Blockchain Based Aadhaar Security System

Praveen G L
Asst.Professor,Computer Science
Mar Baselios College of Engineering and Technology
Thiruvananathapuram,India

Arpana M Chandran
Student,Computer Science
Mar Baselios College of Engineering and Technology
Thiruvananthapuram,India

Niveda S Krishna
Student,Computer Science
Mar Baselios College of Engineering and Technology
Thiruvananthapuram,India

Saranya V S
Student,Computer Science
Mar Baselios College of Engineering and Technology
Thiruvananthapuram,India

Sheril Alex
Student,Computer Science
Mar Baselios College of Engineering and Technology
Thiruvananthapuram,India

*Abstract***— *In India, Aadhaar is one of the main residential identity cards issued by the Indian Unique Identification Authority on behalf of the Central Government. It has a unique 12-digit identification number for each individual who maps a database containing the demographic and biometric data of the user. The data of each of the Indian citizens is stored in 7000 databases located in the Industrial Model Township. But in these days, the privacy and security of Aadhaar is questionable due to recent vulnerabilities and leakage of Aadhaar information. Blockchain-based Aadhaar security system is concerned with user privacy and protection because it uses a Secure Hash Algorithm-256, which is a secure algorithm used in blockchain. That requires the data to be collected, stored and used specifically with knowledge of the information to which it belongs. When using Aadhaar in blockchain, we can see more trusted UIDAI nodes where government and other legal entities can be a part of trusted UIDAI nodes. Such trusted nodes can only verify the blockchain transaction, add new blocks and decrypt the data contained in the blocks. Since we can have multiple nodes in the peer-to - peer network, and in each and every node we can find a complete copy of the blockchain, this will be of benefit if the blockchain is not affected by any nodes that are compromised.***

Keywords—Blockchain, Aadhaar, Registration Portal

I. Introduction

Aadhaar is a unique 12-digit identity number, which Indian tenants or visa holders can voluntarily obtain on the basis of their demographic and biometric data. The data are collected by the Indian Unique Identification Authority (UIDAI), a statutory authority formed in January 2009 by the Government of India under the jurisdiction of the Ministry of Electronics and Information Technology. As you know, Aadhaar contains almost all the details of a person as it relates to all other personal records such as bank details, fingerprints, PAN cards, etc. In addition, the Aadhaar may grant the needed impetus for standardization and digitization of other domains, many of which have been delayed for a long time. The Aadhaar ID can be used for simple development of local IDs to digitize new verticals. More importantly, Aadhaar can make it easier to link local IDs to currently isolated verticals such as census, education, health and immunization records, birth and death records, land registers, property registration, income tax, banking, loans and defaults, police verification and law enforcement, disaster management, security and intelligence and such others. Thus, Aadhaar may not only enable the efficient layout, delivery, monitoring and review of services in each domain individually, but also offer the possibility to use modern data analytics techniques to identify large-scale correlations in user data that may encourage improved design of social policy strategies and early detection and anomaly alert systems.

Therefore, it is very important to store Aadhaar information in a secure manner so that there is no risk of misuse happening as it is a very sensitive collection of data and it is the duty of the government to keep it safe and secure. Current storage practice is in standard database and this method has several downsides. Therefore, we are proposing a system that helps to store the data securely using the Block chain and it is much more efficient in achieving this objective. Developed using HTML, CSS, Bootstrap, JavaScript as the front end design tool, PHP as the server side scripting and MySQL as the backend.

II. BLOCKCHAIN TECHNOLOGY

Blockchain is a highly exciting and innovative technology as it helps to minimize risk, stamp out fraud and offer accountability for various uses in a scalable manner.

III. System analysis

A. Existing System

All of the Aadhaar information are stored in the current system 's usual database, and people who have access to the system can display the same. This type of storage does not provide sufficient security for this sensitive data and although encryption is available, it can be easily decrypted and data may be misused So there needs to be a system that can safely store the data and make sure that no one but the stakeholders can access it. The Repository of the Central ID is hosted on a data center-powered database server. These data are used to meet Aadhaar 's core project goals, such as:

The registration portal is used to receive new customer enrolment requests and to collect new data. After authenticating the individuality of the request, the registrars will record the collected information in the magnetic media from the different logistics service providers. These data are then added to the Aadhaar database after validation.

The authentication application will perform online identity authentication i.e. demographic and biographical details by Questioning the Aadhaar database in the form of a true or invalid response sort that responds to certain queries. De-duplication of biometric data is also allocated a scaled fusion data score for each duplicate record.

Theft identification systems detect identity fraud by identifying duplicity scenarios:

i. Examples include: Enrolling of non-existing applications
ii. To transmit details
iii. Several same applicant attempts to register
iv. User impersonation, etc.
v. The administrative structure includes User management, roles-based authentication, monitoring and recording of statuses.

The Reporting and Analysis framework offers statics for both the public and the partners to register and authenticate. The information portal gives administrative access to public records to internal customers, sponsors, and general knowledge or grievance requests. The contact center interface application provides the functionality for querying and updating the status.

The logistics system software works with the logistics provider for the letter-printing and distribution management.

Disadvantages:

i. Data security flaws
ii. Synthetic fingerprint generators can double the biometrics
iii. Financial transactions without one person's permission
iv. Citizens are afraid that the Government will monitor all their transactions
v. Aadhaar information is stored as a safe location in the Central Identity Data Repository, but we do not know what happens when security breaks down
vi. Is easy to decrypt

B. *Proposed System*

To address the problems of the current architecture, we suggest a secure way of storing data using the Blockchain concept. Under this initiative, we are creating a government web portal, and it contains all the authorities responsible for publicly issuing Aadhaar. Thus, Aadhaar's issuing authority will store all of an individual's sensitive information such as Ration Card No, ID Card No, fingerprints, etc. in different blocks and the same will be stored in a database and only the card will then be issued to individuals. The main advantage is that block has hash values, and the same cannot be deciphered in any way. So data in the database is safe and no hacker can steal the information from it. The Framework includes four modules:

i. Administrator
ii. Authority
iii. User
iv. Bank.

By giving them login credentials, Admin is responsible for adding the authority in question to the program. They can also seek out citizens, and see complaints as well. Authority is responsible for adding citizens to the system, and block creates when a new user is logged in. User may also submit comments to server. We also added a module called Bank where verification of the system is carried out. For example, when a customer visits bank and fills in his data to open an account, bank checks the data against database and that's how the system operates.

When the user is logged in, their fingerprints will also be stored on the system. Identification of user's fingerprint, contact details, address and other personal information is used to create and store a block. When user approaches a bank to open an account, Bank scans the fingerprint. The ID that corresponds to this fingerprint is sent to the portal, using IOT. Bank cross verifies with this ID, by using blockchain, all user information.

C. *Aadhaar Security System Using Blockchain*

In order to define a device, process or system, a system design can be defined as the process of applying different techniques and principles is sufficient detail to allow its physical realization. Therefore, developing a system is a "how to" approach to building a new program. This critical process offers the understanding and operational information required for implementing the program proposed in the feasibility report.

The data architecture converts the data domain model that was generated during the research into the data structure needed to implement the program. The architectural design describes the relationship between major structural components into a functional detail that is required to incorporate the structure recommended in the feasibility report.

Source code is developed, and the software is implemented and validated through testing. Software design from project management point of view is performed in two into the architecture of data and applications.

1) *Modular Design*

In this project, there is five modules. They are admin, District admin, User, Public.

1. Administrator
   a. Add authority
   b. Search citizen
   c. Add messages to authority
   d. View complaints from user
2. Authority
   a. Add citizen

b. Search citizen
c. View messages from admin
d. View complaints from user

3. Users

a. Add complaints to admin and authority

4. Bank

a. create account
b. deposit cash
c. block chain verification

2) *Fingerprint Device Design*

a) Working

The fingerprint device is primarily used with bank for verification purposes in our system. For example, when a client visits bank and fills in his data to open an account, bank checks data against database and this is how the system works. When the user is registered they also store their fingerprints on the system. Identification of user's fingerprint, contact details, address and other personal information are used to create and store a block. When users approach a bank to open an account, Bank scans the fingerprint. The ID that corresponds to this fingerprint is sent to the portal, using IOT. Bank cross verifies with this ID, by using blockchain, all user information. The bank checks if the hash value generated by them and the hash value produced by the fingerprint device is the same if it is checked otherwise.

The bank can only get people to see popular details; they can't see the confidential data of individuals. No-one may access the sensitive data as it will occur as a hash value. The key benefit is that block has hash values, and the same can't be deciphered in any way. Thus data in the database is safe, and no hacker can steal the information from it.

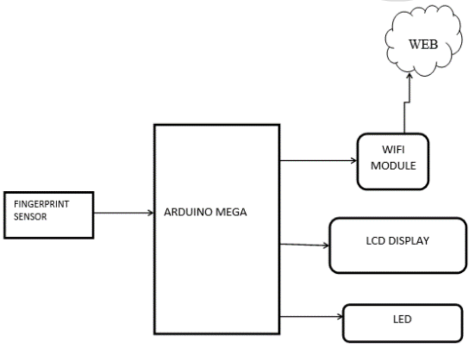

Fig 1 Architecture of the fingerprint Device

b) Components of the device

Power supply: It converts mains alternating current to low-voltage regulated direct current.

Fingerprint sensor: Fingerprint readers are safe and reliable devices for any security authentication. Fingerprint sensors are used for recognizing and authenticating the fingerprint of each user.

LED: Light Emitting Diode is a diode comprising 2pins, one negative and another positive. The long leg pin is positive and the short leg is negative and transmits light from which current flows.

Arduino Mega: The Board of Arduino is the foundation of our system. Entire working of machine depends on this plate. Arduino responds to the opto-coupler 5v supply and traces the user's fingerprint and sends the id to the portal.

Wi-Fi Module: Wi-Fi stands for Wireless Fidelity. We use Wi-Fi which acts as IoT's heart. The output of the Arduino is send to the portal through Wi-Fi.

LCD: The purpose of LCD module is to get visual information.

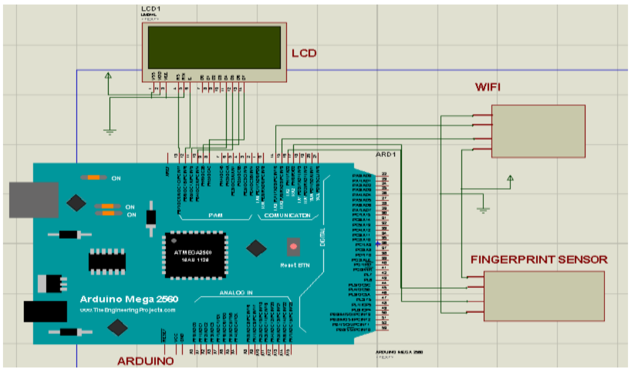

Fig 2 Circuit Diagram of the Fingerprint Device

IV. FUTURE ENHANCEMENT

We may implement face recognition, retina scanning along with finger printing for future reach. Here, however, we only implement our system with banking services, it can also be applied to other departments such as Passport, Certificate issuing authority etc.

V. CONCLUTION

Growing Indian population, immigration from nearby countries as well as various variations in identity cards, such as ration card, voter ID card forced the Indian government to establish 'Unique Identification Authority of India(UIDAI). 'UIDAI's main responsibility is to issue Indian citizens unique identification number (UID) or Aadhaar Number which can be used for all government entities / benefits schemes such as gas subsidies, Mahatma Gandhi National Rural Employment Guarantee Act (MGNREGA). The storage of this data is therefore of paramount importance. We have implemented the most advanced technology, IOT and block chain in this project, which helps to securely store information in an encrypted manner that cannot be accessed by ordinary people. Government of India can use this portal to store all of a particular person's data, as it ensures high security and efficiency. It can also act as a centralized storage system due to the fact that when a user opens a bank account, his information can be extracted and verified using his / her fingerprint by cross-checking the same with the already stored block information. Overall, the portal acts as a one-point contact to efficiently and securely store all sensitive information using the concept of the block chain and IOT technology.

VI. REFERENCES

[1] Venkatasubramanian S, Swarnakamali V, Kaiya J, Vigneshwar A," Aadhaar security through blockchain",2019 International Conference on Current Research in Engineering Science and Technology

[2] S. P.j and G. George, "Blockchain Based Aadhaar Security," International Journal of Engineering & Technology, vol. 7, no. 4.6, p. 398, 2018.

[3] Yi Liu, Ruilin Li, Xingtong Liu, Jian Wang, Chaojing Tang and Hongyan Kang, "Enhancing Anonymity of Bitcoin Based on Ring Signature Algorithm", 2017 13th International Conference on Computational Intelligence and Security
[4] "Enhancing the Health Care Data Security through Blockchain," International Journal of Engineering and Advanced Technology Regular Issue, vol. 8, no. 6, pp. 549–554, 2019.