**Blockchain Based on Securely Sharing a User One to User Two in Database**

**ABSTRACT**:

Mobile edge computing (MEC) is a promising edge technology to provide high bandwidth and low latency shared services and resources to mobile users. However, the MEC infrastructure raises major security concerns 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, when a mobile device joins a subnetwork, it ﬁrst generates lightweight key pairs for digital signature and communication, and broadcasts its public key to neighbouring peer users in the subnetwork blockchain. The blockchain miner in the subnetwork packs all the public key of mobile devices into a block that will be sent to other users in the subnetwork. This enables the mobile device to communicate with its peers in the subnetwork by encrypting the data with the public key stored in the blockchain. When the mobile device moves to another subnetwork in the tree network, all the mobile devices of the new subnetwork can quickly verify its identity by checking its record in the local or higher hierarchy subnetwork blockchain. Furthermore, when the mobile device leaves the subnetwork, it does not need to do anything and its records will remain in the blockchain which is an append-only database. Theoretical security analysis shows that the proposed scheme can defend against the 51% attack and malicious entities in the blockchain network utilizing Proof-of-Work consensus mechanism. Moreover, the backward and forward secrecy is also preserved. Experimental results demonstrate that the proposed scheme outperforms two baselines in terms of computation, communication and storage.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * Unlike the existing blockchain-based key management schemes, the proposed scheme in this paper stores group members. * public keys for encrypted communication in blockchain, and it quickly verifies their identities by their records stored in local or higher blockchain hierarchies when the members are moving around the network. * Most traditional key management schemes are based on a key tree, and the distribution | * Thus, in this paper, we propose a new feature matching ranked search mechanism (FMRSM) for encrypted cloud data. This mechanism uses feature score algorithm (FSA) to create indexes, which allows multi-keywords which are extracted from a document as a feature to be mapped to one dimension of the index. Thus, the storage cost of indexes can be reduced and the efficiency of encryption can be improved. * The purpose of accelerating the encryption process and reducing storage cost |
| **EXISTING ALGORITHM**   * **Hash chain** | **PROPOSED ALGORITHM:-**   * **key management schemes** |
| **ALGORITHM DEFINITION: -**  Block chain, an append-only distributed database, is a successful underlying technique of Bitcoin proposed by Nakamoto in [32]. As shown in Fig. 1, the block chain consists of blocks and a hash chain, in which the order among blocks can be determined by checking the hash value of the previous block head. The characteristics of block chain.include traceability, openness and transparency, decentralization, demonstrable, difficult to be tampered with, etc. Taking the Proof-of-Work (PoW) consensus mechanism as an example, the transactions achieved among nodes (i.e. users) in the blockchain network will be collected by some nodes (i.e. miners). Then the nodes will compete for opportunities to generate the new block, by enumerating the hash values of the previous block head through increasing the random number of the previous block head. Only the hash value meets the requirement of the difficulty number (i.e. a system parameter for controlling the block generation rate of blockchain), | **ALGORITHM DEFINITION: -**  the key management processes. Recently, the emerging blockchain technique provides us a more secure and decentralized environment which attracts the interest of many researcher**s.**  **Distributed key management**  In distributed key management schemes, there are no explicit key distribution center (KDC) and all the members can devote to the management of TEK [7], [13], [14], [22], [23], [24], [25]. The distributed schemes can help to unify the workload of key management and reduce the requirement of central entities. Lou et al. proposed a blockchain-based key management scheme in named data network to solve the problem of lacking mutual trust between sites without trust anchors in [22]. Zhao et al. proposed an efficient key management scheme for health blockchain in [23]. With the help of group-based keys within the context of clustered and distributed key management framework  . |
| **DRAWBACKS:-**   * Security flaws are observed * Low query accuracy * Less overall matching relationship | **ADVANTAGES:-**   * Providing more security * Reducing storage cost |

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS**:

System : Pentium i3 Processor

Hard Disk : 500 GB.

Monitor : 15’’ LED

Input Devices : Keyboard, Mouse

RAM : 2 GB

**SOFTWARE REQUIREMENTS:**

Operating system : Windows 10.

Coding Language : Java.

Tool : Eclipse

Database : MYSQL