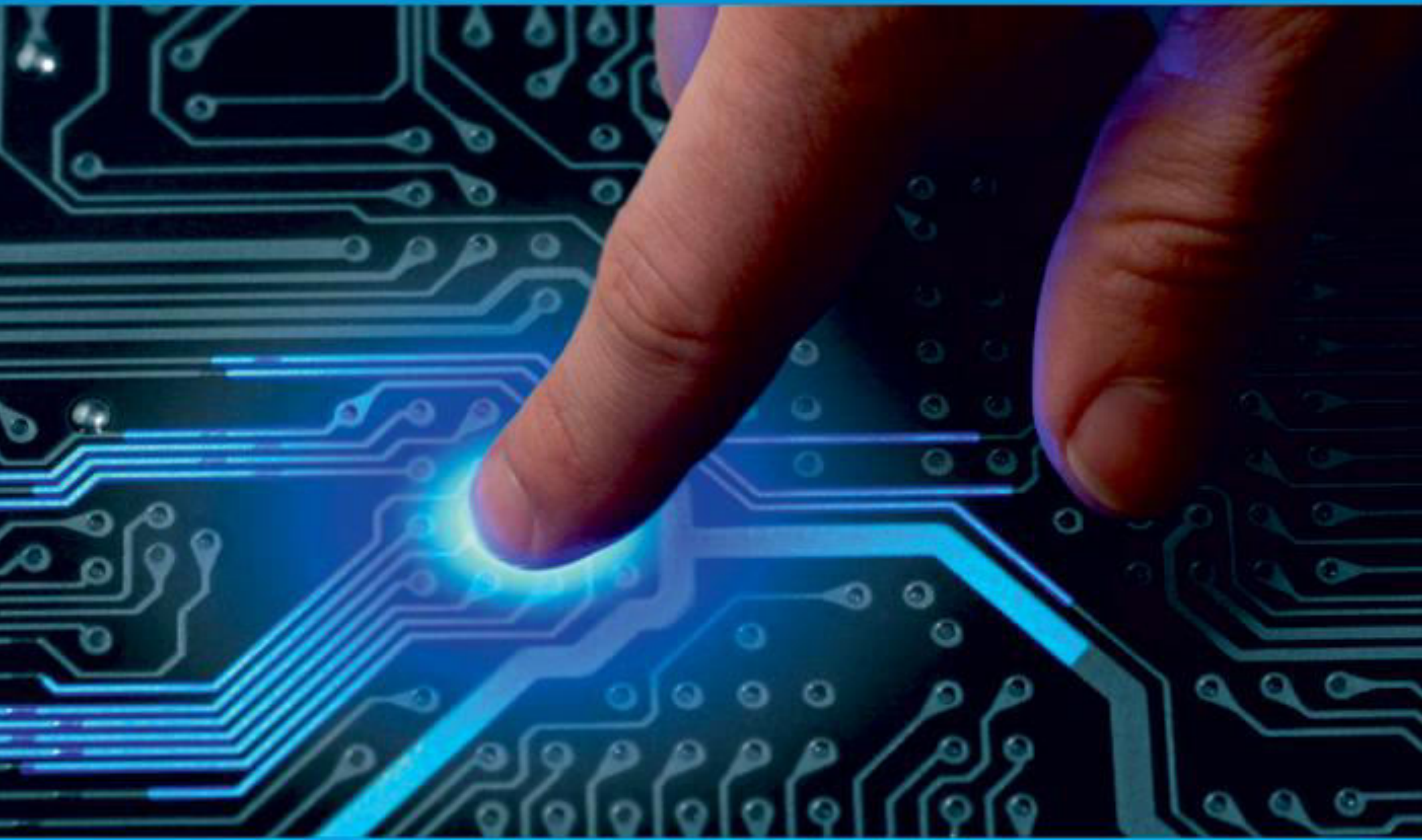
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 12, December 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

Blockchain Based Secure Communication and File Transfer System

Pranav Khedkar, Akanksha Kumbharkar, Vishal Londhe, Prasad Hole, Prof. Abhijeet Cholke

Student, Dept. of Computer Engineering, Trinity Academy of Engineering, Pune, India

Student, Dept. of Computer Engineering, Trinity Academy of Engineering, Pune, India

Student, Dept. of Computer Engineering, Trinity Academy of Engineering, Pune, India

Student, Dept. of Computer Engineering, Trinity Academy of Engineering, Pune, India

Assistant Professor, Dept. of Computer Engineering, Trinity Academy of Engineering, Pune, India

ABSTRACT: Attribute-based Encryption (ABE) is a promising cryptographic conducting tool to guarantee data owners' direct control over their data in public cloud storage. The earlier ABE schemes involve only one authority to maintain the whole attribute set, which can bring a single-point bottleneck on security and performance. Subsequently, some multi-authority schemes are proposed in which multiple sources hold disjoint attribute subsets separately. However, the single-point bottleneck problem remains unsolved. We conduct a threshold multi-authority Cipher text Policy. Attribute Base Encryption (CP-ABE) access control scheme for public cloud storage, named Robust and Auditable Access Control (RAAC) scheme, in which multiple authorities jointly manage a uniform attribute set. Security and performance analysis results show that RAAC is not only verifiable secure when less than t authorities are compromised but also robust when no less than t authorities are alive in the system Furthermore, by efficiently combining the traditional multi-authority scheme with RAAC, we construct a hybrid one, which satisfies the scenario of attributes coming from different authorities and achieves security and system-level robustness. Furthermore, our system is built on blockchain, a revolutionary technology allowing decentralized data sharing. It reduces in centralized systems and allows for fine-grained data access management. Our scheme's security study and evaluation revealed that it has the potential to provide privacy protection, authenticity, and reliability.

KEYWORDS: RAAC, CP-ABE, ABE, Blockchain.

I. INTRODUCTION

Roles and titles are always used to differentiate users' eligibility to access certain ser- vices. A role-based access control (RBC) framework is part of such a mechanism, which describes access controls between users and services. In RBAC, users are related to roles and are connected to role services. This access control is commonly used within an organization, but they must note that RBAC is a versatile framework; that is, roles are often used in a trans-organizational manner. Roles and titles are typically wont to distinguish the eligibility of users to access certain services. Such a mechanism is sculptured because of the role-based access management (RBAC) framework, which describes the access management relation among users and ser- vices. In RBAC, users are related to roles, and roles are related to services. Many organizations and firms use such frameworks in their pc systems to implement their internal access management needs. Communication is an inevitable and essential dimension of human life.

The evolution of communication from the past to today has reached a global area through digitalization. The data that gave name to our era allowed the collecting of extensive data in the communication sector, making this the center of attention by the central systems like states and firms that manage the industry. Blockchain technology empowers users to control their digital identity and share and communicate with trust. Communication applications based on blockchain technology; use asymmetric ciphers, consensusbased algorithms, and P2P network structure. Cryptography protects information from intruders and lets only intended users access and understood it. In Blockchain, cryptography is adapted to ensure the consistency of the data and guard user privacy and transaction information.

II. RELATED WORK

1. **Functional Requirements:-**Functional requirement are the function or features that must be included in any system to satisfy the business needs and be acceptable to the users. Based on the functional requirement that the system must work.In proposed system , the system should be able to perform Tracking and marking student attendance by facial recognition in specific time.

2. **Non – Functional Requirements :-** Non-functional requirement is a description of feature, characteristics and attributes of the system as well as any constraint that may limit the boundaries of the proposed system.
   The non-functional requirements are essentially based on the performance, information, economy, control and security efficiency and services. Based on these non-functional requirement are as follows:
   - User-Friendly.
   - System should provide better accuracy.
   - To perform with efficient throughout and response time.

3. **Assumption :-**

   1. All the software such as eclipse,etc are installed and running on the computers.
   2. The cluster of nodes is formed and running.

4. **Dependencies :-**

   1. It is assumed that user know his/her tasks in organizations.
   2. All parameters are as per the dataset.
   3. Well Trained face image dataset.

5. **User Classes and Characteristics :-** Basic knowledge of using computers is adequate to use this application. Knowledge of how to use a mouse or keyboard and internet browser is necessary. The user interface will be friendly enough to guide the user.

III. PROPOSED ALGORITHM

A. Protocol for Peer Verification :-

```
Input :- User get IP address, User Transaction TID,
Output :- Enable IP address or current query if any connection is valid.
Step 1 : User generate the any transaction DDL, DML or DCL query
Step 2 : Get current IP address If (connection(IP) equals(true)) Flag true Else Flag false End for
Step 3 : if (Flag == true) Peer to Peer Verification valid Else Peer to Peer Verification Invalid End if End for
```

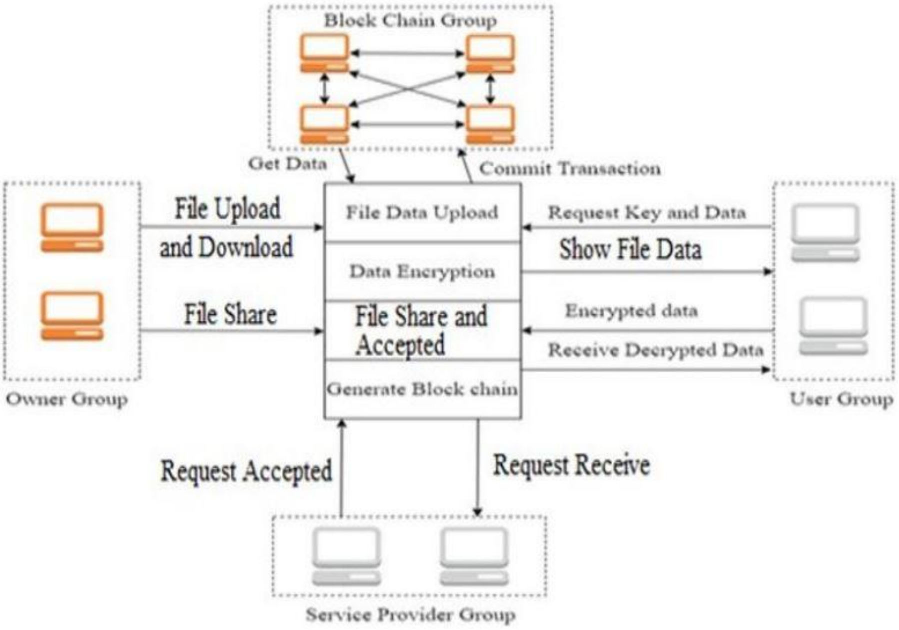
B. Hash Generation:-

```
Input :-Genesis block, Previous hash, data d
Output :- Generated hash H according to given data
Step 1 : Input data as d
Step 2 : Apply SHA 256 from SHA family
Step 3 : Current Hash= SHA256(d)
Step 4 : Return Current Hash
```

C. Mining Algorithm For Valid Hash Creation :-

```
Input : Hash Validation Policy P[], Current Hash Values hash Val Output : Valid hash
Step 1 : System generate the hash Val for i th transaction using Algorithm 1
Step 2 : if (hash Val. valid with P[]) Flag =1 Else Flag=0
Step 3 : Return valid hash when flag=1
```

IV. PROJECT ARCHITECTURE



V. CONCLUSION AND FUTURE WORK

Technology is the interesting inventions of encryption and information communications. This paper presents the evolution of encryption mechanisms and the different encryption methods used in Blockchain. The various security attacks aimed at Blockchain are also discussed. The different security services offered for authentication and privacy and the challenges of Blockchain are discussed in brief. This application can be used to ensure the availability, confidentiality and privacy of the private data that is shared between the users of an organization. Blockchain technology's future scope majorly lies in the field of Cybersecurity. Al-though the Blockchain ledger is open and distributed, the data is secure and verified. This is done through encryption to eliminate vulnerabilities such as unauthorized data tampering.

REFERENCES

1. Secure Peer-to-Peer Communication Based on Blockchain Kahina Khacef(B) and Guy Pujolle(B)Sorbonne University, 4 Place Jussieu, 75005 Paris, France 2019.
2. SoK of Used Cryptography in Blockchain MAYANK RAIKWAR , DANILO GLIGOROSKI , AND KATINA KRALEVSKA Department of Information Security and Communication Technologies 2020
3. A Comprehensive Study of Blockchain Services: Future of Cryptography Sathya AR1, Barnali Gupta Banik2 Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation 2019
4. A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things2020
5. J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, -preserving data aggregation computing in cyber-physical social systems," ACM Transactions on CyberPhysical Systems, vol. 3, no. 1, p. 8, 2019. 6. Gheitanchi, Shahin. Gamified service exchange platform on blockchain for IoT business agility 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020.
6. G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, efficient and geometric range query with access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870885, 2019.
7. K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, Privacy preserving attribute- keyword based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116131, 2017.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING