Advances in Aeronautical Science and Engineering
ISSN: 1674-8190

A Secure Biometric Authentication System Using Blockchain and Decentralized Identifiers

Dr. Sofia Ivanova[1], Mr. Alexander Petrov[2], Ms. Elena Kuznetsova[3] & Mr. Dmitri Novikov[4]
[1] Department of Computer Science, University of St. Petersburg, Russia
[2] Department of Computer Engineering, University of Warsaw, Poland
[3] Department of Information Technology, University of Belgrade, Serbia
[4] Department of Computer Applications, University of Sofia, Bulgaria

ABSTRACT

Most user authentication methods rely on centralized database. If this system is compromised it poses a direct threat to users' identities. This paper proposes a decentralized authentication method, implemented using Hyperledger Indy. It is based on Decentralized Identifiers (DIDs) and the concept of self-sovereign identity. We propose the implementation of biometric storage option via block chain using DIDs.

KEYWORDS: Blockchain, DID, Authentication, Biometric, Storage, Decentralized

1. INTRODUCTION

In today's world customer user profiles are available online. Such information can be used by someone to gain their financial advantages or obtain credits and benefits in other person's name. In digital world, a person's identity can be misused by someone else.

Facial recognition is the natural authority of human identity. It can prevent attacks, spoofing etc. It provides prefect blend of high accuracy and ease of integration. It enables friction free customer experience. Enabling a 'Biometric Blockchain' empowers users to leverage their digital identity in a way which protects their privacy by giving them the power to verify important transactions or interactions.

Digital transactions are made more secure and versatile. In face recognition we establish feature identifiers and compare them with those images enrolled by user, to determine a match. When a match found, our system will create a face template without taking person's actual identity. A digital identity is created by converting the identifiers into a unique and random string of numbers. Once the template is created, the original image can be discarded. In blockchain technology there is no central entity controlling the identities where we can request a new identity, as each user has unique identity. It can't be stolen or used by others.

Hyperledger Indy is used to attain the self sovereign features. It provides a distributed ledger for decentralized identity. For each user, it provides unique DID's, these ID's are resolvable without requiring any centralized resolution authority. It creates a pair wise identifiers, 1:1 relationship between entities. It implements Zero Knowledge Proofs, which prove that some or all data in the set is true without revealing any additional information.

Digital transactions are made more secure and versatile. In face recognition we establish feature identifiers and compare them with those images enrolled by user, to determine a match. When a match found, our system will create a face template without taking person's actual identity. A digital identity is created by converting the identifiers into a unique and random string of numbers. Once the template is created, the original image can be discarded.

2. METHODOLOGY

Most of the current authentication system is based on centralized database for storing the data. It is used as the mechanism, to identify users. The user's identity data are stored in a centralized database. When user submits the documents, authenticator compares the stored value with the submitted document. If they match, the user is provided access. Everyone should provide something to prove their identity for their daily needs such as getting gas, water, etc. Even if some of the authentication system were biometric systems, most of the deployed systems still use the same centralized model.

In traditional system, the identity is given by some of the authorized person such as issuer (or government).The issuer provides a unique identity to each person. When it is provided as a proof, the verifier will check the match with the data stored in the database[1].Information are not stored securely in a centralized database, any fraud can stole data for their own personal needs. By implementing blockchain technology using DIDs , these data

will be safe. No-one will be able to access others data without their knowledge. Each user is assigned with some unique ID's to identify himself [2]. When the user needs any authentication from a third party to access any information they can provide the DID's , instead of providing the whole documents they own[3]. With these ID, user can store their unique data in blockchain. It is robust to system failure and hacking [4].

In this paper, we discuss the specification and implementation of our protocol that uses the decentralized self-sovereign identity [5]. It allows the end users to have the control of accessing their identity by giving consent to the verification process. This protocol provides the following advantages to the user.
1) Control: User can control the storage and access to their identity. Using self-sovereign approach user can hide their data along with biometric capability.
2) Security: It is highly secure because some cryptographic techniques are used to store information.
The proposed system passes through the following phases as depicted in Fig.1:
1) Collection: The first step is to collect data to train the model. A set of images are taken to capture different features of a person.
2) Storage: Data are stored by using some cryptographic method. SHA 256 and MD5 is toused for encryption. Double encryption is used to provide more accurate result. The data are first encrypted with SHA256 and then the encrypted data is again encrypted using the other algorithm.
3)
4) Processing: The Data captured is compared with the one stored in database. It is done at the time of image capture.

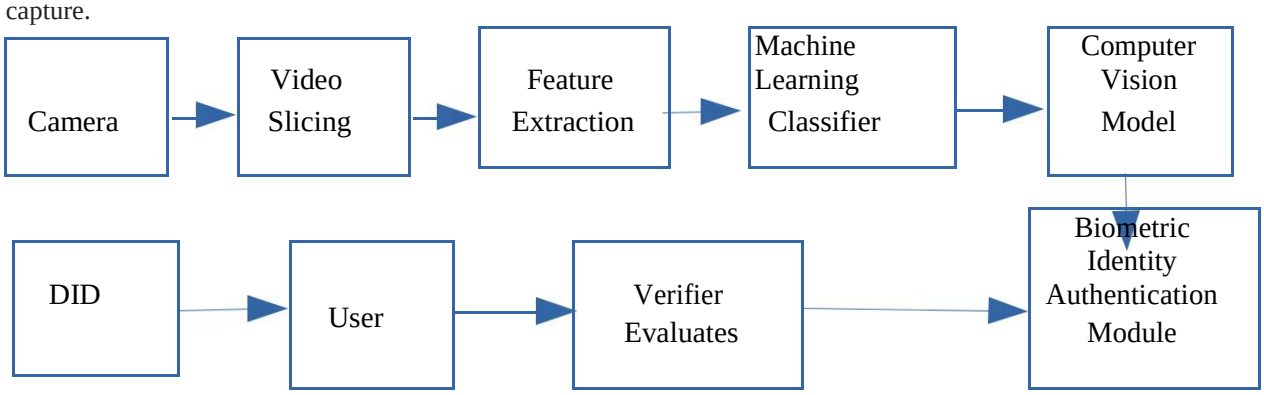

Fig.1 Workflow of the proposed system

Videos are taken through the laptop camera. Then the features are extracted by applying machine learning classifier. Then it is stored in the blockchain. A unique ID is provided to every user. Services are provided to the user after verifying the DID.

3. RESULTS AND DISCUSSION

Instead of any centralized database, users can store data in blockchain that helps to avoid identity theft and identity misuse. Each user can access the document with their own unique ID's. It provides more security. This method can be used to replace Aadhar authentication system. Aadhar details are stored by a centralized system. Nowadays it is used as a mean for every user needs such as mobile connection, bank account creation, acquiring gas connection etc.. In that system ID can be used to ensure one's identity. It is still with a third party, if the third party is corrupted then data can be misused. In order to avoid misuse of personal details by third party the proposed method can be implemented. The new system can be used in office to ensure the details of employees without any written document. It can be used for digital transactions and for attendance registration in companies. It canbe used with the authentication of login account of Google, Facebook and other social media.

4. CONCLUSION

The main contribution of this paper is to avoid centralized system for user authentication. It introduces a decentralized storage structure. It mainly ensures the security of users' data. Users' are given unique ID's. Users' authentication can be done using the data stored in blockchain. It can be used anywhere to authenticate a person.

REFERENCES

[1] Zheng Z, Xie S, Dai H, et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends[C]. IEEE International Congress on Big Data. IEEE, 2017.

[2] Croman K, Decker C, Eyal I, et al. On scaling decentralized blockchains[C]. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016: 106-125.
[3] Sel M, Diedrich H, Demeester S, et al. How Smart Contracts Can Implement 'Report Once'[J]. Social Science Electronic Publishing, 2017, 25(4): 993-101
[4] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery[J]. Acm Transactions on Computer Systems, 2002, 20(4):398-461.
[5] G Wood, Ethereum: A Secure decentralized generalised transaction ledger, Ethereum Project Yellow Paper 151