International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

SECURING AADHAAR DETAILS USING BLOCKCHAIN

E. Poonguzhali[1], R.Saravanan[2], V.S.Prrasanthi[3], P.Sowmyadevi[4]

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

---

Abstract - *Aadhaar is the world's largest unique identification system that holds records of over 1.19 billion Indian residents. Aadhaar collects name, date of birth, gender, address, mobile/email (optional) of residents of India and stores them against the corresponding biometric data. Now as per government rules, this information is linked with users all banks, voter Id, PAN card etc. Imagine if all this user information is leaked or used for bogus purposes by the government. We can't deny that majority of Government officers are corrupted and won't mind manipulation of citizens' information for some extra income. However they're still involved in handling all information and knowledge of Indian citizen, which they will use for anything anytime. Hence it is necessary that in each field in government sectors, only the required and specified information alone must be available to them, rather than revealing all the details of a particular person that may be unnecessary for that specified sector. This can be achieved by applying blockchain technology in Aadhaar cards. The objective of applying Blockchain concept is, since blockchain represents a distributed system, the data once stored is stored forever and cannot be tampered since in a distributed system any modification made is viewed by peers and the validity of entry is checked by everyone in it. Also, the viewing of all details including the details that are meant to be kept private will be hidden from others with the help of using public key and private key concepts. By doing so, a specified sector can view only specific details and it can prevent the wrong usage of other details that are additionally available. It can prevent the modification of data for malicious purposes by any unauthenticated users. This can increase the data security level in government sectors making the private details of people unavailable to everyone.*

***Key Words*: Blockchain Technology, Aadhaar Card, Private Data, Distributed, Unauthenticated Users.**

1. INTRODUCTION

The Aadhaar project is the world's largest national identity project, launched by government of India, which seeks to gather biometric and demographic data of residents and store these during a centralised database. To date, 1036 million users have enrolled within the system, and therefore the government has spent a minimum of 890 million USD on the project. However, recently there has been considerable deliberations over the privacy and security issues associated with the Aadhaar project.

Aadhaar is a 12-digit unique identity number which will be obtained by residents of India, supported their biometric and demographic data. The data is assembled by a statutory authority, the Unique Identification Authority of India (UIDAI). Aadhaar is the world's largest biometric ID system. The detailed personal information being collected is of extremely high importance to a personal. Major financial transactions are linked with information collected in Aadhaar. Data leaks are a gold mine for criminals.

The UIDAI confirms more than 200 government websites were publicly displaying confidential Aadhaar data; though removed now, the data leaked cannot be scrubbed from hackers' databases. Those confidential aadhaar details are stored in a single database and it is maintained by UIDAI. Since the database is centralized there are so many disadvantages. The main disadvantage is that the security threat. If those data are stored in blockchain, data vulnerability will be reduced.

2. LITERATURE SURVEY

Since its inception[1], the blockchain technology has shown promising application prospects. From the initial crypto currency to the current smart contract, blockchain has been applied to many _elds. Although there are some studies on the safety and privacy problems with blockchain, there lacks a scientific examination on the safety of blockchain systems. In this paper, we conduct a scientific study on the safety threats to blockchain and survey the corresponding real attacks by examining popular blockchain systems. We also evaluate the safety improved solutions for blockchain, which might be utilized within the event of varied blockchain systems, and suggest some future directions to stir research efforts into this area.

The blockchain technology[2], witnessed a wide adoption and a swift growth in recent years. This ingenious distributed peer-to-peer design attracted many businesses and solicited several communities far off the financial market. There also are multiple use cases built around its ecosystem. However, this backbone introduced tons of speculation and has been criticized by several researchers. Moreover, the shortage of legislations perceived tons of attention. In this paper, we are concerned in analyzing blockchain networks and their development, focusinon their security challenges. We took a holistic approach to hide the

involved mechanisms and therefore the limitations of Bitcoin, Ethereum and Hyperledger networks. We expose also many possible attacks and assess some countermeasures to discourage vulnerabilities on the network. For occasion, we simulated the bulk and therefore the re-entrancy attacks. The purpose of this paper is to guage Blockchain security summarizing its current state. Thoroughly showing threatening flaws, we aren't concerned with favoring any particular blockchain network.

With the advancement[3] of technology in modern era everything needs to be digitalized to make it more secure and reliable. Nowadays birth certificate is the just age proof of an individual and can be used to apply for a job, for admissions in collages/universities and basis of all the important government document identities like Aadhar card, Pan Card, Passport and other related matters. So identifying the right certificate of any individual may be a major challenge. In the current system, afterbirth of any individual the birth has to be registered with the concerned local authorities within 21 days of its occurrence, then it should be filled up the form prescribed by the Registrar and then Birth Certificate is issued after verification with the actual records of the concerned hospital. However, current methodology used for birth certificate verification is costly and very time-consuming. Therefore, our objective is to propose a theoretical model for issuing birth certificate and verification of genuine birth records using blockchain technology. This technology uses several functions including hash, public/private key cryptography, digital signatures, peer-to-peer networks and proof of work. So in this paper we have developed an efficient and more secure way of storing birth certificate by using Inter Planetary File System (IPFS) and most demanded “blockchain” technology.

Frequent cases of personal[4] data leakage has brought back into the focus the security issues with the different identity sharing mechanisms. A customer is predicted to supply his identity for the authentication by different agencies. The KYC procedures which are used by the banks is completely dependent on the encryption which is slow and it can lead to the loss of customer details to other theirs party financial institutions. This system can be efficient by using the Blockchain technology, which has the potential to automate a lot of manual process and it is also resistant to hacks of any sort. The immutable blockchain block and its distributed ledger is that the perfect complement to the opaque process of KYC. With the addition of the smart contacts fraud detection can be automated. For KYC identity details storage, the banks can develop a shared private blockchain within the bank premise and the same can be used for verifying the documents. This allows the user to get control of their sensitive documents and also makes it easier for banks to obtain the documents they need for compliance.

Blockchain Based Aadhaar[5] uses Blockchain platform for securing Aadhaar information. The system stores the Aadhaar data in a group of computers interconnected to each other. The Blockchain uses a hashing function to transform the data and produces a hash code. The hash code ensures the identity of user is kept secure. The data is stored in blocks within the nodes. The system also uses Ethereum Smart Contracts to make sure to only the authenticated data is acquired by the third parties. The Blockchain based Aadhaar uses distributed databases (decentralized databases) math and cryptography to record transactions, transactional data is secured and the data is stored in distributed small chunks and spreads across the entire network of computers, and so it is difficult to hack these systems than hacking the centralized or traditional servers.

We investigate the privacy[6] and security issues of Aadhaar from a technology opinion. Specifically, we glance over the chances of identification and authentication without consent using the Aadhaar number or biometric data, and unlawful access of Aadhaar data within the central repository. Our examination recommend that privacy protection in Aadhaar would require a) an independent third party which can play the role of an online auditor, b) study of several modern to ols and techniques from computer science, and c) strong legal and policy frameworks that can address the specifics of authentication and identification in a modern digital setting.

Blockchain technologies[7] are gaining massive momentum in the last few years. A blockchain is a shared database, consisting of a ledger of transactions. Blockchains eliminate the problem of trust that affect other databases. It enables full decentralization and independent verification. Data stored in blockchain is tamper proof. So we can store confidential data by creating private blockchain network. In this paper, we will see how to provide security for aadhaar card data.

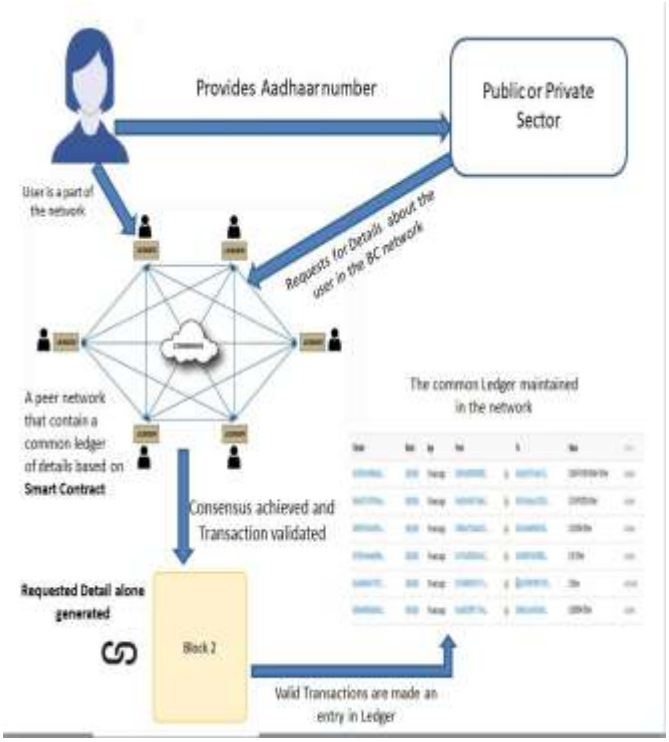
Blockchain technologies[7] are gaining massive momentum in the last few years. A blockchain may be a shared database, consisting of a ledger of transactions. Blockchains eliminates the issue of trust that affect other databases. It enables full decentralization and independent verification. Data stored in blockchain is tamper proof. So we can store confidential data by creating private blockchain network. In this paper, we will see how to provide security for aadhaar card data.

A blockchain is a decentralized[8], disseminated and digital ledger that can’t be altered retroactively without modifying every single blocks and the consensus of the network. Blockchain are often utilized in smart contracts, Banks, IoT devices, management , etc., thanks to recent times flaws and leakage of Aadhaar information (Aadhaar which is that the largest government databases of the Indian citizens) in Internet the security and privacy of Aadhaar became questionable. In order to ensure the security of Aadhaar, Blockchain has the potential to overcome security and privacy challenges in Aadhaar. In this project we are going to generate a Blockchain for Aadhaar database and implement light weight algorithm for efficiency, optimization and scalability along with the Blockchain securing algorithm.

3. PROPOSED SYSTEM

Aadhaar data is stored in a distributed manner spanning across hundreds of computers. The data obtained from the user is encrypted using Hashing Algorithm (SHA-256) which takes the input data and gives a 256-bit Hash code. This Hash code is stored in a block which is mirrored across all nodes. This hash code can be shared with third parties for verification and authentication. This prevents the misuse of Aadhaar Card Number which is linked to a number of services such as Bank account and so on. The Ethereum Smart Contracts is a computer protocol which is used to verify a contract or enforce a negotiation with a contract. The Smart Contracts work only when a certain condition is met. This technology can be used in Aadhaar system to ensure restricted access to the user's personal information. The third parties can access only part of the user data if authenticated. This also prevents the unauthorized access of user data and ensures privacy by using the Ethereum Smart Contract.

4. WORKFLOW DIAGRAM



5. CONCLUSION

Aadhaar concept of giving a unique identity to citizens to provide national security has many advantages and has made obtaining new services easier. If the security of Aadhaar is increased, it could increase the confidence of citizens in Aadhaar. The Blockchain Based Aadhaar solves the current issues plaguing the system and can ensure the security and privacy of user data. The Block Based Aadhaar ensures the ease of services provided by Aadhaar without security concerns.

REFERENCES

[1] Xiaoqi Lia, Peng Jianga, Ting Chenb, Xiapu Luoa, Qiaoyan Wenc, "A survey on the Security of the Aadhaar " (6march 2018)

[2] Joanna Moubarak, Eric Filiol, Maroun Chamoun, "On Blockchain Security and Relevant Attacks" 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)

[3] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-5S3, February 2019

[4] M. Sneha, M. Vibin, T. Krishnaprabu, Aishwarya Mohan, R. Kanmani, S. Bhuvana, "Identity Secured Sharing Using Blockchain" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-5S3, February 2019

[5] Juno Bella Gracia S V, Raghav D, Santhoshkumar R, Velprakash B, "Blockchain Based Aadhaar", (2019) 3rd International Conference on Computing and Communications Technologies(ICCCT). doi:10.1109/iccct2.2019.8824892

[6] Shweta Agrawal, Subhashis Banerjee, Subodh Sharma, "Privacy and Security of Aadhaar".

[7] Venkatasubramanian S, Swarnakamali V, Kaviya J, Vigneshwar A, "Aadhaar security through blockchain" SSRG International Journal of Computer Science and Engineering (SSRG - IJCSE) - Special Issue ICCREST Mar 2019

[8] Sankaranarayanan P.J *, Geogen George2, "Blockchain Based Aadhaar Security" International Journal of Engineering & Technology, 7 (4.6) (2018) 398-400

[9] Karl, Security of blockchain technologies, Ph.D. thesis, Swiss Federal Institute of Technology (2016).

[10] Rajvardhan Oak, Karanveer Singh Jhala, Mrunmayee Khare "Smart Collaboration Mechanism using Blockchain Technology" 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud

[11] H. Hou, "The application of blockchain technology in E-government in China," 2017 26th Int. Conf. Comput. Commun. Networks, ICCCN 2017, 2017.

[12] Safdar Hussain Shaheen, Muhammad Yousaf, Mudassar Jalil : Temper Proof Data Distribution for Universal Verifiability and Accuracy in Electoral Process Using Blockchain, IEEE Conference, 2017.

[13] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in International Conference on Principles of Security and Trust. Springer, 2017, pp. 164–186.

[14] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, 2014.