IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

E-KYC STSTEM USING BLOCKCHAIN TECHNOLOGY: A REVIEW

Manas Patil*[1], Sakshi Patil*[2], Aaditya Patil[*3], Amir Ahmad[*4]

Prof.D.B.Mane[*5]

*[1,2,3,4,5] Department of Information Technology, Smt Kashibai Navale College of Engineering Vadgaon(BK) Pune,Maharashtra,India.

Affilated by Savitribai Phule Pune University.

Abstract—***The electronic know your customer (e-KYC) system allows a banking or identity provider to set up a customer identification data verification process between reliant parties. Most banks deploy their e-KYC system on the cloud due to the efficient resource consumption and high degree of accessibility and availability.The KYC methods employed by banks are entirely reliant on encryption, which is slow and can result in the leakage of consumer information to third-party financial organizations. This system can be made more efficient by utilizing Blockchain technology, which has the potential to automate many human operations while also being resistant to attacks of any kind. The immutable blockchain block and its distributed ledger are an ideal complement to the KYC procedure. Fraud detection can be automated with the addition of smart contacts.We can use any type of KYC to store KYC identification details. As a result, banks can create a shared private blockchain within the bank's premises that can be used to validate documents. This gives the user control over their sensitive documents, while simultaneously making it easy for banks to access the records required for compliance.***

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

I. INTRODUCTION

A. Overview

A Blockchain-based security management system is used to secure bank transactions and to make the KYC process more simple and secure. Blockchain technology is a novel technology that uses mathematical, cryptographic, and economic concepts to maintain a database amongst multiple participants without the need for a third party or central authority. It is a secure, tamper-evident distributed database in which the legality of a transaction may be checked by parties involved in the transaction.

Banks' Know Your Customer (KYC) processes on its consumers are unneeded, inefficient, and costly. As a result, a system is proposed to automate unskilled operations and allow for the sharing of KYC data. Blockchain technology, with its distributed database idea and time-stamped ledgers, can significantly assist banks in improving their KYC procedure.

Know Your Customer (KYC) procedures used by banks on their customers are unnecessary, ineffective, and expensive. As a result, a system is suggested to automate routine tasks and enable KYC data sharing. With its distributed database concept and time-stamped ledgers, blockchain technology can significantly help banks improve their KYC process.

B. Motivation

KYC procedures are typically laborious, repetitive, incompatible, and duplicative, which increases administrative costs and overhead. With its immutable ledger, simplicity of integration, and significantly cheaper operating and infrastructure expenses, a blockchain-based solution is unquestionably a superior choice than the current KYC procedures.

Each bank must organize the security of the data it holds, such as the status of its customers' accounts, their transaction history, etc., because banking information has always attracted the attention of intruders. Blockchain is a distributed shared ledger that records transactions to an unbreakable, permanent chain that can be viewed by the parties to a transaction. This technology can address the weaknesses in transactional cyber-attacks.

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

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 energyexchanging 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 messaging flows. This system allows peers to securely conduct trade transactions while maintaining their anonymity when negotiating energy prices [4].

M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Presenting NRG-coin, a piece of art that depicts decentralised digital money. NRG-coins, whose value is imprinted on an open cash trade market, are used by consumers in the smart grid system to exchange privately generated sustainable energy sources. Similar to bitcoins, this currency offers a number of advantages over fiat money, but unlike bitcoins, it is created by injecting energy into the matrix rather than by distributing energy based on computing impact. They also create a revolutionary method of swapping worldviews when buying and selling environmentally friendly energy in the smart grid network [5].

S. Barber et al gives a piece that claims Bit-coin is a solitary form of electronic cash that has drawn in a sizable following. They do a thorough investigation to understand what made Bitcoin so successful, despite years of study on cryptographic e-money failing to result in a widespread appropriation. Also, they inquire as to how Bitcoin might be a respectable candidate for seemingly endless stable currency [6].

I. Alqassem et al shows how various Bit-coin libraries, APIs, and optional uses are being developed, and how Bit-coin is continually upgraded via an open source network. All things considered, since the distribution of the authority whitepaper, there hasn't been a forthcoming convention comparison or design description. The project shows an in-depth examination of the Bit-coin framework's convention detail and architecture. We view this research as the first step in establishing the standard design for cryptographic currency .

K. Croman et al presents a paper that demonstrates how the growing popularity of block-chain-based digital currencies has made adaptability a necessary and serious task. The study

examines how Bit-primary coin's and secondary bottlenecks prevent its current distributed overlay technology from supporting significantly larger throughputs and lower latencies. These findings suggest that reparameterization of square size and interruption should only be viewed as a first step in achieving future people. Real advancements would also necessitate a fundamental reevaluation of technical approaches[8].

G. W. Peters and E. Panayi shows a work that provides a diagram of the concept of block-chain innovation and how it might disrupt the world of account management by promoting global cash settlement, cunning contracts, automated record-keeping for money, and cutting-edge tools. In this way, they first provide a brief summary of the key components of this innovation as well as the secondgeneration contract-based improvements[9].

L. Luu et al introduces ELASTICO, a work that offers a different widely used understanding standard for authorization-less block chains. The number of exchange squares selected per unit of time increases as the computation control in the system increases in ELASTICO, which scales exchange rates directly with accessible estimation for mining. When it comes to system communications, ELASTICO is effective, allowing sophisticated enemies to use up to one-fourth of the total computational power[10].

III. PROPOSED SYSTEM

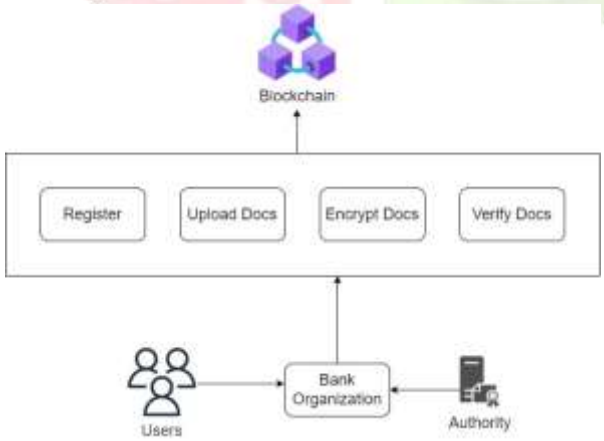

Fig. System Architecture

- In proposed system, we implement a block chain Based KYC system, in which each customer upload a data files and encrypts these data with corresponding key.
- To implement both security preservation and relevant searches, we propose an effective search scheme.
- In this framework, the server is permitted to viably combine various encrypted records, and safely play out the pursuit without uncovering the user sensitive data, neither information documents nor the questions.

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) 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)

The AES encryption algorithm of the proposed system ensures the security. Moreover, proposed system can resist the typical attacks such as the brute-force attack, tampering attack, and collusion attack.

Existing platforms generally rely on strong authentication and apply traditional encryption i.e. DES, Blowfish to not support their security and privacy requirement.

CONCLUSION

Today's Blockchain is similar to the Internet in its early 20s in many aspects. Every day, the advancement of information technology and internet commerce has a greater and greater impact on all aspects of contemporary life. Blockchain technology aims to challenge the conventional understanding of how users communicate with one another online. The primary benefits of Blockchain technology, regardless of mining and tokens, are the total synchronization of operations, integrity, and uniqueness of all processed

information. In terms of data storage, synchronization, loss, and integrity, distributed databases can be improved with the use of blockchain technology.

Although it is still early, business leaders are funding a wide range of blockchain use cases that are supported by business associations. We believe the promise is evident, but the blue sky is too far away, and businesses need to demonstrate use cases and business/technical feasibility before deploying blockchain. We have seen the potential of this technology and the limitations.

ACKNOWLEDGMENT

Express my true sense of gratitude, sincere and sincere gratitude to my guide to the project Prof. D.B.Mane for his precious collaboration and guidance that he gave me during my research, to inspire me and provide me with all the laboratory facilities, This it allowed me to carry out this research work in a very simple and practical way. I would also like to express my thanks and thanks to our coordinator, Prof.V.D.Ghonge ,HOD. Dr.M.L.Bangare and Principle sir and all my friends who, knowingly or unknowingly, helped me during my hard work.

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-topeer 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.