ABSTRACT

In any registration process, it is a hassle to always bring physical documents. Not only that, the process is elongated if they are lost, and will contribute to identity theft if unauthorized persons have access to those documents. Therefore, the objective of this paper is to generate a decentralized system, similar to the concept of blockchain, to allow registered persons to access user's personal records. To further elaborate, this system is designed to be used by three consumers, which are: user, authority, and third-party (requester). Nowadays, majority of systems are susceptible to massive data breaches. However, some researches have theorized that blockchain technology may solve this problem, such as one that uses a real-world example, Aadhaar. In conclusion, this project enhances that the area of blockchain identity is vital in helping society gain control of their personal details. Since most of researches are focused on storage system of businesses using blockchain, personal identities of the people should be digitized on the blockchain as well. An identity verification system that is entirely owned by the individual will increase trust that the data is genuine and reliable.

CONTENTS

INTRODUCTION

The crime of identity theft, an unauthorized access to a person's personal information, has impacted many people especially in the recent years and the numbers increase yearly. According to Javelin Strategy & Research [1], there were approximately one in 15 people likely to be a victim of identity theft in 2017 just in the United States (US). Therefore, having a system which can help consumers in monitoring access to private data would be very beneficial. In this paper, a system called Blockchain-based Identity Verification System is proposed whereby it is a system which stores an individual's personal records on the blockchain. This system uses the security features of blockchain to allow everyone to know who has access to their data. As such, the new system will have three types of consumers, which are: user, authority, and third-party (requester). The user is able to allow third-party to access data and also view list of requesters; the authority is able to upload user's personal records on the blockchain, and verify companies who would like to be registered requesters; and the third-party is able to send request to view data of user. Blockchain is a decentralized database consisting of blocks connected by a hash number. Each block has an address which records ownership and is continuously updated after being verified. Decentralized means that blockchain is a distributed ledger and the information can be viewed and altered by anyone if it is verified by the parties involved [2]. The problems identified in the current traditional system of verifying identities are as such: firstly, paper-based personal records are bulky to store while also posing a safety risk [3]. Secondly, a person has no control over their personal information kept in a distributed database which may lead to identity theft and misuse of data [4], [5]. This system is assumed to be used as a storage system for an individual's personal information, and that they will be accessed by others to verify identity during registration processes. The identity verified using this system would be considered as authentic, with no further verification needed.

LITERATURE SURVEY

I. Shaik Arshiya, B. Aruna, P. Guru Prasad, Ravi Kumar Tenali, "Steganography Security On Bank System" ISSN: 2277-3878, Volume-8, Issue-1, May 2019. They developing an application based on security as the rate of internet users are increasing and most of the users either use internet for money transaction and social media the rate of cybercrime is increasing rapidly and there is a need to secure bank system to prevent customer from cybercrime [1] . we have developed a three-tier architecture in which the concept of image steganography is inspired from google which checks whether it's a human or robot and all the data is applied with encryption and decryption. The customer needs to provide the details during the registration process and the images will be also selected during the time of registration and during the transaction process to be done based on the images selected the admin provides steganography[5] on the given images and the user need to select the original image and if the image that is applied is correct then the puzzle is set up with mathematical expression and user further continues with the following transaction process by generating his one-time password (OTP) and transaction is successful.

EXISTING SYSTEM

The problems identified in the current traditional system of verifying identities are as such: firstly, paper-based personal records are bulky to store while also posing a safety risk [3]. Secondly, a person has no control over their personal information kept in a distributed database which may lead to identity theft and misuse of data [4], [5].

Disadvantages:

1. The process is elongated if they are lost
2. Which may lead to identity theft and misuse of data

PROPOSED SYSTEM

In this paper, a system called Blockchain-based Identity Verification System is proposed whereby it is a system which stores an individual's personal records on the blockchain. This system uses the security features of blockchain to allow everyone to know who has access to their data.

Advantages

1. This project enhances that the area of blockchain identity is vital in helping society gain control of their personal details.
2. An identity verification system that is entirely owned by the individual will increase trust that the data is genuine and reliable.

SYSTEM ARCHITECTURE

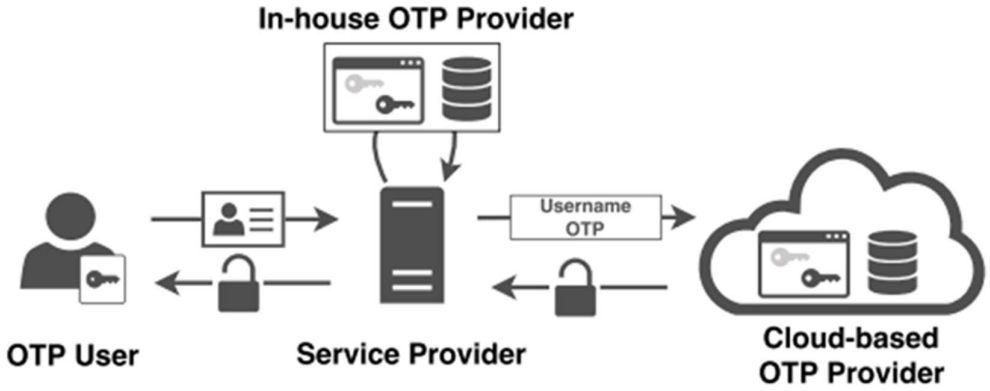

Fig.1: System architecture

SYSTEM REQUIREMENT SPECIFICATION

The following are the hardware and software requirements that have used to implement the proposed system

Hardware Requirements

1. Operating System: Windows Only
2. Processor: i5 and above
3. Ram: 4gb and above
4. Hard Disk: 50 GB

Software Requirement

1. Visual Studio Community Version
2. Nodejs (Version 12.3.1)
3. Python IDEL (Python 3.7)

CONCLUSION

In conclusion, this paper discussed about how a system which enhances the area of blockchain identity is vital in helping the society to gain control of their lives. Since most of researches are focused on storage system of businesses using blockchain, personal identities of the people should be digitized on the blockchain as well. Financial and medical should not be the only emphasis for blockchain-based systems, because eventually every physical data will move on to digitalization. In addition, the main benefits of research in this area will allow users to own as well as control their identity by placing it in a decentralized system to avoid data breaches by applications and services. An identity verification system that is entirely owned by the individual will increase trust that the data is genuine and reliable. It will also help that this system is open and transparent.

REFERENCES

1. Adams and A. M. Sasse, “Users are not the enemy”, Commun. ACM, vol. 42, pp. 40-46, Apr. 1999.
2. D. Wang, Z. Zhang, P. Wang, J. Yan and X. Huang, “Targeted online password guessing: An underestimated threat”, Proc. ACM SIGSAC Conf. Comput. Commun. Secur., pp. 1242-1254, 2016.
3. L. Zhuang, F. Zhou and J. D. Tygar, “Keyboard acoustic emanations revisited”, ACM Trans. Inf. Syst. Secur., vol. 13, no. 1, pp. 3:1-3:26, Nov. 2009, [online] Available: http://doi.acm.org/10.1145/1609956.1609959.
4. T. Zhu, Q. Ma, S. Zhang and Y. Liu, “Context-free attacks using keyboard acoustic emanations”, Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), pp. 453-464, 2014, [online] Available: http://doi.acm.org/10.1145/2660267.2660296.
5. H. Tanaka, O. Takizawa and A. Yamamura, “A trial of the interception of display image using emanation of electromagnetic wave”, J. Nat. Inst. Inf. Commun. Technol., vol. 52, no. 2, pp. 147-155, 2005.
6. L. Cai and H. Chen, “TouchLogger: Inferring keystrokes on touch screen from smartphone motion”, HotSec, vol. 11, pp. 9, Aug. 2011.
7. R. M. Bolle, J. H. Connell and N. K. Ratha, “Biometric perils and patches”, Pattern Recognit., vol. 35, no. 12, pp. 2727-2738, 2002.
8. A. T. B. Jin, D. N. C. Ling and A. Goh, “BioHashing: Two factor authentication featuring fingerprint data and 10okenized random number”, Pattern Recognit., vol. 37, no. 11, pp. 2245-2255, Apr. 2004.
9. S. H. Khan, M. A. Akbar, F. Shahzad, M. Farooq and Z. Khan, “Secure biometric template generation for multi-factor authentication”, Pattern Recognit., vol. 48, no. 2, pp. 458-472, 2015.
10. N. Haller, C. Metz, P. J. Nesser and M. Straw, A One-Time Password System, Fremont, CA, USA, 1998, [online] Available: https://www.ietf.org/rfc/rfc2289.txt.
11. D. M’Raihi, M. Bellare, F. Hoornaert, D. Naccache and O. Ranen, HOTP: An HMAC-Based One-Time Password Algorithm, Fremont, CA, USA, 2005, [online] Available: https://www.ietf.org/rfc/rfc4226.txt.
12. D. M’Raihi, S. Machani, M. Pei and J. Rydell, TOTP: Time-Based One-Time Password Algorithm, Fremont, CA, USA, 2011, [online] Available: https://www.ietf.org/rfc/rfc6238.txt.
13. I. Ion, R. Reeder and S. Consolvo, “ ‘ \$ldots \$ no one can hack my mind’: Comparing expert and non-expert security practices “, Proc. 11th Symp. Usable Privacy Secur. (SOUPS), pp. 327-346, 2015, Available: https://www.usenix.org/conference/soups2015/proceedings/presentation/ion.