International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET22929

Cloud Privacy Protection using BlockChain A Comparative Analysis

Prof. Jenita J, Archit Gaur, Joshua William Paul, Mohammad Ahmad Usmani
Department of Computer Science, HKBK college of Engineering, Bangalore, Karnataka, India

Article Info
Volume 9, Issue 2
Page Number : 75-78

Publication Issue :
March-April-2022

Article History
Accepted : 10 March 2022
Published: 21 March 2022

ABSTRACT

This study aims to analyze the determinants of the regional unemployment rates in West Java Province in the period 2010-2019. Due to the diversity of characteristics between regions, this study uses Geographically Weighted Panel Regression (GWPR) analysis. The results showed that all the independent variables used had a significant effect on the regional unemployment rate in West Java. It is recommended that the government encourage efforts to reduce unemployment in their regions by investing more in real sector development, attracting investors in the manufacturing and service sectors, and improving education and skills.

Keywords: Regional Unemployment, Labor Supply Demand, GWR Panel

I. INTRODUCTION

Cloud computing, as a new computing model, can provide users with services of omnipresence, and reduce the cost of user storage and computing, and improve the convenience of use, thus a lot of and a lot of businesses and people like better to store information in cloud. However, with the event of cloud computing scale and intensification, analysis on fog computing and edge computing has conjointly step by step up, cloud security problems became a very important issue limiting cloud computing development. Access control is also the current research hotspot, the purpose is to use access control to prevent resources stored in cloud from being accessed or stolen by illegal users. The main three service systems of cloud computing, infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), all need to protect relevant resources through access control, so access control plays an important role in cloud.

The paper is mainly focusing on the following objectives:

- An external attacker attacks the trusted centre, tamper with the authorized database stored on the central server, and illegally access or steal the resources stored by users in cloud.
- The system administrator of cloud manages the authorization database and has the right to access and manage the resources, so a malicious system administrator of cloud may take advantage of the privilege to illegally access the resources or

tampering the authorization database to illegally access.

II. LITERATURE SURVEY

In this section, we discuss the current research status of traditional cloud computing access control and then discuss the research status of using blockchain combined with cloud, especially to solve cloud security issues, including cloud access control issues. Finally, makes a brief summary of the current status of cloud access control research.

Furthermore, analysis on the utilization of blockchain to tackle cloud security problems has grown up in quality, however a lot of of it's targeted on specific security problems. First, [1]AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud presented a solution for cloud security without the help of a third party company, which makes it harder for an unauthorized person to access the resource and also takes out the possibility of a system administrator to tamper eith the resource.[2]Block-secure: Blockchain-based scheme for secure P2P cloud storage proposed a distributed cloud storage security architecture, in which files were divided into encrypted data blocks before being uploaded, and then a genetic algorithm was designed to solve the problem of file copy placement. According to the European SUNFISH data integrity problem, [3]Blockchain based database to ensure data integrity in cloud computing settings presented a utilised in cloud database architecture based on the blockchain, to ensure data integrity. [4]Blockchain based system for secure data storage with private key-word search suggested BlockDS, a secure distributed data storage and keyword search service, to replace major storage providers' conventional dependence on a trusted third party in cloud storage. Second, in terms of data sources, [5] Consensus protocols for blockchain-based data provenance suggested a blockchain-based cloud data source framework that uses the blockchain consensus mechanism to tackle the problem of data source dependability in cloud platforms.[6] Provchain:A blockchain based data provenance architecture in cloud environment with enhances privacy and availability proposed a distributed trusty cloud information supply system to stop meddling by aggregation and corroborative cloud information supply's and embedding source information into blockchain transactions. [7]CloudPoS:A proof-of-stake consensus design for blockchain integrated cloud designed a proof of- stake (PoS)based coherence protocol CloudPoS to solve the problem of a consistency model based on an encrypted stream in the traditional data source system and improve security. Finally, in terms of deposit certificate, [8]Blockchain-based verification scheme for deletion operation in proposed a cloud information deletion protocol to unravel the behaviour of change of state users by change of state with information deletion results once cloud server isn't trusty. [9]Blockchain Model of Cloud Forensics proposed a cloud computing electronic forensics model to boost proof preservation supported Merkle tree and formula formula, aiming at determination the centralized electronic forensics in cloud computing atmosphere. [10]A blockchain-based process provenance for cloud forensics combined blockchain and cryptographic signature techniques to propose a cloud forensics scheme, but the scheme relied too heavily on trusted centre nodes CA and provenance auditor (PA).

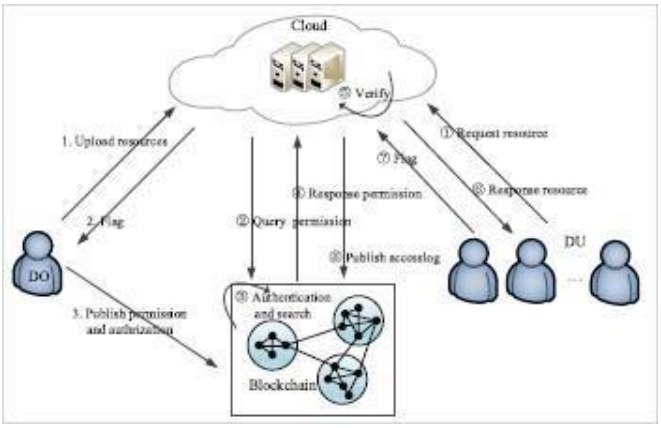
However, the current research using blockchain to solve cloud access control is still in its infancy.[11]MeDShare: Trust-less medical data sharing among cloud service providers via blockchain proposed a system to resolve the medical information sharing drawback of medical huge information servers within the untrusted surroundings, the two-layer blockchain designed by the system was supported a totally consistent mechanism. [12]A

blockchain-based access control system for cloud storage proposed a multi-user system model to unravel the matter of access management of knowledge within the untrusted cloud and style a group of cryptanalytic protocols to make sure key privacy. [13]Towards blockchain- based scalable and trustworthy file sharing proposed an ABE access control in cloud, but ABE was not extensible when the user revoked.

In conclusion, though the educational circle has created plenty of analysis achievements within the on top of, there square measure still several shortcomings within the connected analysis on exploitation blockchain to resolve cloud access control, particularly there square measure few analysis achievements in cloud access control with privacy protection.

III. PROPOSED SYSTEM

We propose Privacy Chain - a block chain-based access control framework with privacy protection in cloud. This Section contains the system model, format, access control, ordination, and revocation. The system model is shown in figure that is consisted of 4 entities: Cloud. It provides authentication and knowledge storage for users.Cloud determines access rights of DU or interact Blockchain. It is open, clear, tamper-proof, and irreversible, and therefore the same because the distributed info, we tend to use it as associate degree authorization policy info for access control. DO. DO upload the resources to Cloud and publishes the resource's access rights to Blockchain. DU. DU will access the resources if he has permission from Cloud. we tend to assume Cloud is semi-trusted, that is, the software package, hardware, uneven key and business processes of the Cloud square measure trusty, however the Cloud militia isn't. Blockchain is assumed to be trusting. First, DO upload the resources to the Cloud so publishes authorization by registration transactions in blockchain. DU sends a resource request to Cloud, and Cloud queries blockchain, and chooses whether or not the request has permission, and reply to the request.



IV. ACKNOWLEDGMENT

A special and an earnest word of thanks to the project guide Prof.Jenita J for their constant assistance, support, patience, endurance and constructive suggestions for the advancement of the project.

V. CONCLUSION

Aim of this paper, in personal user's records sharing scheme with data integrity verifiable based on block chain. Aiming at the problems of privacy disclosure, the new scheme encryption and attribute-based encryption techniques to achieve privacy protection, and provide fine-grained access control.

VI. REFERENCES

[1]. Yang, Caixia & Liang, Tan & Shi, Na & Xu, Bolei & Cao, Yang & Yu, Keping. (2020). AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2985762.

[2]. J. Li, J. Wu, and L. Chen, "Block-secure: Blockchain based scheme for secure P2P cloud

storage," Inf. Sci., vol. 465, pp. 219_231, Oct. 2018, doi: 10.1016/j.ins.2018.06.071.

[3]. G. Edoardo, A. Leonardo, B. Roberto, L. Federico, M. Andrea, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," in Proc. Italian Conf. Cybersecur., Venice, Italy, Jan. 2017.

[4]. H. G. Do andW. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in Proc. IEEE World Congr. Services (SER¬VICES), Jun. 2017, pp. 90_93, doi: 10.1109/SERVICES.2017.23.

[5]. D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," in Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON), Oct. 2017, pp. 469_474, doi: 10.1109/ UEMCON.2017.8249088.

[6]. 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. (CCGRID). Piscataway, NJ, USA: IEEE Press, May 2017, pp. 468_477.

[7]. D. Tosh, S. Shetty, P. Foytik, C. Kamhoua, and L. Njilla, "CloudPoS: A proof-of-stake consensus design for blockchain integrated cloud," in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 302_309, doi: 10.1109/CLOUD.2018.00045.

[8]. Y. Liu, Y. Zhou, R. Lan, and C. Tang, "Blockchain-based veri_cation scheme for deletion operation in cloud," in J. Comput. Res. Develop., vol. 66, no. 10, pp. 2199_2207, 2018.

[9]. F. Huang, L. Xu, and X. Yang, "Blockchain Model of Cloud Forensics," J. Beijing Univ. Posts Telecommun., vol. 40, no. 6, pp. 120_124, 2017.

[10]. Y. Zhang, S. Wu, B. Jin, and J. Du, "A blockchain-based process provenance for cloud forensics," in Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC), Dec. 2017, pp. 2470_2473.

[11]. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14757_14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[12]. I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," in Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus), Jan. 2018, pp. 1575_1578, doi: 10.1109/EIConRus.2018.8317400.

[13]. S. Cui, M. R. Asghar, and G. Russello, "Towards blockchain-based scalableand trustworthy _le sharing," in Proc. 27th Int. Conf. Comput. Com¬mun. Netw. (ICCCN), Jul. 2018, pp. 1_2.

Cite this article as :

Prof. Jenita J, Archit Gaur, Joshua William Paul, Mohammad Ahmad Usmani, "Cloud Privacy Protection using BlockChain - A Comparative Analysis", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 2, pp. 75-78, March-April 2022. Available at doi : https://doi.org/10.32628/IJSRSET22929
Journal URL : https://ijsrset.com/IJSRSET22929