Biometric Identification System in Cloud Computing Using Blockchain

K. Sujana Kumari, G. Murali

Abstract: ***Block-chain is a distributed immutable ledger technology. It consisting of blocks, and each block contains multiple transactions. Block-chain consists a secure hash, timestamp, data of the current block, and the hash value of the previous block. Block- chain records all transactions across the network so that it cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. Biometric identification system usage has increased as it provides an auspicious way to identify users. While compared with traditional authentication methods Biometric is more reliable and convenient. Block-chain was designed initially to solve double spending problems in peer-to-peer payment system of Bitcoin. But, since then it applications gone through the original intended use because of its properties, i.e. decentralization, immutability, no trusted authority and auditability. In this paper we propose how this Block-chain technology can have applied in biometric identification scheme like aadhar in cloud server-to make aadhar more transparent.***

Keywords: Block-chain, Biometric, Immutability, aadhar, cloud.

I. INTRODUCTION

Biometric identification system has been more attention in present days ,since it provides promising way to identify users. Biometric system is nothing but a person can be uniquely identified by a biological traits. Compared with the traditional identification system such as passwords biometric identification system is more trustworthy ,Why because is every individual person having unique identifiers such as fingerprint , iris ,facial patterns etc. Because of these biological traits biometric system is widely applying to many fields.

In biometric identification database owner is responsible to manage the entire national database fingerprint and he will also upload the data into the cloud(ex, Amezon cloud) to overcome the expensive storage and computational cost. In this system the data will be encrypted before uploading into the database

Whenever user needs data then he will sends a query to the database owner,then the database owner generates query by using individuals biometric traits and submits it to the cloud

Then database owner finds the closest match from the cloud and return it to the user. But, the main problem here is designing a protocol, which helps us to store the data into the cloud. Aadhar is a largest unique identification system. It records 1.19 billion Indian resident's records. Aadhar authentication is a procedure wherein aadhar number along with the personnel attributes including biometrics are given to government. By using this aadhar number anyone in the government agency can track your login patterns and access your personnel data[3].

Using Blockchain technology in biometric system like aadhar to make it more transparent to the public.Aadhar can broadcast all the modifications against each user record into the blockchain. In this paper we solve the problem by using Blockcaintechnology, each individual can know the changes against their aadhar record.

II. BACKGROUND WORK

Block-chainisatechnologywhichis cryptographicallydecentralized,distributedledger. This distributed ledger can record transactions within in a network between the systems efficiently valid(verifiable) and unchangeable way[1]. It record transaction sequential chain of blocks. The starting block in the block-chain is also known as genesis block, which doesn't have parent block. Each header block contains version of block, Time stamp, Hash value of parent block, Nonce, Merkle tree root hash and Nbits. Block Version has set of validation rules for block which needs to be followed. Time-stamp is current time as second's. nBit's are threshold value of a block hash in valid aspect. Nonce is an 4- byte field, which generally starts with 0 and increments for every hash value calculation. Parent block hash indicates a 256- bit value of hash which is points to previous block. The Block body consists of all the transactions and the transaction counter.

Every transaction within block- chains, hashing algorithms (Ex SHA) are used to determine state of the block- chain. Block- chains consists of data and hash value of the previous block. Through this hash pointer each block is connected. The hash value depends on not only on the transaction but also hash value of previous transaction. Even a small change in a transaction creates a new hash. This hashing mechanism maintains data is more secure and Immutable. Transaction data. Thus the result of all hashes of the transaction in the block are themselves hashed, then the result is merkle root. Whenever the maximum block- size transactions are added to the block then consensus algorithm will be applied Consensus is a fault-tolerant algorithm, which is used in the blockchain to achieve the required agreement on single state

Revised Version Manuscript Received on 16 September, 2019.

K.SujanaKumari, M.Tech Student, Dept. of Computer Science And Engineering, JNTUA College of Engineering,Pulivendula-516390,Andra Pradesh, India.
(Email: sujana0203@gmail.com)
Dr.G.Murali, Assistant Professor, Dept. of Computer Science And Engineering, JNTUA College of Engineering, Pulivendula-516390,Andra Pradesh, India.

of network or single data value among distributed process.

III. RELATED WORK

A biometric identification system is a pattern identification process in whichgenerate personal recognition by verifying a authenticity of physical characteristics possessed by a user.

In the present work the problem is the government data's are directly sent to the cloud service provider & the assumption is cloud service provider is encrypting & storing the data is not used any block chain & other thing . But it is already proved that our Aadhaar card details are hack able it is hacked &it is already released in the net. So that the old system is unsecured.

Biometric Aadhar system using block- chain every user no need to reveal the personnel data or aadhar number. In this system data will be stored by using hash and this data recorded into the block-chain. So that any changes happening against the user aadhar record and immediately question the authorities[6].

IV. PROPOSED WORK:

In the proposed system we are applying blockchain technology to Aadhar system will make the system robust and trust worthy.Blockchain based aadhar system is much secured. How it is much secured means that aadhaar card details are encrypted in a Government server by using AES algorithm alongwithSHA1hashingtechnique. Only and the encrypted data only sent to the cloud service provider and in this cloud service provider also is giving the second level of security by using the Block chain so that it is highly secure with the previous work.

Advantages of Proposed System

- Data is secure for users
- Increasingtrustaspeer-to- peer network
- Data access by aunthentacion user

System Architecture:

Biometric System Architecture design- identifies the overall structure of the WebApp. This system architecture main goal is to build a system for a WebApp, which provides the information to the users who will visit.

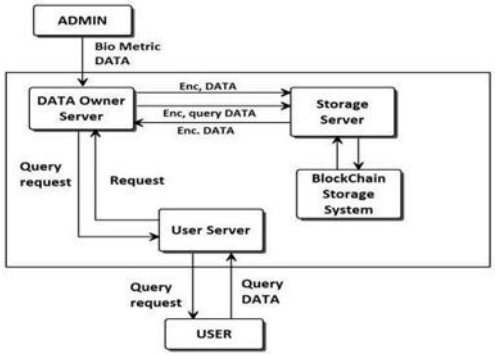

Figure 1: System Architecture

Figure 2 data flow diagram explains how data is going to be stored in the amazon cloud. First select a file and transfer that file to server. Then server receives all the details and generates a Message Digest(MD). Once MD file is generated then it retrieves all the public key belongs to the user group i.e.(MD+Public key)and generates a secure MD.

Secure MD with user Private keys then it generates Ring-Signature and send a mail to all users

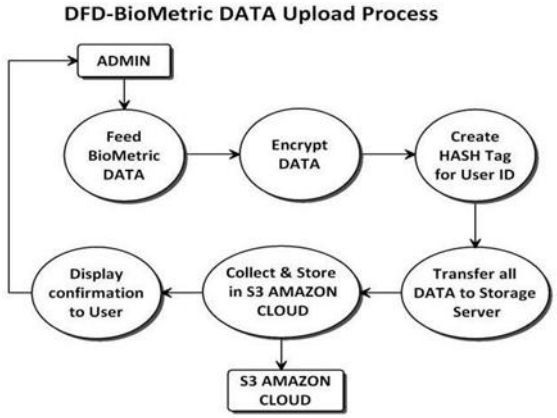

Figure 2: Data Flow Diagram Store data Into Cloud

AES Algorithm:

AES(AdvancedEncryption Standard) is symmetric block chipper .It is a new advanced encryption standard algorithm and it having a capable handling 128 bits block using a key size at 128,192 and 256 bits. Symmetric ciphers use same key for encryption and decryption process. So that the sender and receiver both are must know and use the same key. In this paper we are using AES algorithm to encrypt the data into the cloud[8].

Hashing:

Hash is a function it converts one form of value to another value. Hashing is the process of transforming the group of characters into a stable length of key which represents the original string. The main goal of hashing is to identify and retrieve the values from the database why becauseof it is faster to find values using short key than to find using the original string value.

SHA-1 Algorithm:

SHA-1(Short for Secure Hash Algorithm) is a one of cryptographic hash function algorithms. It is used to check or verify a file has been altered or not. This will have done by creating a checksum. In this paper we are using SHA-1 algorithm to create a hash value in the block-chain.

Block-chain based aadhar system we are using three different types of web servers which are interacting with other server using web server technique.

A. Government Server

Government server is used for government which is accepting citizen data. Whenever user sending a data it will be encrypted in the government server and then the encrypted data only sent to the cloud service provider web server.

B. Cloud Service Provider Server

The second server cloud service provider block chain web server, this server has to accept the data from government server and convert the transaction details into blocks and store it in blockchain storage.

C. End User Server

The third server is user server which will get the query input citizen unique IDand his finger print, this server has to send the data to government server, in turn government server has to send the citizen unique id in hash code format to cloud service provider block chain web server.

Once block chain web server receives the hash code it has to retrieve corresponding block from block chain and send it back to government server. Government server has extract the finger print from the received data and it has to compare the finger print with query input fingerprint if both are matching it has to send citizen data to user web server.

V. RESULT ANALYSIS:

In the previous work the problem is the government data's are directly sent to the cloud service provider & the assumption is cloud service provider is encrypting & storing the data is not used any block chain& other thing . But it is already proved that our Aadhaar card details are hack able it is hacked.

Table1: Depicts state wise biometric aadhar enrolled details without using the Blockcain. From this table we conclude that the government has to make people to aware regards the benefits of aadhar card. So that more number of people enroll themselves and can be banified.

State Name	Numbers of Aadhaar Assigned	Total Population
Haryana	1899321	2361884
Himachal Pradesh	383156	566716
Chandigarh	56167	87776
Dadra&Nagar Haveli	21227	40955
Goa	55554	108545
Uttarakhand	499732	1018460
Pan jab	1046347	2276809
A&N Islands	14631	32210
AndraPradesh	1655019	3806444
Puducherry	44673	105240
Delhi	627866	1525061
Odisha	1643598	3993856
Daman&Diu	7258	17904
Telengana	1152585	2916815
Gujarat	2261638	5854485
Chhattisgarh	1073918	2884275
Jharkhand	1456512	4198056
Karnataka	1890575	5517577
Lakshadweep	1895	5659
Mizoram	43457	135803
West Bengal	2487488	7920324
Madhya Pradesh	2608753	8629282
TamilNadu	1660001	5647395
Kerala	73573	2605488
Maharashtra	2832930	10157823
Arunachal Pradesh	44360	160050
Manipur	78684	287530
Uttar Pradesh	5866026	239999
Bihar	3322220	1550106
Jammu Kashmir	337856	155106
Tripura	69656	361333
Sikkim	8050	47424
Rajasthan	1025770	8468802
Nagaland	1357	220969
Meghalaya	1486	454966
Assam	7277	361602

Table1:StatewiseAadhar Enrolled Dataset

Figure3 shows that the biometric aadhar assigned details in state wise. And from the graph Bihar having more aadhar number of aadhar's enrollment people.

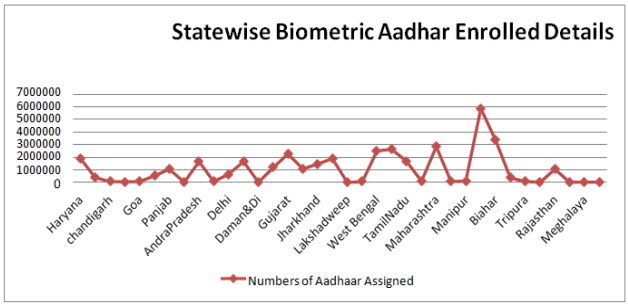

Figure 3 : Total Number of Biometric Aadhar Dataset

During the identification process, the privacy of biometric data should not be protected. Attackers and the semi-honest cloud users learn all about the sensitive information, there is no security to protect our data.

So that we propose privacy preserving biometric identification with block-chain is a much secured. How it is much secured means that aadhaar card details are encrypted in a Government server only and the encrypted data only sent to the cloud service provider and in this cloud service provider also is giving the second level of security by using the Block chain so that it is highly secure with the previous work.

In current trending technologies Blockcain place major role and usage of Blockcain is increasing day by day. Fig4 depicts how the Blockcain size is increasing.

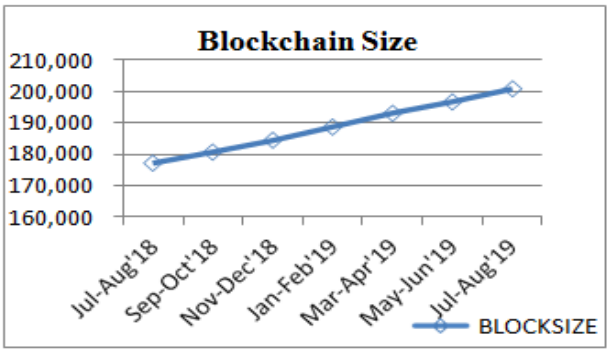

Figure 4 :Blockcain Size

Figure 5: Depicts Average Biometric Aadhar enrolled Details. In Block-chain. This data will be increasing day by day.why because is blockchain based biometric is more secure tan the normal biometric system.

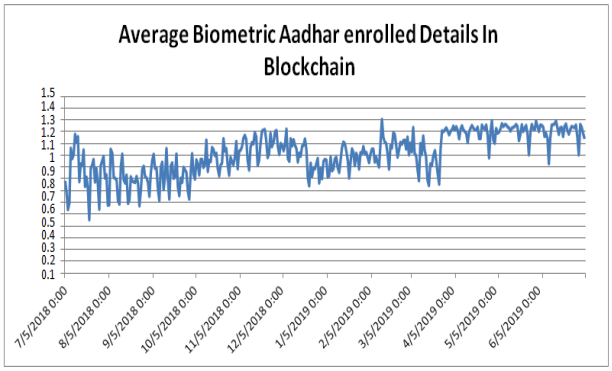

Figure 5 : Average Biometric Aadhar Enrolled Details In Blockcain

VI. CONCLUSION

This paper, we proposed three different web servers which interact with other server using web server technique. One server is used for government it accepts citizen data encrypt and give to cloud service provider web server. The second server is cloud service provider block chain web server, this server will accept the data from government server and convert the transaction details into blocks and store it in block-chain storage. The third server is user server which takes the query input citizen unique ID and his finger print, and this server send the data to government server, in turn government server will send the citizen unique id in hash code format to cloud service provider block chain web server. When block chain web server receives the hash code it will retrieve corresponding block from block chain and send it back to government server.

Government server extracts the finger print from the received data and it will compare the finger print with query input fingerprint if both are matching it send citizen data to user web server.

REFERENCES

1. A.ShantiBruyn, 26-Aug-2017, Blockchain.
2. https://www.logistics.dhl/content/dam/dhl /global/core/documents/pdf/glo-core-blockchain-trend-report.pdf
3. Arpita Krishna Bhat, Mthiyalagan R, Prakruthi K, May 2019, An Efficient and Privacy-Presenting Biometric Identification Scheme in Cloud Computing with Blockchain.
4. RahulAcharya,Smitra Binu,2018,Blockchain Based Examination System Foe Effective Evaluation and Maintenance of examination Records.
5. Bing Xu, Manli Lu, Guang Chen and Nian-Shing Chen, 2018, Exploring Blockchain Technology and its Potential Applications for Education.
6. https://medim.facilelogin.com/making-aadar-better-with-blockcain-ec3aef9852b0
7. ShaoanXie, ZibinZheng, Hongning Dai, Xiangping Chen and Huaimin Wang, 2017, An Overview of Blockchain Technology, Architecture, Consensus and Future Trends.
8. https://www.commonlounge.com/discussion/e32fdd267aaa4240a4464723bc74d0a5
9. https://uidai.gov.in/images/state-wise-aadhaar-saturation.pdf
10. https://www.investopedia.com/terms/s/smart-contracts.asp.