RESEARCH PAPER

A Security and Privacy-Preserving Consortium Blockchain-Based Accessing Control in Mobile Crowdsensing

Dr. Vanita Dnyandev Jadhav[1], Ms. Ankita Sharad Pawar[2], Dr. Lalit V. Patil[3]

[1]Assistant Professor, MTech, PhD, CSE Department, SVERIS College of Engineering, Pandharpur, Maharashtra, India

Email: vdjadhav@coe.sveri.ac.in

[2]Student, Department of Computer Science and Engineering, SVERIS College of Engineering, Pandharpur, Maharashtra, India

Email: aspawar009@gmail.com

[3]Professor, SKNCOE, Pune

Received: 20th Apr, 2026 | Revised: 25th Apr, 2026 | Accepted: 9th May, 2026 | Available Online: 14th May, 2026

ABSTRACT

The reasons why mobile crowdsensing allows people to create tasks and get real-time information on mobile devices include, but are not limited to, traffic information, location-based services, and travel analytics. However, existing systems are a threat to privacy since the profiles of mobile gadgets and maliciously-coded software can be viewed by interested parties. The dataset has information about the tasks of stakeholders and the data that the devices have sensed. This information is stored in confidential blockchains in edge servers. The number of people and devices involved in the system is large, and every individual has his/her personal blockchain to keep his/her privacy. AES is a mobile device data encryption and ECSE is a task keyword encryption which can be accessed and searched. The proposed system involves CBAC model, whereby stakeholders make tasks on keywords and mobile devices send sensed data, which is encrypted using the same keywords. The privacy is maintained by the fact that the encrypted keywords should match to get access to the data. Smart contracts based on solidity take care of making tasks, uploading and accessing data, and the mobile crowdsensing server checks blockchain transactions to make sure they can be added to the consortium blockchain. Block processing times graphs demonstrate the effectiveness of blockchain processes.

Keywords: Consortium Blockchain, Access Control, Mobile Crowdsensing, Privacy Preservation, Elliptic Curve Searchable Encryption, Smart Contracts, Secure Data Sharing, Cache Optimization.

How to cite this article: Jadhav VD, Pawar AS, Patil LV., A Security and Privacy-Preserving Consortium Blockchain-Based Accessing Control in Mobile Crowdsensing. Int J Drug Deliv Technol. 2026;16(44s): 1051-1058; DOI: 10.25258/ijddt.16.44s.115

I. INTRODUCTION

MCS paradigm has emerged as a new method of obtaining data in the large scale using mobile devices that are distributed. There are many things that MCS can be used in such as the monitoring of traffic, the environment and cities and even in marketing travel among others. It leverages the sensing, computing and communication capabilities of mobile devices. In MCS, the stakeholders will establish some sensing tasks with specific requirements and the mobile devices will perform these tasks by sensing the information available about the surrounding environment. The servers gather, store, assemble, and process the data. This enables the stakeholders to make decisions and improve services. This type of crowdsourcing is used to reduce the infrastructure cost, a large area, fast response to changes in dynamic environments [1], [2].

Nonetheless, MCS has critical security and privacy problems. With centralized systems, there is the risk of having a single point of failure, loss of data integrity and illegal access. User profiles, sensitive data about mobile devices and data about tasks are normally stored in a central server. This increases the chances that this information will be leaked in case one attempts to attack it. There is a risk of privacy problems due to the legitimate users abusing the data either deliberately or accidentally. The vast majority of conventional security strategies merely safeguard the encryption of the sensing data transmitted, and it does not protect long-term device profiles, credentials of stakeholders, and access control that is privacy preserving [3], [4]. Such drawbacks undermine stakeholder trust, thus hindering the adoption of MCS in key applications like smart cities and smart transportation [5].

To address these issues, blockchain technology has been proposed since it is safe, open and decentralized. A blockchain stores information on numerous nodes and it is not possible when one node fails and ensures data security. Smart contracts are automatic and safe transactions. Existing MCS solutions using blockchain consist of incentives, reputation, or trusted execution environments to motivate people to join and keep their data safe. However, either of these approaches requires significant computing resources, or they require trusted third parties, which makes them less efficient [6], [7].

In this paper, a CBAC framework of MCS is presented, which considers ECSE to securely search keywords, smart contracts to manage distributed tasks, and privacy-preserving mechanisms of both participants (stakeholders) and mobile devices. Our solution has the ability to provide granular access control, guard against unauthorized access of data, and encourage secure and fast data sharing among remote users thereby overcoming the shortcomings of the existing security solutions to MCS [8].

II. Related Work

However, MCS is a highly active research field over the past few years. It deals with privacy, security, and efficient data collection and storage. User profiling is a significant subset of the process of determining how individuals behave. Ichou et al. [9] investigated the mobile user profile in crowdsensing system. The findings suggest that profiles are useful in data collection depending on the context, but can be a privacy risk when they are not adequately secured. Large MCS networks contain a large amount of personal information, such as location and sensing patterns, that can be used to abrogate the privacy of users of large MCS networks. This has an implication on how to design systems that can simultaneously apply privacy preserving methods and optimal task allocation to protect privacy of users without compromising system performance.

In order to enhance communication among the mobile nodes, Le and Kaddoum [10] proposed an LSTM-based channel access protocol to vehicles in cognitive vehicular networks. Their research is not related to MCS, but it demonstrates that smart models can enhance communication and eliminate lag and possibility of collisions. The concepts of channel access optimization could be applied to MCS networks when there are more than one devices transmitting data. These concepts assist us to know how we can maintain high reliability and efficiency in the way we change environment where we need to collect data in real time to make decisions that are flexible.

Masood et al. [11] studied the security and privacy issues relating to connected vehicle cloud computing, which bears similar traits like MCS. They identified insecurity in privacy, trust management and data sharing and they propose decentralization approaches to prevent threats. These results are in line with MCS systems that have central servers. Large-scale collaborative sensing platforms are made to be more reliable and secure through the use of large numbers of nodes which make the process more difficult to control and verify. This reduces the possibility of unauthorized access and manipulation of data.

Nkenyereye et al. [12] developed a secure crowdsensing system FoVeCC that employs both the fog computing technology and the secure communication technologies. This is a safe, fast method of processing data at the source, and can also be utilized with MCS. With edge or fog computing, data can be processed close to the sensors and on the edge of the network. This reduces latency and the burden on the central servers. These distributed models render things more privately, efficiently, and scalable. They too resolve the issues that arise when you have to roll out something on a large scale and require the low latency to perform tasks and make decisions in real time.

Li et al. [13] propose an electric car charging plan, which safeguards privacy through blockchain and fog computing to ensure that billing and authentication is secure. Anonymity via blockchain and decentralization via fog are relevant to MCS, but are primarily relevant to the automotive industry. These techniques allow data to be secured and enable individuals to obtain valuable information. They also prevent bad people to use user data, which allows people to share jobs and data and maintain their privacy.

Another key aspect of privacy-preserving analytics is known as federated learning. Basudan [14] proposed the federated learning protocol with secure aggregation to the Internet of Everything that enables the model to be trained remotely without sharing the data. Big data can be used in federated methods in MCS without endangering the privacy of the users. These techniques are applied with blockchain to facilitate privacy, accountability and verifiable performance, which fosters trust in crowdsensed networks.

Alamer [15] also investigated the idea of sharing data on the blockchain and came up with a secure way

of caching data on mobile edges to protect privacy and make it easier to access the data stored in the cache. When there are numerous requests to the same operations in MCS, the server may become overloaded. Caching technologies reduce the cost of communication, make it more efficient, and secure the information about users. Another thing that should be determined is who does what. Lin et al. [16] developed a privacy-saving task allocation framework of geographical batch crowdsourcing. MCS can use this model to safely delegate sensing tasks and protect the privacy of the participants and ensure that all the participants are treated fairly and trusted.

Data integrity in cloud is highly required in the distributed systems. Liu et al. [17] suggested a new certificateless public integrity checking mechanism of industrial data storage in the cloud and emphasized the importance of blockchain-based verification of reliable data in the distributed environment. Zhang et al. [18] extended blockchain to federated transfer learning and provided an idea of how to use blockchain to enhance collaborative intelligence in MCS. Another approach to trusted data sharing based on blockchain (called TDS-NA [19]) was also developed by Ou et al. and uses PKI authentication to ensure that the data is authentic and to keep unauthorized individuals out. Dong et al. used a redactable consortium blockchain with multi-authority attribute-based encryption to support accurate access control and secure amendment of blockchain entries, thus ensuring privacy, flexibility and scalability.

All of these results show how important it is to use blockchain, fog computing, federated learning, and complicated cryptographic methods in MCS. Past solutions are mostly restricted to a single area, but a combination of the approaches with mobile crowdsensing opens up new possibilities of solving common problems with privacy, access control, data integrity and scalability. It also provides the foundation to more secure MCS systems.

III. Materials And Methods

The study we are doing considers a CBAC model to enhance security and privacy of mobile crowdsensing. The stakeholders determine sensing tasks by encrypting keywords, and the use of mobile devices to collect and upload data to the system in a safe manner. The blockchains of consortiums run on cloud servers, and the user registration and storage of data are done on the edge servers. It is ECSE that ensures sensitive data is not accessed by unauthorized people by only allowing certain keywords to be used to access it [1]. Ethernet smart contracts are applied to handle the creation, storage and retrieval of tasks in a manner spread out [2]. Using caching, search results can be saved so that the data doesn't have to be searched on the cloud over and over again. This will save on computing and communication expenses and will also ensure that it is safer to verify something on the blockchain [3].

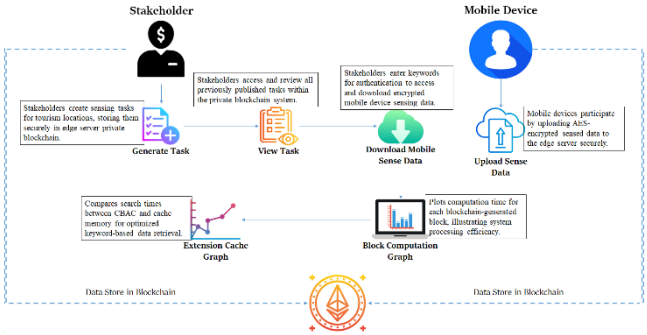


Fig.1. System Architecture

Fig. 1. involves blockchain to handle tourist information. Sensing tasks of tourist locations and storing them on a safe blockchain are carried out by stakeholders. The mobile devices are engaged by transmitting the sensed information (ciphered with AES) to an edge server in a secure manner. Involved people are able to view these tasks and then key in some keywords to obtain the encrypted mobile information. It has a block computation graph that indicates how well the system works and an extension cache graph that indicates how long it takes to search in order to enhance the search functionality through key word search.

A) Blockchain-Based Access Control Framework:

The CBAC system ensures the privacy and safety of people to engage in mobile crowdsensing by splitting up the work between consortium and privately owned blockchains. The edge servers keep the mobile sensing data and user registration data in the individual blockchains privately. The encrypted job index and inter-stakeholder authorization are stored in a consortium blockchain by the cloud. Smart contracts are used by Ethereum to manage the process of checking, storing, and reading information. These transactions can't be changed. Such a many-part approach eliminates single points of failure, opens up, and lets you control access in great detail. CBAC is a controlled and decentralized coordinated system that enables individuals to work together safely, maintain their data separate and verify who has accessed their data in distributed crowdsensing [1].

B) Elliptic Curve Searchable Encryption Integration:

ECSE in order to maintain the privacy of task keywords and searchable information in mobile crowdsensing. The stakeholders encrypt the keywords

with elliptic curve cryptography before putting the job on the blockchain. When the encrypted keywords are retrieved, the encrypted data on the blockchain are compared to the encrypted keywords, and only when there is a match can the encrypted data on the blockchain be retrieved. ECSE offers high cryptographic security with short keys, which implies that high-cost communications and low-cost computations are possible even with limited resources. In combination with blockchain, it makes data private, safe, and easily accessible. This ensures that only authorized individuals are able to access the system, fixes privacy issues with older systems, and offers a safe, efficient and scalable solution to manage mobile crowdsensing tasks [2].

C) AES Encryption for Secure Data Uploads:

The AES is employed to secure mobile information until it is sent to edge servers. The confidentiality and integrity of uploads. All of the devices encrypt the data from their sensors. AES is a desirable method of encrypting information on low-resource devices as it does not require a lot of processing capacity and still offers a high level of encryption. Private blockchains store the encrypted data, which makes an unchangeable ledger. AES can be used with blockchain to provide end-to-end encryption. Only after the keywords have been carefully checked, the user will be allowed to access it. Such an approach ensures that the information related to devices and the stakeholders remains confidential and allows large groups of people to intuit things fast and simply [3].

D) Cache-Based Search Optimization:

The suggested CBAC system has a caching feature that cuts down on the costs of computing and communicating for multiple search requests. In cases where a stakeholder seeks keywords to do a task, the cache will be searched first. If possible, the search result is returned without having to run expensive blockchain searches. When there are no results found, Elliptic Curve Searchable Encryption verification is performed and results are stored in the cache to be utilized later. The approach accelerates the queries of the cloud, makes them more responsive and less resource-consuming. However, there is no risk of insecurity since you still need to be authorized to access the data by comparing the encrypted keywords and verifying the blockchain. Mobile crowd sensing [4] is made scalable, fast and safe by cache.

D) Modules:

This module allows the stakeholders to enroll by providing the information they require.

i) Stakeholder Signup: The information is stored in the private blockchain of the edge server, ensuring its protection. This ensures that it cannot be altered, that credentials can be used later, tasks can be created and that the mobile sensing data can be accessed safely.

ii) Stakeholder Login: The system allows users to log in to the system in a secure manner. Then they can create tasks, view tasks that were already published, view sensed data, and view blockchain calculations. The system allows privacy and security since only individuals who are engaged in the system can access it.

iii) Generate Task: Sensing tasks of a particular place or task are made by stakeholders. The edge server's private blockchain stores the task's data, like keywords and instructions, in an encrypted form. This ensures that mobile devices are enabled to handle and access tasks safely.

iv) View Task: Gives stakeholders a list of activities which already have been published into the private blockchain. This list can be used by them to manage or look up past activity and see how the mobile devices were involved in sensing tasks.

v) Download Mobile Sense Data: The stakeholders must have mobile-sensed information that contain valid task keywords. Such checks ensure downloads are secure and prevents unnecessary downloading requests, which enhance privacy and confidentiality.

vi) Block Computation Graph: Demonstrates the time in seconds to make blocks in a private blockchain so that stakeholders can see how well the system works, how efficient the blockchain is and how long it takes to store and retrieve secure data.

vii) Extension Cache Graph: Compares the time taken to do a search using CBAC to the time taken to get to the search results using cache. This demonstrates the advantages of efficiency, reduced cloud processing, and expedited access to the frequently searched data.

viii) Stakeholder Logout: It securely terminates stakeholder meetings to ensure unauthorized individuals are unable to get in and to protect important work and mobile-sensed data.

ix) Mobile Device Signup & Login: Devices are registered and log in to participate in activities, securely access edge and cloud services, and save data safely.

x) Upload Data: The devices have the ability to select tasks and send AES-encrypted sensing data to the private blockchain to be stored and connected with the correct tasks.

xi) Mobile Device Logout: Terminates device sessions, secures the privacy and integrity of the already

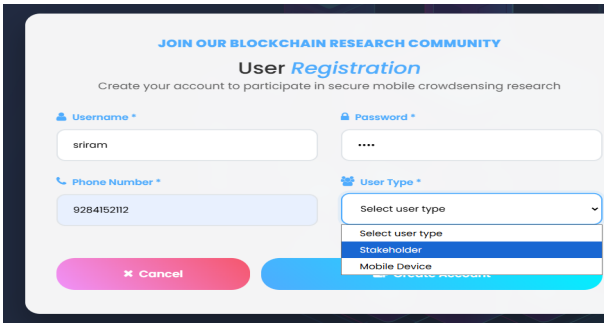
uploaded data, and maintains the privacy and integrity of the system.

IV. EXPERIMENTAL RESULTS

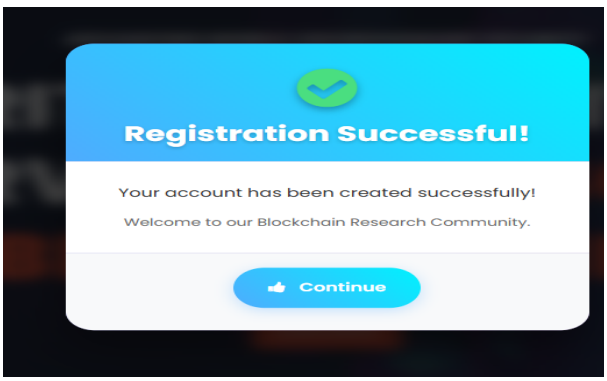
The project can be started by double-clicking on runServer.bat to start the proxy and cloud server. This will take you to the following page:

Using the command line, mirror the local host.

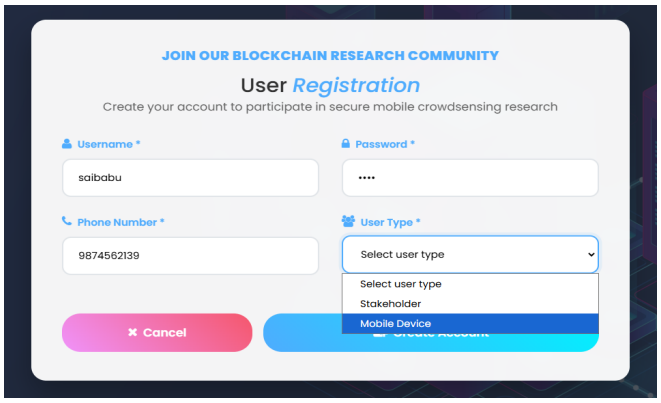
The interface of the project is depicted below. Users are able to register them with the following details:



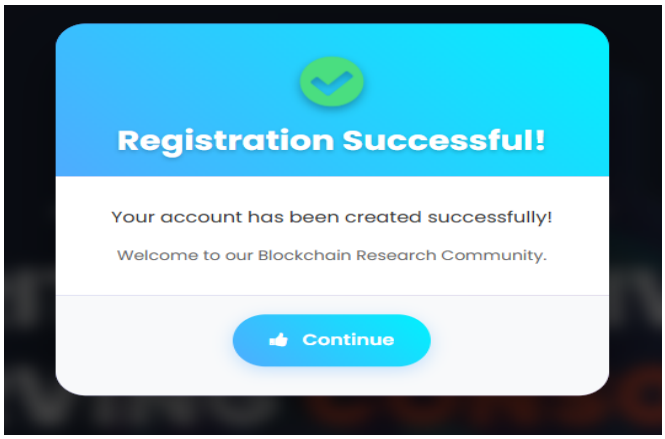
To participate in the crowd-sensing process, create an account, complete the necessary data, and select the kind of user you would like to be.



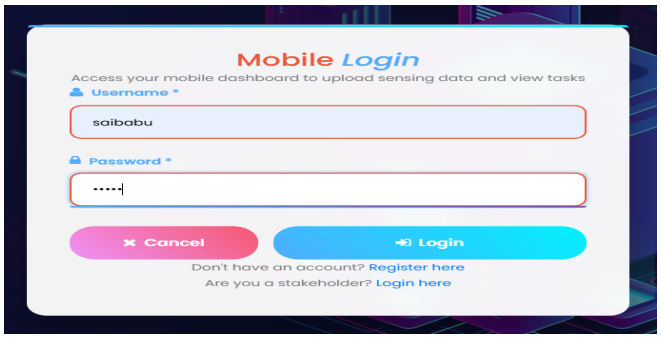
After registering the stakeholder, the data is securely stored in the blockchain.



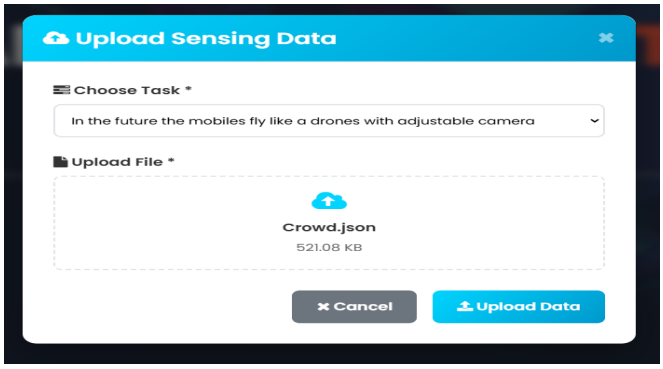
To be a part of the crowd-sensing, you should create an account, fill the necessary information, and select the appropriate user type.



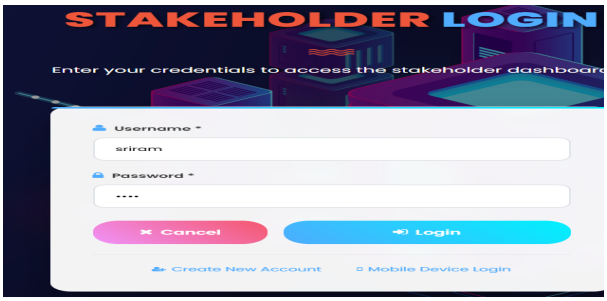
Once the Mobile device has signed in, it is saved to the blockchain.



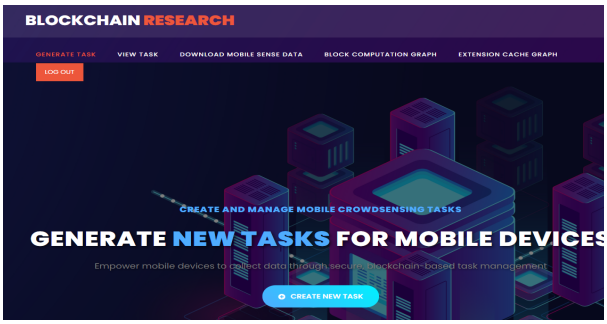
Mobile login allows sharing sensing data and configuring sensing tasks.



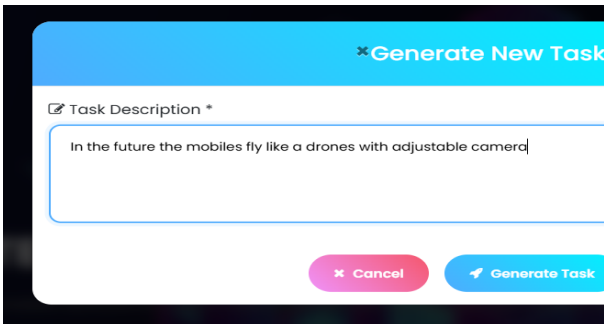
Select a task of crowdsensing and post the appropriate sort of file that you are testing.



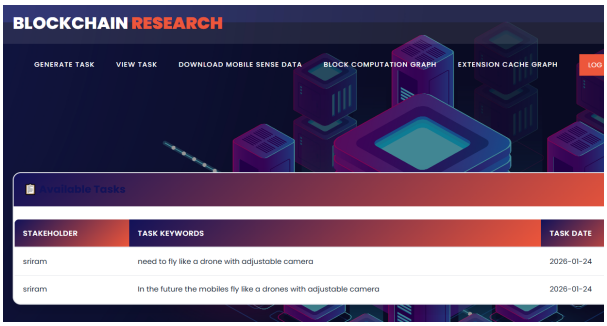
Use your stakeholder login to see and manage research tasks.



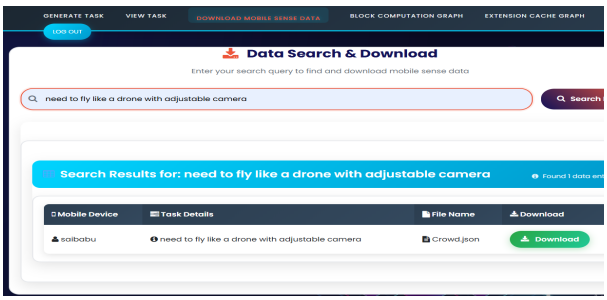
If the stakeholder login is correct, it will take you to the home page, as shown below.



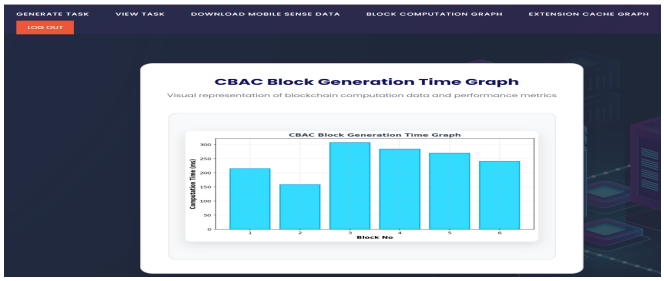
Make crowdsensing research projects that use a blockchain platform.



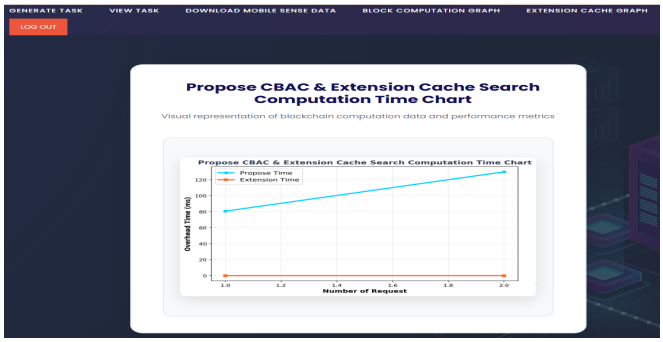
Check the list of occupation and the day you are able to commence.



Look for jobs that have to do with content. Get the files.



The picture shows how CBAC makes blocks. The x-axis demonstrates the number of blocks there are and the y-axis shows the time it takes to find out how many blocks there are.



The figure demonstrates the duration of running the proposed model, as well as the extended version.

V. CONCLUSION

The proposed mobile crowdsensing architecture in this paper incorporates the use of a CBAC to efficiently handle privacy and security issues. The model is founded on a group of activities that stakeholders brainstorm and data that is picked up by mobile devices. This information is securely stored in the edge servers in the form of private blockchains. This allows many individuals and gadgets to be involved and the information to remain confidential. AES encryption ensures that only the mobile device owner can access the data on their device and ECSE ensures that only people who fit the encrypted keywords can see them. In Solidity, tasks, uploading data, and retrieving data back are made using smart contracts. The mobile crowdsensing server will verify all the transactions on the blockchain to ensure that it can be added to the consortium blockchain. The blockchain instance of each stakeholder means that no other stakeholder can access data on one of them. This ensures their information remains confidential and they get to know the source of the information. Cache memory is used to store the results of the previous search to ensure that the subsequent search does not have to go through the cloud. This will ensure that the system functions well. The experiments reveal that the processing cost, as well as the search time, can be

significantly reduced, without compromising the fact that people can easily and safely access the crowdsensing data. Overall, the system can be turned into a highly secure, decentralized, and efficient mobile crowdsensing system by adding CBAC, blockchain, encryption, and cache memory to the system.

Future studies can focus on how the CBAC scheme can be improved by using lightweight cryptography techniques to reduce computational overhead. More complex consensus algorithms can criminalize things to be more scalable, quicker and require less energy. It could be easier to prevent bad actions with machine learning anomaly detection. Improving the system such that real-time crowdsensing systems can be more flexible, scalable, and secure, can also be achieved through smart query prediction to caching and privacy-preserving federated learning to crowdsensing data.

REFERENCES

[1] Wang, W., Yang, Y., Yin, Z., Dev, K., Zhou, X., Li, X., ... & Su, C. (2022). BSIF: Blockchain-based secure, interactive, and fair mobile crowdsensing. IEEE Journal on Selected Areas in Communications, 40(12), 3452-3469.

[2] Zhou, Y., Tong, F., Kong, C., He, S., & Cheng, G. (2025). Towards Efficient, Robust, and Privacy-Preserving Incentives for Crowdsensing Via Blockchain. IEEE Transactions on Mobile Computing.

[3] Peng, T., Guan, K., & Liu, J. (2022). A privacy-preserving mobile crowdsensing scheme based on blockchain and trusted execution environment. IEICE TRANSACTIONS on Information and Systems, 105(2), 215-226.

[4] Zhao, K., Tang, S., Zhao, B., & Wu, Y. (2019). Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing. IEEE Access, 7, 74694-74710.

[5] Tao, X., & Hafid, A. S. (2021). ChainSensing: A novel mobile crowdsensing framework with blockchain. IEEE Internet of Things Journal, 9(4), 2999-3010.

[6] J. Guo, X.Ding, T. Wang,andW.Jia, ‘‘Theoretical design of decentralized auction framework under mobile crowdsourcing environment,’’ Theor. Comput. Sci., vol. 939, pp. 250–260, Jan. 2023.

[7] A. Alamer, J. Ni, X. Lin, and X. Shen, ‘‘Location privacy-aware task recommendation for spatial crowdsourcing,’’ in Proc. 9th Int. Conf. Wireless Commun. Signal Process. (WCSP), Oct. 2017, pp. 1–6.

[8] A. Srivastava, A. Prakash, and R. Tripathi, ‘‘QoS aware stochastic relaxation approach in multichannel CR-VANET: A junction-centric geographic routing protocol,’’ J. Ambient Intell. Humanized Comput., vol. 14, no. 8, pp. 11103–11121, Aug. 2023.

[9] S. Ichou, S. Hammoudi, A. Benna, and A. Meziane, ‘‘Mobile user profile in the context of mobile crowd sensing,’’ in Advanced Computational Techniques for Renewable Energy Systems, 2023, pp. 170–182.

[10] T.-D. Le and G. Kaddoum, ‘‘LSTM-based channel access scheme for vehicles in cognitive vehicular networks with multi-agent settings,’’ IEEE Trans. Veh. Technol., vol. 70, no. 9, pp. 9132–9143, Sep. 2021.

[11] A. Masood, D. S. Lakew, and S. Cho, ‘‘Security and privacy challenges in connected vehicular cloud computing,’’ IEEE Commun. Surveys Tuts., vol. 22, no. 4, pp. 2725–2764, 4th Quart., 2020.

[12] L. Nkenyereye, S. M. R. Islam, M. Bilal, M. Abdullah-Al-Wadud, A. Alamri, and A. Nayyar, ‘‘Secure crowd-sensing protocol for fog based vehicular cloud,’’ Future Gener. Comput. Syst., vol. 120, pp. 61–75, Jul. 2021.

[13] H. Li, D. Han, and M. Tang, ‘‘A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing,’’ IEEE Syst. J., vol. 15, no. 3, pp. 3189–3200, Sep. 2021.

[14] S. Basudan, ‘‘A privacy-preserving federated learning protocol with a secure data aggregation for the Internet of everything,’’ Comput. Commun., vol. 223, pp. 1–14, Jul. 2024.

[15] A. M. A. Alamer, ‘‘A secure and privacy blockchain-based data sharing scheme in mobile edge caching system,’’ Expert Syst. Appl., vol. 237, Mar. 2024, Art. no. 121572.

[16] Y. Lin, Y. Jiang, Y. Li, and Y. Zhou, ‘‘Privacy-preserving batch-based task assignment over spatial crowdsourcing platforms,’’ Comput. Netw., vol. 241, Mar. 2024, Art. no. 110196.

[17] Q. Liu, X. Zhang, J. Xue, R. Zhou, X. Wang, and W. Tang, ‘‘Enabling blockchain-assisted certificateless public integrity checking for indus trial cloud storage systems,’’ J. Syst. Archit., vol. 140, Jul. 2023, Art. no. 102898.

[18] W. Zhang, Z. Wang, and X. Li, ‘‘Blockchain-based decentralized federated transfer learning methodology for collaborative machinery fault diagnosis,’’ Rel. Eng. Syst. Saf., vol. 229, Jan. 2023, Art. no. 108885.

[19] Z. Ou, X. Xing, S. He, and G. Wang, ‘‘TDS-NA: Blockchain-based trusted data sharing scheme with PKI authentication,’’ Comput. Commun., vol. 218, pp. 240–252, Mar. 2024.

[20] Y. Dong, Y. Li, Y. Cheng, and D. Yu, ‘‘Redactable consortium blockchain with access control: Leveraging chameleon hash and multi-authority attribute-based encryption,’’ High-Confidence Comput., vol. 4, no. 1, Mar. 2024, Art. no. 100168.