reshma kanse anurag group

by RRP_VMR_AMP_HM_RRK_XYZ_PQR_ bharti

Submission date: 01-Apr-2023 06:49AM (UTC-0700)
Submission ID: 2050982569
File name: Inspents_PaperReview_V2.0.docx (167.91K)
Word count: 2806
Character count: 16409

A Reliable Multi-Factor Authentication Method Using Blockchain Foundation for Safe Online Banking in the Public Cloud

Rohit Shendge[1], Indrajit Datar[2], Adwait Shinde[3], Anurag Gulavane[4], Prof. Reshma Kanse[5]

[1,2,3,4] BTech Student and [5]Asst. Prof of Department of Computer Science and Business Systems,
Bharti Vidyapeeth Deemed University, Department of Engineering and Technology
Navi Mumbai

Abstract: Blockchain has established itself as a significant financial software system. They are based on a safe distributed ledger data structure. They are becoming increasingly popular in the world today. People appear to be discovering new ways to use the blockchain's power for intuitive applications that provide solutions to real-world problems. A crucial part of these systems, mining, adds data of prior transactions to the distributed ledger. Every 10 minutes, a block (the structure containing transactions) is mined Miners compete by attempting to use a cryptographic hash technique to solve a challenging mathematical problem. When a block is solved, the transactions contained within it are considered confirmed, and the Bitcoin involved in the transactions is available for spending. Users can reach a strong and secure consensus for every transaction thanks to the Blockchain. Cryptocurrencies are a major application of blockchain. They require robust, secure mining algorithms, and because they are peer-to-peer systems by design, they rely on miners to validate transactions because they lack a central authority to mediate transactions. Companies seeking to save costs and improve efficiency are drawn to the promise of new blockchain and distributed ledger technology (DLT). If completely implemented, it will make it possible for banks to process payments faster and more precisely while simultaneously reducing transaction processing costs and the requirement for exceptions.. Therefore, we find the need to upgrade our banking system to mediate transactions and to this new technology. In this proposed system we design and develop custom blockchain technology with SHA, Mining and Chain Consensus Algorithm for provide security and privacy of secure baking transactions and also addition of designing a secure authentication technique with the help of keylogging secure authentication methodology. Blockchain is a framework which is provide peer-to-peer (P2P) verification and validation protocols and using this protocols provide security and privacy of banking transaction systems.

Keywords: - Blockchain, distributed ledger technology (DLT), mining, transactions, consensus, cryptocurrencies, secure banking transactions, authentication, keylogging etc.

I. INTRODUCTION

A blockchain system can be compared to a

straightforward incorruptible encrypted database that holds crucial and private user data. The system is accessible to everyone using the programme, and it is maintained by a network of computers. Blockchain functions as a pseudo-anonymous system, but although being tamper-proof in terms of data-integrity, it has a privacy problem because all transactions are visible to the public. To manage sensitive user records across a few MNC premises and devices for heterogeneous users, access control had to be properly implemented. Blockchain isn't meant to be a massively scalable storage solution. When viewed in the context of a framework for safe banking, the blockchain's weak issue would be significantly supplemented by a decentralized storage solution. A decentralised system like the blockchain network is more dependable than centralised ones since there is no single point of attack or failure. Yet, because every bitcoin transaction is visible to everyone and public, there is presently analytics software that can identify community members only based on transaction data.

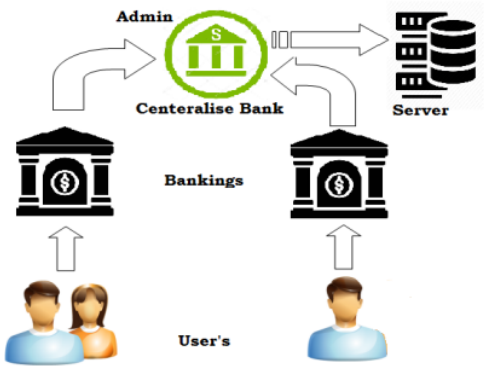

Fig.1: System Overview

The system overview in this study is shown in Figure 1, and the most crucial module is the implementation of the blockchain, which includes two different types of records: blocks and transactions. A higher level of security is created for banking applications through the use of cryptographic algorithms, specifically SHA for the creation of hash functions, mining for confirming the validity of hashes, smart contracts for implementing system policies, and consensus for validating blockchain transactions across all peer-to-peer nodes. Another significant challenge concerns data storage and accessibility, which can be addressed by merging keyword and content-based encryption schemes with the Secret Shamir hashing mechanism.

II. RELATED WORK

The writers are Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen. Blockchain and smart contracts are used in "A Digital Certificate." [1] A digital certificate system based on blockchain technology will be introduced to address the problem of certificate counterfeiting. A digital certificate with anti-counterfeit and verifiability may be created using the immutable nature of blockchain. In this system, creating a digital certificate is done in the manner listed below. Afterwards, make a digital copy of the paper certificate along with any other related information, and insert it into the database. In the interim, determine the digital copy's hash value. The block of the chain system should then contain the hash value. A relevant QR-code and query string code will be generated

by the system and can be appended to the printed certificate. The method not only drastically reduces the dangers associated with certificate loss, but also increases the authenticity of various paper-based certificates thanks to the immutability of the blockchain. Blockchain Security Uses and Challenges by Tevisophea Heng, Wenlin Han, Aryan Familrouhani, and Devin Cao [2] Blockchain technology is used both now and in the future, but it is a concept that is frequently misunderstood. Blockchain is used by several apps to improve security and privacy.

Nonetheless, there are unavoidable drawbacks and rising worries. In order to make future research more effective, we look at common security applications in blockchain, explain their main issues, and discuss other blockchain concerns in this paper. Authors Luca Spalazzi, Marco Baldi and several other authors developed the "Validation Utilizing Public Ledgers and Blockchain" certificate.

[3] Without public key infrastructures, online services that rely on certificate-based authentication—including e-commerce, e-government, online banking, email, social networking, cloud services, and many others—cannot continue to function (PKIs). The dependability and security of certificate revocation lists, which must be accessible and genuine each time a certificate is used, are one of the major failure areas of current PKIs.

Since the certification authority (CA) that issued a set of certificates often also stores the CRL for that set of certificates, a single POF is established in the system. A Simple Simulation Tool for Network Design, Stability, and Planning is called "BlockSIM." [4] In this article, we present BlockSIM, a thorough and open-source simulation tool made specifically for blockchain systems. By running simulations and fine-tuning system settings, BlockSIM enables blockchain builders to evaluate the performance of their envisioned private blockchain networks. By comparing the results of our simulations with actual blockchain networks, this paper demonstrates the effective utilization of BlockSIM for designing and constructing scalable and resilient blockchain systems. Furthermore, we illustrate how architects may leverage BlockSIM to develop tangible blockchain networks through a practical use case. A Scalable and Lightweight Blockchain Protocol is "Proof-of-Property." [5] The method presented in this article draws on Ethereum's principle that the state of the system should always be retained in the most recent block, but it goes one step further by incorporating the pertinent data from the most recent system information into new transactions. This allows other participants to validate incoming transactions without having to download the entire blockchain.This concept has the potential to facilitate the utilization of scalable blockchain technology in scenarios that may not require an infinite and comprehensive record of transactions.

In the paper titled "Blockchain and Smart Contract for Digital Document Verification" by

S. Sunitha Kumara and D. Saveetha, it is suggested that the integration of blockchain technology and smart contracts can enable the secure verification of digital documents. The proposed system entails uploading not only the degree certificate but also the individual's entire personality and behavioral patterns using a personal identification code onto the blockchain platform. As a result of its unchanging nature, it is retained in the block chainThe student must upload a diploma or other form of identification to the electronic certificate system before requesting an e-certificate. The system will review the documentation provided by the college, organisation, or institution in response to a request for an e-certificate, obtain the assurance, and then store the serial number and e-certificate on the block chain. A QR code will be generated by the system and sent to the user. Just the certificate serial number and QR code provided by the e-certification provider should be sent when filing an application for a corporation. Dr. Murat Kantarcioglu and Arvind Ramachandran Utilizing blockchain technology and smart contracts to control data provenance in a secure way. [7]In this study, we leverage the blockchain technology as a foundation to simplify the acquisition, validation, and administration of dependable data provenance. Our suggested method records tamper-proof data trails using smart contracts and the open provenance model (OPM). Given that a sizable portion of participants are reliable, our research shows that the suggested architecture can efficiently and securely capture and authenticate provenance data while also avoiding any fraudulent adjustments to the recorded data.

Ahmad B Ayyed Using the block chain technique, a secure voting system storage service is provided. [8] The utilization of a blockchain-based system is anticipated to result in a secure, reliable, and confidential platform that could potentially boost voter turnout and enhance public trust in governmental institutions.

The study, "An Empirical Study of Decentralized Blockchain-based Applications," [9] In this study, 734 dapps from three well-known open dapp marketplaces—namely, Ethereum, State of the Dapp, and DAppRadar—are thoroughly empirically investigated. We examine the patterns in the organisation of smart contracts in dapps and examine the adoption of dapps. We draw some conclusions from the research in order to help dapp consumers and developers better understand and use dapps.

Critical Path Analysis and Identification for Smart Contracts, or "sCompile." [10] This study suggests an alternate mechanism for automatically locating key programme routes in a smart contract. (with many function calls, including inter-contract function calls), classifying the paths according on their importance, removing the paths if they are impractical, or otherwise showing the paths with clear warnings for user examination. Critical pathways are those that entail

financial transactions, and we give priority to those that might break crucial assumptions. Symbolic execution strategies are only used on the top-ranked critical paths for scalability. Our strategy has been put into practise in the sCompile tool, which has been used to create 36,099 smart contracts. The findings of the trial demonstrate that compiling is effective, taking, on average, 5 seconds for one smart contract.

III. PROPOSED METHODOLOY

Nowadays, security is a major concern. 99% of data is processed online and saved on a reliable server. But, when a user puts their data on an approved server, data must be transmitted and received over a secure communication channel, and security difficulties arise. Lately, the majority of data has been handled in the following applications or fields: healthcare, e-commerce, internet baking, education, and business applications, among others. All of these services are used through the internet, and there are several opportunities for diverse assaults in online services.To address these issues we implementation of a trusted framework for online banking in the public cloud using multi-factor authentication using The blockchain framework provides a secure environment that shields against diverse forms of attacks, as illustrated in the accompanying fig.2.

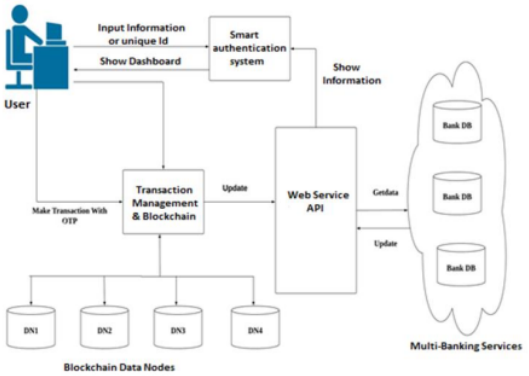

Fig.2: Proposed Architecture Diagram

As seen in Fig. 2, all of these solutions rely on creating a unique (custom) blockchain and using it to store all transaction records insecurely. The security of data records can only be guaranteed through the use of a system based on software technology. In order to enhance transaction transparency for end-users, it is advisable to implement a dynamic smart contract that incorporates a consensus mechanism. [7].

IV. CONCLUSION

This study proposes a safe and effective method of storing data on the cloud (localhost). Data security in a decentralized structure is provided via blockchain-based cloud storage with data encryption. The proposed architecture for security model is appropriate for early measures employed in banking transactions that integrated blockchain technology [10]. The methods used to build the system model are effective, quick, and offer great security for data stored in the cloud. Due to the system's design, it is more resilient and resistant to numerous security attacks made by unauthorised users who try to steal and disseminate user data files' contents for their own gain. The overall banking

process is now considerably more convenient as a result of the huge increase in banking transaction security. [9].

ACKNOWLEDGMENT

I express my appreciation to the creators of the research materials and their publishers for making them accessible. Moreover, I am thankful for the guidance and insightful recommendations from the supervisor and reviewer, and acknowledge the necessary technological infrastructure and support provided by the educational institution.

REFERENCES

[1] Sabout Nagaraju and LathaParthiban, "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," Open Access Journal of Cloud Computing: Advances, Systems and Applications (2015)

[2] Dorri, S. S. Kanhere and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," arXiv: 1608.05187 [cs], 2019.

[3] Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EICon- Rus), 2018 IEEE Conference of Russian IEEE, 2018.

[4] Yang, Huihui, and Bian Yang. "A Blockchain-based Approach to the Secure Sharing of Healthcare Data." Proceedings of the Norwegian Information Security Conference. 2020.

[5] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006.

[6] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based crypto-system and blockchain." Journal of medical systems 42.8 (2018): 152.

[7] Michalevsky Y, Joye M. "Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy".

[8] Wu, Axin, et al. "Hidden policy attribute- based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.

[9] Khan S, Khan R. "Multiple authorities' attribute-based verification mechanism for Blockchain micro-grid transactions". Energies. 2018 May; 11(5):1154.

[10] Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.

[11] Monika D. Rokade, Dr. Yogesh Kumar Sharma, "Deep and Machine Learning Approach's for Anomaly based Intrusion Detection of Imbalanced Network Traffic." IOSR journal of Engineering (IOSR JEN), _ISSN (e): 2250-3021, ISSN(p): 2278-8719

[12] Monika D. Rokade, Dr. Yogesh Kumar Sharma, "MLIDS: A Machine Learning Approach for Intrusion Detection for real time Network Dataset." 2021 International Conference on

Engineering Smart Computing and Informatics (ESCI), IEEE.

[13] Monika D. Rokade, Dr. Yogesh Kumar Sharma. (2020) "Identification of Malicious Activity for Network Packet using Deep Learning." International Journal of Advance Science and Technology, 29(9s), 2324-2331.

[14] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, 2008.

[15] D. J. Hwang and K. Lee, "Analysis of security threats and solutions in payment systems," Information Security Journal: A Global Perspective, vol. 25, no. 2, pp. 50–58, 2016.

[16] T. Dierks and C. Allen, "The TLS Protocol Version 1.3," Internet Engineering Task Force, 2018.

[17] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, 2008.

[18] P. Koshy, D. Koshy, and P. McDaniel, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," in Financial Cryptography and Data Security, 2014, pp. 469–485.

[19] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.

[20] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[21] A. Shamir, "How to Share a Secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

[22] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[23] B. A. Forouzan, Cryptography and Network Security: Principles and Practice, McGraw-Hill Education, 2015.

[24] B. C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," IEEE Communications Magazine, vol. 32, no. 9, pp. 33–38, 1994.

[25] J. Salowey et al., "The Secure Sockets Layer (SSL) Protocol Version 3.0," Internet Engineering Task Force, 1996.

[26] M. C. Rosu, M. Danubianu, and M. V. Rosu, "Blockchain Solutions for the Digital Banking Revolution," Procedia Economics and Finance, vol. 23, pp. 200–204, 2015.

[27] P. Koshy, D. Koshy, and P. McDaniel, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," in Financial Cryptography and Data Security, 2014, pp. 469–485.

[28] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum.org, 2014.

[29] D. J. Hwang and K. Lee, "Analysis of security threats and solutions in payment systems," Information Security Journal: A Global Perspective, vol. 25, no. 2, pp. 50–58, 2016.

[30] C. N. Chuang, Y. C. Liao, and Y. C. Chen, "A Privacy-Preserving Cloud-Based Electronic Health Record System Based on Blockchain Technology," Journal of Medical Systems, vol. 42, no. 8, p. 139, 2018.

[31] J. Huang et al., "A Trusted e-Contract Signing Framework Based on Blockchain," IEEE

reshma kanse anurag group

ORIGINALITY REPORT

8%	8%	3%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ijcseonline.isroset.org Internet Source	6%
2	ijsrst.com Internet Source	1%
3	ijcnis.org Internet Source	1%
4	usenix.org Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		