IDENTITY CONSENT MANAGEMENT USING BLOCKCHAIN

Dr. S. Geetha[1], Pushpa valli[2], Muraliprasath.A[3], Gokulnath.D[4], Saravanan.S[5]

[1]Assistant Professor, Department of Information Technology,
Sri Manakula Vinayagar Engineering College, Puducherry
[2]Assistant Professor, Department of Information Technology,
Sri Manakula Vinayagar Engineering College, Puducherry

[3]Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry
[4]Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry
[5]Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry

Abstract - *In our digital world, access to personal data has turn an item of concern, with challenging security and privacy aspects. Attacks make digital trust a top challenge in many domains. Currently rely on intermediaries for storing and sharing passenger and operation data. Blockchain will eliminate that barrier, decreasing the provider's confidence on intermediaries and enabling rapid computerized transaction processing, real-time information sharing, and minimal system maintenance. The developed solution uses Blockchain to provide digital identity as a service to help airlines share data safely and securely when passengers board connecting flights and other services like Taxi, Ticketing, Food and Beverages etc. It provides a digital verification of passenger data for airlines and other airport partners without exposing the original data. Blockchain is a shared, immutable ledger for recording the history of transactions. It promotes a new generation of transactional applications that help establish accountability and transparency. Blockchain provides an incompatible level of accountability for how data is handled based on its tamper resistant data store and its consensus mechanism used to modify the data. Blockchain uses cryptography to support transaction confidentiality along with access controls to prevent unauthorized user access. Blockchain's replicated ledgers, shared and synchronized among multiple independent parties, are fit for the seamless journey.*

***Key Words*: Blockchain, Identity management, Immutable, Digital Identity, Auto revoke.**

1.INTRODUCTION

Blockchain assures to resolve current issues of trust, security, control, and transparency in a complex ecosystem of industry players. Blockchain is the fast emerging among airports and airlines as the priority technology for making the travel experience more efficient and it creates a transparent, accurate, and reliable leger for digital transactions that allow airlines to perform operations and tasks more efficiently. With traditional record keeping, information can be isolated, not verifiable, and quickly outdated. These features make the data untrustworthy and clearly not perceptive. Using blockchain, it offers the opportunity to raise the level of accountability and insight in the data and helps to prove compliance against specific regulations. The decentralized computer system captures, encrypts, and time stamps each transaction made by any member of the network, and then packages the transactions into data blocks that are continuously recorded in a shared digital ledger.

The blockchain-based application exhibits real-time data on a shared ledger with all participating parties. A consensus mechanism guarantees that all parties agree to any changes and updates made to the ledger. Since all members of the network hold the same version of the ledger at all times, and the records can't be altered, blockchain builds trust among network members without the need for the third-party intermediaries that many value chains rely on.

The Firebase cloud is used to store the original data and other metadata of the user in the cloud, for verification process through the application and also the storing of personal data in the blockchain is not advisable because for example, the address of the user or person is stored in the blockchain once the data is stored in the blockchain it can't involve any changes further due to its immutability property.

2. IDENTITY MANAGEMENT USING BLOCKCHAIN

In the section below, different types of identity management are discussed.

2.1 Data SILO's

[17] SILO Organizational silos typically don't share an equivalent priorities, goals or maybe an equivalent tools, so departments operate as individual business units or entities within the enterprise.

Silos occur due to how a corporation is structured. Managers are liable for one specific department within a

corporation and every manager has different priorities, responsibilities and vision. Often, managers aren't conscious of the priorities and goals of other departments and there's little communication, collaboration and teamwork between these business units.

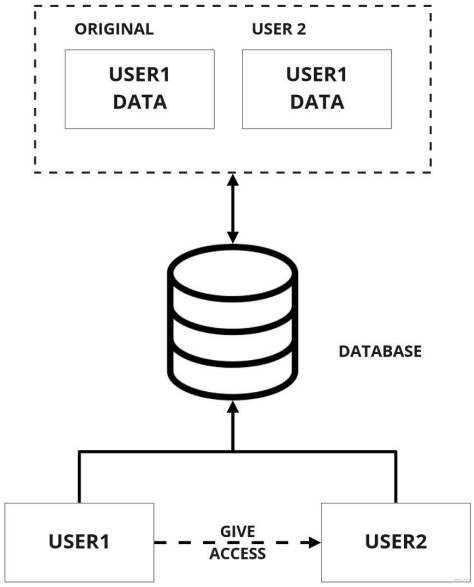

Figure 1:

The silos mentality is basically an organizational way of thinking. It occurs when departments or management groups don't share information, goals, tools, priorities and processes with other departments. The silo mentality is believed to impact operations, reduce employee morale and should contribute to the general failure of a corporation or its products and culture. Today, managers are tasked with breaking the silo mentality to make sure information flows freely between all departments in a corporation. Where the replicas of the data in silos are higher and also wastage of resources.

2.2 Graph database

[18] A graph approach to Identity Management, Handle organizational changes easily in one place and have them automatically affect your entire organization and its systems. It defines all the user, entities and partners using the fully connected graph with metadata models. The Graph based database also involves employers, partners, consumers, suppliers, and external services and resources to have the secure management of the enterprise or the individual data in the graph database. It creates directories of any size greater than the lakhs and lakhs of user and entities for maintaining the directories of users the graph structure responsive scale. It helps in creating complex, fully-connected, data access control structures, approval chains structures. It Build and maintain any combination of ordered and unordered user and enterprises and organizational approved access structures. Even with enormous, highly-connected Identity Management datasets of entities and resources, Neo4j's native-graph query engine traverses millions of relationships per second to maintain application performance and user productivity. It can allow you to query relationships in any direction, you can use it to perform a variety of top-down and bottom-up with faster retrial of data from the graph. The queries like, application which are accessible by an user, does the specific group of user is allowed to access the application, and also it can what are the resources or data are managed or governed by the user, enterprise and organisation. It can identify which user can access the resources and which user can change the settings. The graph-based identity management solution has higher performance and it requires relational approaches into millisecond response times. Such speed makes graph-based Identity Management particularly applicable for applications with large resources, including social networks, customer portals, content management, document systems and federated services.

3. Proposed Method

The proposed method will help the user to have personal data access control in the digital world. The user can give consent to any user using the public key if each and every user is considered as a node in the network or the user will have a particular signature or hash value to uniquely identify the user in the network and the access rights is given.

The user can define which data to share and to whom can be shared and the time period for accessing the user data once the time reaches the limit the access will be revoked automatically.

The key or unique hash value is shared in QR format with some encryption, once the QR is scanned the public key is decrypted and filled in the appropriate field in web or android application.

If the user is sharing the data to one of the users or partners like a ticket booking agent, the application will pre process that the agent is a valid or not.

The first and foremost step is to set up the user data using the validator nodes which may be the Government organization or Working organization. The user will create a transaction using the name and a unique id's may be Aadhar, license which is used for the organization to identify the requestor uniquely.

Then the validator send the additional data about the requestor as a signed transaction. The transaction data is accessed through the web3 API, the hashed data is decoded then stored in the cloud because as mentioned in the given problem statement the user data is not to be stored in the blockchain so we store the data in the firebase cloud.

In the process of verification of the identity the hash value is came into account, that is the hashed data is given access

to the airport partner of airport checking services so that we can verify the hashed data instead of using the original data.

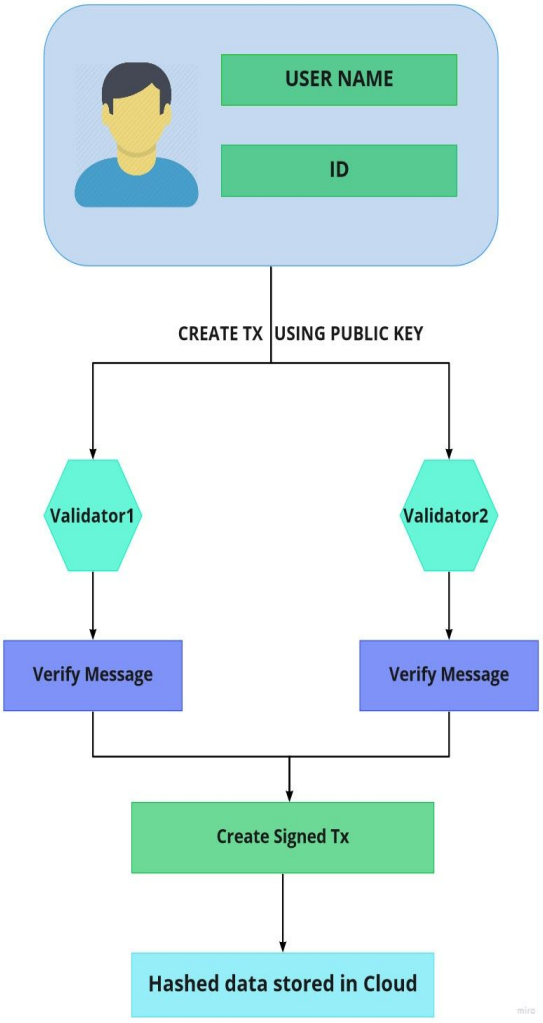

Figure1: Creating a wallet in Blockchain

The figure 2 explains the grant and revoke access to the airport, airport partner, F&B and taxies etc. The first step is to setup the user data from the validator, the user has to upload the keystore.txt file which stores the public address of the ethereum node which may be the airport, airport partner etc.

Then the access permission is defined in the transaction and an authentication ID is given to the viewer of the data, When the transaction and auth key is generated the viewer is validated by the authID which is given to the viewer (i.e) airport, airport partners.

When you enter the airport you have to verify the identity with the airport so that you can use the hash value instead of the original data. So on that process of verification or authentication data value is shared to airport or airport partners.

Whenever you grant permission to a specific address there is another option to revoke the access from the airport or airport partner. You can specify the time period

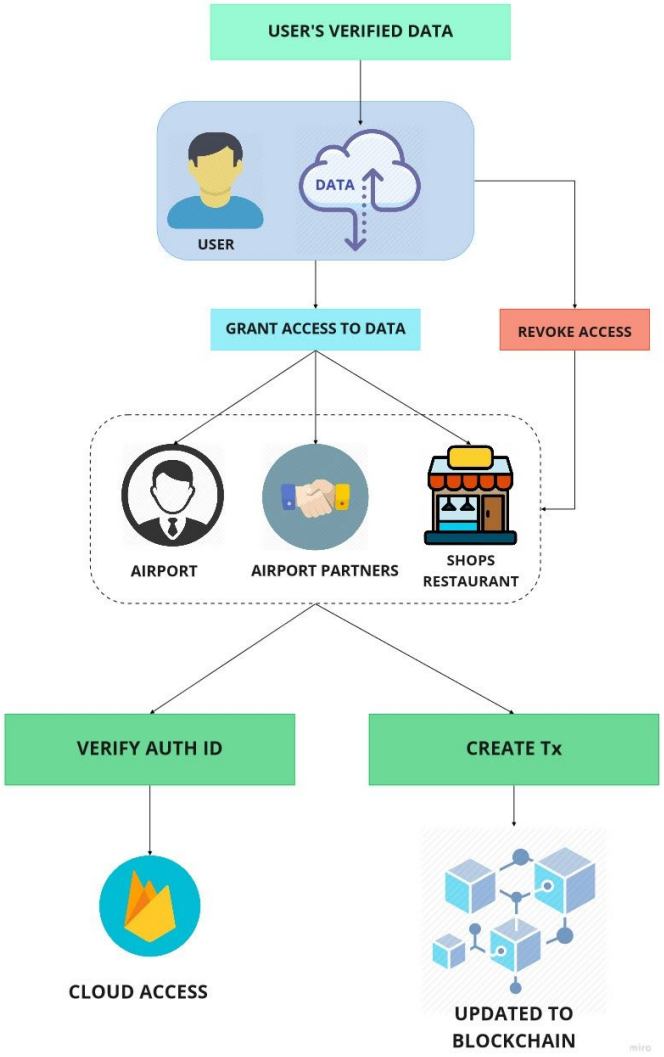

Figure 2: Give consent to the user data and revoke access

to access your data so that no longer the airport or airport partner can't view your data after that period of time.

REFERENCES

[1] Identity Management Schemes on the Blockchain ,Paul Dunphy and Fabien A.P. Petitcolas https://www.computer.org/csdl/magazine/sp/2018/04/msp2018040020/13rRUILtJpk

[2] Blockchain for Identity Management by Ori Jacobovitz

[3] An Identity Management System Based on Blockchain Yuan Liu, Zheng Zhao, Guibing Guo, Xingwei Wang, Zhenhua Tan, Shuang Wang Software Colledge Northeastern University Shen Yang.

[4] A Blockchain-based Personal Data and Identity Management System Benedict Faber, Georg Michelet1, Niklas Weidmann1, Raghava Rao Mukkamala, Ravi Vatrapu1,2 1Centre for Business Data Analytics, Copenhagen Business School, Denmark 2Department of Technology, Kristiania University College, Oslo, Norway

[6] Blockchain Identity Management System Based on Public Identities Ledger, Sead Muftic, Rockville.

[7] Integrating Blockchain for Data Sharing and Collaboration Healthcare Applications Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu, Danyi Li1y, Institute of Information Engineering, Chinese Academy of Sciences.

[8] J. H. Clippinger, "Why Self-Sovereignty Matters," https://idcubed.org/chapter-2-self-sovereignty-matters/, [Online; accessed7-March-2017].

[9] Weimin Luo, Jingbo Liu, Jiang Xiong, and Ling Wang. Defending against whitewashing attacks in peer-to-peer file-sharing networks. In Proceedings of the 4th International Conference on Computer Engineering and Networks, pages 1087–1094, 2015.

[10] G. D. P. Regulation, "Regulation (eu) 2016/679 - directive 95/46," Official Journal of the European Union (OJ), vol. 59, pp. 1–88, 2016.

[11] C. Tankard, "What the gdpr means for businesses," Network Security, vol. 2016, no. 6, pp. 5–8, 2016.

[12]J. Carter and M. N. Wegman, "Universal classes of hash functions," Journal of Computer and System Sciences, vol. 18, no. 2, pp. 143 – 154, 1979.

[13] N. Kaaniche and M. Laurent, "A blockchain-based data usage auditing architecture with enhanced privacy and availability," in Network Computing and Applications (NCA), 2017 IEEE 16th International Symposium on, pp. 1–5, IEEE, 2017.

[14] A. Yasin and L. Liu, "An online identity and smart contract management system," in Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual, vol. 2, pp. 192–198, IEEE, 2016.

[15] Fromknecht, C., et al., "A Decentralized Public Key Infrastructure with Identity Retention', MIT, Class 6,857 Project, Nov. 11, 2014.

[16] Fromknecht, C., et al., "CertCoin: A Namecoin based decentralized Authentication System', MIT. Class 6.857 Project, May 14, 2014.

[17] What is an Information Silo (IT Silo)? Webopedia Definitionwww.webopedia.com/TERM/information_silohttps://www.webopedia.com/TERM/I/information_silo.html

[18] Graph Databases for Identity Neo4j Graph DatabasePlatformhttps://neo4j.com/business-edge/identity-and-access-management/