WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

BLOCKCHAIN BASED ON SECURELY SHARING DATA FROM USER ONE TO USER TWO

N.Vivek Acharya[1], S.Sunil Kumar[2], Ms.M.Mamatha[3]

Student, Department of Computer Science Engineering, MGIT, narojuvivekacharya_cse225a0512@mgit.ac.in
Student, Department of Computer Science Engineerimg, MGIT, shamarthisunilkumar_cse225a0513@mgit.ac.in
Assistant Professor, Department of Computer Science Engineering, MGIT, mmamatha_cse@mgit.ac.in

ABSTRACT:

Mobile edge computing (MEC) is a promising edge technology to provide high bandwidth with to mobile users. However, the MEC infrastructure raises major security when the shared resources involve sensitive and private data of users. This paper proposes a novel blockchain-based key management scheme for MEC that is essential for ensuring secure group communication among the mobile devices as they dynamically move from one subnetwork to another. In the proposed scheme, This paper proposes a blockchain-based key management scheme for Mobile Edge Computing (MEC) to ensure secure group communication as mobile devices move across subnetworks. Each device generates key pairs and shares its public key via a subnetwork-specific blockchain. This enables secure communication using public key encryption and quick identity verification when devices switch subnetworks. The scheme preserves backward and forward secrecy, resists 51% attacks, and shows improved storage efficiency compared to existing methods

Keywords: Mobile Edge Computing , Data Security , Blockchain

I. INTRODUCTION:

Mobile Edge Computing (MEC) offers low-latency, high-bandwidth services but also introduces significant security concerns due to the sharing of private user data. Previous studies have shown vulnerabilities in MEC, where all users are considered untrusted. Secure communication in such an environment depends heavily on effective key management. However, device mobility makes it challenging to maintain secure group communication, especially when devices move between subnetworks. This mobility incurs computation, communication, and storage overheads due to the need for rekeying. Therefore, key management schemes must support both dynamic group membership and dynamic user location. Centralized methods like the Logical Key Hierarchy aim to minimize message overhead, while distributed and decentralized approaches handle mobility better. Still, key management in large-scale wireless networks remains challenging. Real-time services demand fast rekeying for maintaining backward and forward secrecy. Furthermore, dependence on centralized entities raises critical security concerns in such systems**.**

II. PROBLEM DEFINATION:

Mobile Edge Computing (MEC) is an emerging technology that offers high-bandwidth, low-latency services by bringing computation and storage closer to mobile users. However, the frequent movement of mobile devices across subnetworks introduces significant security challenges, particularly in protecting sensitive user data during communication. Traditional key management schemes face difficulties in handling dynamic group membership and mobility, often leading to high computation, communication, and storage overheads. Ensuring forward and backward secrecy remains complex, and reliance on centralized key management entities creates scalability and trust issues. To overcome these limitations, this project proposes a blockchain-based key management scheme tailored for MEC networks. By leveraging blockchain's decentralized, tamper-proof nature, the system provides secure and efficient key distribution without relying on a central authority. It enables mobile devices to seamlessly and securely communicate across subnetworks, supports dynamic membership changes, and simplifies the rekeying process. The proposed solution aims to enhance scalability, reduce system overhead, and strengthen data confidentiality and integrity, ultimately making MEC networks more secure, efficient, and reliable.

III. LITERATURE SURVEY:

Mobile Edge Computing (MEC), a new model defined by the European Telecommunications Standards Institute (ETSI), is an advancement network architecture because it offers computation and storage at the cellular network edges like base stations and edge nodes which are closer to mobile users. The advancement of 5G technology increases the benefits users receive since it improves latency, reduces network congestion, and optimizes

application performance. The rapid deployment of new services and flexible fusion of IT with telecommunications allows third-party developers to interface directly with the RAN. However, the IT/telecom fusion MEC provides changes to traditional network structures which alongside decentralization and dynamism introduces challenging security and privacy issues. These issues are further compounded by the frequent mobility of users and devices across subnetworks during the transmission of sensitive data. Fog computing, often regarded as an extension of cloud computing to the edge, is also challenged with application mobility, geo-distribution, location awareness, and low latency. Therefore, privacy and security concerns in fog and MEC computing pose considerable obstacles to industrial adoption and demand sophisticated and scalable solutions.

One MEC and fog networks critical security aspects is group communication security which relies on efficient key management.

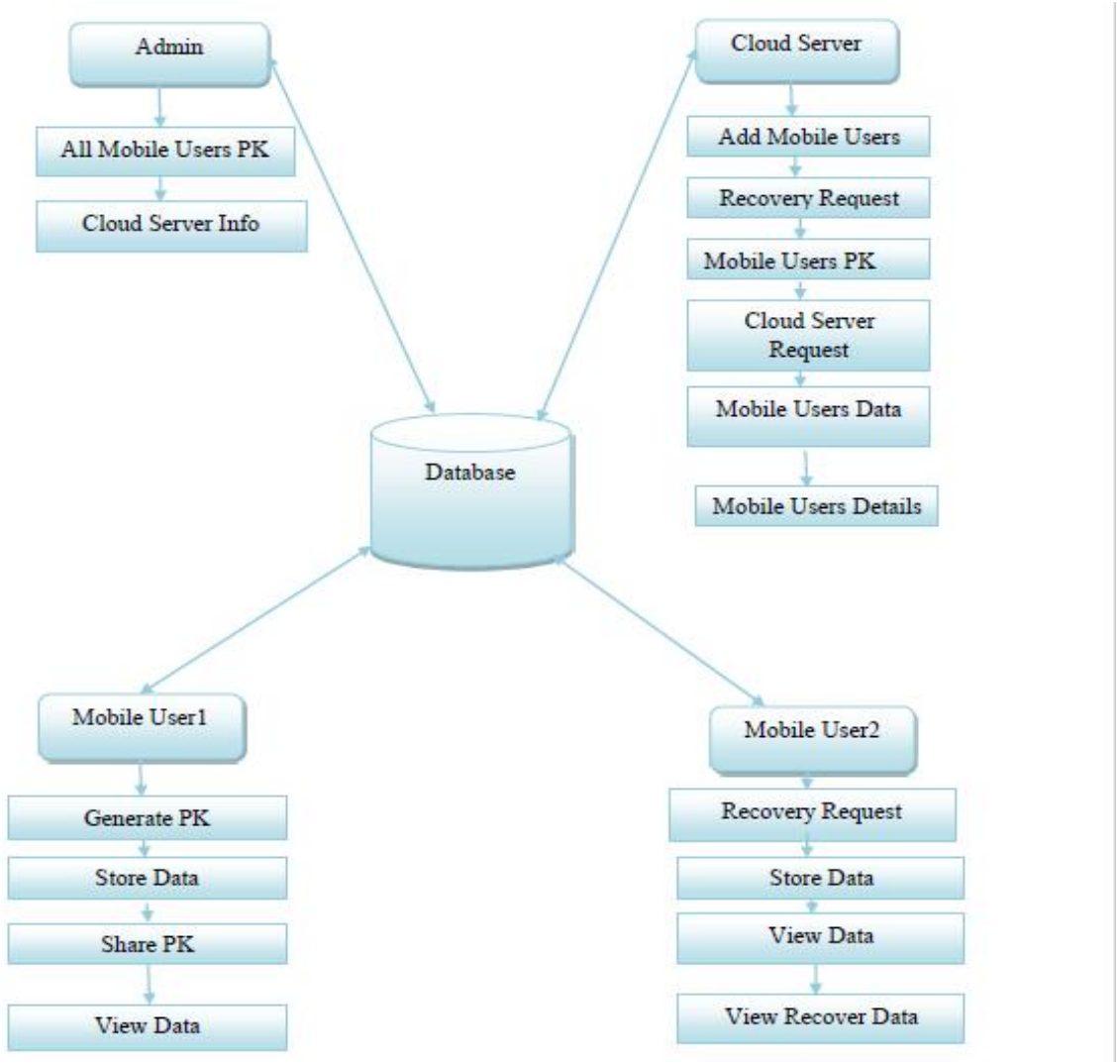


Fig 1: System Architecture of Sharing Data from one user to another user

This architecture represents a secure data sharing and recovery system within a mobile cloud computing environment. At the core of the architecture is a centralized database that stores all critical information, including public keys (PKs), user data, recovery requests, and cloud server details. The **Admin** is responsible for managing the initial setup, which includes collecting and storing all mobile users' public keys and cloud server information into the database. The **Cloud Server** plays a vital role in managing mobile user registration, processing recovery requests, accessing users' public keys, and retrieving or storing mobile user data and details as needed. There are two types of mobile users depicted in the system. **User 1** is primarily responsible for generating a public key, securely storing data, sharing the public key for authorized access, and viewing stored data. In contrast, **User 2** has the additional capability of initiating a data recovery request, which is processed through the cloud server. User 2 can also store data, view it, and access recovered data when needed. The interaction between these components ensures secure communication, efficient data sharing, and robust recovery mechanisms in case of data loss or transfer. This setup is ideal for scenarios that require secure data handling, access control, and reliable data recovery in mobile cloud environments

IV. PROPOSED SYSTEM:

Key management schemes:

In distributed key management schemes, there are no explicit key distribution center (KDC) and all the members can devote to the management. The distributed schemes can help to unify the workload of key management and reduce the requirement of central entities.. proposed a blockchain-based key management scheme in named data network to solve the problem of lacking mutual trust between sites without trust users. It has an efficient key management scheme for block chain . With the help of group-based keys within the context of clustered and distributed key management framework.

Implement a hierarchical key distribution model where a centralized MEC controller handles key updates at higher levels, while edge nodes manage local group keys for nearby devices.This decentralized structure helps reduce communication overhead by localizing key management, minimizing the need for global updates when a device moves across subnetworks.

1.Use a hybrid cryptosystem that combines symmetric encryption for fast operations with asymmetric encryption for secure key exchange. This approach can reduce computation time and provide a balance between performance and security. This system should enable efficient key generation, distribution, and storage even in highly mobile environments.

2.Implement a hierarchical key distribution model where a centralized MEC controller handles key updates at higher levels, while edge nodes manage local group keys for nearby devices. This decentralized structure helps reduce communication overhead by localizing key management, minimizing the need for global updates when a device moves across subnetworks.

V. IMPLEMENTATION, RESULTS AND DISSCUSSION:

To implement and run the above project architecture effectively, it is essential to install and set up the required software components in the specified versions. First, Java version 8 must be installed, as it provides the necessary runtime environment and development tools compatible with the project's backend code and libraries. Next, both 32-bit and 64-bit versions of MySQL should be installed to ensure compatibility with different system architectures and to manage the project's database operations efficiently. Additionally, a MySQL GUI (such as MySQL Workbench or a similar graphical interface tool) should be installed to facilitate easier database management, query execution, and data visualization. Lastly, NetBeans IDE version 8.1 must be set up as the primary integrated development environment for writing, compiling, and running the Java-based components of the project. Proper installation and configuration of these software tools are crucial for successful development, execution, and testing of the secure data sharing and recovery system.

RESULTS

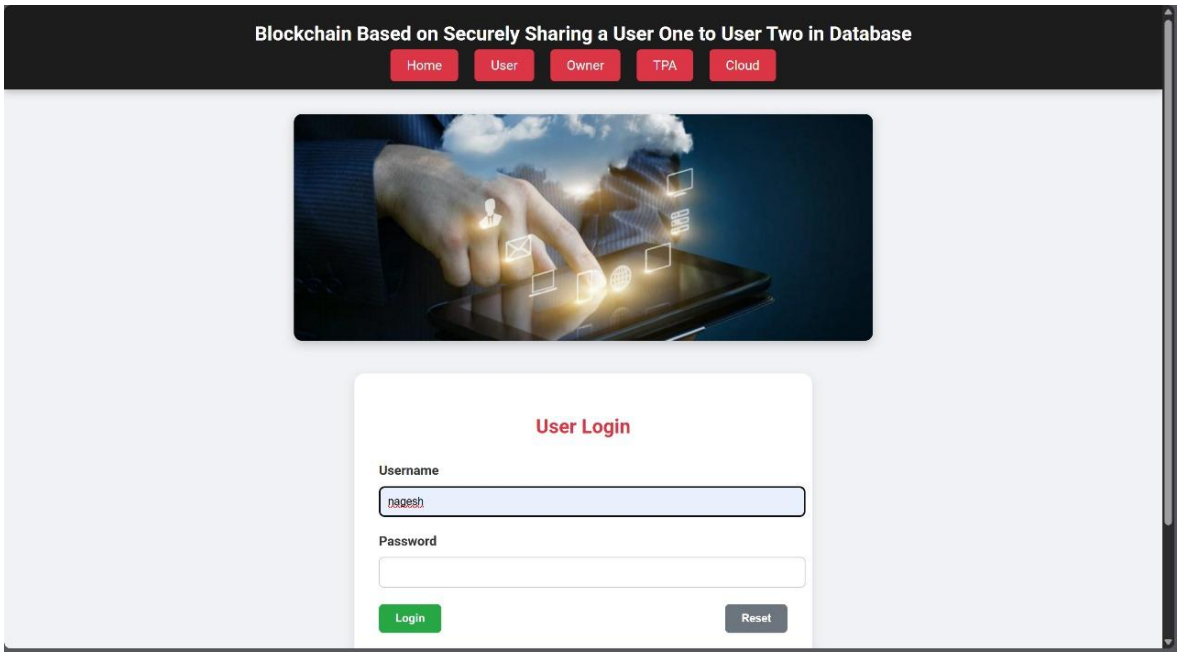


Fig: User login page

The image shows the login page of a web-based project titled **"Blockchain Based on Securely Sharing data from User One to User Two ."** It features a navigation bar with modules like Home, User, Owner, TPA, and Cloud, indicating role-based access. The interface includes a user login form where users can enter their credentials to access the system. This platform facilitates secure data sharing and recovery between users using blockchain and cloud technologies, with each role having specific permissions and functions within the system.

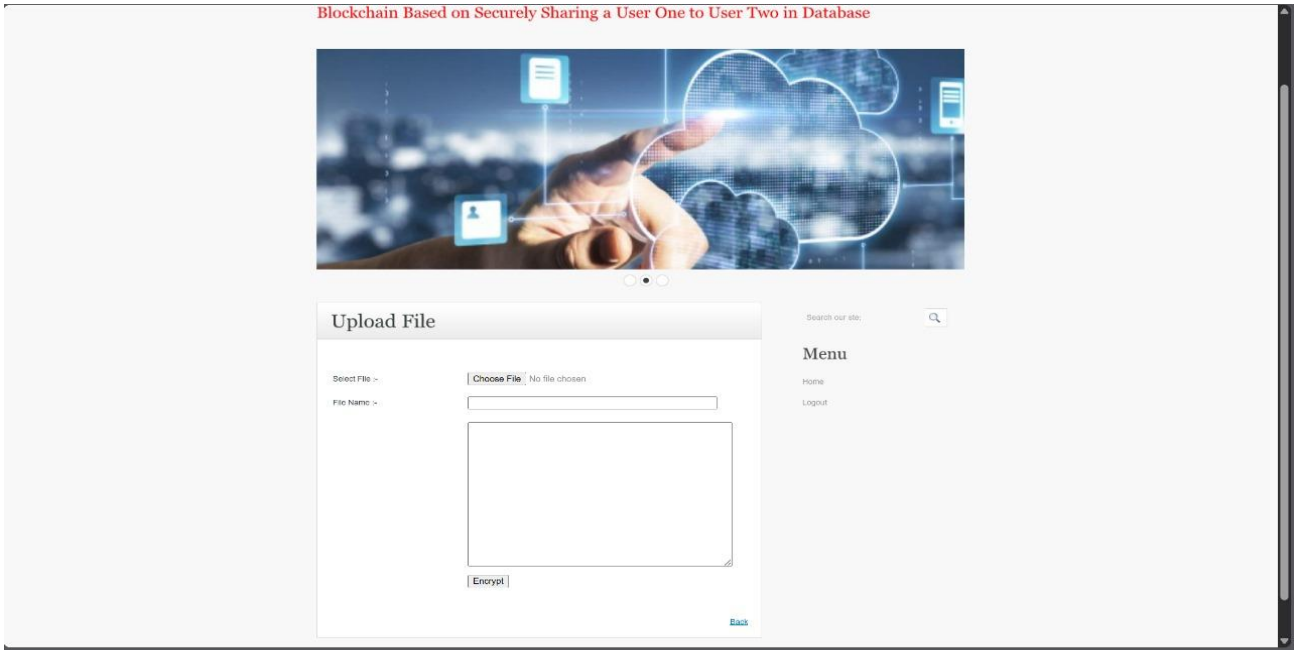
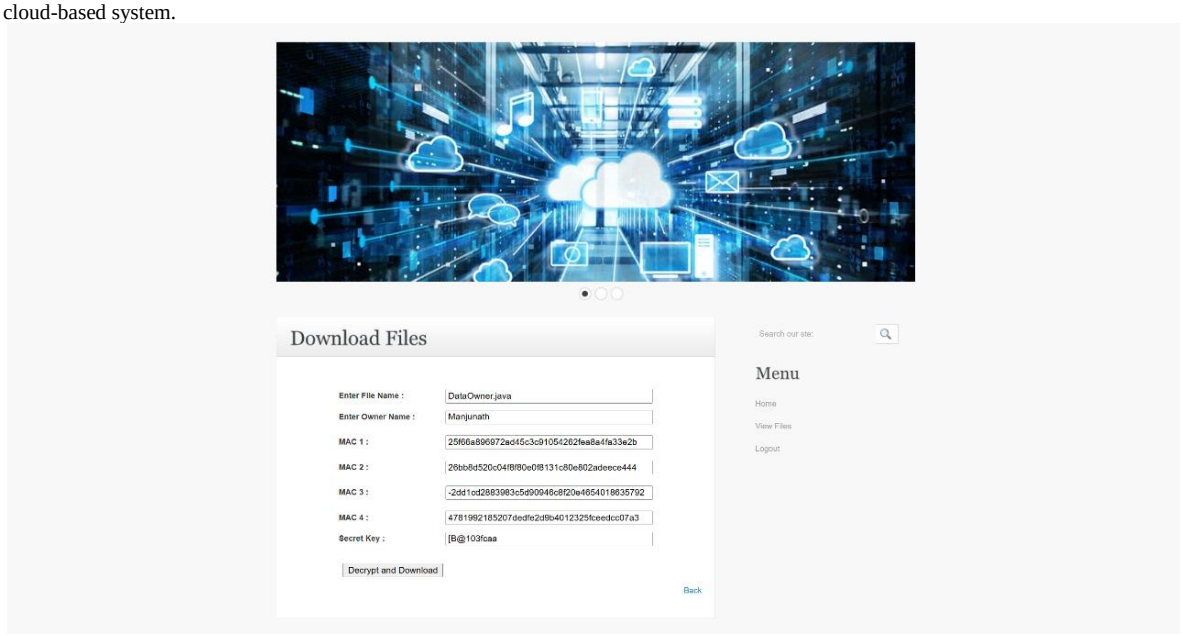


Fig: Upload file by user one

The image displays the **file upload interface** of a blockchain-based data sharing system titled **"Blockchain Based on Securely Sharing Data from User One to User Two."** It features an upload section where users can **select a file**, enter a **file name**, and optionally add a **description or data** in the text box before clicking the **"Encrypt"** button. This indicates that uploaded data is securely encrypted before storage or sharing. The page also includes a **cloud-themed image** and a **side menu** with options like Home and Logout, emphasizing secure file handling and user session control within the cloud-based system.



Fig;The file has been encrypted and the digital signature as been given ,by pressing decrypt it will decrypt

The image shows the **file download and decryption interface** of the blockchain-based data sharing system. Users are required to input the **file name**, **owner name**, and multiple **MAC (Message Authentication Code) values**, along with a **secret key** to ensure secure file access. Upon providing the correct credentials and keys, users can click the **"Decrypt and Download"** button to securely retrieve and access the file. The cloud-themed image above emphasizes the use of cloud storage, while the side menu offers navigation options like Home, View Files, and Logout, supporting a secure and organized user experience.

VI. CONCLUSION

This project proposes a blockchain-based key management scheme for secure communication among mobile devices in Mobile Edge Computing (MEC) environments, especially during subnetwork transitions. By leveraging blockchain's decentralized and tamper-resistant nature, the scheme addresses key generation, distribution, and storage challenges while eliminating reliance on vulnerable centralized systems. It enables dynamic access control and seamless authentication without static infrastructure, ensuring secure real-time data exchange. Security analysis under a 51% attack scenario confirmed the system's resilience, and experimental results showed low latency, minimal overhead, and strong scalability—highlighting its effectiveness for secure mobile communication and data sharing in next-generation MEC architectures.

VII. FUTURE SCOPE

In the future, the proposed blockchain-based key management system can be enhanced by integrating stronger encryption methods, such as homomorphic or quantum-resistant cryptography, to improve security against advanced threats. Real-time attack detection using AI/ML can be implemented for immediate response and dynamic key regeneration. The system will also be scaled to support a large number of mobile users, ensuring secure communication in dense MEC environments. Additional improvements include enabling secure key management across multiple subnetworks and domains, adopting lightweight blockchain models to reduce resource usage, and incorporating privacy-preserving techniques to protect user identities and meet regulatory standards.

REFERENCES

[1] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.
[2] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in International conference on wireless algorithms, systems, and applications. Springer, 2015, pp. 685–695.
[3] M. S. Yousefpoor and H. Barati, "Dynamic key management algorithms in wireless sensor networks: A survey," Computer Communications, 2018.
[4] M.-L.MessaiandH.Seba,"A survey of key management sschemes in multi-phase wireless sensor networks," Computer Networks, vol. 105, pp. 60–74, 2016.
[5] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," IEEE/ACM Transactions on Networking (TON), vol. 8, no. 1, pp. 16–30, 2000.
[6] D. Wallner, E. Harder, and R. Agee, "Key management for multicast: Issues and architectures," Tech. Rep., 1999.
[7] C. Esposito, M. Ficco, A. Castiglione, F. Palmieri, and A. De Santis, "Distributed group key management for event notification confidentiality among sensors," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 566–580, 2020.
[8] B. Daghighi, M. L. M. Kiah, S. Iqbal, M. H. U. Rehman, and K. Martin, "Host mobility key management in dynamic secure group communication," Wireless Networks, pp. 1–19, 2017.
[9] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, 2017. [Online]. Available:
[10] W. H. D. Ng, M. Howarth, Z. Sun, and H. Cruickshank, "Dynamic balanced key tree management for secure multicast communications," IEEE Transactions on Computers, vol. 56, no. 5, 2007.
[11] Y. Sun and K. R. Liu, "Hierarchical group access control for secure multicastcommunications,"IEEE/ACMTransactionsonNetworking, vol. 15, no. 6, pp. 1514–1526, 2007.
[12] D.-H. Je, J.-S. Lee, Y. Park, and S.-W. Seo, "Computation-andstorage-efficient key tree management protocol for secure multicast communications," Computer Communications, vol. 33, no. 2, pp. 136–148, 2010.