ISSN 2347–3657

International Journal of
Information Technology & Computer Engineering

Volume 13, Issue 2s, 2025

A Comprehensive Block Chain – Inteprated Framework For Security Cloud Computing

Mohd Numan Nizamuddin[1], M.A Muntasir[2], Fawwaz Baig[3], Mr. Mohd Basit Mohiuddin[4]
[1,2,3]B.E Students, Department Of BE IT, ISL Engineering College, Telangana India.
[4]Assistant Professor, Department Of IT, ISL Engineering College, Telangana India.
mohdnuman187@gmail.com

ABSTRACT

Due to its wide accessibility, cloud services are susceptible to attacks. Data manipulation is a serious threat to data integrity which can occur in cloud computing – a relatively new offering under the umbrella of cloud services. Data can be tampered with, and malicious actors could use this to their advantage. Cloud computing clients in various application domains want to be assured that their data is accurate and trustworthy. On another spectrum, blockchain is a tamper-proof digital ledger that can be used alongside cloud technology to provide a tamper-proof cloud computing environment. This paper proposes a scheme that combines cloud computing with blockchain that assures data integrity for all homomorphic encryption schemes. To overcome the cloud service provider's (CSP) ultimate authority over the data, the proposed scheme relies on the Byzantine Fault Tolerance consensus to build a distributed network of processing CSPs based on the client requirements. After certain computations performed by all CSPs, they produce a master hash value for their database. To ensure immutable data is produced, master hash values are preserved in Bitcoin or Ethereum blockchain networks. The master hash values can be obtained by tracking the block header address for verification purposes. A theoretical analysis of the overhead costs associated with creating master hash values for each ofthe cryptocurrencies is presented. Wefound thatEthereum leads to lowerclient financial costs and better online performance than Bitcoin. We also specify the data security requirements the proposed scheme provides, the ground-level implementation, and future work. The proposed verification scheme is based on public cryptocurrency as a back-end service and does not require additional setup actions by the client other than a wallet for the chosen cryptocurrency

I. INTRODUCTION

Data security is frequently characterised by data security threats. The area of cloud computing is no different as it is prone to various threats. The primary reason for this is that cloud computing combines many different technologies in its operation. It is paramount to use the process of risk management to balance the benefits of security risks, and cloud computing [1]. Cloud Security Alliance (CSA) [2] is a non-profit organisation set up for the purpose of enforcing general security. CSA has laid out essential shared responsibilities for cloud service providers (CSPs) and the clients to mitigate the risks associated with cloud computing. The The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Chi Chen . job of the CSP is to record, design and implement the client security control and internal security control. The design and implementation are carried out using a tool known as Consensus Assessments Initiative Questionnaire (CAIQ). A cloud consumer uses a Cloud Control Matrix (CCM) to document the people in charge of implementing specific controls and the manners in which they go about it. Also, a high-level process model for cloud security management has been developed to cater to the significant variations of the process model that are likely to occur in building a cloud project, as illustrated in Fig. 1. The essence is to find out the necessary requirements, structure the architecture, and find any missing spaces according to the underlying cloud platform's capabilities. Despite the CSP's attempts to establish a strong security base, such arrangements are rarely substantive from the data owners' perspective, especially when it comes to trusting the CSP itself. This is compounded by the fact that the growth of cloud computing technology leads to new security vulnerabilities and amplifies existing ones. A recent CSA survey [3] compiled the most significant security issues within cloud computing, classifying the top 11 threats into 14 security domains which can be divided into either the governance or operational domains. The governance domain focuses on strategic and policy issues within a cloud computing environment, whereas the operational domain focuses on tactical security concerns. Table 1 shows how an enterprise opens itself to many commercial, financial, technical, legal, and compliance risks if it adopts a CSP as it is. Most security concerns lead to various threats like identifying spoofing, tampering with data repudiation, information disclosure, denial of service, and elevation of privilege. Data breaches is at the forefront of threat ranking trend analyses conducted by CSA through 2011, 2016, and 2020 [3], [5], [6]. If such security breaches occur, it

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP452-456

would seriously undermine the validity and trust of a cloud-based service. A data breach is an event where an unauthorised entity releases, analyses, steals or uses essential, safe or confidential information. A data breach can either be the primary purpose of a targeted attack or a result of human error, implementation vulnerabilities or inadequate security procedures. The leak of any information not meant for public access is considered a data breach. [7] noted that either encryption and keys vulnerabilities or data storage cryptography vulnerabilities could lead to data breaches. More explicitly, the absence of appropriate encryption algorithms and a poor key management mechanism can contribute to encryption, and key-related failures that directly impact data confidentiality and completeness [8]. Weak key management, defective, insecure, and outdated encryption methods allow data storage to be susceptible to threats [9], [10]. This has been further supported in [11] which highlighted that weak encryption techniques contribute to the most significant risk. As with any information security management system, fundamental cloud security requirements include confidentiality, integrity, and availability [12]. The problem of data breaches is directly related to confidentiality and privacy. Confidentiality requires that sensitive client data is not disclosed to a unauthorised entity, whereas privacy refers to the rights of a client to have control over how its data is handled. Encryption algorithms are utilised to achieve both data confidentiality and privacy requirements. There have been various cryptographic schemes proposed to preserve the security of stored data and/or processed data. Various symmetric key encryption algorithms have been used for cloud computing platforms [13]. [14] proposed applying AES to encrypt hard disc data in XEX-based tweaked-codebook mode with ciphertext stealing (XTS). [15] provided data confidentiality, privacy, and availability by employing proxy re-encryption in conjunction with decentralised deletion code. [16] has released a secure storage model for cloud data based on Reed-Solomon (SECRESO) model. They adhere to data security, integrity, availability and error tolerance by improving Reed-Solomon code-based encryption, as well as relying on a log-based backup. [17] established an hourglass protocol to encrypt data files which, at the same time, enables users to check the accuracy of the encrypted file. Although the use of encryption algorithms like AES can be used to protect data transmitted to the cloud, some findings indicate that traditional cryptographic algorithms are more appropriate for traditional IT infrastructure rather than cloud computing environments [18]. One of the main reasons is that the stored data requires decryption before any calculation can be performed [19]. Despite the merits of the previous proposals in providing adequate security for data-at-rest, it is not feasible for data processing on an external server. Homomorphic encryption (HE) has been proposed to overcome this issue. HE, an asymmetric key encryption scheme, allows calculations to be performed on the encrypted data by a third party without disclosing the corresponding keys. Many HE schemes have been proposed in recent years with the goal of improving cloud computing security [20]–[22]. In contrast, because CSP is a centralised management approach, HE alone cannot fulfil IND-CCA2 security notions against tampering. Therefore, client data is exposed to administrative risks that may cause data loss or undisclosed manipulation in the database. In order to employ decentralisation and enhance the manipulation transparency of homomorphically encrypted data, blockchain (BC) technology is the one possible solution. Several studies have relied on BC in restructuring the cloud to solve several security issues [23]–[25]. However, they suffer from complicated configuration setup, and the embedding requires a huge effort and budget. In this paper, we overcome these existing problems by proposing a verification scheme based on the notions of BFT and blockchain technology. More than one CSP will be hired to store and perform computations on client data. Each CSP will have to periodically compute a master hash value of their database to be stored on a public blockchain such as Bitcoin or Ethereum. These CSPs do not need to collaborate or communicate with one another. A client can compare these master hash values to detect if data tampering has occurred. This distributed verification system fulfils the requirements of confidentiality (HE will be used for encryption), and integrity because data modifications by the CSPs can be detected by comparing master hash values stored on the blockchain. The rest of this paper is structured as follows: In Section II, we provide a detailed explanation of both HE and BC as they play a major role in solving the problem of CSP centralisation in processing client data. Next in Section III, we introduce the proposed scheme. The results, discussion and recommendations for future work are detailed in Section IV. Finally, Section V provides the conclusion of our proposed scheme

2-LITERATURE SURVEY

Title: Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges

AUTHORS: Jinglin Zou ,Debiao He,Sherali Zeadally,Neeraj Kumar,Huaqun Wang

The approach entails a methodical examination of the literature to find studies on the integration of

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP452-456

blockchain technology and cloud computing for improved security. We categorize and evaluate recent works, look into the performance boosts that cloud computing brings to blockchain, assess market trends, pinpoint issues, and offer suggestions for further research. By fusing blockchain technology with cloud computing, the Regulatory uncertainty regarding data privacy and compliance, potential performance bottlenecks from increased computational overhead, interoperability issues between diverse blockchain and cloud platforms, and the complexity of securely managing cryptographic keys To sum up, the amalgamation of blockchain technology and cloud computing offers auspicious prospects for augmenting security and tackling obstacles inherent in the contemporary computing terrain. suggested system seeks to improve security and tackle issues like data integrity, privacy protection

Title: Blockchain Based Cloud Computing: Architecture and Research Challenges

AUTHORS: Ch V N U Bharathi Murthy, Lawanya Shri M, Seifedine Kadry, Sangsoon Lim

A review of the body of research on the difficulties facing cloud computing—particularly in relation to data security and management—was part of the methodology. A survey was then made to evaluate earlier research that combined blockchain technology and the cloud. The suggested system combines cloud computing and blockchain technology to solve issues with data management, security, compliance, and dependability. It seeks to improve the reliability and effectiveness of cloud-based systems while maintaining data integrity and privacy Blockchain integration with cloud computing is not without its challenges, despite its potential benefits. These include potential performance bottlenecks, scalability issues brought on by the computational overhead of blockchain consensus mechanisms, complexity in setting up and maintaining hybrid systems, and worries To sum up, combining blockchain technology with cloud computing presents viable answers to issues like data security and dependability. But it also comes with challenges like performance, scalability, and regulatory issues.

Title: Security in Cloud Computing Using Blockchain: A Comprehensive Survey

AUTHORS: Sagnik Jana, Rahul Modak, Koushik Majumder, Anurag Dasgupta

As part of the methodology, a thorough literature review is conducted to examine current security concepts in blockchain technology and cloud computing. It looks at blockchain-based cloud security solutions and compares them to see how effective they are. To improve security, the suggested system combines blockchain technology with cloud computing. It makes use of the tamper-proof and decentralized nature of blockchain technology to guarantee data integrity and authentication. Blockchain integration with cloud computing is not without its challenges, despite its potential. The scalability problems with blockchain may make it less useful in large-scale cloud environments. To sum up, blockchain technology has a lot of potential to improve cloud computing security.

Title: Cloud Computing Access Control Using Blockchain

AUTHORS: Manal Ayyadh Alshammari, Hedi Hamdi, Mahmood A. Mahmood, A. A. Abd El-Aziz

As part of the methodology, current access control challenges in cloud computing are analyzed, the features of blockchain technology are studied, integration opportunities are explored, scalability issues are assessed, consensus mechanisms are evaluated, implementation costs are taken into account, and challenges such as fault resolution due to blockchain immutability are highlighted. The suggested system combines cloud computing and blockchain technology to improve access control. Permissions and access policies are transparently recorded on an unchangeable ledger. Difficulties include access control transaction processing delays and scalability problems brought on by possible network congestion. Effectively integrating blockchain and cloud technologies gives rise to integration challenges.

3-METHADOLOGY

1.CSP1 & CSP2-- These modules represent two different cloud service providers.

THEY accept encrypted files, Master Hashes, and filenames from the Cloud User module.

2.Cloud User: The Cloud User is the client or end-user of the system. They perform the following actions:

3.Upload File: Through this feature, The user can upload files to the system

4.FHE Encrypt & outsource to CSP's: After uploading, the user's file is encrypted using FHE and then outsourced to multiple CSPs (CSP1 and CSP2). The system generates a Master Hash for each file before uploading it to the cloud.

5.Download & Decrypt File: The user can download and decrypt files when needed. This ensures that the user can access the original content.

6.Master Hash Blockchain Verification: The user can request data verification. The system invokes the Ethereum Blockchain, where Master Hash codes for all files are stored. The Blockchain calculates the stored file's Master Hash and compares it with the one received from the user. If they match, the verification is successful, indicating that the data is secure.

4-REQUIREMENTS ENGINEERING

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP452-456

HARDWARE REQUIREMENTS

- PROCESSOR : i5 and above
- RAM : 8 GB and above
- ROM : 25 GB and above

SOFTWARE REQUIREMENTS

- Node js
- Python 3.7.0
- Visual studio community version

FUNCTIONAL REQUIREMENT

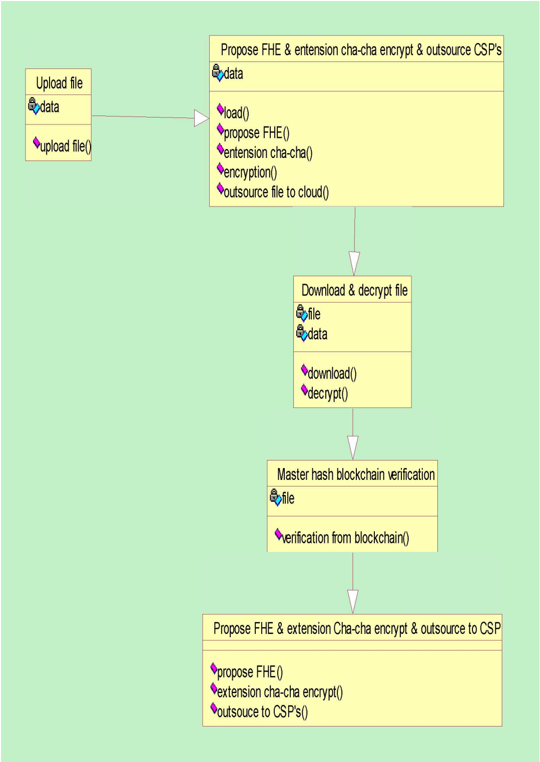
1. CSP1
2. CSP2
3. Cloud User
   - ☐ Upload File
   - ☐ FHE Encrypt & outsource to CSP’s
   - ☐ Download & Decrypt File
   - ☐ Master Hash Blockchain Verification

NON-FUNCTIONAL REQUIREMENTS

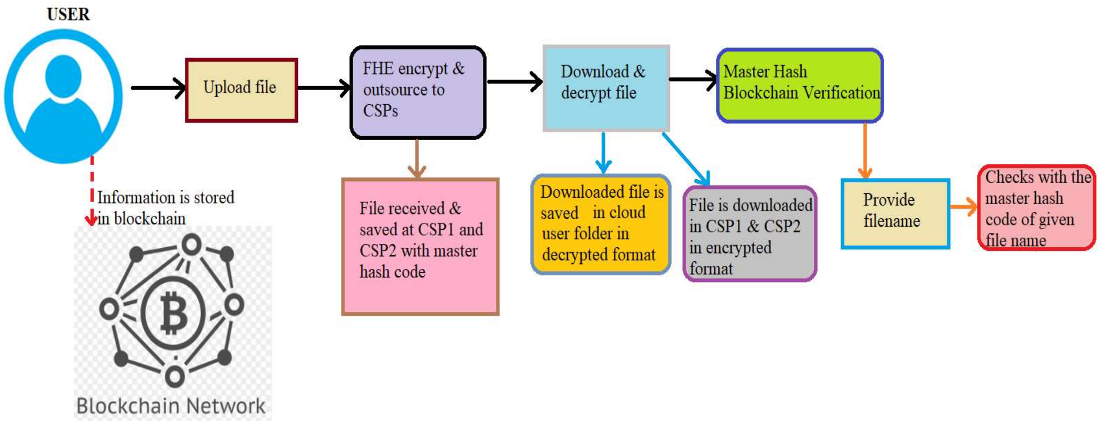
- ➢ Usability
- ➢ Security
- ➢ Availability
- ➢ Maintainability
- ➢ Efficiency

5-DESIGN ENGINEERING

CLASS DIAGRAM


Upload file
data
upload file()
Propose FHE & entension cha-cha encrypt & outsource CSP's
data
load()
propose FHE()
entension cha-cha()
encryption()
outsource file to cloud()
Download & decrypt file
file
data
download()
decrypt()
Master hash blockchain verification
file
verification from blockchain()
Propose FHE & extension Cha-cha encrypt & outsource to CSP
propose FHE()
extension cha-cha encrypt()
outsouce to CSP's()

SYSTEM ARCHITECTURE


USER
Upload file
FHE encrypt & outsource to CSPs
Download & decrypt file
Master Hash Blockchain Verification
Information is stored in blockchain
Blockchain Network
File received & saved at CSP1 and CSP2 with master hash code
Downloaded file is saved in cloud user folder in decrypted format
File is downloaded in CSP1 & CSP2 in encrypted format
Provide filename
Checks with the master hash code of given file name

6-IMPLEMENTATION

- ➢ Blockchain’s smart contracts are deployed to securely store Master Hashes generated for each file. These hashes serve as tamper-proof data references.
- ➢ Blockchain provides data security and decentralization by distributing data across multiple nodes, making it highly resistant to tampering.

Real-time user alerts for data integrity are enabled through blockchain technology. Users can verify data authenticity by comparing Master Hashes stored on the blockchain

7-CONCLUSION

- The project successfully enhances data security in cloud computing by integrating blockchain technology.
- It provides real-time user alerts for data integrity, addressing the risks of data alteration.
- The project incorporates multiple cloud service providers (CSPs) for flexible cloud services while ensuring data security through Fully Homomorphic Encryption (FHE) for direct computation on encrypted data.
- The establishment of a Master Hash generation system supports tamper-proof data, securely stored on the blockchain for decentralization and security.
- Ethereum smart contracts securely store file hash codes on the blockchain, further enhancing data security.
- The project conducts an analysis of payments for Master Hash storage and access, considering Ethereum's GAS prices.
- This project sets a robust example for securing cloud data through blockchain, paving the way for safer and more trustworthy cloud computing.

REFERENCE

- Jinglin Zou ,Debiao He,Sherali Zeadally,Neeraj Kumar,Huaqun Wang , et. al., “Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges” published in IJISAE open Access.
- Ch V N U Bharathi Murthy, Lawanya Shri M, Seifedine Kadry, Sangsoon Lim, et. al., “Blockchain Based Cloud Computing: Architecture and Research Challenges” published in researchgate open Access.
- Sagnik Jana, Rahul Modak, Koushik Majumder, Anurag Dasgupta, et. al., “Security in Cloud Computing Using Blockchain: A Comprehensive Survey” published in researchgate open Access.
- Manal Ayyadh Alshammari, Hedi Hamdi, Mahmood A. Mahmood, A. A. Abd El-Aziz , et. al., “Cloud Computing Access Control Using Blockchain” published in ijisae open Access.
- Lubal Utkarsh Balu , et. al., “Blockchain Technology for Cloud Security and Data Integrity” published in JETIR open Access.

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP452-456