International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Personalized Secure E-Identity Locker Using Blockchain

Indu Dokare[*1], Atharva Deshmukh[*2], Yash Diwan[*3], Purav Rathod[*4], Krishna Zanwar [*5]

[1*]*Assistant Professor, Dept. of computer Engineering, Vivekanand Education Society's Institute of Technology, Maharashtra,India*

[2*-5*]*Student, Dept. of computer Engineering, Vivekanand Education Society's Institute of Technology*

Abstract - ***Blockchain*** *technology is revolutionizing the society by empowering new types of* ***disintermediated*** *digital platforms. There is a critical demand for* ***secure*** *identity storage systems as there have been identity management challenges for example* ***security***, ***privacy***, *and* ***usability*** *since the dawn of the Internet. As identity cards include the personal information similarly Personalized Secure E-Identity locker will be a storage for all the documents of a person eg. Aadhar Card, Passport etc. The documents will be stored in a file which will be* ***encoded*** *using encryption methods.* ***Blockchain*** *technology may offer a solution to deal with this issue by delivering a* ***secure*** *system without the need for a trusted, central authority. It can be used for storing an identity on the blockchain, making it easier to manage for individuals, giving them greater control over who has their personal information and how they access it.*

1. Introduction

Blockchain is a decentralized and public ledger, which has introduced tremendous changes during the last few years with applicability on financial use cases (e.g. remittance) and nonfinancial use cases (e.g. documents).Users can trust the blockchain as it is leveraging consensus mechanisms to validate and gather the transactions in blocks. Blockchain is additionally considered as an open ledger where online transactions are recorded and users can connect, send and verify their transactions. In other words, it is a digitized system in order to account the records. These records are a set of mathematical rules which are incorporated to stop the illegal intrusion. In order to include the data into the blockchain, users and nodes, which obtain an authorize-able address from the blockchain, need to set up and communicate with smart contracts to send and retrieve data to/from the blockchain. Moreover, blockchain works on the subsequent rules; it represents decentralized, transparent and secure systems. Decentralized systems are basically user to user or peer to peer operations without involving any central hub or authority. Transparency can be ensured as the data is being embedded in the system publicly. Security provides the encryption technology supporting public and private keys. For example, in bitcoin, the public key represents the user as address and private key acts as a password to access the transaction.

As the current systems for storing documents are based on centralized servers, it implies that the owners of the system have direct access to the sensitive data of the users making it vulnerable for data theft and other corrupt practices. The system might also be vulnerable to hacking which may lead to serious threat to the data of the users. Moreover if there is a server damage in the current system , it would lead to a loss of user data which motivates to use blockchain and decentralized server systems in this project to safely store the sensitive data of the users. In the proposed system blockchain is used to store and retrieve the user ID. In order to contact the user, blocks can be retrieved and validated. Also, it is made secure and encrypted by implementing blockchain internally and externally; internally for accessing the list and externally to follow the identities. There are multiple ways of validation in order to retrieve documents from blockchain. Decentralized can also be called user to user or peer to peer operation without involving any central hub or authority. The system designed in this project has Transparency, which means the data is being embedded in the network publicly. Security offers the encryption technology supporting public and private keys. For example, in bitcoin, the public key represents the user as address and private key acts as a password to access the transaction.

2. Literature Survey

There are already several spectacular open-source Blockchain projects in the market however they have restricted functionality.

cloud storage has relied almost exclusively on large storage providers, who act as trusted third parties to transfer and store data. This model poses a number of issues including data availability, high operational cost, and data security. Hoang Giang Do, Wee Keong Ng proposed a system [1] that uses blockchain as the backbone for off-chain data storage access, permission grant and search token generation.

The private key generator has the ability to decrypt all data stored in the cloud server, which may bring serious

problems such as key abuse and privacy data leakage. Shangping wang , yinglong zhang , and yaling zhang proposed a framework [2] that combines the decentralized storage system interplanetary file system, the Ethereum blockchain, and ABE technology. In this framework, the data owner has the ability to distribute secret key for data users and encrypt shared data by specifying access policy, and the scheme achieves fine-grained access control over data. Cloud storage is one of the leading options to store massive data, however, the centralized storage approach of cloud computing is not secure. Meet Shah, Mohammedhasan Shaikh, Vishwajeet Mishra, Grinal Tuscano proposed a system [3] where the user's file is encrypted and stored across multiple peers in the network using the IPFS (InterPlanetary File System) protocol. IPFS creates a hash value. The hash value indicates the path of the file and is stored in the blockchain

3. Implementation details

In the proposed system, blockchain will be implemented by IPFS (InterPlanetary File System) which is an immutable server. It will help to make the system more secure. Users will first have to register in this system. Every user will have a personalized unique password and to add more protection will also have a biometric scanner to login. After successful login, the user will be able to upload documents. In the process of uploading the documents, the system will first encrypt the files containing the documents and the encrypted file will be uploaded to ipfs server. When the file is getting uploaded, it will be stored as a block in the blockchain server. At the same time the transaction hash will be maintained by ethereum. When the document is uploaded successfully it will be stored as a block in the blockchain. Similarly for retrieval of the documents, the user will first have to login. The system will display the documents already uploaded by the user. The user can download the required document by clicking on the download button. The block containing the document will get downloaded. As the document is stored in encrypted format, first it will be decrypted and then would be displayed to the user. As the designed system uses IPFS which is an immutable server , once a document is uploaded, it would be securely stored forever. It can not be deleted even by the user.

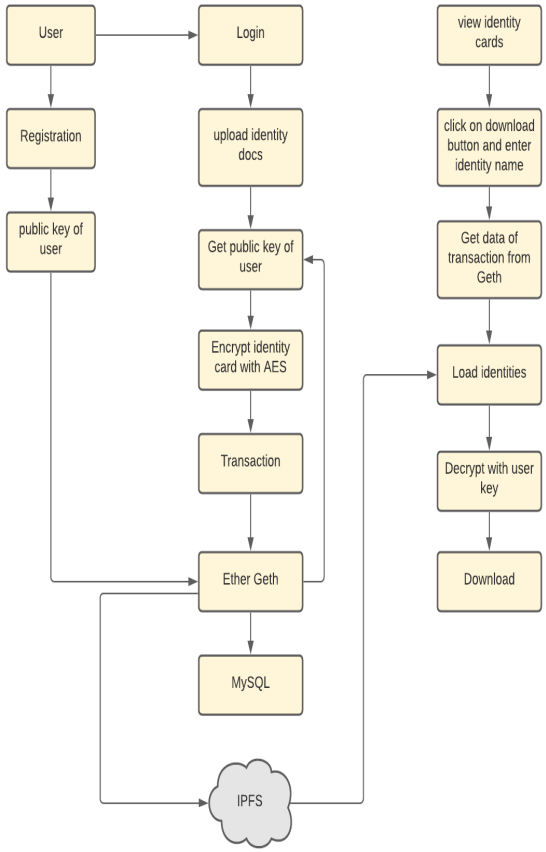

Fig-1:Block Diagram of E-secure identity card

4. Conclusion

The proposed platform takes the advantage of the blockchain in order to create a globally trusted document storing system. Thus by using the Personalized Secure E-Identity Card, users will be able to safely submit documents to various institutions/ Government bodies without the fear of data theft. The users will also be relieved from the fear of losing the documents as they will be stored in digital format. It will also facilitate the user to personalize the card with only the required documents providing the feature of addition or deletion of a document.

5. References

[1] H. G. Do and W. K. Ng, "Blockchain-Based System for Secure Data Storage with Private Keyword Search," 2017 IEEE World Congress on Services (SERVICES), Honolulu, HI, 2017, pp. 90-93, doi: 10.1109/SERVICES.2017.23.

[2] S. Wang, Y. Zhang and Y. Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access

Control in Decentralized Storage Systems," in IEEE Access, vol. 6, pp. 38437-38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[3] C. Rahalkar and D. Gujar, "Content Addressed P2P File System for the Web with Blockchain-Based Meta-Data Integrity," 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, 2019, pp. 1-4, doi: 10.1109/ICAC347590.2019.9036792.

[4] G. Malik, K. Parasrampuria, S. P. Reddy and S. Shah, "Blockchain Based Identity Verification Model," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 2019, pp. 1-6, doi: 10.1109/ViTECoN.2019.8899569.

[5] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan and S. Wang, "An Identity Management System Based on Blockchain," 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, 2017, pp. 44-4409, doi: 10.1109/PST.2017.00016.

[6]Z. Zhao and Y. Liu, "A Blockchain based Identity Management System Considering Reputation," 2019 2nd International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, 2019, pp. 32-36, doi: 10.1109/ICISCAE48440.2019.221582.

[7] S. V. Juno Bella Gracia, D. Raghav, R. Santhoshkumar and B. Velprakash, "Blockchain Based Aadhaar," 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2019, pp. 173-177, doi: 10.1109/ICCCT2.2019.8824892.

[8] M. Shah, M. Shaikh, V. Mishra and G. Tuscano, "Decentralized Cloud Storage Using Blockchain," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 2020, pp. 384-389, doi: 10.1109/ICOEI48184.2020.9143004.