IoT Devices, AES Encryption, Local Sensitive Hashing (LSH), Elliptic Curve Cryptography (ECC).

1. INTRODUCTION:

Ranging from smart cities to transportation, healthcare, and energy management, the "internet of things (IoT)" includes a wide spectrum of uses that greatly improve user experiences and services. Many of which are smart towns, transportation, healthcare, and energy management, the internet of things (IoT) includes a wide spectrum of applications [6] [10]. Forecasts factor to exponential growth of the IoT sector, with investments hitting $4.3 trillion and more than 30 billion linked devices by 2024 producing huge volumes of data needing efficient management and sharing [10]. Green data exchange among IoT devices improves contextual awareness, hence enabling coordinated actions and smart decision-making [3][5]. effective data

exchange is hampered, however, via issues including mistrust, data manipulation, illegal access, and privacy issues, which create data silos blocking IoT progress [7][8]. In IoT data sharing systems, the use of blockchain era provides a transparent and tamper-proof framework guaranteeing data integrity and authenticity and building confidence among IoT ecosystem members [2][6]. Proposed to solve problems of data security and privacy in industrial IoT systems, blockchain-based solutions might thereby improve the dependability of IoT networks [4] [18]. This work offers an "edge-based Blockchain secure data Sharing Scheme (EB-SDSS)", which uses blockchain and edge computing technologies to solve latency, privacy, and performance issues, hence allowing safe and quick data sharing inside IoT contexts [1][14][15].

2. OBJECTIVES:

Enhancing secure and efficient data sharing in edge-assisted IoT environments is vital for reducing latency and ensuring trust. This work proposes a lightweight cryptographic framework combining blockchain, advanced encryption, and optimized search mechanisms to support scalable, real-time IoT data exchange.

(1) To design a decentralized data sharing scheme using edge servers and blockchain technology, ensuring tamper-proof and trustworthy communication between IoT devices and servers while minimizing latency and dependency on centralized cloud infrastructure, thereby improving real-time responsiveness in distributed IoT ecosystems.

(2) To implement a lightweight security mechanism integrating AES encryption, certificate-less signatures, and Shamir's Secret Sharing to protect sensitive IoT data, reduce cryptographic overhead, eliminate complex certificate management, and ensure secure key distribution across resource-constrained edge and IoT environments.

(3) To enhance data retrieval efficiency by employing "Locality-Sensitive Hashing (LSH)" for fast search operations on blockchain-stored data and optimize repeated queries using cache memory, along with adopting "Elliptic Curve Cryptography (ECC)" for robust encryption with minimal key size and computational cost.

3. REVIEW OF LITERATURE/ RELATED WORKS:

Its promise to solve the issues of data privacy, security, and efficient sharing has drawn great interest at the junction of IoT, edge computing, and blockchain. With an eye towards using blockchain to strengthen safety and integrity, several research have investigated different ways to improve IoT data management and sharing. Blockchain technology's use in IoT has been hotly debated as a way to guarantee tamper-proof data sharing and openness. Using consortium blockchain to offer trust and integrity in vehicular networks, Cui et al. [1] developed a blockchain-based system for secure data sharing among automobiles. Manogaran et al. [21] applied this idea to smart industries, creating a blockchain-assisted secure data sharing architecture for IoT-based devices. This paper underlined how blockchain may guarantee the security and authenticity of data in industrial environments.

Yu et al. [3] investigated blockchain-enhanced data sharing in industrial IoT systems further, proposing a technique for traceable and direct revocation that guarantees critical information is shielded from illegal access. Aiming at the difficulty of guaranteeing secure and private data exchanges among many stakeholders, Zheng and Cai [5] suggested a privacy-preserved data sharing model for several parties in industrial IoT networks in a similar manner.

Regarding edge computing, various research have shown its capacity to lower latency and enhance IoT system performance. Recognising edge computing as a key element for reaching low-latency data processing in such contexts, Xie et al. [25] performed a survey on blockchain technology applied to smart towns. Chen et al. [27] investigated edge computing in healthcare applications, hence facilitating quick and secure data sharing for electronic health facts. Shamir's secret sharing approach used in several studies [23][30] has also been recognised as a helpful cryptographic technique to strengthen the security of key management in remote IoT networks.

Recent developments have also brought together edge computing and blockchain to solve the scalability and performance constraints of conventional cloud-based solutions. Xu et al. [35] showed the viability of merging facet and blockchain for comfy communication by suggesting a blockchain protocol for wireless networks beneath hostile settings. a few have additionally proposed the inclusion of "elliptic curve cryptography (ECC)" as a more green encryption technique, therefore guaranteeing good security and lowering computational load [23][19].

Privacy-preserving methods have been extensively investigated in the field of data sharing. For instance, Lu et al. [23] looked at how federated learning used with blockchain can let industrial IoT share data while preserving anonymity. Likewise, "local sensitive hashing (LSH)" methods have been investigated for efficient seek operations over blockchain-stored data, offering rapid access to large-scale IoT datasets while preserving anonymity [35] [17].

This body of work emphasises the changing terrain of IoT data exchange, where the combination of blockchain and area computing offers a hopeful answer to the issues of privacy, security, and performance. Building on these developments, the suggested "erea-based Blockchain secure data exchange Scheme (EB-SDSS)"offers a quick and safe framework for IoT data exchange via using blockchain's tamper-proof qualities and the performance advantages of edge computing.

Table 1: Comparison Table for Related Work

Sl. No	Area & Focus of the Research	The result of the Research	Reference
1	Secure data sharing and access control in IIoT environments.	Reduced key sizes and overhead with enhanced traceability and revocation.	K. Yu, L. Tan., et.al., (2021). [3]
2	Dynamic pricing and resource optimization in edge-enabled IoT systems.	Improved service quality and provider profits through intelligent pricing.	T. Wang, Y. Lu, J. Wang., et.al., (2021) [13]
3	Blockchain protocol optimization for multihop wireless network environments.	Enhanced efficiency and fault tolerance in wireless blockchain communication.	M. Xu, C. Liu, Y. Zou., et.al., (2021) [17]
4	Secure decentralized learning with blockchain and privacy-preserving techniques.	Improved learning efficiency with strong privacy and fault tolerance.	M. Xu, Z. Zou, Y. Cheng., et.al., (2023) [18]
5	Blockchain integration with cloud computing using shared-memory consensus.	Achieved efficient, secure blockchain performance in cloud environments.	M. Xu, S. Liu, D. Yu, X. Cheng, et.al., (2022) [19]

4. MATERIALS AND METHODS:

The suggested "edge-based Blockchain secure data Sharing Scheme (EB-SDSS)" allows safe and quick facts sharing among IoT devices, area servers, and cloud servers by combining edge computing with blockchain technology. Addressing the demand for safe data exchange in IoT systems, blockchain as a decentralised and distributed ledger guarantees data integrity and transparency by means of tamper-proof, hash-based transactions [1], [7], [14]. Data is secured during transmission using AES symmetric encryption, hence guaranteeing secrecy and data protection [4], [5]. "Local sensitive Hashing (LSH)" is used to improve data retrieval efficiency by enabling quick and scalable access to shared information [11], [13]. moreover, Shamir's secret sharing system is used to secure cryptographic keys, hence reducing key management issues and guaranteeing strong security of sensitive data [12], [3]. offering a complete solution for safe data sharing in IoT and industrial settings, this method combines the low-latency capabilities of edge computing with the distributed security of blockchain [2], [19].

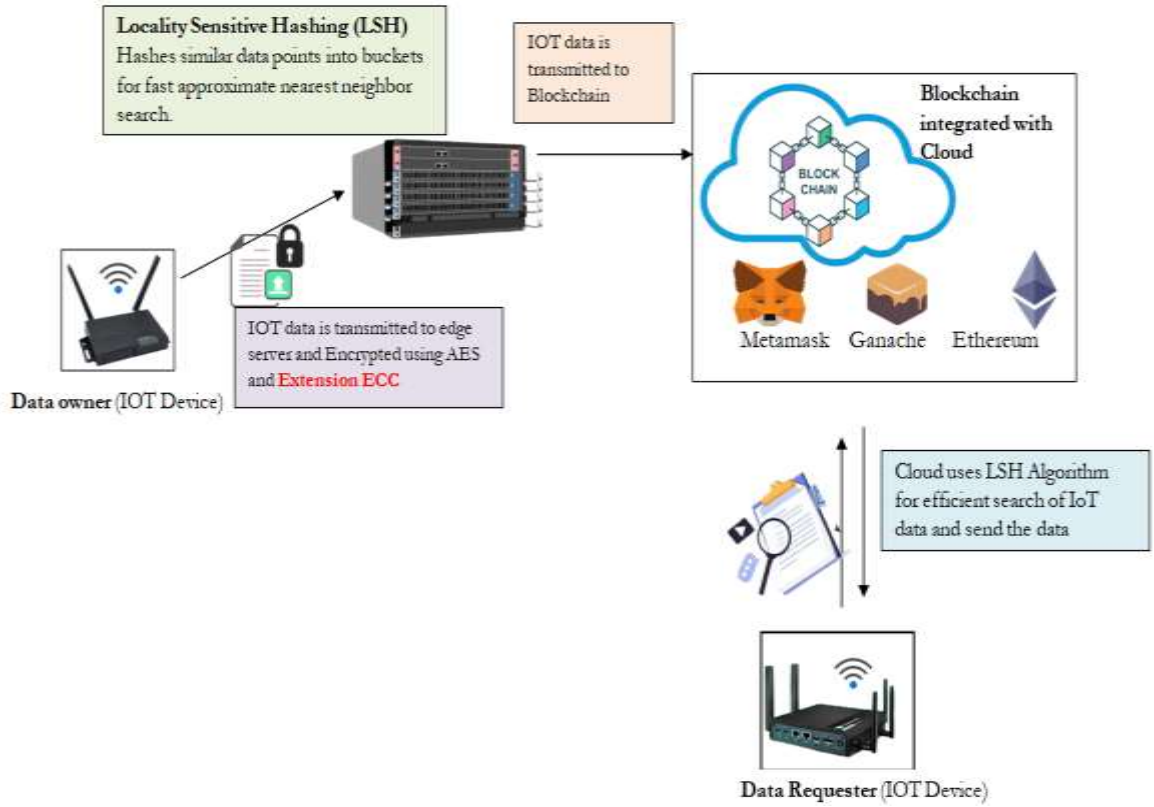


Fig 1: Proposed Architecture

This graphic (Fig.1) depicts a safe IoT data-sharing system combining "Locality sensitive Hashing (LSH)" and blockchain for efficient and comfy data transfer. Before delivering collected data to a part server [4], [5], IoT devices (data owners) encrypt it using AES and extended ECC. Using technologies including Metamask, Ganache, and Ethereum for safe storage and transaction control, the encrypted data is subsequently sent to a blockchain [7], [19]. By hashing comparable facts into buckets for quick approximate closest neighbour searches, LSH improves data retrieval [11], [13]. Data requesters seek the cloud; LSH guarantees data integrity and privacy [3], [14] even as it allows rapid recovery.

4.1 Implementation:

The disclosed system's implementation combines blockchain, IoT, and sophisticated cryptographic approaches for green seek and safe statistics management. Usingblockchain, the user Signup and Login modules guarantee safe registration and authentication, hence protecting data integrity [7], [14]. files are encrypted with AES and ECC methods in the file add module, and signed using a bilinear hash code, therefore ensuring data secrecy and integrity; hash codes are recorded on the blockchain for traceability [4], [5], [12]. For quick data retrieval, the LSH search module uses "local sensitive Hashing (LSH)", caching search results on the edge server to accelerate following queries [11], [13]. Efficiency Graphs display the execution times for signing, encryption, and search operations. While Cache memory keeps previously searched queries, hence lowering computing burden and enhancing search performance [3], [6], [19], ECC improves encryption efficiency for IoT devices.

4.2 System Modules:

To implement this project we are using the given modules.

4.2.1 User Signup

This module lets first-time user's sign up for the program. stored safely on the blockchain, user information guarantees its integrity and authenticity [7], [14].

4.2.2 Cloud IoT User Login

Registered users authenticate their credentials against the blockchain to log into the system, hence guaranteeing safe access to the platform and guarding against illegal entry [6], [7].

4.2.3 Data Owner File IoT Upload

files can be uploaded by users; a bilinear hash code is produced utilising the blockchain for signing and validating file integrity. A "local sensitive Hashing (LSH)" vector is generated from the file contents while AES symmetric method and ECC encrypts files. stored in the cloud, the file's signing hash code and LSH vector are kept in the edge Blockchain server [4], [5], [11], [12].

4.2.4 LSH Data User Search

With the edge server applying the LSH algorithm to locate pertinent files depending on similarity, users do key-word searches. by using cache memory to keep past seek results, this module enhances retrieval speeds for repeated queries and lowers the LSH vector search load [11], [13].

4.2.5 Proposed Efficiency Graph

including signature algorithm key setup, signing messages, verifying messages, and encryption times for AES and ECC algorithms, this module produces graphs to show the execution times of several activities. It emphasises the speed and efficiency performance benefits of ECC for IoT systems [3], [4], [12].

4.2.6 Extension Efficiency Graph

using the suggested LSH technique with cache memory, this module shows search operation execution times. It contrasts search times to show the improved retrieval speed made possible by the cache memory increase [11], [13].

4.3 Extension:

by means of major improvements, the project's extension seeks to maximise data recovery as well as the encryption process.

4.3.1 Elliptic Curve Cryptography (ECC)

ECC uses a more efficient cryptographic method to replace conventional AES encryption. ECC is better appropriate for IoT devices under limited resources since it offers equal security to AES but with smaller key sizes and less computational load [4], [12]. In IoT settings, this change improves the performance of encryption and decryption processes.

4.3.2 Cache Memory

edge servers provide cache memory to keep previously searched queries and their results. by avoiding duplicate calculations, this greatly increases data retrieval performance by reducing the requirement for repeated searches in the "local sensitive Hashing (LSH)" vector [11], [13]. by guaranteeing quicker retrieval for repeated queries, the cache improves the general system efficiency.

4.4 Technical Implementation:

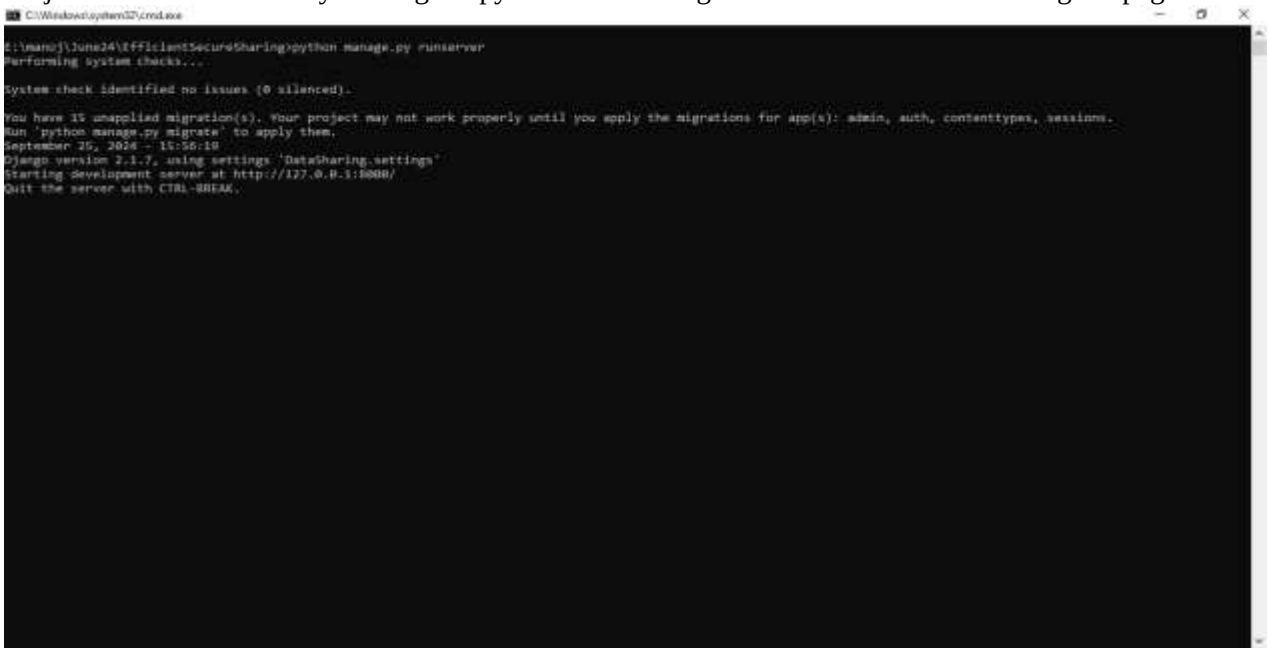
Property and hire information are stored on the blockchain using the Ethereum platform, which uses smart Contracts written in Solidity to do so. The next actions describe how to carry out the plan:

- To launch the Ethereum tool [6], [7], go to the hello-eth/node-modules/bin directory and double-click the runBlockchain.bat file.
- Run the migrate command to deploy the smart contract. A contract address created by this is utilised in Python to connect with the blockchain [1], [4].
- Using Python to call the smart contract using its address for saving and retrieving data, you may interface with the Blockchain. The Python script's comments indicate how the contract [5], [3] interacts with the system.

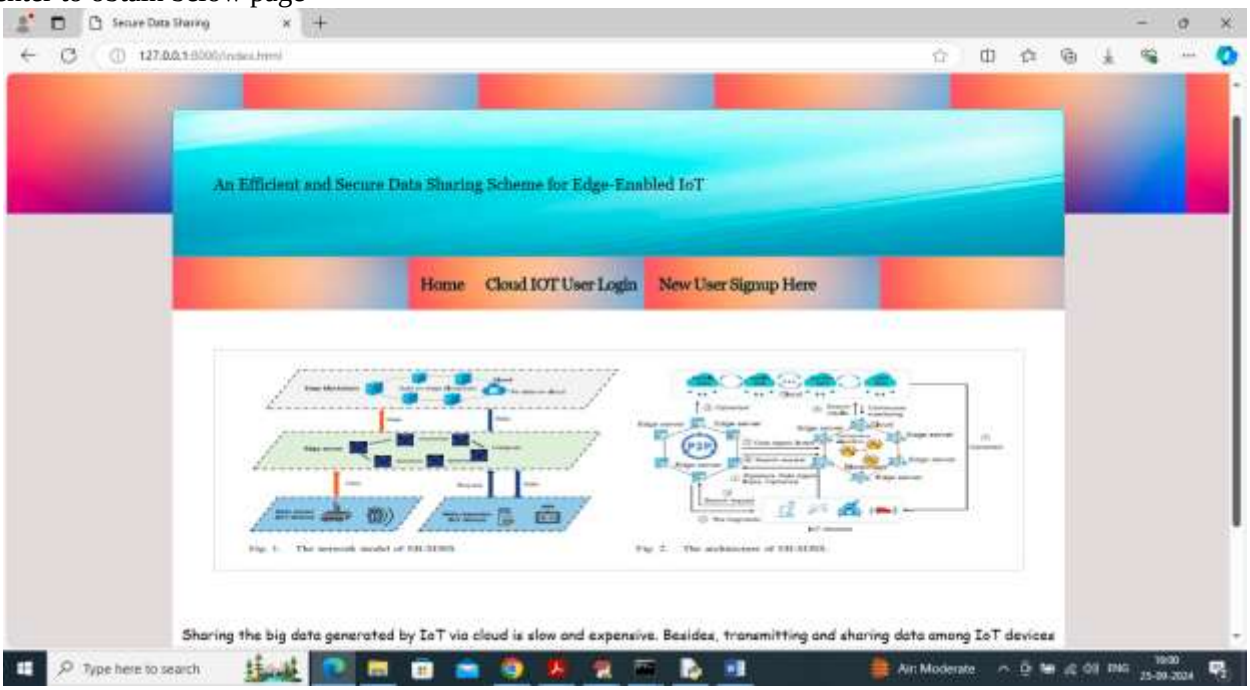
Reducing fraud and guaranteeing openness in property transactions, this blockchain-based system provides a strong and safe foundation for controlling lease and mortgage operations [2], [14].

5. RESULTS AND DISCUSSION:

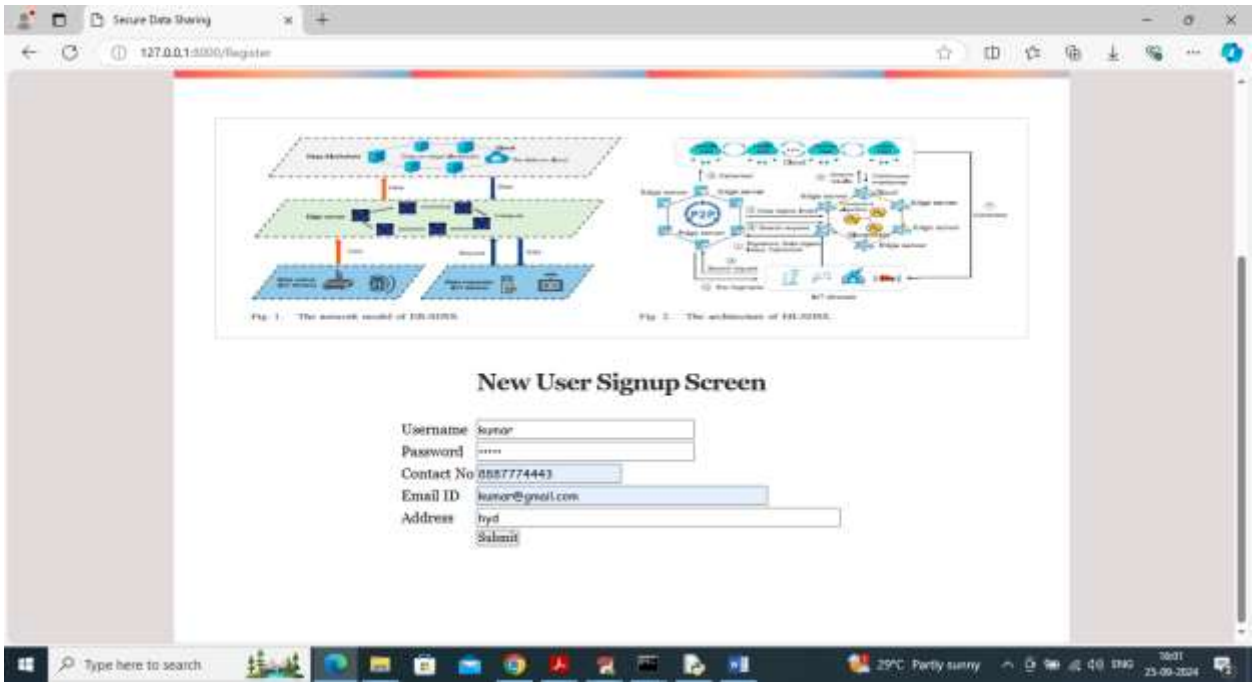
Project double click runs by starting the python server using the 'run.bat' file and retrieving the page below.



Python server launched in above screen; now open browser, type http://127.0.0.1:8000/index.html and hit enter to obtain below page

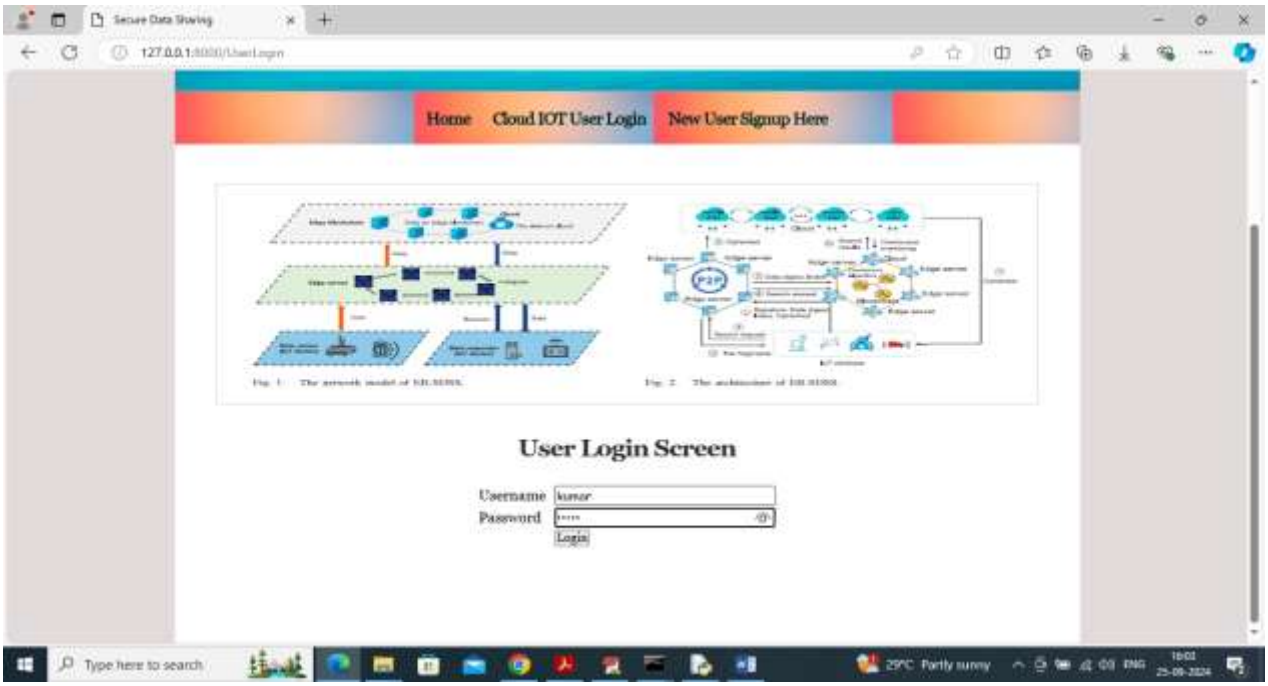


To reach beneath page, click on 'New user Signup' option in above screen

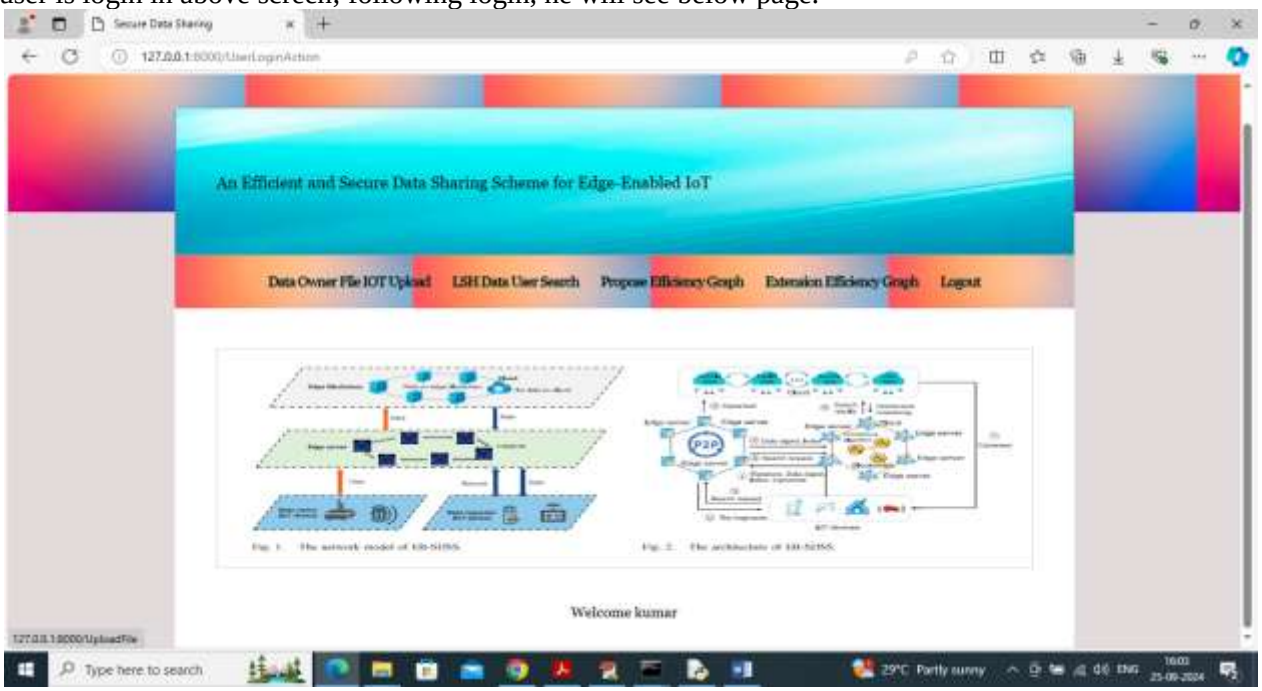


user is login in above screen; following login, he will receive below page.

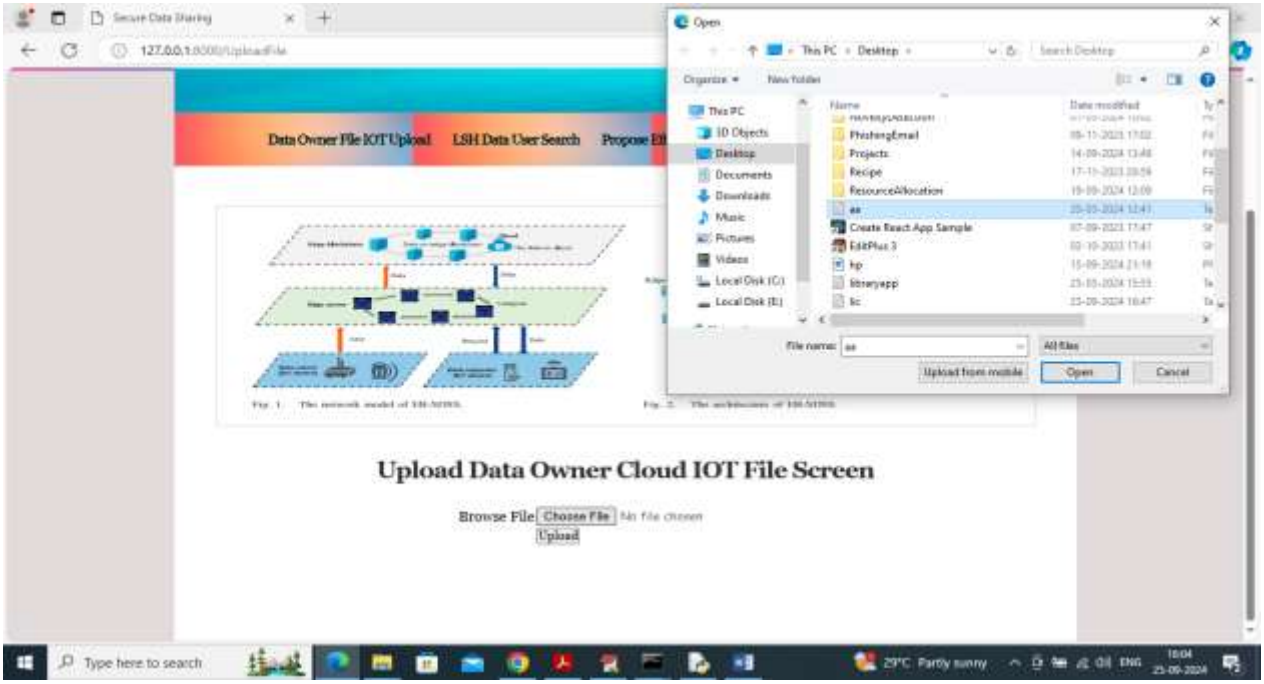
In above screen user detailed saved in Blockchain and then i am showing all log details collected from Blockchain which contains details like Block no, transaction no, hash code and many other details. showing above information allows you to inform your guide that info are saving on Blockchain. To get below page, now click on 'user Login' link



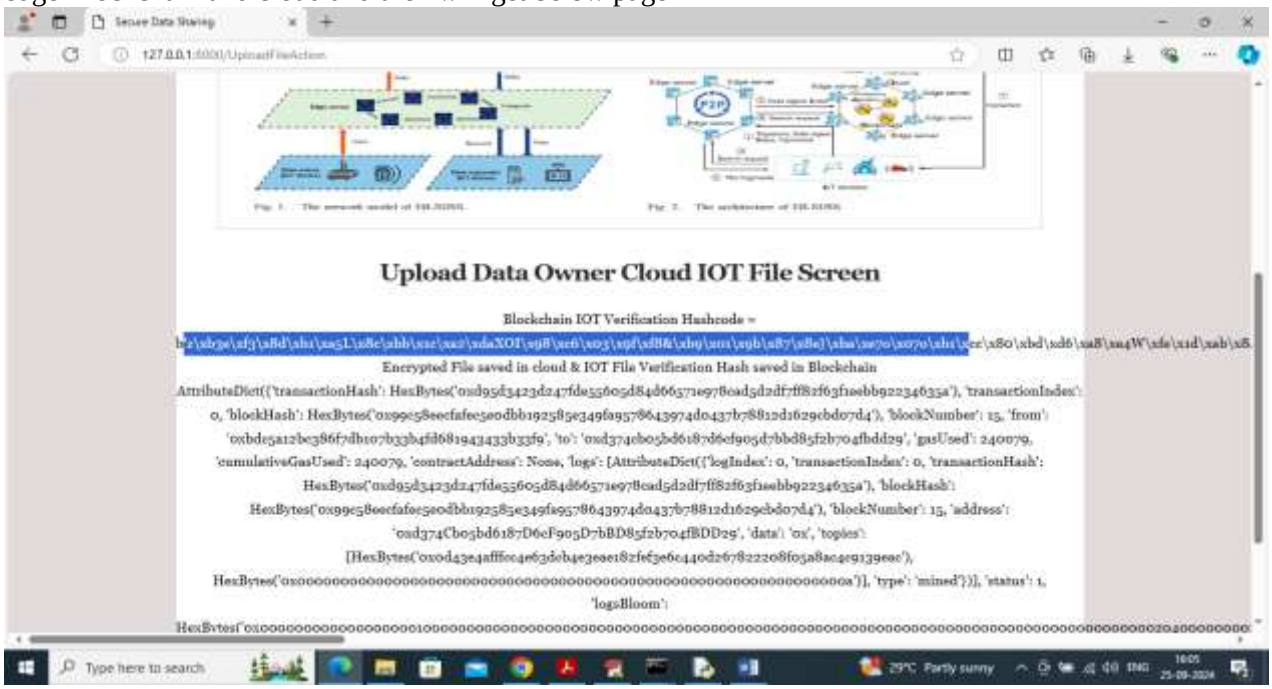
user is login in above screen; following login, he will see below page.



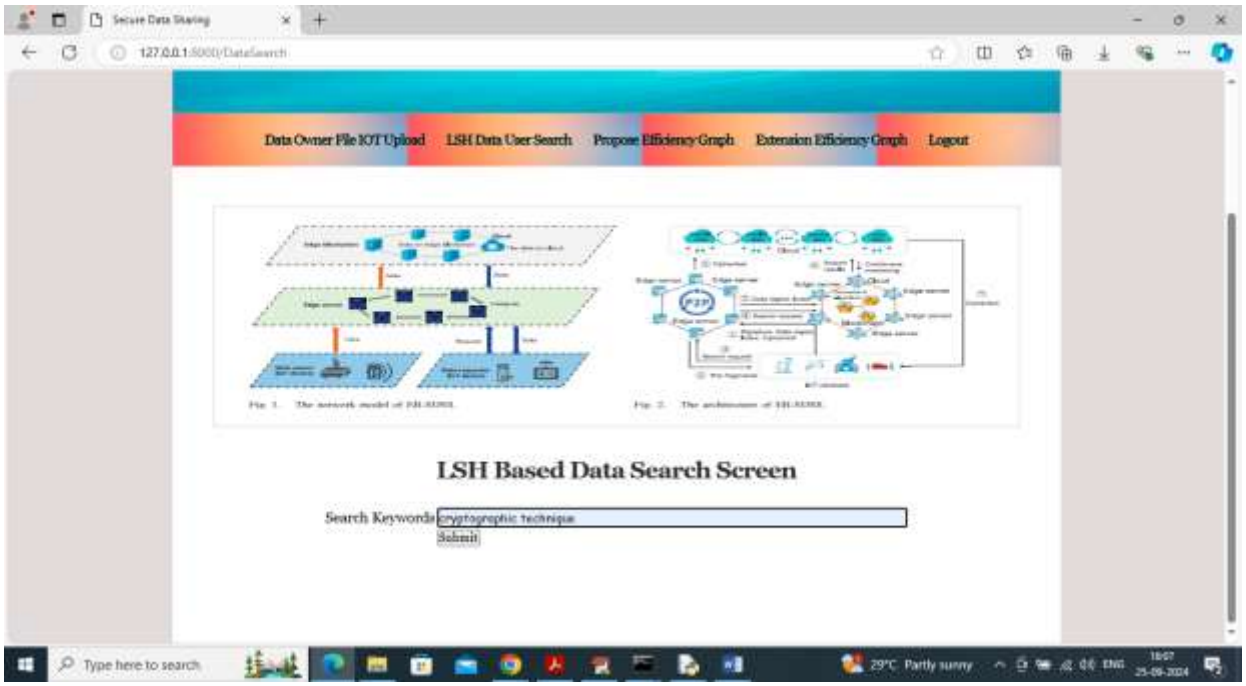
user can click on 'data owner file IOT upload' link in above screen to upload file to edge and cloud server



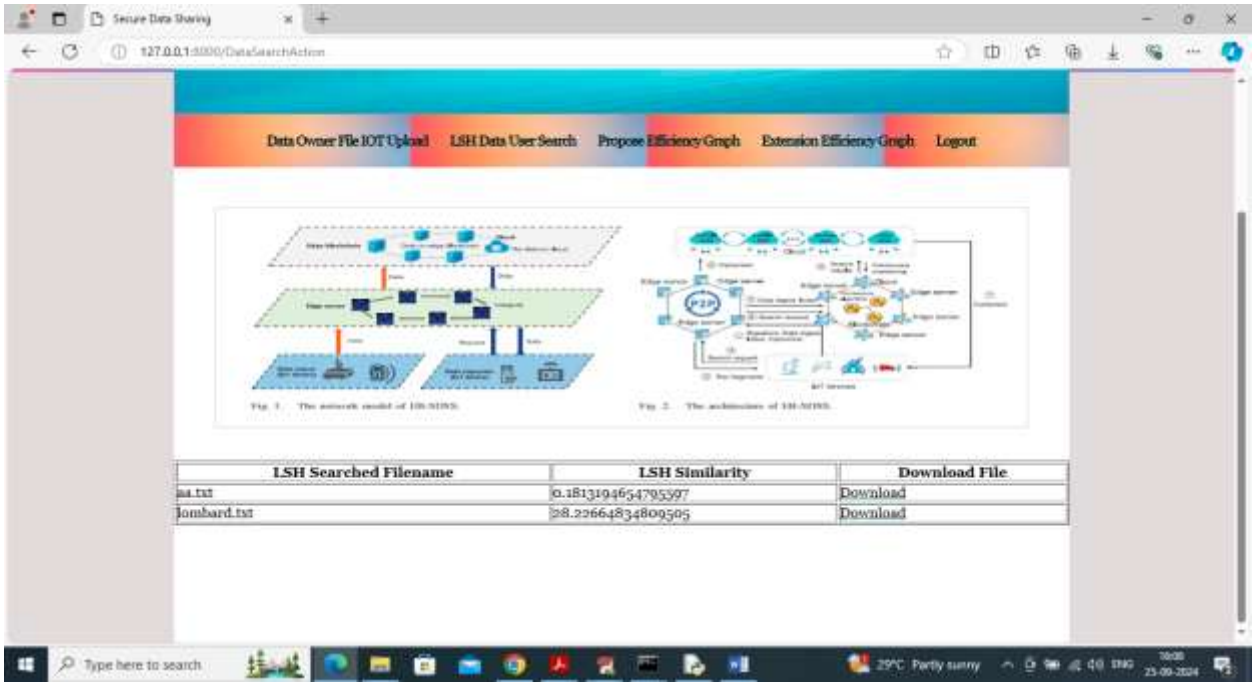
In above screen selecting and uploading file and then click on 'Open and 'upload' button to save file in edge Blockchain and cloud and then will get below page



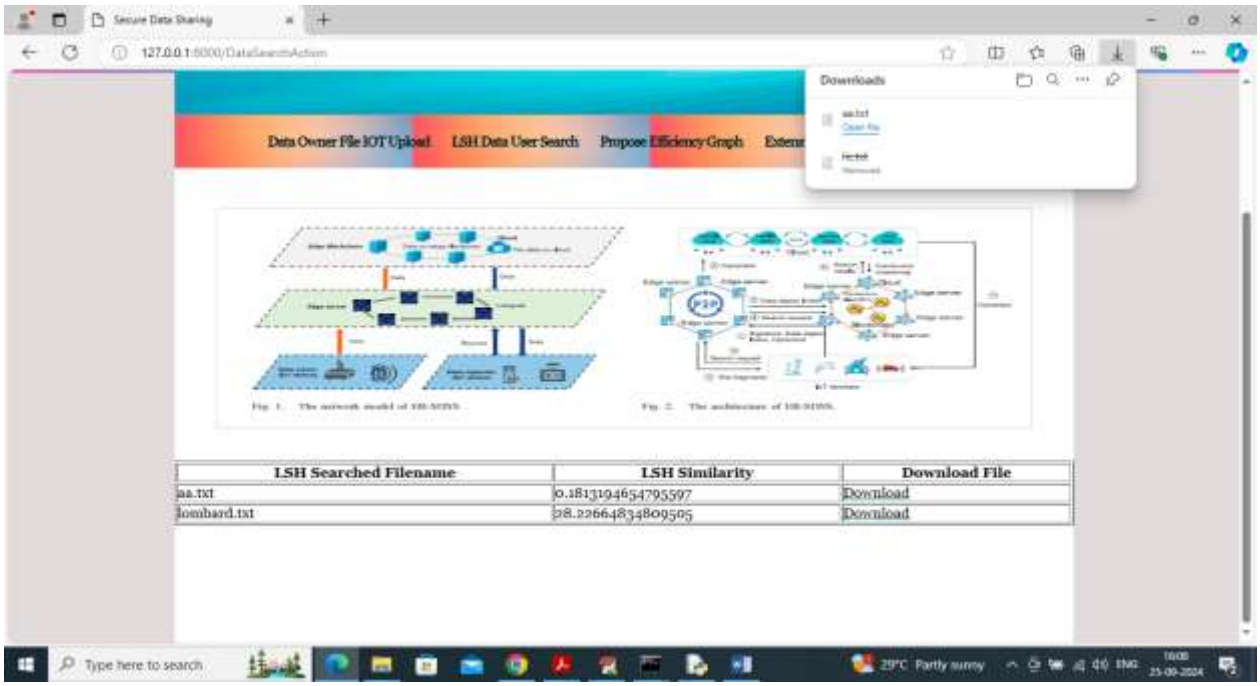
The above screen in blue colour text shows SIGNING hash code produced from uploaded file, then details are saved in Blockchain and all log information acquired from Blockchain after storage is displayed. Likewise, you may submit any quantity of files. Now click on the link for 'LSH data user search' to obtain below search option



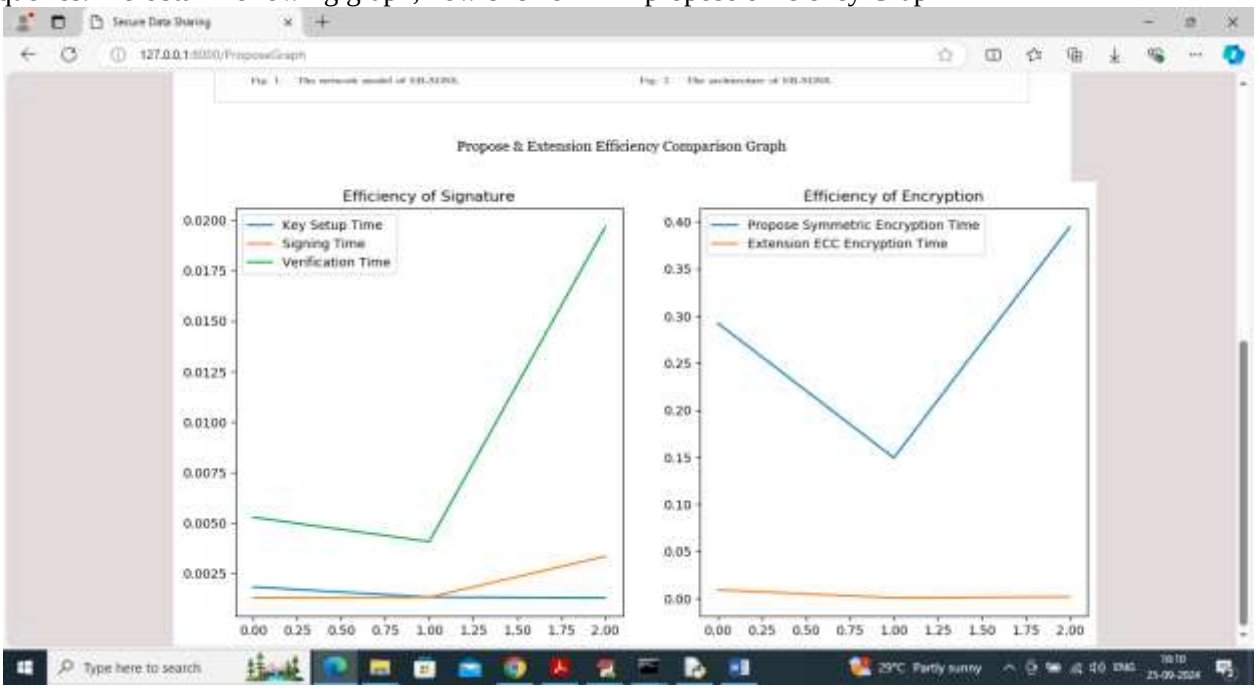
Above screen typed some terms to search and then press button to receive details from Blockchain LSH search



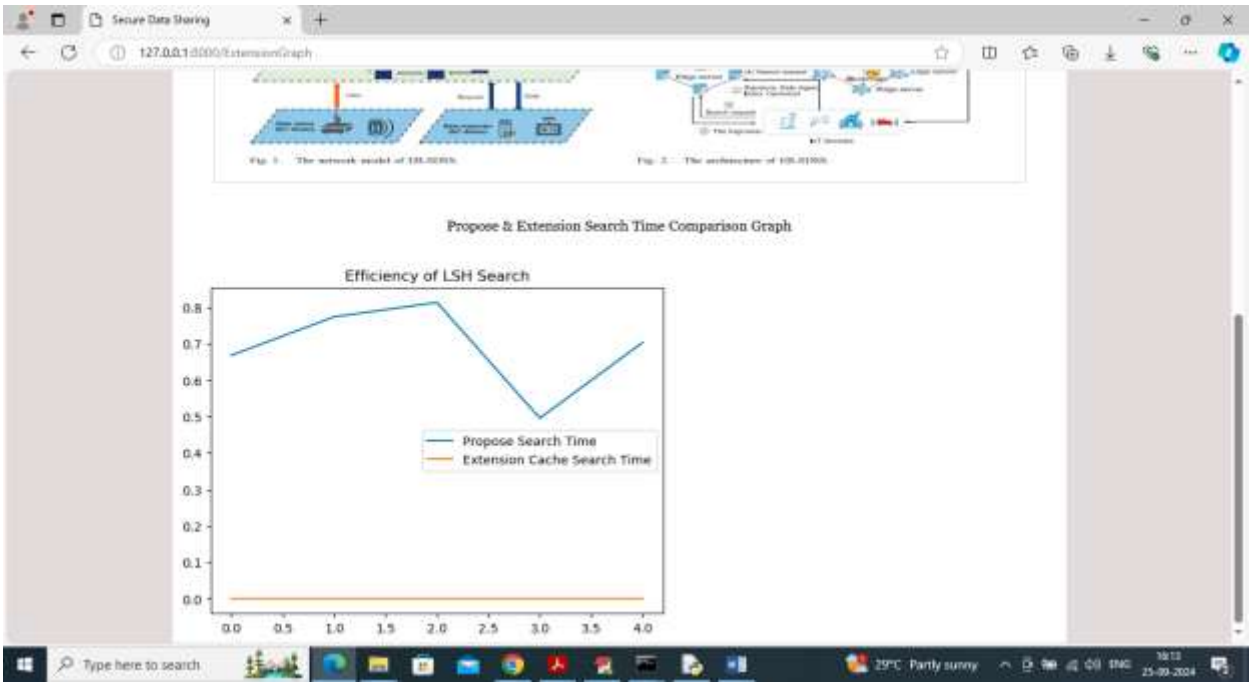
Above screen obtained search result from LSH along with file names, similarity score and 'download' option. Clicking at the download link allows us to obtain file in decrypted form.



Above screen in browser address bar shows file downloaded and likewise you may look for any number of queries. To obtain following graph, now click on link 'propose efficiency Graph'



In above screen in first graph showing 'efficiency of signature' where x-axis indicates number of file uploaded and y-axis indicates execution time and each line indicates various 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 methods can see 'Extension ECC' tool less execution time and its faster than propose algorithm. To obtain below graph, now click on 'Extension efficiency Graph' link



In above graph showing efficiency of search time with propose and extension cache approach. Above graph's x-axis is 'number of query search' and y-axis is 'search Time'; blue line shows proposed LSH search time and orange line shows Cache search time.
Likewise, by following the aforementioned panels, you can execute full code.

6. CONCLUSION:

By guaranteeing tamper-proof storage and verification of data, blockchain technology integration promotes trust and integrity in information shared among IoT devices. The method lowers data transfer time to cloud servers by using edge servers located nearer to IoT devices, hence greatly improving reactivity and general performance. Using"local sensitive Hashing (LSH)" and caching strategies, data retrieval is optimised so that pertinent information may be accessed fast and the processing burden is lowered. The use of certificate-less signature systems inside the blockchain architecture also enhances device authentication, hence guaranteeing safe and dependable data transmission over the network. The system uses AES symmetric encryption with lightweight Elliptic Curve Cryptography (ECC) to strike a compromise between strong encryption and performance efficiency, hence lowering execution time while preserving good security. In edge-enabled IoT contexts, this combination guarantees a secure and efficient foundation for data transfer.
Future Scope:may concentrate on expanding the system to manage the growing user base of IoT devices, hence guaranteeing effective data sharing as the IoT ecosystem develops. "Artificial intelligence (AI) and machine learning (ML)" combined can improve data analysis, predictive maintenance, and decision-making, hence enhancing user experience and operational efficiency. Enabling interoperability with various blockchain networks can also help to enable clean data sharing and cooperation across different IoT devices, hence promoting an extra connected and efficient ecosystem. Future versions might also give enhancing real-time data processing capacity top priority since applications in smart towns, healthcare, and industrial automation want quick reactions.

REFERENCES:

[1] Cui, J., Ouyang, F., Ying, Z., Wei, L., & Zhong, H. (2022). Secure and efficient data sharing among vehicles based on consortium blockchain. *IEEE Trans. Intell. Transp. Syst.*, 23(7), 8857-8867.

[2] Swapna, G. (2023). A Drug-Target Interaction Prediction Based on Supervised Probabilistic Classification. *Journal of Computer Science*, 19(3), 1203-1211.

[3] Yu, K., Tan, L., Aloqaily, M., Yang, H., & Jararweh, Y. (2021). Blockchain-enhanced data sharing with traceable and direct revocation in IioT. *IEEE Trans. Ind. Informat.,* 17(11), 7669-7678.

[4] Viswanath, G. (2024). Machine-Learning-Based Cloud Intrusion Detection. *International Journal of Mechanical Engineering Research and Technology*, 16(5), 38-52.

[5] Zheng, X & Cai, Z. (2020). Privacy-preserved data sharing towards multiple parties in industrial IoTs. *IEEE J. Sel. Areas Commun.,* 38(5), 968-979.

[6] Swapna, G., & Bhaskar, K. (2024). Malaria Diagnosis Using Double Hidden Layer Extreme Learning Machine Algorithm With Cnn Feature Extraction And Parasite Inflator. *International Journal of Information Technology and Computer Engineering,* 12(4), 536-547.

[7] Chaudhary, R., Jindal, A., Aujla, G.S., Aggarwal, S., Kumar, N., & Choo, K. K. R. (2019). BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. *Comput. Secur*., 85(2), 288-299.

[8] Viswanath, G., & Swapna, G. (2025). Diabetes Diagnosis Using Machine Learning with Cloud Security. *Cuestiones de Fisioterapia,* 54(2), 417-431.

[9] Jindal, A., Aujla, G. S., & Kumar, N. (2019). Survivor: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. *Comput. Netw.,* 153(1), 36-48.

[10] Viswanath, G. (2024). Improved Light GBM Model Performance Analysis and Comparison for Coronary Heart Disease Prediction. *International Journal of Information Technology and Computer Engineering,* 12(3), 658-672.

[11] Cui, B., Liu, Z., & Wang, L. (2016). Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage. *IEEE Trans. Comput*., 65(8), 2374-2385.

[12] Viswanath, G., (2024). Enhancing Cloud Security: A Block chain-Based Verification Framework for Multi-Cloud Virtual Machine Images. *Frontiers in Health Informatics*, 13(3), 9535-9549.

[13] Wang, T., Lu, Y., Wang, J., Dai, H. N., Zheng, X., & Jia, W. (2021). EIHDP: Edge-intelligent hierarchical dynamic pricing based on cloud-edge-client collaboration for IoT systems. *IEEE Trans. Comput.*, 70(8), 1285-1298.

[14] Viswanath, G. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. *Evolutionary intelligence*, 14(2), 691-698.

[15] Li, R., Song, T., Mei, B., Li, H., Cheng, X., & Sun, L. (2019). Blockchain for large-scale Internet of Things data storage and protection. *IEEE Trans. Services Comput.,* 12(5), 762-771.

[16] Viswanath, G. (2023). A Real-Time Case Scenario Based On URL Phishing Detection Through Login URLS. *Material science and technology*, 22(9), 103-108.

[17] Xu, M., Liu, C., Zou, Y., Zhao, F., Yu, J., & Cheng, X. (2021). wChain: A fast fault-tolerant blockchain protocol for multihop wireless networks. *IEEE Trans. Wireless Commun.,* 20(10), 6915-6926.

[18] Xu, M., Liu, C., Zou, Y., Zhao, F., Yu, J., & Cheng, X. (2023). SPDL: A blockchain-enabled secure and privacy-preserving decentralized learning system. *IEEE Trans. Comput.,* 72(2), 548-558.

[19] Xu, M., Liu, S., Yu, D., Cheng, X., Guo, S., & Yu, J. (2022). CloudChain: A cloud blockchain using shared memory consensus and RDMA. *IEEE Trans. Comput.,* 71(12), 3242-3253.

[20] Choo, K. K. R., Gritzalis, S., & Park, J. H. (2018). Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities. *IEEE Trans. Ind. Informat.,* 14(8), 3567-3569.

[21] Manogaran, G., Alazab, M., Shakeel, P. M., & Hsu, C. H. (2022). Blockchain assisted secure data sharing model for Internet of Things based smart industries. *IEEE Trans. Rel*., 71(1), 348-358.

[22] Viswanath, G. (2022). A Smart Recommendation System for Medicine using Intelligent NLP Techniques. *2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)*, 3(2), 1081-1084.

[23] Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Informat.,* 16(6), 4177-4186.

[24] Swapna, G., & Bhaskar, K. (2024). Early-Stage Autism Spectrum Disorder Detection Using Machine Learning. *International Journal of HRM and Organizational Behavior*, 12(3), 269-283.

[25] Xie, J., et.al. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Commun. Surveys Tuts.,* 21(3), 2794-2830.

[26] Viswanath, G. (2024). Multiple Cancer Types Classified Using CTMRI Images Based On Learning Without Forgetting Powered Deep Learning Models. *International Journal of HRM and Organizational Behavior,* 12(3), 243-253

[27] Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Gener. Comput. Syst*., 95(1), 420-429.

[28] Viswanath, G., & Swapna, G. (2024). Health Prediction Using Machine Learning with Drive HQ Cloud Security. *Frontiersin Health Informatics*. 13(8), 2755-2761.

[29] V. Winnarasi, V., A, B. Vaishnavi, A. B., &and A. Veluppal, A. (2024). Enhanced Breast Cancer Diagnosis: Leveraging Customized Transfer Learning with Machine Learning and Attention Mechanisms for Histopathology Image Classification. *7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*, 2024(1), 1540-1545.

[30] Viswanath, G., & Swapna, G. (2025). Data Mining-Driven Multi-Feature Selection for Chronic Disease Forecasting. *Journal of Neonatal Surgery*, 14(5s), 108-124.

[31] Chen, N., Li, J., Zhang, Y., & Y. Guo, Y. (2022). Efficient CP-ABE scheme with shared decryption in cloud storage. *IEEE Trans. Comput.,* 71(1), 175-184.

[32] Viswanath, G. (2024). Personalized Breast Cancer Prognosis through Data Mining Innovations. *Cuestiones de Fisioterapia*, 53(2), 538-548.

[33] Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019). Integrated blockchain and edge computing systems: A survey some research issues and challenges. *IEEE Commun. Surveys Tuts*., 21(2), 1508-1532.

[34] Viswanath, G. (2021). Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage. *Turkish Journal of Computer and Mathematics Education*, 12(9), 545-554.

[35] Xu, M., Zhao, F., Zou, Y., Liu, C., Cheng, X., & Dressler, F. (2023). BLOWN: A blockchain protocol for single-hop wireless networks under adversarial SINR. *IEEE Trans. Mobile Comput.,* 22(8), 4530-4547.

[36] Shantha Spandana, R. R., et.al. (2025). Secure and Scalable Data Management in Medical Systems via Decentralized Privacy Framework. *International Journal of Health Sciences and Pharmacy (IJHSP),* 9(1), 126-139. DOI: https://doi.org/10.5281/zenodo.15487830

[37] Anil Kumar, T., et.al. (2025). AI-Powered Precision Diagnosis of Thyroid Anomalies in Ultrasound Scans. *International Journal of Health Sciences and Pharmacy (IJHSP),* 9(1), 160-169. DOI: https://doi.org/10.5281/zenodo.15495261

[38] Bhaskar, K., et.al. (2025). Advanced Hybrid Learning Architecture for Precision Cardiovascular Risk Assessment. *International Journal of Health Sciences and Pharmacy (IJHSP),* 9(1), 50-61.

DOI: https://doi.org/10.5281/zenodo.15448632

[39] Yatheendra, K., et.al. (2025). AI-Driven Hematological Analysis for Proactive Dengue Diagnosis. *International Journal of Health Sciences and Pharmacy (IJHSP),* 9(1), 196-210.

DOI: https://doi.org/10.5281/zenodo.15541467

[40] Sunil Kumar Reddy, T., et.al. (2025). Interpretable AI for Precision Brain Tumor Prognosis: A Transparent Machine Learning Approach. *International Journal of Health Sciences and Pharmacy (IJHSP),* 9(1), 180-195. DOI: https://doi.org/10.5281/zenodo.15523628

[41] Bhaskar, K., et.al. (2025). Collaborative Intelligence for Securing Next-Generation Healthcare Systems Against Cyber Risks. *International Journal of Health Sciences and Pharmacy (IJHSP),* 9(1), 85-95. DOI: https://doi.org/10.5281/zenodo.15469623

****