ENABLING TRUST AND PRIVACY PRESERVING E-KYC SYSTEM

[1]MR. K.RAGHAVENDAR, [2]KALAM SATHISH KUMAR, [3]G.SANTOSH KUMAR, [4]SRIGADHA KRISHNASAI, [5]MD THANVEER AHMED

[1](Assistant Professor) ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

[2345]B,tech scholar ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

ABSTRACT

The electronic know your client (e-KYC) may be a system for the keeping money or character supplier to set up a client character information confirmation handle between depending parties. Due to the effective asset utilization and the tall degree of openness and accessibility of cloud computing, most banks actualize their e-KYC framework on the cloud. Basically, the security and protection of e-KYC related records put away within the cloud gets to be the significant issue. Existing e-KYC stages by and large depend on solid verification and apply conventional encryption to back their security and security prerequisite. In this show, the KYC framework proprietor scrambles the record with their host's key and transfers it to the cloud. This strategy actuates encryption reliance and communication and key administration overheads. In this paper, we present a novel blockchain-based e-KYC plot called e-KYC TrustBlock based on the ciphertext arrangement quality based encryption (CP-ABE) strategy official with the client assent authorization to provide believe, security and security compliance. In expansion, we introduce attribute-based encryption to empower the security protecting and fine-grained get to of delicate exchanges put away within the blockchain. At last, we conduct tests to appear that our framework is productive and adaptable in hone.

1.INTRODUCTION

Electronic-Know Your client (-KYC) is advantage that banks or financial teach (FIs) provide overseeing account operation related to confirmation and affirmation of character electronically to their clients for advancing taken a toll efficiency and client fulfillment e-KYC system FIs to electronically affirm their client character and recuperate KYC data for both individual and corporate clients. To apply the e-KYC system, cash related teach either utilize off- the- rack e-KYC computer program totally arranged with basic capacities or make their claim. At that point, they can pass on the system as an on-premise or a cloud-based appear. Due to the float of the outsourcing illustrate, most wanders have grasped the cloud as the favored arrange for lodging their "' system and data. "' A cloud-based e-KYC system gives a more successful and versatile confirmation technique compared to the host-based ! e-KYC confirmation technique where records got to be be affirmed by implies of the centralized have. This causes a action bottleneck and single point of dissatisfaction issue. In addition, the traceability of the affirmed trade is compelled since all trades happening inside the system are completely managed by the provider. All things considered, the security and security issue of a cloud-based course of action may be a concern for various potential endeavors.

More often than not since e-KYC system found on the cloud store client data files and it may be seen by any open cloud tenants or undoubtedly the cloud advantage providers (CSPs). To address this issue, most banks and FIs ought to actualize an encryption instrument in extension to the strong confirmation highlight given by the CSPs. To this conclusion, banks and FIs having the e-KYC system got to scramble the e-KYC information _les some time recently they are transferred to the cloud. When the depending parties inquire for affirmation, the have party can either perform the affirmation by either interpreting the _le and sending back the affirmation of the affirmation result to the requestor or transmitting the copy of mixed _les at the side the unscrambling key to the requestor.

This to start with approach presents the overheads related to the affirmation get ready, communication, and centralized unscrambling though the final said approach must handle key organization especially secure key sharing. Especially, key disavowal and key re-generation inside the cloud e-KYC environment have not been tended to by any explore works. In case the client would like to drag back his consent from any banks or FIs, they have no right to store the client's personality data any longer. In like way, the data ought to be completely deleted and the translating key ought to be denied. Any banks or FIs sharing the denied key got to be recoup a key to completely guarantee that unauthorized banks or FIs cannot get to the client's data put absent inside the cloud . In expansion to the already specified "!issues, taking off cloud e-KYC stages do not grant shared information for the trade happening within the e-KYC affirmation available for take after capacity !. As of late, square chain development has pulled in huge charmed by a number of wanders in various businesses checking the keeping money and budgetary division. There's a creating captivated in utilizing e-KYC stages that utilize piece chain and cloud system "!%!. Piece chain innovation truly progresses the decentralized framework empowering straightforwardness, agility, steadfastness, and cost-effectiveness for trade planning and organization in a multi-user and multi-provider environment. Inside the piece chain system, a savvy contract which may be a self-executing program that can be executed on the piece chain enables the mechanized execution of framework bases or capacities beneficially. This enables the comfort and programmability of any systems running on the square chain orchestrate. For a long time, a number of investigate works related to piece chain-based KYC have proposed to supply the 2 decentralized affirmation and confirmation prepare. Be that as it may, there are inadequacies that have not been totally understood by existing works.in bigin no works that give an electronic client's consent work with the strong non-repudiation property which is an fundamental necessity of security controls such as the Common Data Act (GDPR) [18] the KYC enrollment prepare.

Moment, most existing works neglect the assurance of trade put absent inside the adroit contract and square chain. In expansion to the character or credential chronicles that are mixed on the cloud capacity, the assurance of all e-KYC taking care of trades such as exchange status sharing, data starting affirmation, and smart contract that contains person data put absent inside the square chain ought to be ensured. At final, most works have a limited highlight to permit the clients to urge to and overhaul their accreditations found on the cloud advantage paid by the FI. In this paper, we point to address such inquire about holes by showing a secure and viable square chain-based e- KYC chronicles enrollment and affirmation handle with lightweight key cryptographic traditions run within the cloud Interplanetary Record Framework (IPFS). To energize the foundational security prerequisite with respect to the user's consent collection, we make a keen contract to create and uphold the assent to be carefully checked by the client.

The consents will be methodicallly put away in a square chain having a tamper-proof property which is profitable for analyzing. With respect to the data assurance issue, we propose an optimized cryptographic convention by applying symmetric encryption with open key encryption to scramble the customers' credential _les and utilize the cipher content approach attribute-based encryption (CP-ABE) to scramble the piece chain trades. Since CP-ABE gives a oneto-many encryption with fine-grained access control, it permits many FIs to urge to common mixed value-based data inside the blockchain of the same client based on the get to arrangement defined. Particularly, we arrange the approach update calculation to empower capable re encryption based on a less complicated course of action tree structure. At long final, our framework licenses clients to overtake their e-KYC information with any banks or FIs locks in within the piece chain. The updated e-KYC data is broadcasted within the record and the synchronization of the updated data is done by the careful quick contract.

2.LITERATURE SURVEY

At show, blockchain development and sharp contracts have been utilized in various application ranges. Particularly, blockchain-based recognizing verification and confirmation framework have been proposed by various works and it has been outlined that a blockchain is beneficial for recognizing confirmation and affirmation organization. Be that because it may, the strategy of e-KYC is much more complicated than clear confirmation task. Or possibly, it incorporates secure credential enrollment, KYC file organization, secure and lightweight affirmation get ready between clients, distinctive FIs, and a given blockchain arrange. In extension, unused sorts of blocked off and spoofing attack to the KYC system ought to be be countered . Afterward ask almost works related to a blockchain- based e-KYC center on defining a framework for secure client identity organization and capabilities affirmation as well as optimizing the communication overhead of the interaction among money related building up. Inside, the makers proposed a KYC file affirmation plot utilizing the IPFS system and blockchain advancement.

In this approach, the clients select their identity course of action with the bank and their accreditations are hashed and mixed by utilizing gpg4win as an encryption device. In any case, this paper does not concern itself with the security and traceability of trades inside the blockchains. In Shabair et al. proposed a blockchain-based KYC inside the outline of proof-ofconcept (PoC) system. The proposed system was conducted in private blockchain circumstances over the Grid'5000 a large-scale dispersed organize. Norvill et al. shown a framework that grants mechanization and permissioned record sharing over the blockchain to decrease the KYC get ready. In Allah et al. proposed a HyperledgerFabric organize for KYC optimization appear. In this illustrate, the client has full right to have the shrewd contracts in which client KYC information is put away within the spread record database. In any case, these works did not address the security and key organization issue of KYC handle. In Kapsoulis et al. proposed a way to execute e- KYC system utilizing savvy contracts and IPFS. In this work, KYC report operations such as make, inspected, upgrade and eradicate are done through the set of shrewd contacts.

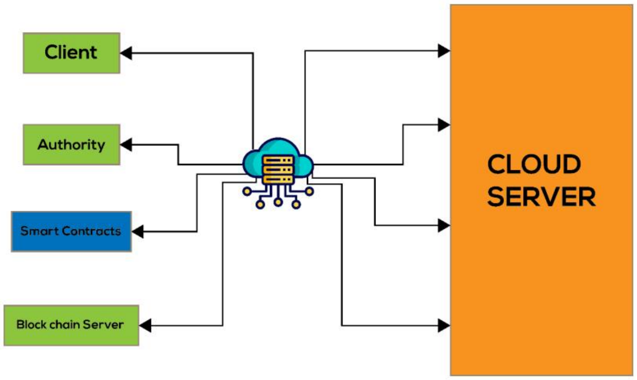
The KYC files are put absent inside the IPFS and through the private contract procedure. The security of the KYC trade is managed by specific centers within the blockchain with chairman benefits. Be that because it may, there are no encryption utilized to secure the KYC data. With regard to the security protecting method associated for securing blockchain database, CP-ABE has gotten the thought of a number of ask almost works . In Bramm et al. proposed a Blockchain-based Dispersed Attribute-Based Encryption (BDABE) conspire licenses the qualities to be made and eradicated effectively at any time by a trade on the blockchain. The proposed plan supports mapping between various property pros to dole out the properties to the clients. It offers the flexibility for supporting secure and proficient client characteristics administration in the blockchain system. In Fan et al. proposed a traceable data sharing contrive utilizing blockchain and CP-ABE. In this contrive, data is mixed by a CP-ABE procedure and a secret key can be produced based on the system parameters available within the private blockchain. Inside the blockchain, the data proprietor can get the identity of data buyer and control data sharing based on the predefined get to course of action.

Yuan et al. and Wu et al. utilized a CP-ABE approach to bolster information security protection and fine-grained sharing inside the blockchain system. In these plans, any changes to the data are recorded on the blockchain and the get to course of action is executed to supervise the unmistakable authorizations of get to. In case there's any key misuse case begun by any pernicious clients or specialists, the system gives survey trails to back the traceability of cryptographic operations and trade works out. Guo et al. proposed a traceable attribute-based encryption with lively get to control (TABE-DAC) plot based on the combination of CP-ABE based straight riddle sharing plot (LSSS) and blockchain. The proposed conspire accomplishes negrained sharing of mixed private data on cloud, traceability of users' private key spillage, and versatile approach overhaul. The makers additionally displayed a hash work inside the key and ciphertext time to diminish the 4 computation gotten of such operations. In Gao et al. proposed a secure ciphertext-policy and property covering up get to control plot and blockchain. The CP-ABE is utilized to secure the data put absent inside the blockchain. In any case, this plan businesses composite orchestrate bunches for their crypto execution which comes about in exorbitant computation brought. As of late, Dwevedi et al. proposed a Zero-Knowledge Affirmation (ZKP) verification conspire and the encryption plot called ZKNimple for supporting lightweight encryption in IoT-based applications.

With the proposed plot, the affirmation is accomplished through the ZKP property though the security of key exchange and data is protected through password-authenticated technique and Feistel encryption. In, Bhaskaran et al. proposed a arrange and execution of a sharp contract for consent-driven and double-blind data sharing on the Hyperledger Surface blockchain organize. The adroit contract for creating customer's consent was made and disseminated on the blockchain. The makers additionally shown open key sharing on the blockchain to distinctive providers for scrambling the report. In any case, the consent given by the client has no progressed signature authoritative.

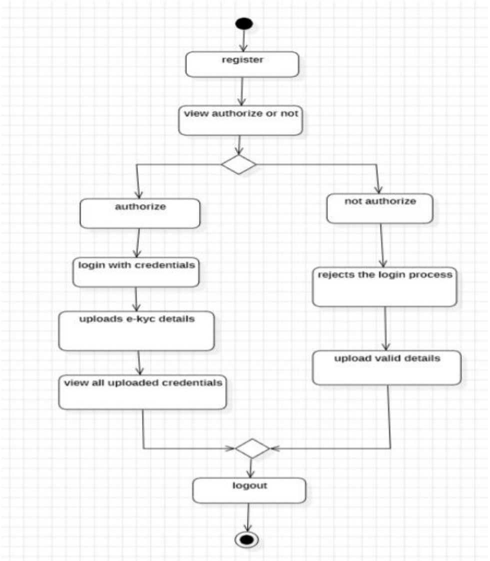
3.SYSTEM DESIGN

3.1 SYSTEM ARCHITECTURE:



ISSN: 2366-1313

ACTIVITY DIAGRAM:



4.OUTPUT SCREENS

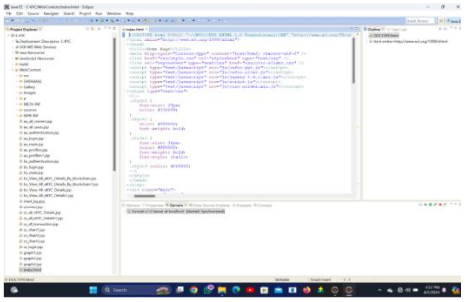
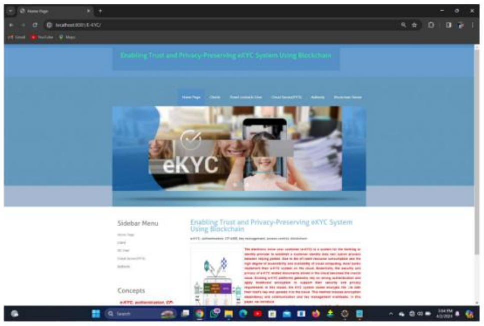
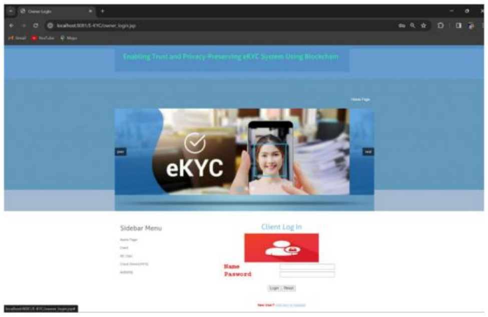


Fig 4.1:Code



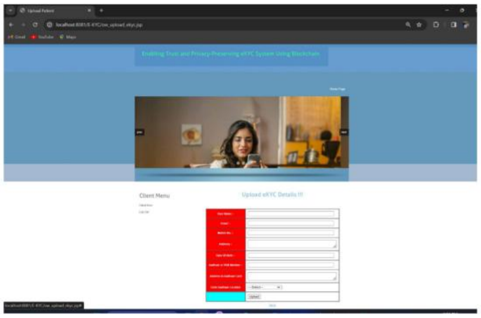
Enabling Trust and Privacy-Preserving eKYC System Using Blockchain

Fig 4.2: Home page



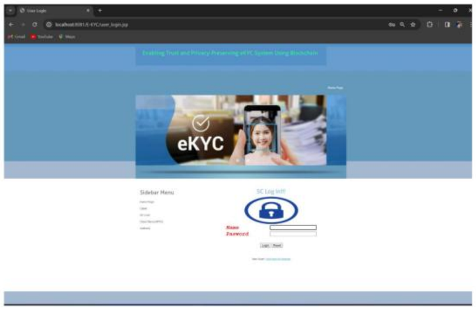
Enabling Trust and Privacy-Preserving eKYC System Using Blockchain

Fig 4.3:Client login page



Enabling Trust and Privacy-Preserving eKYC System Using Blockchain

Fig 4.4:Upload e-Kyc Details



Enabling Trust and Privacy-Preserving eKYC System Using Blockchain

Fig 4.5:Smart Contract login page

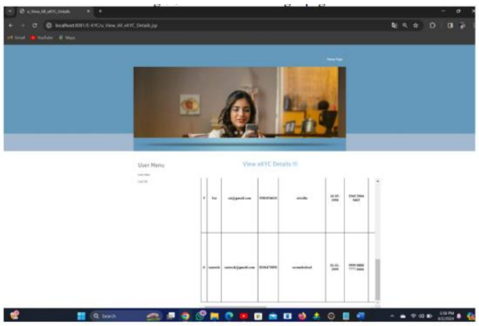


Fig 4.6:View all kyc and Verify

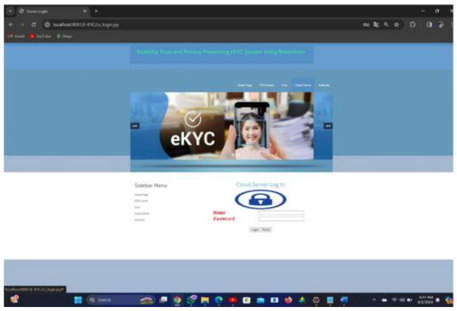

Enabling Trust and Privacy-Preserving eKYC System Using Blockchain
eKYC
Sidebar Menu
Cloud Server Log In
Name
Password

Fig 4.7 :Cloud Server Login page

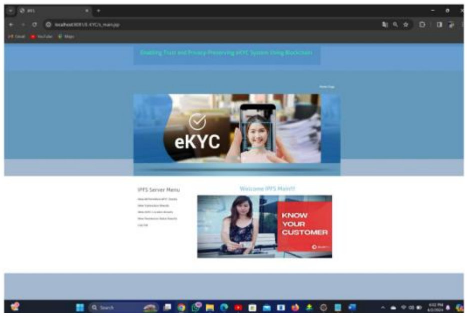


Fig 4.8 :Cloud Server dashboard

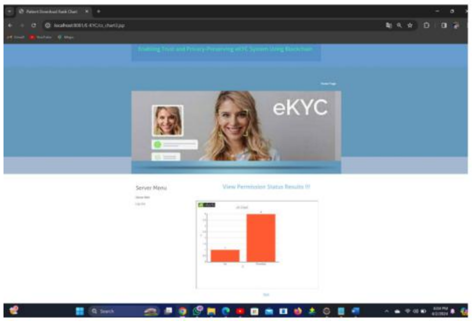


Fig 4.9: View Permission and Status Results

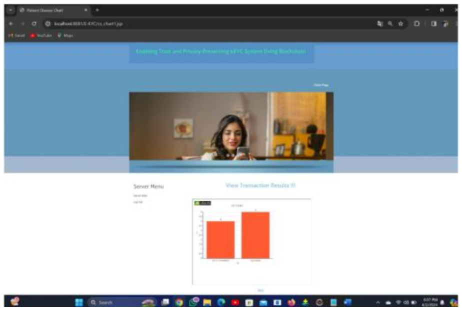


Fig 4.10: View Transaction Results

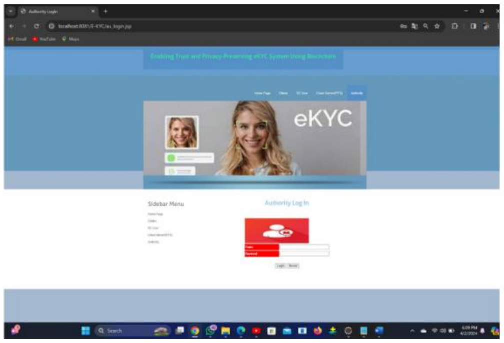


Fig 4.11: Authority login page

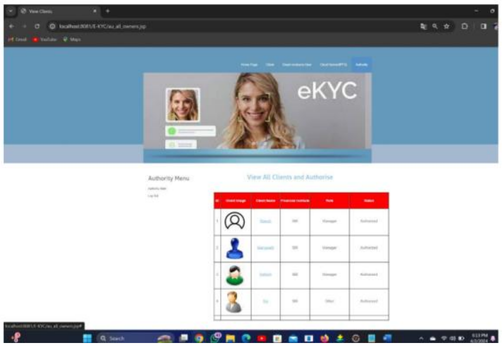


Fig 4.12: View All Clients and Authorize

5.CONCLUSION

We have displayed the privacy-preserving e-KYC approach based on the piece chain. Our proposed plot conveys secure and decentralized verification and confirmation of the e-KYC handle with the user's assent authorization include. In our conspire, the protection of both customers' character records put away within the cloud is ensured by the symmetric key and open key encryption whereas the sensitive transaction information put away within the piece chain is scrambled by symmetric key encryption and CP-ABE. Our plot too permits the KYC information to be overhauled by the information proprietor or the client. In expansion, we formulated an get to arrangement upgrade calculation to empower energetic get to authorization. For the assessment, we performed comparative investigation between our plot and related works in terms of the computation taken a toll, the communication fetched, and execution.

The exploratory comes about appeared that our conspire beats existing plans in terms of execution, comprehensive KYC compliance highlights, and the scalable get to control component. For future works, we'll test a bigger test of information within the genuine cloud environment and measure the throughput of the framework in pleasing tall number of e-KYC enrollment and confirmation demands. In expansion, we are going explore the method to empower bunch confirmation of eKYC exchanges put away within the piece chain with the searchable encryption include

6.FUTURE ENHANCEMENT

For future works, we'll test a bigger test of information within the genuine cloud environment and degree the throughput of the framework in pleasing high number of e-KYC enrollment and confirmation demands. In expansion, we'll examine the strategy to empower clump confirmation of e-KYC exchanges put away within the blockchain with the searchable encryption include.

7.REFERENCE

[1] Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, and M. Hu,``Distributed blockchain-based authentication and authorization protocol for smart grid," Wireless Communication . Mobile Computer., vol. 2021, pp. 1_15,Apr. 2021, doi: 10.1155/2021/5560621.

[2] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, ``Blockchain technology the identity management and authentication service disruptor: A survey," Int. J. Adv. Sci. Eng. Inf. Tech., vol. 8, pp. 1735_1745, Sep. 2018.

[3] A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan, M. S. Bhuiyan, M. S. Kaiser, M. S. Kaiser, M. A. Yousuf, and M. A. Yousuf, ``Secure and transparent KYC for banking system using IPFS and blockchain technology," in Proc. IEEE Region Symp.(TENSYMP), Jun. 2020, pp. 348_351.

[4] M. Pic, G. Mahfoudi, and A. Trabelsi, ``Remote KYC: Attacks and counter measures, "in Proc. Eur. Intell. Secur.

Informat. Conf. (EISIC), Nov. 2019,pp. 126_129.

[5] W. Shbair, M. Steichen, and J. François, ``Blockchain orchestration and experimentation framework: A case study of KYC," in Proc. 1stIEEE/IFIP Int. Workshop Manag. Managed Blockchain (Man Block),Jeju Island, South Korea, Aug. 2018, pp. 23_25.

[6] R. Norvill, M. Steichen, W. M. Shbair, and R. State, ``Demo: Blockchain for the simplification and automation of KYC result sharing," in Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC), May 2019, pp. 9_10,doi: 10.1109/BLOC.2019.8751480.

[7] T. Mikula and R. H. Jacobsen, ``Identity and access management with blockchain in electronic healthcare records," in Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD), Prague, Czech Republic, Aug. 2018,pp. 699_706.

[8] S. Wang, R. Pei, and Y. Zhang, ``EIDM: A ethereum-based cloud user identity management protocol," IEEE Access, vol. 7, pp. 115281_115291,2019, doi: 10.1109/ACCESS.2019.2933989.

[9] N. Ullah, K. A. Al-Dhlan, and W. M. Al-Rahmi, ``KYC optimization by blockchain based hyperledger fabric network," in Proc. 4th Int. Conf. Adv. Electron. Mater., Computer. Software. Eng. (AEMCSE), Mar. 2021,pp. 1294_1299.

[10] N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke ,and T. Varvarigou, ``Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture," Future Internet, vol. 12, no. 41, pp. 1_13, 2020.