WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Block-Chain Approach, To Guarantee The Probity Of The Cloud Data Delivered In A Distributed Environment

Dr. A. Satyanarayana[1], S. Bhanu Charan[2], M. Naga Rikit[3], M. Yashwanth[4], M. Niharika[5], Md. Zaid Siddqui [6]

[1]Prof Department of CSE & Siddhartha Institute of Technology & Sciences.
[2,3,4,5,6] Department of CSE & Siddhartha Institute of Technology & Sciences.

A B S T R A C T

Cloud servers allows data owners to transmit and store securely encrypted information that numerous users can access. However, once data is exported to the cloud, data owners have limited access to their data, and external tools are used for managing it. Several scientific approaches use algorithms for encryption to restrict unauthorized access to data, but they neglect the difficulty of maintaining track of valid changes performed on the data. As provenance data contains private information, it should be unchangeable and protected from adversaries because it can be used to determine the integrity of data. This paper proposes using block-chain network to secure access logs in an efficient way. A flexible framework is created, tested, and evaluated, with the results demonstrating that our model may accurately improve the data provenance security. This work takes into account two types of data users, as well as their separate roles and permissible behaviour on the outsourced data. In short, this job ensures the data's trustworthiness, as well as the verification and administration of the outsourced data. The experimental findings demonstrate our solution's efficiency and scalability.

Keywords: Cloud Servers, Unauthorized Access, Provenance Data

1. INTRODUCTION

With the rising amount of data generated daily through the use of various apps, services to store and manage the data are required [1]. With the advent of cloud computing, it is now possible to obtain storage and processing services [2]. In general, cloud service providers (CSPs) make infrastructures available for data storage and processing by charging a fee per use. These services reduce the expenses of establishing and maintaining systems designed to fulfill in-house data requirements indicated by a data stakeholder [3]. As a result, people and organizations are drawn to use computer and storage services provided by third parties and made available on demand. As a result, stakeholders must have faith in the service. As a result, stakeholders must rely on service providers to securely preserve their data and corresponding metadata [4]. Users generally encrypt data before storing it since the data can be vulnerable to unauthorized usage [5].

Adopting outsourced storage with CSPs presents a hurdle in terms of access control. This problem stems from the use of data in which various users are permitted varied access privileges, posing a problem in the development and management of decryption keys. The potential remedy to this issue is to create fine-grained access control over outsourced encrypted data [6]. Attribute-based encryption (ABE) [7] and secret-sharing [8] approaches provides an array of options to determine which users have access to the data. However, this method falls short of providing means to ensure trust in the use (origin and alterations) of data throughout its life cycle.

The development of data provenance systems to ensure confidence in data interchange systems could be one answer to this problem. A provenance system offers information indicating where the data originated, who owns the data, and the many alterations the data has undergone. These include the location of the data as well as the numerous timestamps associated with its generation and use. The deployment of a provenance system, on the other hand, does not completely undermine trust. The key challenge is gathering, storing, and maintaining the confidentiality and privacy of provenance information. Implementing a method or technology that assures the security and privacy of provenance information is critical. Furthermore, provenance information should be verifiable without jeopardizing the privacy and security of individuals the data [9].

In this paper, we propose a block chain-based provenance system for a data-sharing ecosystem. Our solution uses the block chain network and intelligent contracts to eternally store and validate metadata aggregated as logs from events and may be applied to a wide range of use cases. The suggested approach ensures user verifiability when obtaining data from CSPs. Our system's design enables authorised system participants to perform write operations on data while also giving the data owner with access and control over the outsourced data. The paper's contributions are summarised below.

Based on an on-chain and off-chain process classification, we propose and build a block chain architecture for attaining provenance in a data-sharing ecosystem.

We emphasize a data owner's ability to retain control over outsourced data. This is accomplished by ensuring that all data modifications are confirmed with permission from the data owner based on access policies that specify actions that are applied to the data.

We provide a block chain data view that underlines the importance of a tamper-proof log in enabling traceability through the aggregate of data transactions that are part of event logs.

We give a performance evaluation and analysis of the system on an ethereum block chain proof of concept, confirming the feasibility of implementing the proposed solution.

2. LITERATURE SURVEY

“Big data analytics,” in Springer Briefs in Computer Science.
AUTHORS: B. N. Silva, M. Diyan, and K. Han,Berlin, Germany: Springer.
Big data is a new force in global economic and societal change. The world's data collecting is approaching a tipping point for big technological advances that could usher in new approaches to decision making, city management, finance, and education. While data challenges such as volume, variety, velocity, and veracity are increasing, the real impact is dependent on our ability to identify the 'value' in the data using Big Data Analytics tools. Big Data Analytics presents a significant challenge in the design of highly scalable algorithms and systems to integrate data and find substantial hidden values from diverse, complicated, and massive datasets. Potential breakthroughs in Big Data Analytics include innovative algorithms, techniques, systems, and applications that reveal meaningful information. extracting hidden insights from Big Data in an efficient and effective manner.

Security issues in cloud computing.

AUTHORS: M. Vijaya kumar , V. Sunitha , K. Uma, and A. Kannan, J. Adv. Res. Dyn.
There is no doubt that cloud computing has numerous benefits, but it also has certain security concerns. The following are some security issues in cloud computing:Data Loss

- Interference of Hackers and Insecure API’s
- User Account Hijacking
- Changing Service Provider
- Lack of Skill
- Denial of Service (DoS) attack

3. PROPOSED SYSTEM

We propose a blockchain-based provenance system for a data-sharing ecosystem in this paper. Our solution uses the blockchain network and smart contracts to eternally store and check metadata aggregated as logs from events and can be applied to a wide range of use cases. The suggested approach ensures user verifiability when acquiring data from CSPs. Our system's framework allows authorized system participants to perform write operations on data while also giving the data owner with access and control over the outsourced data. This article's contributions are summarised below.

- Based on on-chain and off-chain process categorization, the system proposes and implements a blockchain architecture for attaining provenance in a data-sharing environment.
- The system emphasises a data owner's capacity to retain control over outsourced data. This is accomplished by ensuring that all data modifications are confirmed with consent from the data owner based on access policies that specify actions that are applied to the data.
- The solution provides a blockchain data view that highlights a tamper-proof log in establishing traceability through the aggregation of data transactions that form part of event logs.
- The system gives a performance evaluation and analysis of the system on an ethereum blockchain proof of concept, confirming the feasibility of Implementing the proposed solution.

BLOCK DIAGRAM

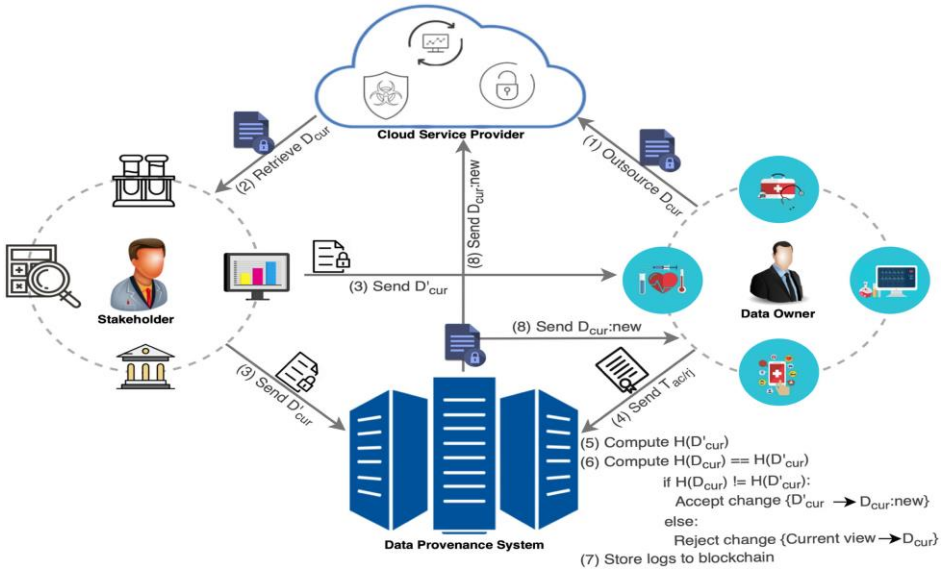

Fig.1. Provenance Procedure: Data State Management.

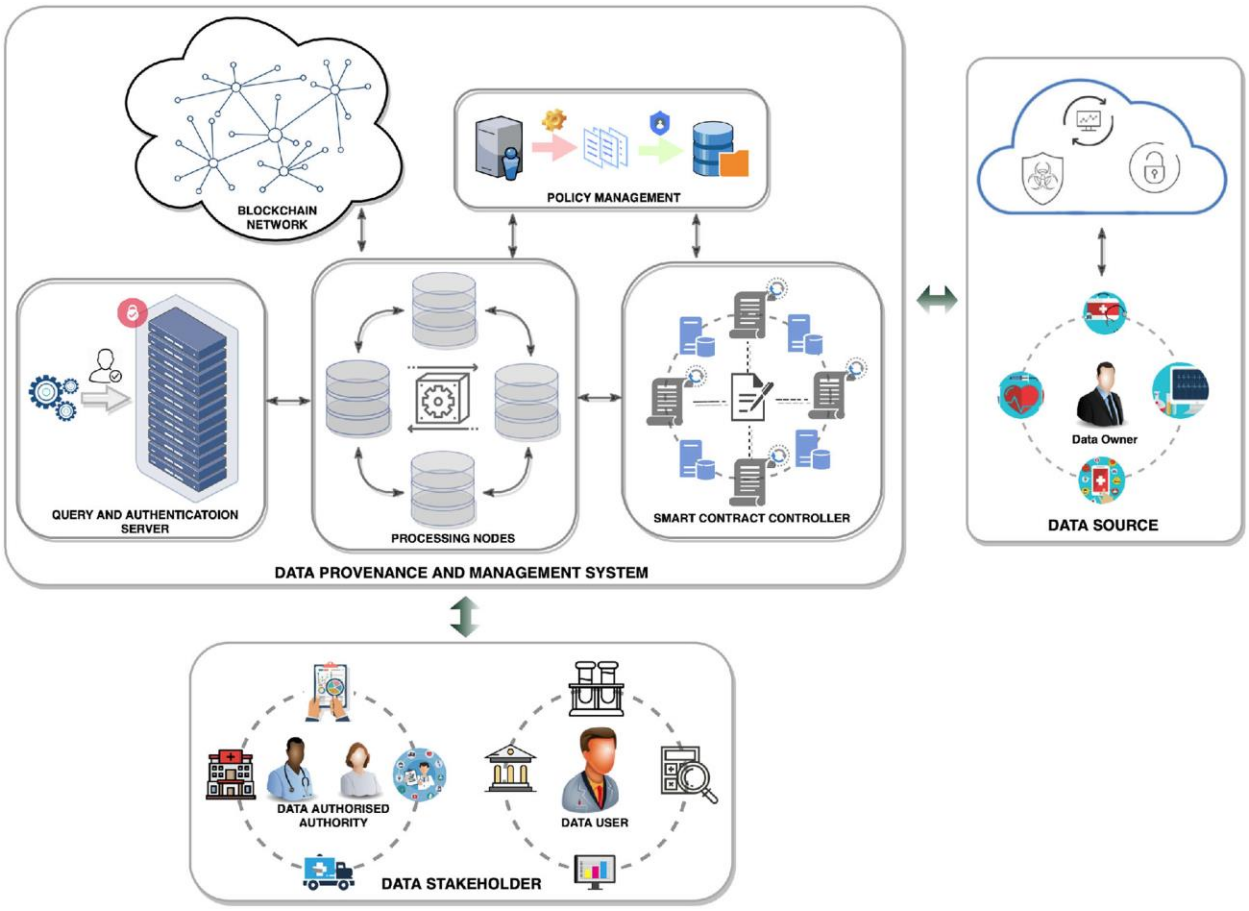

Fig.2. Subsystems of the Provenance Architecture.

4. CONCLUSION

Block chain technology, in conjunction with smart contracts, is employed in this work to provide efficient access control to outsourced data in provenance systems. An owner can control and monitor an outsourced encrypted health record using the technology offered. The designed system paradigm assures that user verifiability is efficiently realised and that data is immutably saved and validated. The implementation of smart contracts allows for penalties to be levied to system defaulters by constant monitoring of activities performed on data by system members, together with enforced revocation. Finally, our solution assures data confidentiality, integrity, and authorization, thereby making the system secure. Experiment results suggest the efficiency and scalability of our proposed method based on its performance solution.

5. REFERENCES

[1] B. N. Silva, M. Diyan, and K. Han, "Big data analytics," in Springer Briefs in Computer Science. Berlin, Germany: Springer, 2019.
[2] A. Lele, "Big data analytics," in Smart Innovations, Systems, and Technologies.Berlin, Germany: Springer, p. 3–3, 2019.
[3] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proc. Workshop Hot Top. Cloud Comput., HotCloud'09,2020.
[4] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," J. Netw. Comput. Appl. vol. 79, pp. 88–115, 2017.
[5] M. Vijayakumar, V. Sunitha, K. Uma, and A. Kannan, "Security issues in cloud computing," J. Adv. Res. Dyn. Control Syst., vol. 4, no. 1, pp. 1–13,2017.
[6] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of IoT and big data for e-health," Futur. Gener. Comput. Syst., vol. 86, pp. 1437–1455, 2018.
[7] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACMConf. Comput. Commun. Secur., 2007, pp. 89–98.
[8] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," Inf. Syst., vol. 48, pp. 132–150,2015.
[9] D. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. L. Njilla, "Data provenance in the cloud: A blockchain-based approach," IEEE Consum. Electron. Mag., vol. 8, no. 4, pp. 38–44, Jul. 2019.
[10] R. K. Lomotey, J. C. Pry, and C. Chai, "Traceability and visual analytics for the Internet-of-Things (IoT) architecture," World Wide Web, vol. 21,pp. 7–32, 2018.

[11] E. Nwafor, A. Campbell, D. Hill, and G. Bloom, "Towards a provenance collection framework for internet of things devices," in Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov., 2017, pp. 1–6

[12] M. H. Chia, S. L. Keoh, and Z. Tang, "Secure data provenance in home energy monitoring networks," in Proc. 3rd Annu. Ind. Control Syst. Secur. Workshop, 2017, pp. 7–14.

[13] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput., May 2017, pp. 468–477.

[14] A. Ramachandran and D. Kantarcioglu, "Using blockchain and smart contracts for secure data provenance management," 2017, arXiv:1709.10000.

[15] M. Sigwart, M. Borkowski, M. Peise, S. Schulte, and S. Tai, "A secure and extensible blockchain-based data provenance framework for the Internet of Things," Pers. Ubiquitous Comput., 2020, pp. 1–15.

[16] H. Olufowobi et al., "Data provenance model for Internet of Things (IoT) systems," in Proc. Serv.-Oriented Comput.-ICSOC Workshops: Revised