ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue.2 April 2024

A DATA INTEGRITY VERIFICATION SCHEME FOR CENTRALIZED DATABASE USING SMART CONTRACT AND GAME THEORY

[1] Medak Shravani,[1] Chembeti Mrudula, [1]Danda Anushka Reddy, [2]G. Shekar

[1]UG Student In Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad.

[2]Assistant Professor In Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad.

Abstract

Currently, many companies and institutions use centralized or distributed databases to store massive amounts of data. However, the use of un trusted centralized third-party auditors can result in security issues because these auditors may be malicious and tamper with or delete user data. This poses a significant challenge for ensuring the reliability of the data verification results. Although introducing a third-party auditor can help address this issue, it may also be untrustworthy and collude with the database service provider to forge false data verification results. In this study, we propose a data integrity verification scheme using smart contracts (DIV-SC) to address this challenge in a centralized database environment. Our approach utilizes block chain technology as a decentralized third-party auditor, ensuring that the information stored on the block chain is immutable and cannot be tampered with maliciously. In addition, smart contracts deployed on the block chain can ensure that the verification procedures are correct and are not affected by any malicious party. We also leverage game theory to improve the reliability of multiple verifications, reduce verification time and improve overall performance. Our proposed scheme reduces the total verification time consumption by up to 53.44% while increasing the number of verifiable times by nearly 3.8 times, compared to conventional data integrity verification schemes.

I INTRODUCTION

Since the introduction of centralized databases, data security has been a significant concern that cannot be ignored. This issue presents numerous challenges that must be addressed. Centralized databases are heavily centralized with a system architecture composed of a processor,

ISSN2454-9940

www.ijasem.org

Vol 18, Issue.2 April 2024

associated data storage device, and other peripheral devices. Data management within the system is under the central control of the service provider. However, centralization creates a major security problem as it cannot guarantee the reliability of the data integrity verification results. For instance, in pursuit of greater benefits, the service provider managing the database may engage in malicious tampering behaviour with user-stored data or delete data that users infrequently access to conserve their resources. Subsequently, the service provider can deceive the user by returning the false data integrity verification results. Users lack evidence to prove that the verification results are forged, as direct access to the database's contents is not possible owing to data security concerns. Database is a database system spread across multiple locations or nodes, with each node responsible for a portion of the database. The data were stored on multiple computers, with each computer able to access and retrieve the data. However, despite the decentralization characteristics of distributed databases, each node or computer in the physical network is a centralized service provider that controls a part of the database, which makes it susceptible to the same data integrity verification problems as centralized databases. Block chain technology has gained significant attention owing to its potential to create secure and decentralized systems. At its core, a block chain is a distributed ledger that records transactions securely and transparently. This makes it possible to create tamper-proof records that can be, verified without the need for central authority. An important component of block chain technology is the smart contract. A smart contract is a self-executing agreement written in code and stored on the block chain. It can automatically execute and enforce terms of agreement between two or more parties without the need for intermediaries. Smart contracts are secure and transparent, and can reduce costs and increase efficiency by removing intermediaries and automating processes. Block chain technology and smart contracts have the potential to transform various industries and revolutionize the way data are secured. After establishing a decentralized third-party verification platform with block chain, the method of ensuring the reliability of each verification is very simple: generate a corresponding data digest for the data that needs to be verified later and store the digest in the smart contract on the block chain.

ISSN2454-9940

www.ijasem.org

Vol 18, Issue.2 April 2024

When verification is required, the database service provider generates a corresponding digest based on the data stored by itself, and then sends the digest to the smart contract for comparison. If the digest sent by the service provider is consistent with the digest stored in the smart contract, the service provider has not tampered with or deleted the data. However, after the first verification, the service provider can save the digest and delete the original data. In the subsequent verification, the saved digest is sent directly to the smart contract to deceive the verification result. The most straightforward solution is to regenerate a new digest for the data after each verification is completed; however, this will greatly increase the time required for verification, which is not conducive to the verification of large volume files and large-batch files. Therefore, it is necessary to design a new verification method that can ensure the reliability of multiple verifications without degrading verification performance. Game theory is a mathematical model that studies the strategic interaction between rational decision-makers, and is a method for studying the phenomena of a struggle or competition nature. Games are usually composed of the following elements: players, strategy, payoff, information, and rationality. Interdependence is the essence of game theory methods, that is, each party's payoff depends not only on its strategy, but also on the strategies of other players. The goal of game theory research is how to reach an equilibrium state because changes in the strategies of the players in the game will cause changes in income, so each player will adjust their strategies to maximize their income. In such cases, a ''stable'' strategy option is worth investigating. After each player chooses their strategy, there is no motivation to change the current strategy, and a stable state is formed. This stable state is called ''Nash equilibrium'

II LITERATURE SURVEY

An attribute based controlled collaborative access control scheme for public cloud storage

AUTHOR:*Y. Xue, K. Xue, N. Gai, J. Hong, D. S. Wei, and P. Hong*

In public cloud storage services, data are outsourced to semi-trusted cloud servers which are outside of data owners' trusted domain. To prevent untrustworthy service providers from accessing data owners' sensitive data, outsourced data are often encrypted. In this scenario, conducting access control over these data becomes a

challenging issue. Attribute-based encryption (ABE) has been proved to be a powerful cryptographic tool to express access policies over attributes, which can provide a fine-grained, flexible, and secure access control over outsourced data. However, the existing ABE-based access control schemes do not support users to gain access permission by collaboration. In this paper, we explore a special attribute-based access control scenario where multiple users having different attribute sets can collaborate to gain access permission if the data owner allows their collaboration in the access policy. Meanwhile, the collaboration that is not designated in the access policy should be regarded as a collusion and the access request will be denied. We propose an attribute-based controlled collaborative access control scheme through designating translation nodes in the access structure. Security analysis shows that our proposed scheme can guarantee data confidentiality and has many other critical security properties. Extensive performance analysis shows that our proposed scheme is efficient in terms of storage and computation overhead.

Methodologies for data quality assessment and improvement.

AUTHOR:C. Batini, C. Cappiello, C. Francalanci, and A. Maurino.

The literature provides a wide range of techniques to assess and improve the quality of data. Due to the diversity and complexity of these techniques, research has recently focused on defining methodologies that help the selection, customization, and application of data quality assessment and improvement techniques. The goal of this article is to provide a systematic and comparative description of such methodologies. Methodologies are compared along several dimensions, including the methodological phases and steps, the strategies and techniques, the data quality dimensions, the types of data, and, finally, the types of information systems addressed by each methodology. The article concludes with a summary description of each methodology.

Block chain for supply chain traceability: Bus. Requirements and critical success factors.

AUTHOR:G. M. Hastig and M. S. Sodhi

We seek to guide operations management (OM) research on the implementation of supply chain traceability systems by identifying business requirements and the factors critical to successful implementation. We first motivate the need for implementing

traceability systems in two very different industries—cobalt mining and pharmaceuticals—and present business requirements and critical success factors for implementation. Next, we describe how we carried out thematic analysis of practitioner and scholarly articles on implementing block chain for supply chain traceability. Finally, we present our results pertaining to the needs of different stakeholders such as suppliers, consumers, and regulators. The business requirements for traceability systems are curbing illegal practices; improving sustainability performance; increasing operational efficiency; enhancing supply-chain coordination; and sensing market trends. Critical success factors for implementation are companies' capabilities; collaboration; technology maturity; supply chain practices; leadership; and governance of the traceability efforts. These findings provide a nascent measurement model for empirical work and a foundation for descriptive and normative research on block chain applications for supply chain traceability.

III EXISTING SYSTEM

Block chain technology has gained significant attention owing to its potential to create secure and decentralized systems. At its core, a block chain is a distributed ledger that records transactions securely and transparently. This makes it possible to create tamper-proof records that can be verified without the need for central authority. An important component of block chain technology is the smart contract. A smart contract is a self-executing agreement written in code and stored on the block chain. It can automatically execute and enforce terms of agreement between two or more parties without the need for intermediaries. Smart contracts are secure and transparent, and can reduce costs and increase efficiency by removing intermediaries and automating processes. Block chain technology and smart contracts have the potential to transform various industries and revolutionize the way data are secured.

Disadvantages:

- Security risks
- Collection and storage
- Operational costs

IV PROBLEM STATEMENT

The use of block chain technology has opened up new possibilities for resolving the challenges mentioned earlier. Block chain is a decentralized digital ledger that stores authorized data that has been hashed and protected. The data ledger is unchangeable; each error or update is traced

back to the source. Decentralization, tamper-evident information, and information transparency are all fundamental features of block chain. As a result, a block chain system enables the creation of a transparent, open, safe, and reliable data exchange environment for connecting big data from many disciplines. Creating decentralized big data storage with consensus model is very difficult one. Since for every data transfer operation the system needs to verify its validation through PoW or PoS.We implemented a public consensus mechanism for big data storage to overcome the communication cost and energy consumption.

V PROPOSED SYSTEM

we propose a data integrity verification scheme using smart contracts (DIV-SC) to address this challenge in a centralized database environment. Our approach utilizes block chain technology as a decentralized third-party auditor, ensuring that the information stored on the block chain is immutable and cannot be tampered with maliciously. In addition, smart contracts deployed on the block chain can ensure that the verification procedures are correct and are not affected by any malicious party. We also leverage game theory to improve the reliability of multiple verifications, reduce verification time and improve overall performance. Our proposed scheme reduces the total verification time consumption by up to 53.44% while increasing the number of verifiable times by nearly 3.8 times, compared to conventional data integrity verification schemes.

ADVANTAGES

- Advertising, clinicians, transportation, fraud detection and tourism marketing.
- Systems are difficult due to the challenges in processing.

VI ALGORITHM USED

Conventional Scheme

To demonstrate that our designed scheme can reduce the total verification time consumption, we compared the total verification time consumption between DIV-SC and the conventional scheme without applying the proposed game theory-based verification mechanism. In the conventional scheme, the user generates only one seed for the update result and not multiple seeds. When verifying, the user will choose to use this seed for verification, reset the seed and calculate the corresponding hash value again after

the verification is completed. In the conventional method, this problem can be solved by resetting the seed and recalculating the corresponding hash value after each verification; however, this will increase the total verification time, and data can only be validated once before resetting the seed. DIV-SC solves this problem by introducing a new verification mechanism based on game theory while further reducing the total verification time and increasing the total number of verifications before resetting the seed

VII IMPLEMENTATION

- ***User Interface Design***

Input : Enter Login name and Password

Output : If valid user name and password then directly open the home page otherwise show error message and redirect to the registration page.

- ***User***

Input : Data User Login name and Password

Output: If valid user name and password then directly open the Data user home page otherwise show error message and redirect to the data user login page.

- ***Admin***

Input : Enter the owner name and password

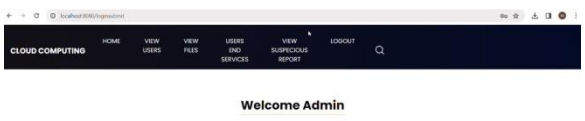
Output : If valid owner name and password then directly open the data owner home page otherwise show error message and redirect to the data owner login page.

- **Security**

Input : Enter the Cloud Server name and password

Output: If valid Cloud Server name and password then directly open the Cloud Server home page otherwise show error message and redirect to the cloud Server login page.

VIII RESULTS

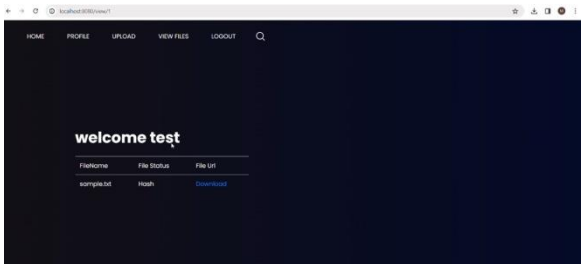


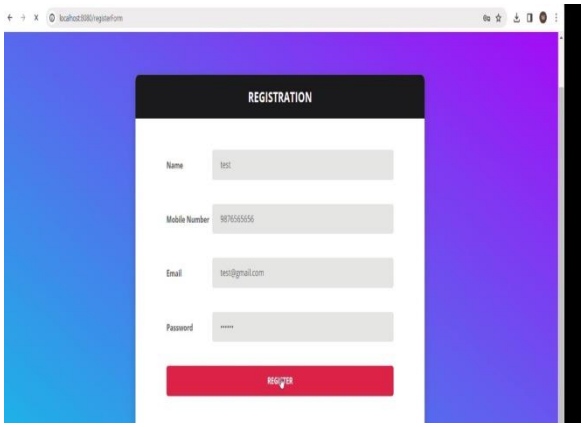
INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

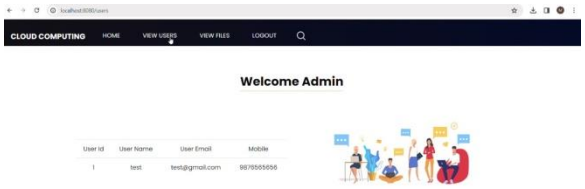
ISSN2454-9940

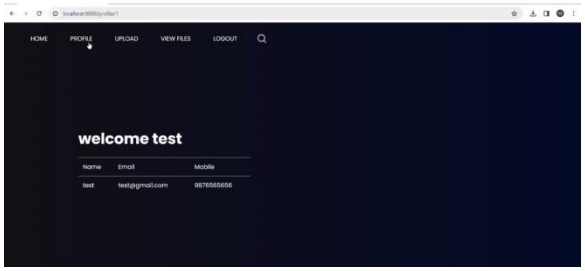
www.ijasem.org

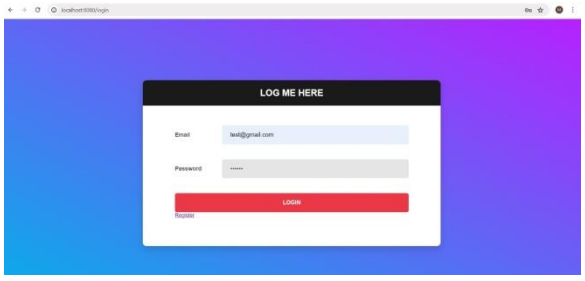
Vol 18, Issue.2 April 2024











VIII CONCLUSION

The security and privacy of big data storage network is affected by third parties control architecture and it's required more attention. We discussed significant issues with the big data storage platforms and suggested an effective way to solve them by implementing a safe framework. To ensure secure and safe data storage in big data contexts, our main goal is to build a reliable and complete architecture based on a block chain. We set up a virtual block chain on the distributed storage network to test the effectiveness of the proposed approach. We combined the block chain with the adaptable finality consensus mechanism to achieve decentralized data storage. We used a consensus mechanism based on the highway protocol for building blocks in the big data storage architecture. We improved the security and privacy of massive data storage by using adjustable finality conditions to secure the

security of new blocks. To demonstrate the high scalability and mobility of our framework and reduce traffic overheads, we employed baseline models to assess the security requirements of the new user device. We conducted a performance of our suggested framework to confirm its effectiveness and identify areas that require improvement in subsequent studies. In future we plan to develop energy-efficient consensus mechanism for edge computing data transfer in the context of big data

REFERENCES

[1] C. Cichy and S. Rass, ‘‘an overview of data quality frameworks,’’ IEEEAccess, vol. 7, pp. 24634–24648, 2019.

[2] J. Gantz and D. Reinsel, ‘‘the digital universe in 2020: Big data, biggerdigital shadows, and biggest growth in the Far East,’’ IDC iView, IDC Analyze Future, vol. 2007, pp. 1–16, Jan. 2012.

[3] J. Hu and A. V. Vasilakos, ‘‘Energy big data analytics and security: Challenges and opportunities,’’ IEEE Trans. Smart Grid, vol. 7, no. 5, pp. 2423–2436, Sep. 2016.

[4] R. Kitchin, ‘‘Big data, new epistemologies and paradigm shifts,’’ Big Data Soc., vol. 1, no. 1, Apr. 2014, Art. No. 205395171452848.

[5] M. Anshari and S. A. Lim, ‘‘E-government with Big data enabled through smartphone for public services: Possibilities and challenges,’’ Int. J. PublicAdmin., vol. 40, no. 13, pp. 1143–1158, Nov. 2017.

[6] W. K. Caldwell, G. Fairchild and S. Y. Del Valle, ‘‘Shrivelling influenza incidence with centres for disease control and prevention web traffic data: Demonstration using a novel dataset,’’ J. Med. Internet Res., vol. 22, no. 7, 2020.

[7] Z. Su and Q. Xu, ‘‘Security-aware resource allocation for mobile social big data: A matching-coalitional game solution,’’ IEEE Trans. Big Data, vol. 7, no. 4, pp. 632–642, Oct. 2021.

[8] B.-Q. Huang, G.-Y. Cao, and M. Guo, ‘‘Reinforcement learning neural network to the problem of autonomous mobile robot obstacle avoidance,’’ in Proc. Int. Conf. Mach. Learn. Cybern., 2005, pp. 85–89.

[9] Y. Hong, ‘‘Reading the 13th five-year plan: Reflections on China’s ICT policy,’’ Int. J. Commun., vol. 11, pp. 1755–1774, Jan. 2017.

[10] Y. Shi, Z. Shan, J. Li, and Y. Fang, ‘‘How China deals with big data,’’ Ann. Data Sci., vol. 4, no. 4, pp. 433–440, Dec. 2017.

[11] I. Ashraf, Y. Park, S. Hur, S. W. Kim, R. Alroobaea, Y. B. Zikria, and S. Nosheen, ‘‘A survey on cyber security threats in IoT-enabled

maritime industry,'' IEEE Trans. Intell. Transp. Syst., vol. 24, no. 2, pp. 2677–2690, Feb. 2023.

[12] A. Sasikumar, N. Senthilkumar, V. Subramaniyaswamy, K. Kotecha, V. Indragandhi, and L. Ravi, ''An efficient, provably-secure DAG basedconsensus mechanism for industrial Internet of Things,'' Int. J. Interact.Design Manuf., vol. 2022, pp. 1–11, May 2022.

[13] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. DeCaro, and J. Yellick, ''Hyperledgerfabric: A distributed operating system for permissioned blockchains,'' in Proc. 13th EuroSys Conf., 2018, pp. 1–15.

[14] D. B. Gajić, V. B. Petrović, N. Horvat, D. Dragan, A. Stanisavljević, V. Katić, and J. Popović, ''A distributed ledger-based automated marketplace for the decentralized trading of renewable energy in smart grids,'' Energies, vol. 15, no. 6, p. 2121, Mar. 2022.

[15] T. Duong, A. Chepurnoy, L. Fan, and H.-S. Zhou, ''TwinsCoin: A cryptocurrency via proof-of-work and proof-of-stake,'' in Proc. 2nd ACMWorkshop Blockchains, Cryptocurrencies, Contracts, May 2018, pp. 1–13.