International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Blockchain Based Access Control System for Cloud Storage

Kamisetty Vinay

Sri Indu College of Engineering and Technology, ECE Department, Hyderabad, India
vinayk8188[at]gmail.com

Abstract: ***With the development of internet technology, the volume of data is increasing. To handle the large amount of data more and more applications are turning to the cloud to increase storage capacity. Platform is a place where user can store a large amount of data and access that data easily. However, it must ensure the security of shared information. Our approach provides an access control over the data stored in the cloud without provider participation. Using a block chain based decentralized ledger, our system provides immutable of all meaningful security events. Only cipher texts of hash codes are transferred through the blockchain ledger. Our system is implemented using smart contracts and it is tested on Ethereum block chain platform.***

Keywords: Ciphertext, Security, Ethereum block, Cryptography protocols

1. Introduction

Cloud storage like any other untrusted environment needs the ability to secure share information. Our approach provides an access control over the data stored in the cloud without the provider participation. The main tool of access control mechanism is ciphertext-policy attribute-based encryption scheme with dynamic attributes. We propose a set of cryptographic protocols ensuring privacy of operations requiring secret or private keys. Only ciphertexts of hash codes are transferred through the blockchain ledger.

Like any other untrusted environment, cloud storage requires the ability to secure share transfer information. Without the involvement of the cloud provider, our technique gives access control over the data kept there. The ciphertext-policy attribute based encryption method with dynamic characteristics is the fundamental instrument of the access control mechanism. We offer a collection of cryptographic protocals for operations requiring secret or private keys that ensure anonymity. The blockchain ledger only allows ciphertexts of hash codes to be transmitted.

2. Literature Survey

In the year 2017, the author named Sukhodolskiy I. A., Zapechnikov S. V. [4]. Worked on an access control model for cloud storage using attribute based encryption. It describes a multi-user system for controlling access to cloud based datasets. Each user in the system is given a set of qualities that define his identity in the system. The encrypted datasets that will be shared among users are kept in the cloud, with cryptographic access control. The system uses a multi – authority attribute based encryption technique as its foundation. Our system includes a certificate Authority that is independent of the cloud service provider and singed Revocation Lists to boost security. Our protype uses an API to communicate with existing cloud storage. Instead of attributing the computational burden to a single party, it is divided among a wide number of users

In the year 2011, Lewko A and Waters B worked on decentralizing attribute-based encryption. In that work, [6].they proposed A Multi-Authority Attribute-Baes Encryption (ABE) scheme is proposed. Any party may become an authority in our system, and no global coordination is required beyond the formation of an initial set of shared reference parameters. By generating a public key and providing private keys to distinct users that represent their qualities, a party can operate as an ABE authority. Any Boolean formula may be used to encrypt data over attributes supplied by any collection of authorities. Finally, no central authority is required in our system.

In the year 2015, [8]. Horvath M worked on attribute based encryption optimized for cloud computing. In this work, we proposed the goal of this research is to improve attribute based encryption for cloud data access control. We focus on giving the encryptor complete control over access rights, enabling viable key management even when numerous independent authorities exist, and enabling viable user revocation, which is crucial in reality. Our major contribution is an identity based adaptation of Lewko and Waters decentralized CP-ABE method. Our revocation approach is made possible by eliminating the computational weight of a revocation event from the cloud service provider in exchange for some long-term, but acceptable overhead in the encryption and decryption algorithms executed by the customers. As a result, the overhead of processing is spread out among a large number of processors

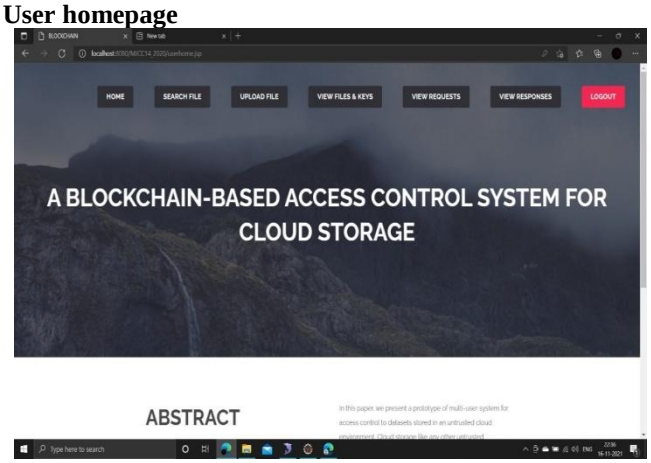
3. Proposed System

The project uses a decentralized scheme to control access to encrypted data in cloud environments. The approach provides an access control over the data stored in the cloud without the provider participation. The admin also checks the variation of file keys and can specify dynamic access policy

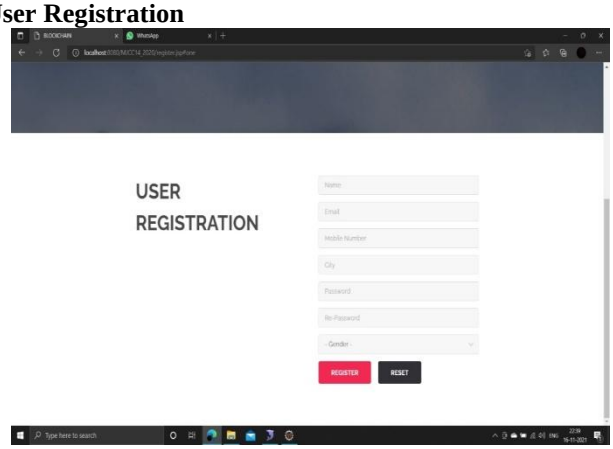
Advantages:
1) Information is secured
2) Without provider participation the data can be stored in the cloud
3) It can applicable for different data type, for instance, multimedia information, electronic documents, etc

4. Result

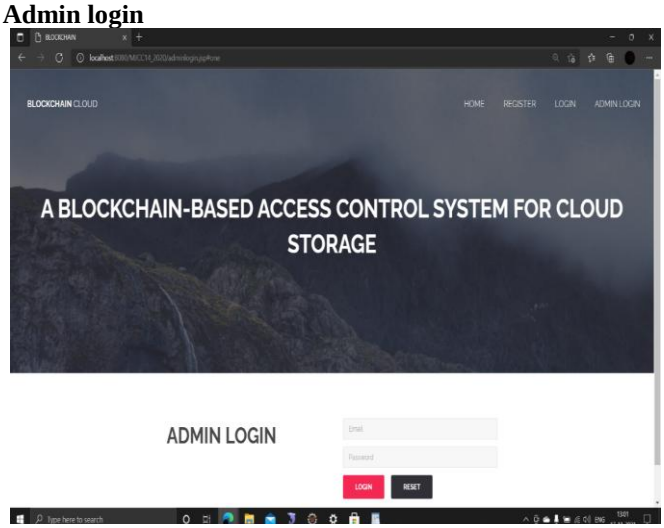
User homepage



User Registration



Admin login



5. Future Scope

To manage access to encrypted data in cloud settings, the project employs a decentralized approach. Without the involvement of the cloud provider, this solution allows access control over the data kept there. The administrator can also establish a dynamic access policy and examine the variation of file keys.

References

[1] TheBoxcryptor website [online]. (2017) Available: https://www.boxcryptor.com/en/
[2] Papa R. a., Redfield M., Zeldovich N. CryptDB protecting confidentiality with Encrypted Query processing. In Proceeding of the Twenty-Third ACM Symposium on Operating Systems Principles, Pages 85-100, 2001
[3] Poddar R., Boelter T., PapaR.Arx: A Strongly Encrypted Data base System. (2016) IACR Cryptology e Print Archive.[online]. Available: https://eprint.iacr.org/2016/591
[4] Sukhodolskiy I. A., Zapechnikov S. V. An access control model for cloud storage using attribute-based encryption. In Young Researches in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of R ussian
[5] McConaghy T., Marques R., Muller A. BigchainDB: A Scalable Blockchain Database (2016) BigchainDBcwhitepaper.[online].Available: https://www.bigchaindb.com/whitepaper/bigchaindbwhitepaper.
[6] Lewko A. and Watters B. Decentralizing attribute-based encryption. Springer, 2011,pp.568-588
[7] OASIS Standard. eXtensible Access Control Markup Language(XACML)Version 3.02013.154p
[8] Horvath M. Attribute-Based Encryption Optimized for Cloud Computing. In SOFSEM 2015, LNCS 8939,PP.566-577.
[9] YuanW.Dynamic Policy Update for Ciphertext – policy Attribute – Baes Encryption. LACR Cryptology ePrintArchive, 2016,457
[10] Russian state standard 34.12 2015. Cryptogtaphic protection of information. Moscow, Standartinform publ., 2015.25p.(In Russian)