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: 7.301
Volume 3, Issue 10, May 2023

Designing a Secure and Private Electronic Know your Customer (E-KYC) System using Blockchain Technology

Yash Tambe, Salman Ahmad, Bhushan Nakhate, Aditya Chougale, Prof. Priyanka Raikar
Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Abstract: *The electronic Know Your Customer (e-KYC) system plays a crucial role in establishing customer identification and data verification processes among relevant parties. Cloud deployment is a popular choice for e-KYC systems due to its resource efficiency, accessibility, and availability. However, existing KYC methods heavily rely on encryption, which can be slow and potentially expose consumer information to unauthorized financial entities. To address these challenges, this paper proposes leveraging Blockchain technology to enhance the efficiency and security of the e-KYC system. By utilizing the inherent properties of Blockchain, such as immutability and distributed ledger, the KYC process can be strengthened. Additionally, the introduction of smart contracts enables automation of fraud detection. To achieve this, a shared private Blockchain can be implemented within the bank's infrastructure, ensuring that KYC identification details are securely stored and verified. This approach provides users with control over their sensitive documents while facilitating banks' access to compliance-related records.*

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

I. INTRODUCTION

1.1 Overview

A Blockchain-based security management system is implemented to enhance the security of bank transactions and simplify the Know Your Customer (KYC) process. Blockchain technology, utilizing mathematical, cryptographic, and economic principles, enables the creation of a distributed database that eliminates the need for a central authority or third party. It provides a secure and tamper-evident platform where transaction validity can be verified by involved parties.

The current KYC procedures employed by banks on their customers are unnecessary, inefficient, and costly. To address these issues, an automated system is proposed that facilitates the sharing of KYC data. By leveraging the distributed database concept and time-stamped ledgers of blockchain technology, banks can significantly enhance their KYC processes.

KYC procedures often involve repetitive tasks, lack compatibility, and lead to duplication, resulting in increased administrative costs and overhead. Compared to the current KYC procedures, a blockchain-based solution offers advantages such as an immutable ledger, easy integration, and substantially lower operational and infrastructure expenses.

Due to the sensitive nature of banking information, including customer account status and transaction history, each bank must prioritize the security of the data it holds. Blockchain serves as a distributed shared ledger, recording transactions in an immutable and permanent chain accessible only to transaction parties. This technology effectively addresses vulnerabilities to transactional cyber-attacks.

To meet security and privacy requirements, existing e-KYC platforms commonly rely on strong authentication and traditional encryption methods.

II. RELATED WORK

R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens propose two electric car configurations that minimize the impact of the charging process on the power grid during business hours. This trading strategy offers

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: 7.301
Volume 3, Issue 10, May 2023

financial benefits to all participants involved. The authors utilize an activity-based technique to predict the daily schedule and travels of a synthetic population in Flanders, Belgium [1].

Y. Xiao, D. Niyato, P. Wang, and Z. Han analyze communication network flow and functional elements to enable Delay-Tolerant Networks (DTNs). They highlight design concerns regarding the practical implementation of DTNs and present a method for delay-tolerant remote control communication systems, allowing devices to plan information transmission and energy exchange based on available energy sources [2].

J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain describe a project that incentivizes Plug-in Hybrid Electric Vehicles (PHEVs) to modify local power demands for their own benefit. They explore the use of a consortium blockchain innovation to enhance exchange security without relying on a trusted third party. The authors propose a framework called PETCON (restricted P2P electricity trading with a consortium blockchain) to illustrate the activities of limited peer-to-peer power trading [3].

N. Z. Aitzhan and D. Svetinovic address the issue of transaction security in decentralized smart grid energy trading without relying on trusted third parties. They present a proof-of-concept for a decentralized energy trading system that utilizes blockchain technology, multiple signatures, and anonymous encrypted messaging flows. This system enables secure trade transactions while maintaining the anonymity of peers during energy price negotiations [4].

M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Presenting introduce NRG-coin, a decentralized digital currency used by consumers in the smart grid system to exchange privately generated sustainable energy sources. NRG-coins have a value determined in an open cash trade market and differ from bitcoins as they are created by injecting energy into the matrix. The authors also propose a revolutionary method for trading environmentally friendly energy in the smart grid network [5].

S. Barber et al. conduct an extensive investigation into the success of Bitcoin as a form of electronic cash and examine the factors that contributed to its widespread adoption. They explore Bitcoin's potential as a viable candidate for stable currency and analyze its characteristics and advantages [6].

I. Alqassem et al. discuss the development of various Bitcoin libraries, APIs, and optional applications, highlighting the continuous upgrades and open-source nature of Bitcoin. They provide an in-depth examination of the protocol specification and architecture of the Bitcoin framework, considering it as the initial step in establishing a standard design for cryptographic currency [7].

K. Croman et al. present a paper addressing the scalability challenges faced by blockchain-based digital currencies. They examine the bottlenecks and limitations of the current distributed overlay technology of Bitcoin and emphasize the need for reevaluation and technical advancements to achieve higher throughput and lower latencies [8].

G. W. Peters and E. Panayi provide an overview of blockchain innovation and its potential to disrupt the field of financial management. They discuss global cash settlement, smart contracts, automated record-keeping, and cutting-edge tools as key components of this innovation, with a focus on second-generation contract-based improvements [9].

L. Luu et al. introduce ELASTICO, a consensus protocol for permissionless blockchains. ELASTICO scales transaction rates directly with available computation power, allowing for increased block selection based on the system's computational capacity. The authors highlight the effectiveness of ELASTICO in system communications and its resilience against sophisticated adversaries [10].

III. PROPOSED SYSTEM

In the proposed system, we have developed a blockchain-based KYC system where customers can upload their data files and encrypt them using corresponding keys. To ensure both security and efficient searching, we have designed an effective search scheme. In this framework, the server is capable of combining encrypted records and performing searches without exposing sensitive user data, including both data files and queries.

3.1 Algorithm Details

Encryption Algorithm: AES (Advanced Encryption Standard)

AES is a symmetric encryption algorithm used to convert plaintext into ciphertext. It was developed as an improvement over the weaknesses of DES, such as its vulnerable 56-bit key and 64-bit block size. AES utilizes a 128-bit block size

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: 7.301
Volume 3, Issue 10, May 2023

and supports 128-bit keys. The algorithm we employ in this project is Rijndael, which is a variant of AES and provides encryption for the data owner's files.

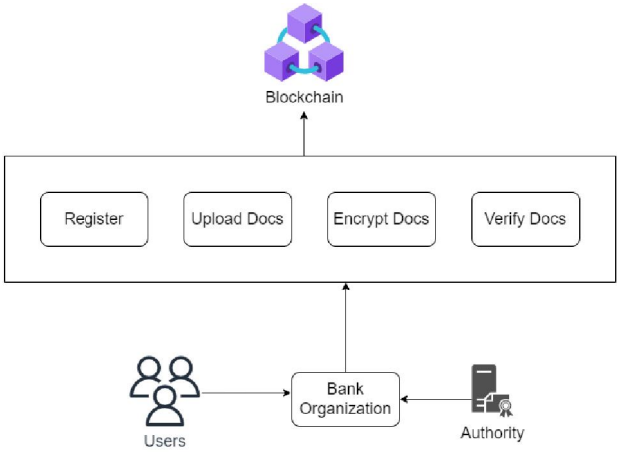

Fig. System Architecture

Input:
128_bit /192 bit/256 bit input (0, 1)
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)
Hash Algorithm: MD5 (Message-Digest Algorithm)
MD5 is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value, typically represented as a 32-digit hexadecimal number. It is commonly used for data integrity verification and has various applications in cryptography. The steps involved in MD5 include processing the input data as blocks of 512 bits, performing multiple rounds of operations for each block, and utilizing constants derived from trigonometric sine functions. Many modern programming languages provide built-in functions for MD5 algorithm implementation.

IV. RESULT AND DISCUSSION

Figure 5: overall system execution graph

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: 7.301
Volume 3, Issue 10, May 2023

The experiments were conducted using a personal computer with the following configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, running Windows 7 operating system. The backend database used was MySQL 5.1, and the application development tool used for designing code was Eclipse. The web application was executed on a Tomcat server.

V. CONCLUSION

Blockchain technology is currently at a stage comparable to the early days of the Internet. The continuous advancements in information technology and online commerce have a significant impact on various aspects of modern life. The goal of blockchain technology is to revolutionize how users interact and communicate online. Beyond concepts like mining and tokens, the key advantages of blockchain technology include the complete synchronization of operations and the integrity and uniqueness of all processed information. By incorporating blockchain technology, distributed databases can enhance data storage, synchronization, data loss prevention, and data integrity.

While it is still in its early stages, many business leaders are investing in various blockchain use cases supported by business associations. The potential of blockchain is evident, but it is essential for businesses to demonstrate practical use cases and assess the feasibility from both technical and business perspectives before implementing blockchain solutions. We acknowledge the immense potential of this technology while also recognizing its current limitations

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.