ISSN No:-2456-2165

Multiple Authority Identity Sharing Using SHA

Pulivarthi Chandrasekhar[1], T.Mahesh[2], Sk.Khaja Babu[3], Gontla Kowshik[4] ,N. Naveen[5]
[1,2,3,4,5]B-tech Students, Assistant Professor Department of Computer Science, KL Deemed to be University.

Abstract:- Identity is a set of claims about a person, place or thing. This usually comprises of first and last name, birth date, nationality, and some form of national identity for people, such as passport number, phone number (SSN), driving license, etc. These data points are issued and stored in centralized databases (central government servers) by centralized bodies (governments). For different purposes, physical forms of identification are not easily obtainable to every human being.

Approximately 1.1 billion individuals around the world have no means of claiming possession of their identity. This leaves one seventh of the world's population unable to vote in elections, own land, open a bank account, or find jobs in a fragile state. The failure to obtain identity documents jeopardizes the access of an individual to the financial system and in turn, restricts their rights People with officially recognised identification types continue to lack full ownership. They have a fragmented experience of online identity and unknowingly miss the importance that their details creates. We can store identity on a decentralized network by using block chain technology. We can develop an application that offers access so that users can store their information and avoid data tampering, and we will also provide access to the individual who needs our information.

I. INTRODUCTION

All the Details such as personal information contact information, biographical information, technical information, financial information and educational information, communication information are to be stored in a secure manner in a block.

By using block chain technology we can store our details in a secure way. In this project we are developing a application which can use this block chain technology for storing details so that they are not altered and provide security to the users information.

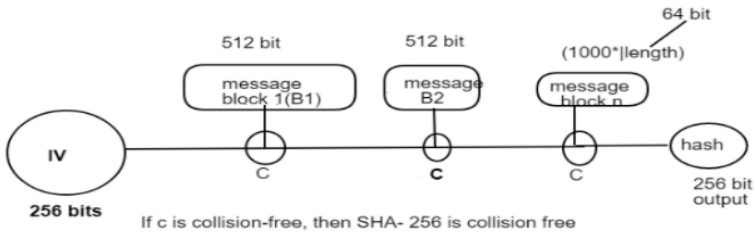
Block chain technology is a distributed public ledger, decentralized, tamper proof.
Public Ledger – Block chain technology is transparent, so that all the nodes in a block chain will validate the new block.
Decentralized – No central server/authority is required for block chain.
Tamper proof – A node in a block chain will only validate the block but can't change the information in the block.

- *Background Information*

Block chain technology uses SHA-256 algorithm which is unbreakable till now for joining the nodes of a blockchain .The nodes of a block chain are connected by using previous hash. First block of a block chain is called as Genesis block.This block did not contain previous hash values since it is first block. The system has to store the details of the user securely and based on the type of request of requester he has to show the required details. If the requester did not given access to the data the requester won't get the data.

As system is using block chain technology at most it can stores 2Mb of data, more that if we want to store a server is to be used.As we are using block chain, no one can alter the data as it is tamperproof. If anyone want to change the details of the person they can't be changed because of immutable property of block chain. The blocks should be pointer to another block by the previous hash,Every time when a new block is added all the nodes over block chain validate the node. As we are using block chain technology, we use SHA-256 algorithm for connection of blocks.

This process hasgreater transparency and we can use smart contracts. Traceability is easy in this process. As we are using block chain, the system is decentralized and the parties donot have to trust each other.



SHA -256 Algorithm

➢ *Statement of the problem*

The current system of identity management is neither safe nor secure. You are requested toidentify yourself at any point via various government-authorized IDs such as Voter ID, Passport, Pan Card, etc.

Sharing multiple IDs contributes to questions about privacy and data breaches. Therefore, via decentralized networks, the blockchain will pave the road to self-sovereign identity, which ensures

1.privacy
2.trust
3.where identity documents are secured
4.where identity documents are verified
5.where permissioned participants endorse identity documents

Everyone regularly uses identity documents which without explicit permission, are exchanged with third parties and stored at an undisclosed location.

Identity records are used if a person wants to apply for a loan, open a bank account, purchase a sim card, or book a ticket.

The weakest point of the existing identity management system is considered by government institutions, banks, and credit agencies, since they are vulnerable to data theft and hacking.

Therefore the blockchain has the ability to remove intermediaries while allowing individuals to freely control their identity. But we need to consider how identity management functions and what the problems in the current phase are before we transition to blockchain.

➢ *Purpose of the study*

There will not be any personal user identity information stored on a centralized server. All records identifying users are stored on their IPFS-backed computer making it secure from mass data breaches. The use of IPFS-supported Blockchain identity management does not allow any hacker to steal identifiable information. There will be no single point of failure because the scheme will be decentralized (SPOF). (SPOF). That part of the system represents a single point of failure-if it fails, the system will stop working.

➢ *Research question*

The primary question guiding the study include:

- What are the forms of validating identity of a person using online?
- How does online identity verification differs from the present paper identity verification ?

➢ *Objectives of the study*

The objectives of the studyare:

To explain the various ways in which online copyright infringement takesplace.

- To explain how Identity Management falls undercybersecurity.
- How online identity management system using block chain change the present situation.
- To compare the existing paper system and the system which is developed using block chain technology as proposed system.

II. LITERATUREREVIEW

➢ *Introduction*

Data such as Name, Address, E-mail, Age, Phone number, Date-of-birth, Designation, Father name, mother name,surname will be used to identify a person.Generally people are identified using these fields but some people have common names or other fields except unique fields like E-mail, Identity number, Social security number, License number, Aadhar number etc.

But all these details of personal details are stored in a central government server's which are under government. The government stores all the details of a person to provide identity and the citizenship.If any person/authority want some other person details then the person give his details by paper

documentation provided by the government in which it contains the signature of government authority.

If a person lost his identity then it will become a problem for him which causes problems of voting , land issues etc. It will be a complex process for government if some people lost their document in typical cases to provide the same document to the individual. In some critical cases the people who lost their identity wont get access to some of the resources he/she want.

It will may take 2-3 weeks for government to provide the required documentation. Some time's the paper document may get changed/altered by some other people, so that the original person get affected.

This all the troubles can be resolved by using Blockchain technology, because it is decentralized, tamperproof and transparent. Blockchain does not have any central authority to store details.

All the proceedings of a block chain are store in a block and the blocks will arranged in a chain format. Miners will add new block by computing the hash values. Since it is public ledger, all people will look all the transactions.

So it will be helpful for us to store each individual detail's in block chain and provide to the authorities/people who want other people details. The person/authority who want the data will request for other people and if the other person accept request the authority/person will get access to data.

III. METHODOLOGY

➢ *Introduction*

This is the first module of our project. The user role is to login using login window. This module was implemented for the protection purpose from unauthorized users. At the time of login in we have to enter login credential like E-mail and password and provide the role. It'll validate the username and password. If we enter any invalid E-mail or password it'll shows like invalid username or password error message.

It'll give protection for our project. Therefore database contain E-mail and password, jdbc always try`s to validate the user login. It well provide the security and preventing from unapproved user enters into the application. In our project we tend are using Html and css for making style. Here in this we will validate the login user.

➢ *Hypothesis*

H1: Online copyright infringement is a crime that has negatively affected society over the years with multiple internet diverseness and availability.
H2: The most affected audiences include the artists and content creators.

➢ *Proposed System:*

With transparency, protection and many more features, blockchain technology supports many industries, adding value to their businesses. It is therefore all set to transform, in a highly safe way, the existing work of identity management as well.

The use of blockchain identity management provides four advantages:
1.Unique ID
2.Consent
3.Decentralized
4.A Universal Ecosystem

Unique ID :A unique identity number will be obtained by each user who registers on the blockchain identity management system.

Consent: A blockchain identity management scheme would not store the data of any user. In addition, in order to allow regulated data disclosure, the system uses smart contracts.

Decentralized:
There will not be any personal user identity information stored on a centralized server as it is decentralized.

IV. RESULTS AND DATAANALYSICS

➢ *Data Requester Request For Information*

Here the user who request data has to register first and login again to request data. Data requester has options like request for driving license information, request for Aadhar card information and if the user approve the request then requester will get his/her information and access his data. Requester can check the request status weather it is approved or rejected.

➢ *User Uploads File Or Data*

In this module, user will have to login or register and have to upload some files i.e. driving license or aadhar card etc., in PDF or JPG format. The uploaded data will get encoded and loaded in the database. User can also create wallet.

➢ *Send Information For Requester*

Data user will logging in and approve the request of requester and If the user approve the request then requester will get his/her information and access his data.

➢ *Requester Checks The Data*

Here data requester will register and login and request for some files uploaded by the data owner. Requester checks all requested data of data user.

➢ *User Accepts The Request*

User receives notification after getting log in. here there will be the request sent by other data user. If they accept means, data will be sent for requester. The notification will be sent to the requested data user for getting information with acceptance notification. Otherwise it will get be rejected.

V. IDENTITY THEFT CASES BEFORE THE WIDE SPREAD OF THEINTERNET

Type of theft / age	Cases (%)
Id Theft	**33**
Cyber crime	**76**
18-39 years	**70**
Id Theft	**22**
Cyber crime	**81**
40+ years	**60**

Table IV.I: table showing cases against time on years

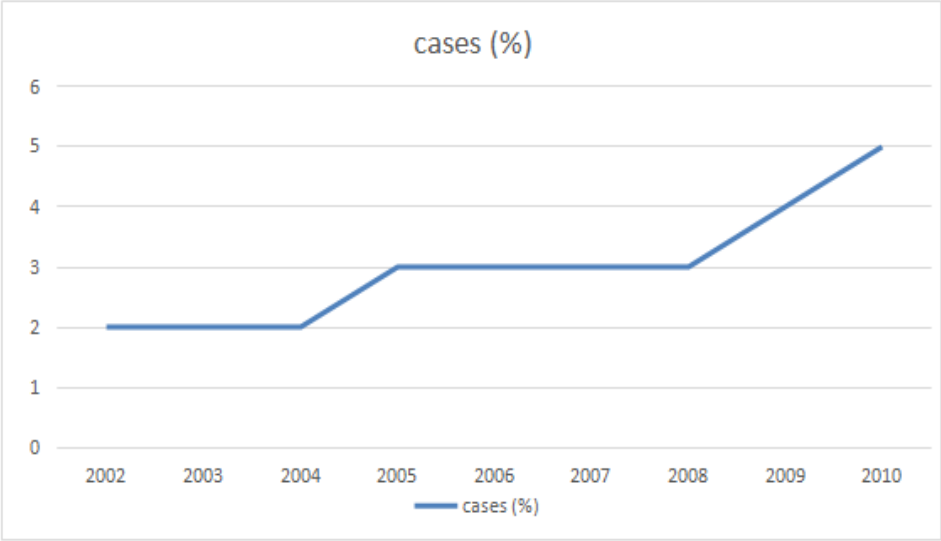


Figure IV.I: Graph showing cases before the wide spread of internet against time in years

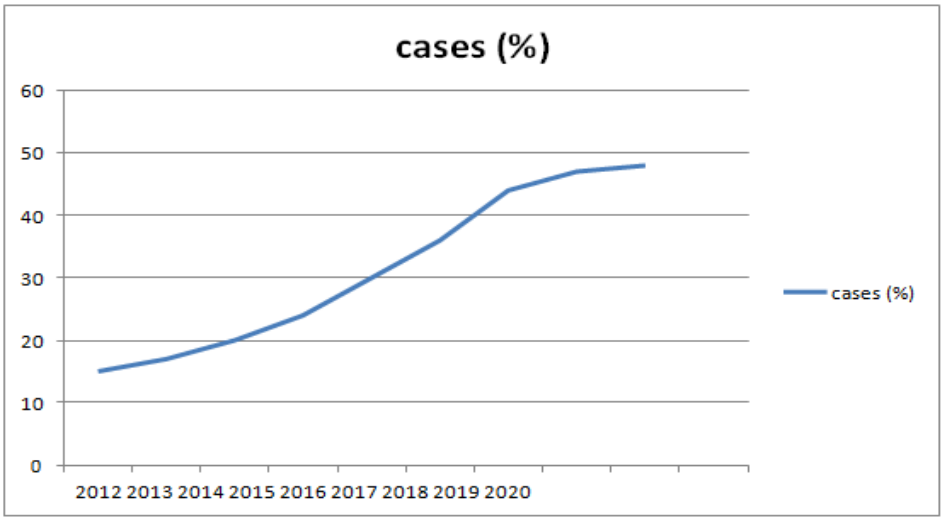


Figure IV.II: Graph showing the percentage of theft cases against time in years.

VI. WORK FLOW

VII. DISCUSSION

Hashing is a technique used to convert plain text into a hash called a check substantiation verification. It is used to check the integrity of the data. So, we can utilize this technique in order to maintain our data not to tamper or corrupted. We can use this hashing technique in our database tables to maintain blocks connected to each other. In this framework, the hash is generated by merging the phone number and voter id of an individual. To generate the hash, we can use the SHA-256 algorithm. outputs a value that is 256 bits. We are using SHA-256 because it is more complex to unencrypt.

VIII. CONCLUSION

When comparing with existing scheme the proposed system will provide strongest security guarantee. We have alsoconducted an analysis test , which demonstrates security to the user information is efficient. The details can be shared to the client within in no time. The main drawback of the existing is due to lot of time taking process and paperwork the

details can be altered easily. For providing the security guarantee we are using block chain technology. Because block chain technology is decentralized and tamperproof we also investigated how to utilize block chain technology performance and security. Here we are using Sha-256 algorithm for hashing the details. It plays an important for storage of details.

We can also extend this project like storing the data in the cloud server. We are verifying the user identity using hash value which are generated in time of registration. Currently this project holds the information like Aadhar card and license details. This project can be further extended to storing the entire details of the user.

RECOMMENDATIONS

1. There should be a system where a individual is identified and prove their identity by online.
2. The identity theft solud has to be decreased so that every individual has their own identity safely and securely with out any tampering.
3. The platforms in which the intellectual dat is being uploaded should be secured and protected such that it would be difficult to obtain anything illegally from these platforms.

REFERENCES

[1]. Basit Shahzad, Jon Crowcroft, "Trustworthy Electronic Identity management Using Adjusted Blockchain Technology", 2019.
[2]. https://www.investopedia.com/terms/b/blockchain.asp
[3]. https://www.movable-type.co.uk/scripts/sha256.html
[4]. https://searchsecurity.techtarget.com/definition/one-time-password-OTP
[5]. H. G. Do and W. K. Ng, 2017 IEEE Honolulu, HI, 2017, pp. 90-93, doi: 10.1109/SERVICES.2017.23.
[6]. R.Silhavy, P. Silhavy, and Z. Prokopová, in Advanced Techniques in Computing Sciences and Software Engineering. Dordrecht, The Netherlands: Springer, 2010, pp. 477–479 decision. *Korea Copyright Commission*, *33*(3), 111-150. https://doi.org/10.30582/kdps.2020.33.3.111
[7]. Saikia, N. (2010). Hyperlinks and Copyright Infringement. *SSRN Electronic Journal* https://doi.org/10.2139/ssrn.1566724