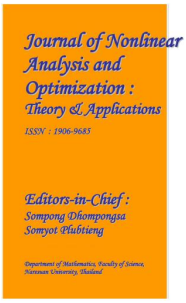
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



IMPROVING CLOUD SERVER SECURITY BY HARNESSING THE POWER OF BLOCKCHAIN

Komandla Sai Teja (20641A6740), Btech Student, CSE (Data Science), Vaagdevi College of Engineering

Ponna Sai Teja (20641A6752), Btech Student, CSE (Data Science), Vaagdevi College of Engineering

Naini Anuvamshik (21645A6712), Btech Student, CSE (Data Science), Vaagdevi College of Engineering

Vaddepally Karthikeya(21645A6721), Btech Student, CSE (Data Science), Vaagdevi College of Engineering

Mrs. P. Mounika, Assistant Professor, Department of CSE (Data Science), Vaagdevi college of Engineering

ABSTRACT

In modern times, sharing data is the one of the very few things which is done by anyone and everyone. Much of this sharing is done digitally, i.e., over the internet, which makes it the most recurrent way of doing the sharing globally. Enablement of the sharing is aided using copious Cloud Service Providers, allowing the end user, not only the ability of sharing the data but also, storing it. But with the amenities, comes the risk of intentional and unintentional manipulation of the tons of data that is stored and shared in every minute. Breaches like Data Piracy, Hack Attacks etc. are the most common threats that tempers with security of the cloud in these times. It is the need of the hour to make the sensitive data stored by the user safe from intentional/unintentional misuse/manipulation. Thereby, it is necessary to make this system more secure to ensure and maintain the confidentiality of the user data. In this paper, we have ventured the introduction of a system that anchorage Blockchain for securing the data over the cloud. To

ensure safety of the user's data, blockchain enables a prominent Controlled Access Mechanism. This mechanism accredits the user to share personalized hyperlinks deliberated to a single user. This approach logs details of all the actions and operations that are being done on or with the data and are at owner's disposal at all points. Actual Proprietary and privacy are few of the many benefits which are provided by this solution ensuring a more secure cloud space for the data.

1. INTRODUCTION

The accessibility of servers and storages for processing and storing data, software packages enabling analytical analysis of the data digitally enabling the flexibility of the resources acknowledging working anywhere is often refer to as Cloud Computing. Thereby, like any other thing available on the internet even cloud computing requires security. Even though the cloud vendors and the creators do provide us with secure solutions,

we need to stay updated because as the technology is advancing so are the hackers, crackers and people with a destructive mindset [2]. Procedures and technologies securing cloud environment enablers resistant to both implicit and explicit security related threats are necessitated under Cloud Security. No matter how secure the system is, it always is vulnerable in some way or the other. Like for instance, Cloudflare a renowned cloud security service provider publicized that back in 2016, a censorious bug in one of its software caused a data leak and that affected at least 2 million websites, which including many internet companies such as uber and 1password. [7]. Hence, blockchain technology came into the picture. Initial introductory of the Blockchain technology was made through the introduction of Bitcoin. As Blockchain is a known to be a crystalline mechanism which provides secured and innominate transactions, many cryptocurrencies and many others utilize it [10, 3]. Every transaction or process that takes place is recorded as a "block".

Those are then connected with the ones before and after [2, 11]. Processes or Transactions are locked together in the form of an irreversible chain, hence, creating a blockchain, improvising on the security of the data, including, and not limited to privacy and integrity of the data.

2. LITERATURE SURVEY

TITLE: "Proof-Of-Work Consensus Approach InBlockchain Technology For Cloud And Fog Computing Using Maximization-Factorization Statistics"

ABSTRACT: In this paper, we discussed an efficient statistical method with proof-of-work consensus approach for cloud and fog computing. With this method, solution with precise probability in minimal time is realized. We have used the expectation maximization algorithm and polynomial matrix factorization. The advantages of this statistical method are the less iteration to converge to the consensus solution and easiness to configure the complete mathematical model as per the requirement. Moreover, the energy and memory consumption are also less which make this approach appealing for cloud and fog computing. The experimental results also show that the proposed approach is significantly efficient in terms of time and memory consumption. This novel approach seems beneficial for Internet-of-Things (IoT), one of the most fast-growing technologies in network computing.

TITLE:"A blockchain future to Internet of Things security: A position paper, Digital Communications and Networks"

ABSTRACT: In the past few years block chain has gained lot of popularity because blockchain is the core technology of bitcoin. Its utilization cases are growing in number of fields such as security of Internet of Things (IoT), banking sector, industries and medical centres. Moreover, IoT has expanded its acceptance because of its deployment in smart homes and city developments round the world. Unfortunately, IoT network devices operate on limited computing power with low storage capacity and network bandwidth. Thus, they are extra close to attacks than other end-point devices such as cell phones, tablets, or PCs. This paper focus on addressing significant security issues of IoT and maps IoT security issues in contradiction of existing solutions found in the literature. Moreover issues that are not solved after implementation of blockchain are highlighted.

TITLE:"Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks"

ABSTRACT: As an emerging decentralized secure data management platform, blockchain has gained much popularity recently. To maintain a canonical state of blockchain data record, proof-of-work based consensus protocols provide the nodes, referred to as miners, in the network with incentives for confirming new block of transactions through a process of "block mining" by solving a cryptographic puzzle. Under the circumstance of limited local computing resources, e.g., mobile devices, it is natural for rational miners, i.e., consensus nodes, to offload computational tasks for proof of work to the cloud/fog computing servers. Therefore, we focus on the trading between the cloud/fog computing service provider and miners, and propose an auction-based market model for efficient computing resource allocation. In particular, we consider a proof-of-work based blockchain network, which is constrained by the computing resource and deployed as an infrastructure for decentralized data management applications. Due to the competition among miners in the blockchain network, the allocative externalities are particularly taken into account when designing the auction mechanisms. Specifically, we consider two bidding schemes: the constant-demand scheme where each miner bids for a fixed quantity of resources, and the multi-demand scheme where the miners can submit their preferable demands and bids. For the constant-demand bidding scheme, we propose an auction mechanism that achieves optimal social welfare. In the multi-demand bidding scheme, the social welfare maximization problem is NP-hard. Therefore, we design an approximate algorithm which guarantees the truthfulness, individual rationality and computational efficiency. Through extensive simulations, we show that our proposed auction mechanisms with the two bidding schemes can efficiently maximize the social welfare of the blockchain network and provide effective strategies for the cloud/fog computing service provider.

TITLE:"Controllable and trustworthy blockchain-based cloud data management"

ABSTRACT: In recent years, there have been efforts to deploy blockchain in a broad range of applications and in different domains, such as the critical infrastructure sectors. Generally, blockchain can be leveraged to establish a fair and transparent data sharing environment, where unauthorized modification to the data can be audited and traced. There are, however, known limitations of blockchain-based solutions, such as a significantly weakened networking control capability due to the distributed nature of such solutions. In addition, decisions recorded on a blockchain cannot be changed and there is the risk of majority attack (also known as 51% attack).

Seeking to mitigate these limitations, in this paper we propose a controllable blockchain data management (CBDM) model that can be deployed in a cloud environment. We then evaluate its security and performance, in order to demonstrate utility.

TITLE:"Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges"

ABSTRACT: Blockchain, as the underlying technology of crypto-currencies, has attracted significant attention. It has been adopted in numerous applications, such as smart grid and Internet-of-Things. However, there is a significant scalability barrier for blockchain, which limits its ability to support services with frequent transactions. On the other side, edge computing is introduced to extend the cloud resources and services to be distributed at the edge of the network, but currently faces challenges in its decentralized management and security. The integration of blockchain and edge computing into one system can enable reliable access and control of the network, storage, and computation distributed at the edges, hence providing a large scale of network servers, data storage, and validity computation near the end in a secure manner. Despite the prospect of integrated blockchain and edge computing systems, its scalability enhancement, self organization, functions integration, resource management, and new security issues remain to be addressed before widespread deployment. In this survey, we investigate some of the work that has been done to enable the integrated blockchain and edge computing system and discuss the research challenges. We identify several vital aspects of the integration of blockchain and edge computing: motivations, frameworks, enabling functionalities, and challenges. Finally, some broader perspectives are explored.

TITLE:"Using Blockchain in Cloud Computing to Enhance Relational Database Security"

ABSTRACT: Cloud computing has now become a verystandardised concept in our society. However, many modern applications need a better level of security that includes saving data from internal breaches. Thus, cloud databases need effective security mechanisms to keep track of data modifications. This paper will introduce the enhanced structure of cloud relational database (RDB) based on blockchain technology (BC) named BC over cloud-RDB. Through a self-verification mechanism, it enables the client to detect and prevent erroneous RDB manipulation. We proposed two systems to improve cloud-RDB namely, agile BC-based RDB

and secure BC-based RDB. Both are distributed among several cloud service providers based on the Byzantine Fault Tolerance consensus. Additionally, both rely on linking records to each other using the SHA-256. At the same time, secure BC-based RDB uses a proof-of-work consensus to make data offensive operation impossible. On the basis of performance of both systems' and security analysis, the agile BC-based RDB is highly suggested for the high throughput database. On the other hand, the secure BC-based RDB is recommended for RDB that contains sensitive data and low throughput performance. The improved RDB is flexible and can be operated according to the data owner's specifications.

TITLE:"Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions"

ABSTRACT: Through virtualization and resource integration, cloud computing has expanded its service area and offers a better user experience than the traditional platforms, along with its business operation model bringing huge economic and social benefits. However, a large amount of evidence shows that cloud computing is facing with serious security and trust crisis, and building a trust-enabled transaction environment has become its key factor. The traditional cloud trust model usually adopts a centralized architecture, which causes large management overhead, network congestion and even single point of failure. Furthermore, due to a lack of transparency and traceability, trust evaluation results cannot be fully recognized by all participants. Blockchain is a new and promising decentralized framework and distributed computing paradigm. Its unique features in operating rules and traceability of records ensure the integrity, undeniability and security of the transaction data. Therefore, blockchain is very suitable for constructing a distributed and decentralized trust architecture. This paper carries out a comprehensive survey on blockchain-based trust approaches in cloud computing systems. Based on a novel cloud-edge trust management framework and a double-blockchain structure based cloud transaction model, it identifies the open challenges and gives directions for future research in this field.

TITLE:"Establishing Trust despite attacks in cloud computing: a survey"

ABSTRACT: Cloud computing has become an integral part of our lives as it provides on-demand, rapid provisioning of services with ease of implementation, accessibility and flexibility.

The pay-as-you-use aspect is very attractive for customers who usually pay fixed price for resources whose usage does not tally with the cost of purchase. In this paper, we present a survey on security in cloud computing despite various attacks. It presents the various security aspects in the services provided by the cloud such as IaaS, PaaS and SaaS. Since virtualization is used vastly in cloud, we take a look at the various attacks virtual machines are subjected to. Trusted computing was introduced for the customers to be assured that the resources they use over cloud is reliable. Further, we also observe how remote attestation plays a role to assure trustworthiness and how the Trusted Platform Module is used in the attestation mechanism. The paper thus provides an overall view of existing techniques to secure and trust cloud and its components.

TITLE:"Trust models for services in cloud environment: a survey"

ABSTRACT: Trust remains one of the biggest challenges in cloud computing. At the global level, users do not have enough knowledge about the trust, reputation and reliability of service providers. In cloud environments, consumers make complex decisions, requiring trust for several services and different reasons. These decisions cannot be grouped in isolation because they have many interrelated aspects, as these features affect each other in a dynamic way. This paper throws light on different Trust Models developed and their drawback with respect to resource security. A strong Trust Model is recommended to enhance the reputation of the services in Cloud. The aim of this paper is to give a classification of the most relevant of trust models in recent years. Moreover, a simple set of guidelines for matching the most suitable trust model category to a given service is provided in this work.

TITLE:"A survey on blockchain for information systems management and security"

ABSTRACT: Blockchain technologies have grown in prominence in recent years, with many experts citing the potential applications of the technology in regard to different aspects of any industry, market, agency, or governmental organizations. In the brief history of blockchain, an incredible number of achievements have been made regarding how blockchain can be utilized and the impacts it might have on several industries. The sheer number and complexity of these aspects can make it difficult to address blockchain potentials and complexities, especially when

trying to address its purpose and fitness for a specific task. In this survey, we provide a comprehensive review of applying blockchain as a service for applications within today's information systems. The survey gives the reader a deeper perspective on how blockchain helps to secure and manage today information systems. The survey contains a comprehensive reporting on different instances of blockchain studies and applications proposed by the research community and their respective impacts on blockchain and its use across other applications or scenarios. Some of the most important findings this survey highlights include the fact that blockchain's structure and modern cloud- and edge-computing paradigms are crucial in enabling a widespread adaption and development of blockchain technologies for new players in today unprecedented vibrant global market. Ensuring that blockchain is widely available through public and open-source code libraries and tools will help to ensure that the full potential of the technology is reached and that further developments can be made concerning the long-term goals of blockchain enthusiasts.

3. EXISTING SYSTEM

The existing system for the project titled "Server Security in Cloud Computing Using Blockchain" addresses the prevalent challenges associated with data sharing and storage in the digital landscape. In the current scenario, where the majority of data sharing occurs digitally over the internet, Cloud Service Providers play a crucial role in facilitating this process. However, this convenience is accompanied by significant risks, including intentional and unintentional manipulation of vast amounts of data, leading to common threats such as Data Piracy and Hack Attacks. Recognizing the urgency to bolster the security of cloud systems and protect sensitive user data from potential misuse, the existing system proposes the integration of Blockchain technology. By anchoring Blockchain for securing data over the cloud, the system introduces a Controlled Access Mechanism. This mechanism empowers users with personalized hyperlinks, tailored to individual data access, while logging all actions and operations for transparency and accountability. The use of Blockchain ensures data integrity, tamper resistance, and a decentralized ledger, providing users with a more secure cloud space and addressing the imperative need for maintaining the confidentiality of user data in the digital age.

3.1 LIMITATIONS

Scalability Challenges:

Blockchain systems, especially those based on public decentralized networks, may face scalability challenges as the number of users and transactions increases. This can potentially impact the performance of the system, leading to delays and higher resource requirements.

Integration Complexity:

Integrating Blockchain technology into existing cloud computing infrastructure can be a complex task. Ensuring seamless interoperability with diverse cloud service providers and applications may pose challenges and require significant development efforts.

Energy Consumption:

The consensus mechanisms employed in many Blockchain networks, such as Proof of Work (PoW), can be energy-intensive. This poses environmental concerns and may be a limitation for cloud-based systems aiming for sustainability and reduced energy consumption.

Regulatory Uncertainties:

The regulatory landscape surrounding Blockchain and cloud computing is still evolving. Uncertainties in compliance requirements and legal frameworks may pose challenges in ensuring that the implemented system adheres to regional and industry-specific regulations.

User Adoption and Education:

Blockchain technology, with its decentralized and cryptographic nature, may be unfamiliar to many end-users. Achieving widespread adoption may require educational efforts to inform users about the benefits of the proposed security system and how to effectively navigate and interact with the Blockchain-based features. User reluctance or lack of understanding could impact the successful implementation of the system.

4. PROPOSED SYSTEM

The proposed system titled "Server Security in Cloud Computing Using Blockchain" aims to revolutionize the security paradigm of cloud-based data storage and sharing. Building upon the recognition of vulnerabilities in the existing system, the proposed framework introduces a robust security architecture by leveraging Blockchain technology. The core innovation lies in the implementation of a Controlled Access Mechanism, facilitated by Blockchain, which grants users personalized hyperlinks for data access while ensuring the integrity and confidentiality of the stored information. Smart contracts play a pivotal role in automating and enforcing access control rules within the Blockchain network. The system not only addresses the pressing concerns of intentional and unintentional data manipulation but also enhances transparency and accountability by maintaining a detailed and immutable log of all user actions. Through the integration of Blockchain, the proposed system offers heightened security features, such as tamper resistance and decentralized consensus, thereby establishing a more trustworthy and resilient cloud space for sensitive user data. The envisaged benefits encompass enhanced security, user privacy, and a streamlined approach to data management in the cloud.

4.1 ADVANTAGES

Enhanced Security Through Blockchain:

The incorporation of Blockchain technology fortifies the security of the cloud system by providing a tamper-resistant and decentralized ledger. This inherent security feature ensures the integrity of data, making it resistant to unauthorized access or manipulation.

Controlled Access Mechanism:

The proposed Controlled Access Mechanism, enabled by Blockchain, introduces a personalized and user-centric approach to data access. Users are granted unique hyperlinks, offering a fine-grained control over who can access their data, thereby reducing the risk of unauthorized sharing.

Transparent and Immutable Log:

The system maintains a detailed and immutable log of all actions and operations performed on the data. This transparency enhances accountability, allowing users to track and verify every interaction with their stored information, thereby mitigating the risk of data breaches and ensuring data integrity.

Privacy Assurance:

Through the use of Blockchain's cryptographic techniques and controlled access mechanisms, the proposed system ensures a higher level of privacy for user data. Users have greater control over who can access their data, reducing the likelihood of unintentional exposure or unauthorized sharing.

Decentralized and Resilient Architecture:

The decentralized nature of Blockchain enhances the resilience of the system. By distributing the data across a network of nodes, the proposed system reduces the risk of a single point of failure, providing a more robust and reliable infrastructure for cloud-based data storage and sharing.

MODULES

Blockchain Integration Module:

This module focuses on integrating Blockchain technology into the existing cloud infrastructure. It includes the deployment of smart contracts, consensus mechanisms, and cryptographic techniques to establish a tamper-resistant and decentralized ledger for secure data transactions.

Controlled Access Mechanism Module:

The Controlled Access Mechanism module is designed to implement personalized and fine-grained access controls for user data. It involves the generation of unique hyperlinks for data access, smart contract development to enforce access rules, and mechanisms for user-friendly management of access permissions.

Smart Contracts and Automation Module:

Smart contracts play a crucial role in automating and enforcing the access control policies defined within the system. This module involves the development and deployment of smart contracts to facilitate automated, trustless, and transparent execution of predefined rules for data access and sharing.

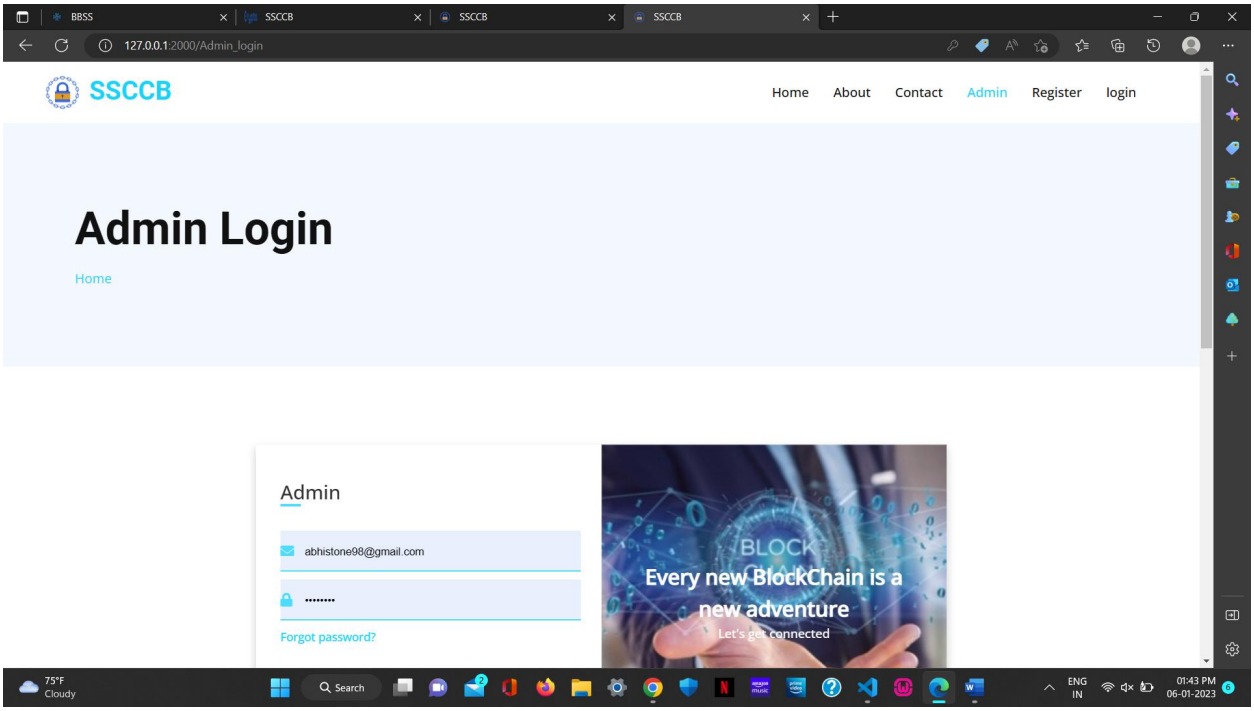
User Interface Module:

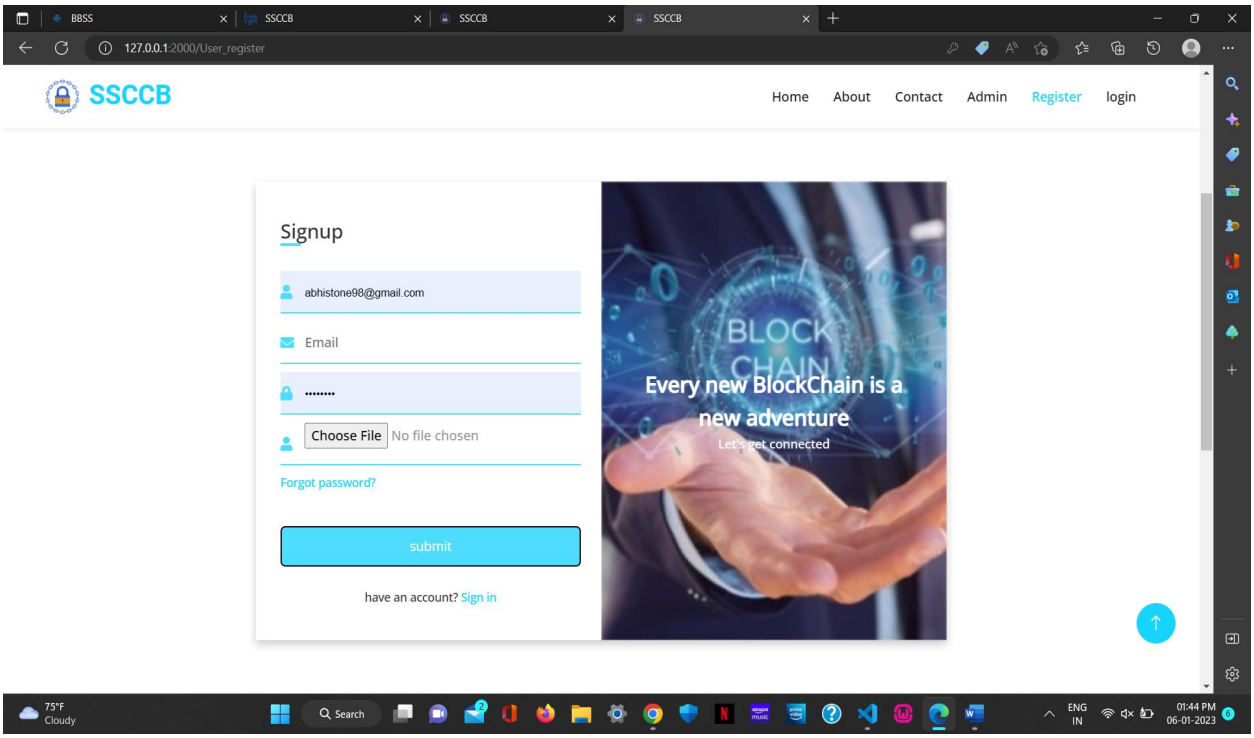
The User Interface module focuses on creating a user-friendly front-end for seamless interaction with the Blockchain-based security system. It includes features for generating personalized access links, monitoring data access logs, and managing user-specific security settings. A well-designed interface enhances user experience and facilitates effective utilization of the system.

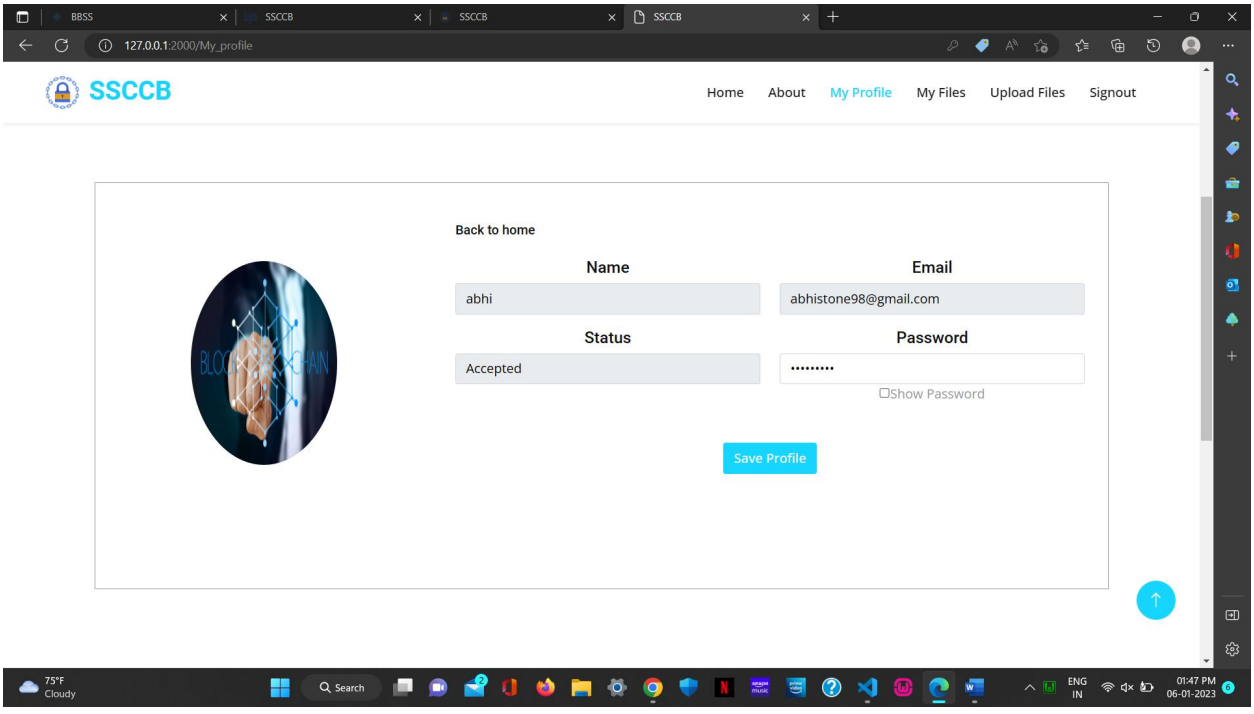
Logging and Monitoring Module:

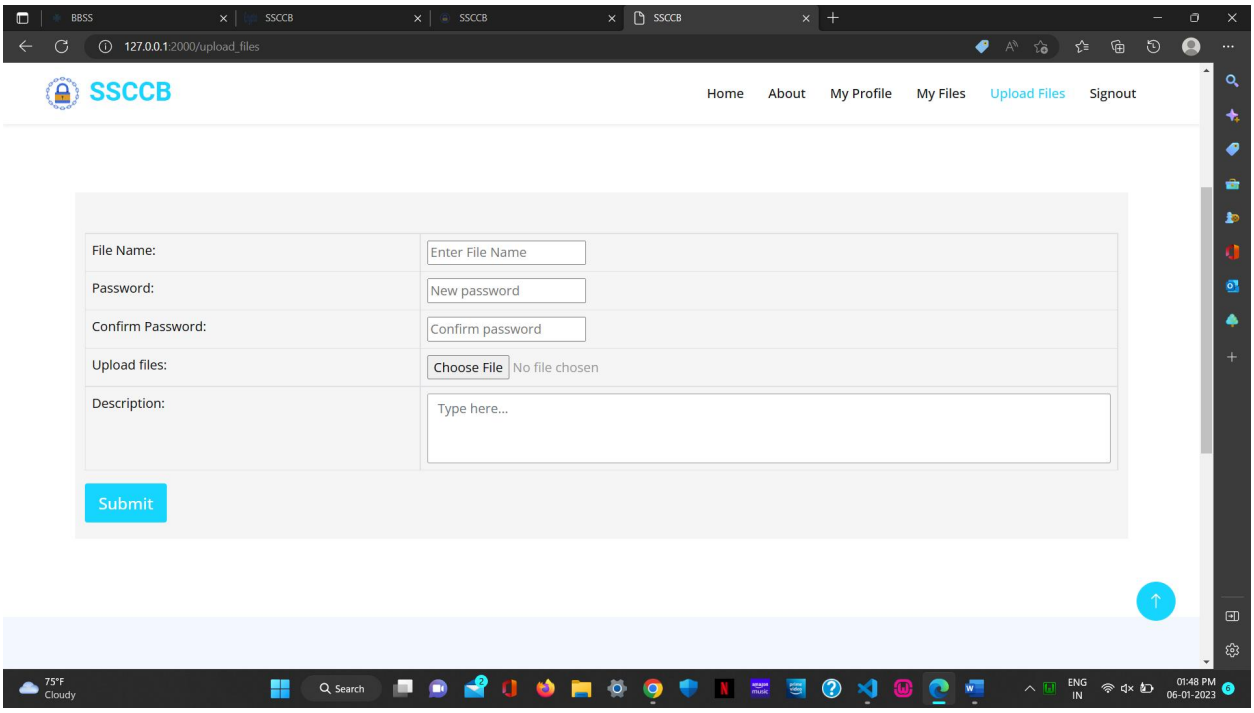
This module is dedicated to capturing and storing detailed logs of all user actions and operations performed on or with the data. It includes mechanisms for timestamping, logging, and storing these activities in a secure manner. The logging and monitoring module enhances transparency, accountability, and aids in forensic analysis in the event of security incidents or breaches.

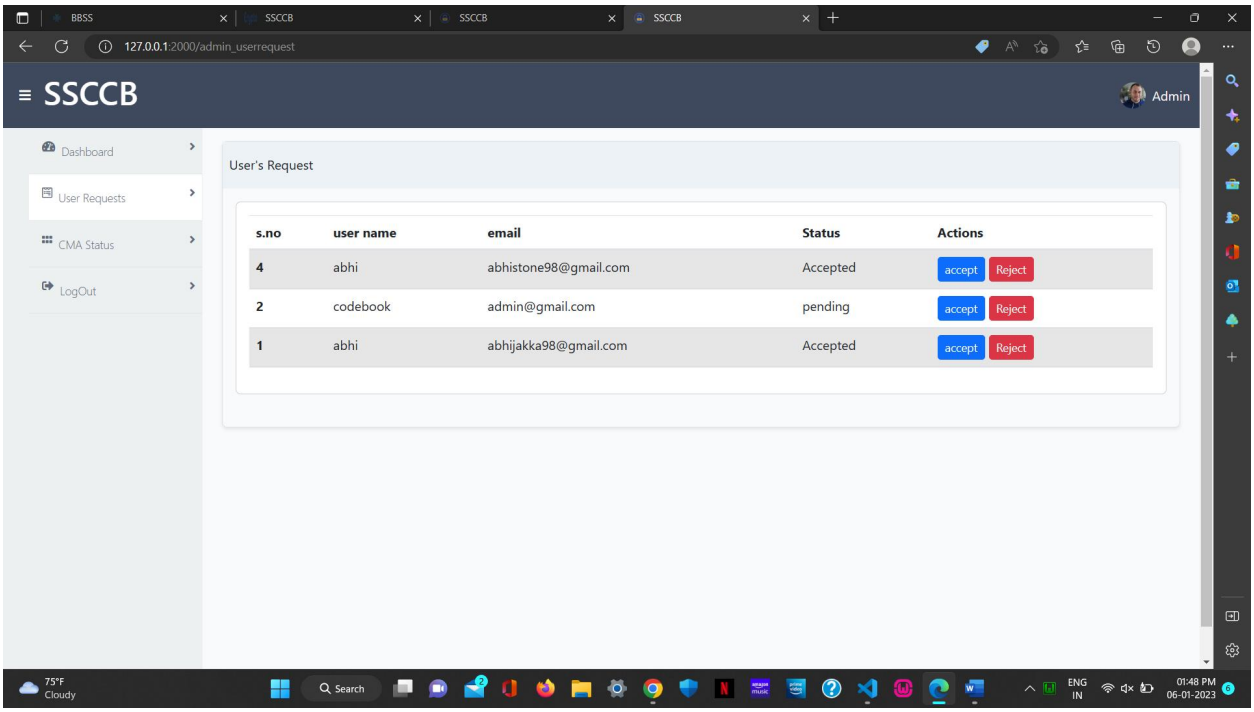
5. Expected Results

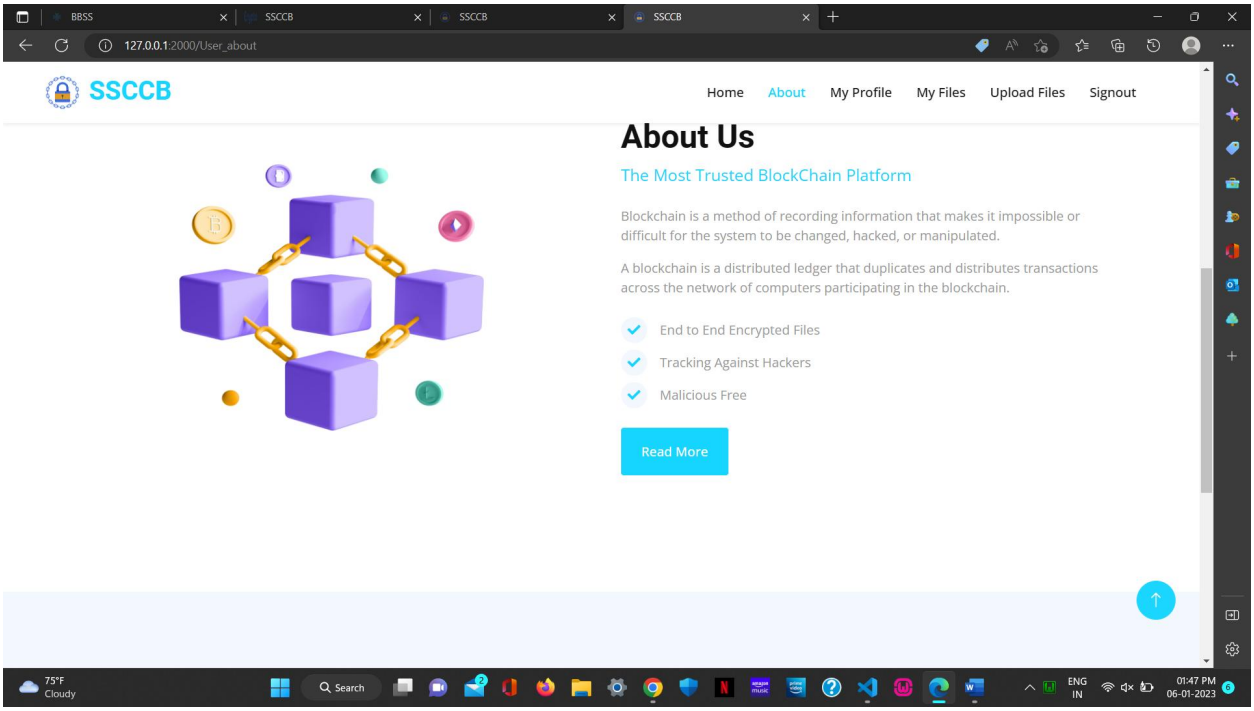



SSCCB
Home
About
Contact
Admin
Register
login
Signup
abhistone98@gmail.com
Email
Choose File
No file chosen
Forgot password?
submit
have an account? Sign in
Every new BlockChain is a new adventure
Let's get connected


SSCCB
Home
About
My Profile
My Files
Upload Files
Signout
Back to home
Name
abhi
Email
abhistone98@gmail.com
Status
Accepted
Password
Show Password
Save Profile


BBSS
SSCCB
SSCCB
SSCCB
127.0.0.1:2000/upload_files
SSCCB
Home
About
My Profile
My Files
Upload Files
Signout
File Name:
Enter File Name
Password:
New password
Confirm Password:
Confirm password
Upload files:
Choose File
No file chosen
Description:
Type here...
Submit
75°F
Cloudy
Search
ENG
IN
01:48 PM
06-01-2023


SSCCB
127.0.0.1:2000/admin_userrequest
Admin
Dashboard
User Requests
CMA Status
LogOut
User's Request
s.no
user name
email
Status
Actions
4
abhi
abhistone98@gmail.com
Accepted
accept
Reject
2
codebook
admin@gmail.com
pending
accept
Reject
1
abhi
abhijakka98@gmail.com
Accepted
accept
Reject


SSCCB
127.0.0.1:2000/User_about
Home
About
My Profile
My Files
Upload Files
Signout
About Us
The Most Trusted BlockChain Platform
Blockchain is a method of recording information that makes it impossible or difficult for the system to be changed, hacked, or manipulated.
A blockchain is a distributed ledger that duplicates and distributes transactions across the network of computers participating in the blockchain.
End to End Encrypted Files
Tracking Against Hackers
Malicious Free
Read More

6. CONCLUSION

In this paper, we have proposed for integration of cloud computing development with blockchain development for giving predominant security in the cloud environment. This paper confirms the integration of cloud advancement with blockchain advancement by showing up exploratory results done by the computer program utilizing java programming language. Blockchain integration with cloud security makes a distinction in getting the result more secure and specific for the users as well as the clients in various ways like

a) User inputs are stored in a new text file.

b) RSA Algorithm is used for encryption as well as decryption on the text file mentioned above.

c) Storing the encrypted file in the cloud. Agreeing to a large wide variety of papers which have been investigated, most clients and analysts of the blockchain pay extra consideration to the utility of blockchains and innovation itself, however much less attention and research to security. We think blockchain secrecy research and higher level security, particularly application layer security calls for persistent consideration and research. I’m hoping that the paintings of this paper can alarm the professionals.

7. REFERENCES

[1] Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, Reji Thomas, Tai-Hoon Kim, "Proof-Of-Work Consensus Approach In Blockchain Technology For Cloud And Fog Computing Using Maximization-Factorization Statistics", IEEE Vol-6 Issue-4, 2019

[2] M.Banerjee, J.Lee, KKR Choo, "A blockchain future to Internet of Things security: A position paper, Digital Communications and Networks", 2017

[3] Yutao Jiao, Ping Wang, DusitNiyato, KongrathSuankaewmanee, "Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks", IEEE vol-30 issue-9, 2019

[4] Liehuang Zhu, Yulu Wu, KekeGai, Kim-Kwang Raymond Choo, "Controllable and trustworthy blockchain-based cloud data management", Future Geneation Computer Systems, vol-91, February 2019

[5] Ruizhe Yang, F. Richard Yu, Pengbo Si, Zhaoxin Yang, Yanhua Zhang, "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges", IEEE vol-21 issue 2, 2019

[6] RubaAwadallah and AzmanSamsudin, "Using Blockchain in Cloud Computing to Enhance Relational Database Security", IEEE, vol-9, 2021

[7] Wenjuan Li, Jiyi Wu, Jian Cao, Nan Chen, Qifei Zhang and RajkumarBuyya, "Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions", Springer, 2021

[8] M.Chandni, N. P. Sowmiya, S. Mohana, M. K. Sandhya, "Establishing Trust despite attacks in cloud computing: a survey", IEEE, 2017

[9] Enas F. Rawashdeh, Inas I. Abuqaddom, Amjad A. Hudaib, "Trust models for services in cloud environment: a survey", IEEE, 2018

[10] David Berdik, SafaOtoum, Nikolas Schmidt, Dylan Porter, YaserJararweh, “A survey on blockchain for information systems management and security”, Science direct, 2021

[11] Omar Ali, Ashraf Jaradat, AtikKulakli and Ahmed Abuhalimeh, “A comparative study: blockchain technology utilization benefits, challenges and functionalities”, IEEE, VOL-9, 2021

[12] Osama F. AbdelWahab, Aziza I. Hussein, Hesham F. A. Hamed, Handy M. Kelash, Ashraf A.M.Khalaf, “Efficient combination of RSA Cryptography, Lossy, and Lossless Compression steganography techniques to hide data”, Science Direct, vol- 182, 2021