EMBEDDING A BLOCKCHAIN TECHNOLOGY PATTERN INTO THE QR CODE FOR A DIGITAL IDENTITY MANAGEMENT

Ms.M. Sasikala Computer Science and Engineering & Dhirajlal Gandhi College of Technology
Ms.N. Akshiya Computer Science and Engineering & Dhirajlal Gandhi College of Technology
Mr.LG. Dharanish Computer Science and Engineering & Dhirajlal Gandhi College of Technology
Mr.M. Koodalingam Computer Science and Engineering & Dhirajlal Gandhi College of Technology

---***---

Abstract - The traditional identity systems of today are fragmented, insecure, and exclusive. Blockchain enables more secure management and storage of digital identities by providing unified, interoperable, and tamper-proof infrastructure with key benefits to enterprises, users, and IOT management systems. The term 'Blockchain' actually means a block of data that has been recorded over a certain amount of time and is grouped and cryptographically linked to a previous set of data forming a chain of events. It enhances trust across a business network. All events which occurred on the blockchain, are recorded on a distributed ledger. Thus the blockchain works by providing a way to track and transfer data that is transparent, safe, auditable, and resistant to outages. In this technology, there is no central authority verification needed for settlements hence making the process faster and cheaper.

Key Words: Blockchain, IOT, cryptography, interoperable

1. INTRODUCTION

The digital identity authentication ensures that the verification of subject and protection of sensitive information is the key component of trustworthiness in the identity management. Users have to exchange their personal information with organizations in exchange of services. To overcome stealing, misusing or manipulating these data in central approach, services providers are required to provide many factor authentications along with management of identities which further complicates the systems. Besides central approach, federated instances provides access to multiple sites with same credentials. However, the control and ownership of data still remains in the hand of identity service provider. The contemporary approaches in identity management challenge the designers for expert security reviews and usability analyses concerning user experience and interaction with active agents in the identity infrastructure. The recent work to eliminate the central service providers is one unique digital identity that is build, managed and controlled by identity owner. Such identity that provides user centric data ownership is called self-sovereign identity.

2. Body of Paper

Existing System : store our most valuable information on centralized government databases with numerous single points of failure. A recent study shows that personally identifiable information is the most targeted data for breaches, comprising 97% of all breaches in 2018.From security perspective, solutions and regulations are developed and already concerning personal data. The exchange of information between communication agents is ambiguous and hard to keep track of what data is shared as compare to actual granted access. The anonymity of identity is affected by degree of link-ability of personal data. As digital identity is compartmentalized into different context (personal identifiable information (PII), non-PII), It is important to provide selective disclosure of (PII) and track PII to overcome issues of personal data privacy.

Proposed System: Blockchain identity management systems could be used to eradicate current identity management system. The decentralized identifier(DID)is a pseudo-anonymous identifier created for a person, company, object, etc. Each DID is secured by a private key. The private key owner can prove that they own or control their identity. Each DID is often associated with a series of credentials(verifiable credentials)that attest to specific characteristics of that DID (e.g., Name, DOB, Address, License Number). Once paired with a decentralized identity, users can present the verified identifier in the form of a QR code to prove their identity and access certain serv m,v ices. The service provider verifies the identity by verifying the proof of control or ownership of the presented attestation — the attestation had been associated with a DID and the user signs the presentation with the private key belonging to that DID. If they match, access is granted. The employee accesses the different information they need to follow up on their leave. They can also submit a leave request. The leave management module administrator can use this page, with each employee profile, to add or delete leave entries for each employee. The leave entitlement status table gives the calculation for each type of leave. It provides a quick view of the leave days earned, days requested, days taken and the balance, including the intended period for each type of leave. Supervisors can track, approve or reject absences submitted by their team members. This is the process approval step. If on leave themselves, a manager can delegate another company employee to validate leave requests submitted by their team members. This is one of the many advantages of our leave management software. A table lists all leave requests pending validation. For each entry, the manager can mention the reasons for their decision. Leave requests can be approved by the manager, the director (manager's manager) or any other employee designated in the configuration. Note that you can define up to 5 approval levels in the workflow with the possibility of having several approvers at each level. The HR manager (or any other person entitled to administrate the leave module) can generate an absence report at any point for any period of time. It is possible to filter the report per employee category, per location, per team and per employee. To facilitate human resources management, the person in charge can also export this report in an XML format file, immediately usable in Excel (or any other spreadsheet software compatible with the XML format). As a result, the data is consolidated and can be easily used for payroll processing. If payroll management is outsourced, the HR department can share this file with the accounting firm in charge of payroll processing.

3. CONCLUSIONS

Thus the blockchain technology was used in the implementation of secured Identity Management Application using Blockchain. It allows for users to create and manage digital identities through the combination of the following components:Decentralized identifiers, Identity management, Embedded encryption . In this technique, there is no chance to make a crypto fraud/attack and hence it eliminates the human inter mediatory. Also it offers the following benefits: Decentralized Public Key Infrastructure (DPKI) Decentralized Storage Manageability and Control. The proposed model is executed in a complete distributed mode where transactions are validated, approved, and recorded (stored in all databases) by all the peers in the blockchain rather than storing it in one central database. Hence, it outperforms the traditional centralized identity management in the perspective of information security. In the proposed model, all the participants' nodes are connected to each other and no one can modify the data in the chain so as to ensure the safety of the identity related data. Moreover, blockchain is a solution for trusted digital record since once it has been recorded; it can be accessed and checked the identity authentication any time.

FUTURE ENHANCEMENTS

It is the concept that people and businesses can store their own identity data on their own devices; choosing which pieces of information to share to validators without relying on a central repository of identity data. These identities could be created independent of nation-states, corporations, or global organizations.

REFERENCES

1. Pilkington, M., Blockchain technology: principles and applications, Research Handbook on Digital Transformations, University of Burgundy, France, 2016
2. M. Sharples and J. Domingue, "The blockchain and kudos: a distributed system for educational record, reputation and reward", Proceedings of 11th European Conference on Technology Enhanced Learning (ECTEL), Lyon, France, 2015, pp.490-496.
3. Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin", Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp.184-191.
4. R. Khan et al., "Blockchain based land registry system using Ethereum Blockchain", Journal of Xi'an University of Architecture & Technology, Xi'an University of Architecture & Technology, China, 2020, pp. 3640-3648.
5. V. L. Lemieux, "Trusting records: is Blockchain technology the answer?", Records Management Journal, Emerald Group Publishing Limited, Bingley, UK, 2016, pp. 110- 139.
6. Y. Liu et al., "Blockchain-based identity management systems: A review", Journal of Network and Computer Applications, Elsevier Ltd., 2020, pp.1-11.
7. M. Kuperberg et al., "Blockchain Usage for Government-Issued Electronic IDs: A Survey", Advanced Information Systems Engineering Workshops, Springer Nature Switzerland, 2019, pp. 155-167.
8. K. Mudliar et al., "A comprehensive integration of national identity with blockchain technology", International Conference on Communication information and Computing Technology (ICCICT), IEEE, Mumbai, India, 2018, pp. 1-6.
9. R. Rivera, et al., "How digital identity on blockchain can contribute in a smart city environment," International Smart Cities Conference (ISC2), Wuxi, 2017, pp. 1-4.
10. Xavier, O. F. and Majlinda, Z., Research Handbook on Digital Transformation, Edward, Elgar publishing, Cheltenham, UK and Northampton, MA, USA.