IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 3, February 2024

Document Storage and Verification System Using Blockchain Technology

Prathamesh Sinkar, Gaurav Shende, Sudhir Patil, Mohit Pawar, Prof. Supriya Jagtap
Department of Computer Engineering
Smt. Kashibai Navale College of Engineering, Pune, India

Abstract*:* *A banking or identity provider can set up a customer identification data verification process between reliant parties with the use of the electronic know your customer (e-KYC) system. Due to its high degree of accessibility and availability and its efficient resource usage, the majority of banks choose to implement their e-KYC system on the cloud. All of the KYC procedures used by banks rely on encryption, which is a cumbersome process that may cause consumer data to be disclosed to unaffiliated financial institutions. Blockchain technology can be used to increase the efficiency of this system because it can automate a lot of human labor and is impervious to attacks of all kinds. The distributed ledger and immutable blockchain block make the perfect addition to the KYC process. The use of smart contacts can automate the identification of fraud. Any kind of KYC can be used to store information related to KYC identity. Consequently, financial institutions can establish a shared private blockchain on their premises for the purpose of document validation. This allows the user to maintain control over their private documents while also simplifying the process for banks to obtain the records needed for compliance.*

Keywords: e-KYC, authentication, AES, key management, access control, blockchain

I. INTRODUCTION

Overview

Bank transactions are secured by a Blockchain-based security management system, which also streamlines and secures the KYC procedure. Blockchain technology is a cutting-edge innovation that maintains a database amongst numerous participants without the need for a central authority or third party by utilizing mathematical, cryptographic, and economic concepts. A transaction's legality can be verified by parties involved in the transaction using this safe, tamper-evident distributed database.

The Know Your Customer (KYC) procedures that banks use on their customers are unnecessary, expensive, and inefficient. In light of this, a system to automate inexperienced tasks and permit the exchange of KYC data is suggested. With its distributed database concept and time-stamped ledgers, blockchain technology can greatly help banks enhance their KYC process.

Banks deploy costly, pointless, and counterproductive Know Your Customer (KYC) processes on their customers. Consequently, a system to facilitate KYC data sharing and automate repetitive activities is recommended. Blockchain technology, with its distributed database idea and time-stamped ledgers, can greatly assist banks in streamlining their KYC procedure.

KYC processes are usually time-consuming, repetitive, incompatible, and redundant, which raises overhead and administrative costs. An immutable ledger, ease of integration, and much lower infrastructure and operating costs make a blockchain-based solution a clear winner over the existing KYC processes.

Because financial information has long drawn the attention of hackers, each bank must arrange the security of the data it possesses, including the condition of its clients' accounts, their transaction history, etc. Blockchain is a distributed shared ledger that allows the participants to a transaction to view each other's transaction records on an unbreakable, everlasting chain. With this solution, the vulnerabilities in transactional cyberattacks can be addressed.

Strong authentication and conventional encryption are typically used by existing e-KYC platforms to satisfy their security and privacy requirements.

DOI: 10.48175/IJARSCT-15527

II. RELATED WORK

R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens offer the idea of two electric car configurations that significantly reduce the impact of the charging process on the power grid during business hours. All users involved in the trading process will benefit financially from this trading strategy. Predicting the daily schedule and travels of a synthetic population for Flanders uses an activity-based technique (Belgium) [1].

Y. Xiao, D. Niyato, P. Wang, and Z. Han Analyze the potential flow and functional elements that communication networks can use to enable DET. Several design concerns regarding how to apply DET in practise are highlighted. A perfect method is developed for delay-tolerant remote control communication systems, in which every remote powered device can plan its information-transmission and energy-exchanging operations according to the availability of current and future energy sources [2].

J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain describes a project that aims to respond to requests by incentivizing PHEVs to change local power demands in their own self-interests. Yet, given the real difficulties with exchange security and security insurance, they look at a prospective consortia block-chain innovation to increase exchange security without relying on a trusted outsider. To depict the specific activities of limited P2P power trading, a framework for restricted P2P electricity trading with a consortium block-chain (PETCON) technique is provided[3].

N. Z. Aitzhan and D. Svetinovic provides a piece of work that deals with the problem of transaction security in decentralised smart grid energy trading without relying on reliable third parties. We have created a proof-of-concept for a decentralised energy trading system employing blockchain technology, multiple signatures, and anonymous encrypted

III. PROPOSED SYSTEM

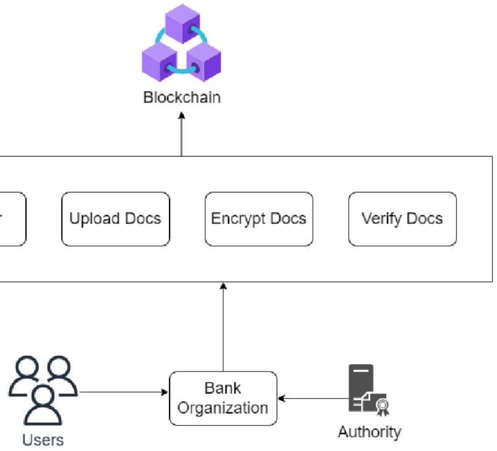

Fig. System Architecture

- The suggested solution employs a block chain-based KYC method, wherein every client uploads data files and encrypts them using a matching key.
- We suggest an efficient search technique that combines security preservation with pertinent searches.
- Within this framework, the server may effectively merge many encrypted records and conduct the investigation safely without disclosing any sensitive user information, information documents, or inquiries.

Algorithm Details

AES Algorithm for Encryption.

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.
Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256 bit input (0, 1)

DOI: 10.48175/IJARSCT-15527

Secret key (128_bit) +plain text (128_bit).
Process:
10/12/14-rounds for-128_bit /192 bit/256 bit input
Xor state block (i/p)
Final round:10,12,14
Each round consists: sub byte, shift byte, mix columns, add round key.
Output:
cipher text(128 bit)

MD5(Message-Digest Algorithm)

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.
Steps:
A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.
The output of a message digest is considered as a digital signature of the input data.
MD5 is a message digest algorithm producing 128 bits of data.
It uses constants derived to trigonometric Sine function.
It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.
Most modern programming languages provides MD5 algorithm as built-in functions

IV. RESULT AND DISCUSSION

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and Jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcat server.

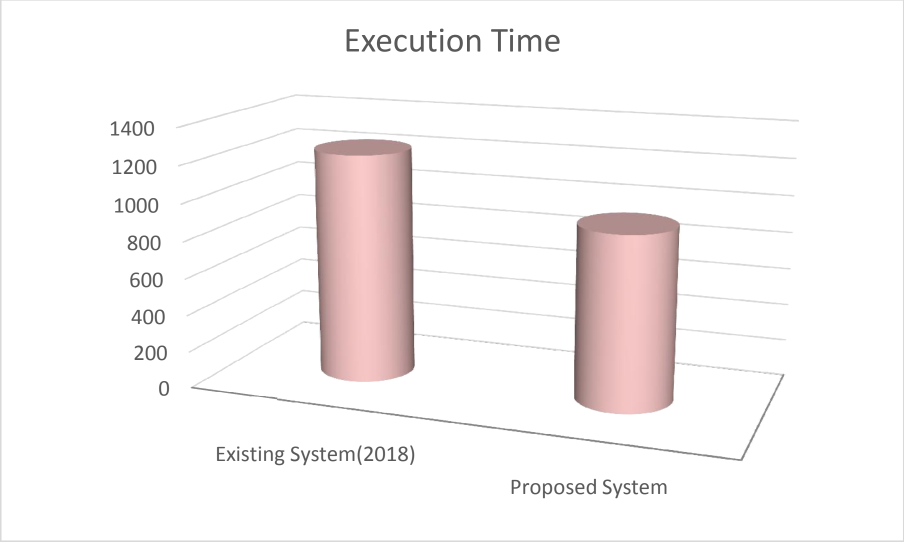

Figure 2: overall system execution graph

V. CONCLUSION

In many ways, the Blockchain of today is comparable to the Internet of the early 20th century. Every day, the impact of online commerce and information technology advancements on all facets of modern life grows. The goal of blockchain

DOI: 10.48175/IJARSCT-15527

technology is to upend the current wisdom of online user communication. Regardless of mining or tokens, the main advantages of Blockchain technology are complete operational synchronization, data integrity, and uniqueness of all processed data. Blockchain technology can enhance distributed databases in terms of data storage, synchronization, loss, and integrity corporate groups are supporting a variety of blockchain use cases that are being funded by corporate leaders, even if it's still early. Though we think the promise is clear, companies must first show use cases and technical/business viability before implementing blockchain technology. Both the advantages and disadvantages of this technique have been demonstrated.

REFERENCES

[1] SOMCHART FUGKEAW ” Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain” IEEE ACCESS 2022.

[2] R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, “Peer to peer energy trading with electric vehicles,” IEEE Intell. Transp. Syst. Mag., vol. 8, no., pp. 33–44, Fall 2016.

[3] Y. Xiao, D. Niyato, P. Wang, and Z. Han, “Dynamic energy trading for wireless powered communication networks,” IEEE Commun. Mag., vol. 54, no. 11, pp. 158–164, Nov. 2016.

[4] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, “Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains,” IEEE Trans. Ind. Informat., vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[5] N. Z. Aitzhan and D. Svetinovic, “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,” IEEE Trans. Depend. Sec. Comput.

[6] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now, “Nrgcoin: Virtual currency for trading of renewable energy in smart grids,” in Proc. IEEE 11the Int. Conf. Eur. Energy Market, 2014, pp. 1–6.

[7] S. Barber et al, “Bitter to better-how to make bitcoin a better currency,” in Proc. Int. Conf. Financial Cryptography Data Security, 2012, pp. 399–414.

[8] I. Alqassem et al., “Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis,” in Proc. IEEE Internet Things, IEEE Int. Conf. Green Comput. Commun. IEEE Cyber, Physical Social Comput. 2014, pp. 436–443.

[9] K. Croman et al., “On scaling decentralized blockchains,” in Proc. Int. Conf. Financial Cryptography Data Security, 2016, pp. 106–125.

[10] G. W. Peters and E. Panayi, “Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money,” in Banking Beyond Banks and Money. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.

[11] L. Luu et al., “A secure sharding protocol for open blockchains,” Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 17–30.

DOI: 10.48175/IJARSCT-15527