BE FINAL YEAR PROJECT

Digital Identity Management Using Blockchain

Shrineeth Kotian - XIEIT181925
Manish Kumavat - XIEIT181926
Dixit Patel -XIEIT181936

Nov 17, 2021

DIGITAL IDENTITY MANAGEMNET USING BLOCKCHAIN

SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS OF THE DEGREE OF

BACHELOR OF ENGINEERING

IN

INFORMATION TECHNOLOGY

BY

SHRINEETH KOTIAN

MANISH KUMAVAT

DIXIT PATEL

UNDER THE GUIDANCE OF

Prof. SULOCHANA BISHNOI

(Department of Information Technology)

INFORMATION TECHNOLOGY DEPARTMENT

XAVIER INSTITUTE OF ENGINEERING

UNIVERSITY OF MUMBAI

2021-2022

XAVIER INSTITUTE OF ENGINEERING

MAHIM CAUSEWAY, MAHIM,

MUMBAI - 400016

CERTIFICATE

This to certify that

SHRINEETH KOTIAN	(XIEIT181925)
MANISH KUMAVAT	(XIEIT181926)
DIXIT PATEL	(XIEIT181936)

Have satisfactorily carried out the PROJECT work titled "**DIGITAL IDENTITY MANAGEMENT USING BLOCKCHAIN** **"** in partial fulfillment of the degree of Bachelor of Engineering as laid down by the University of Mumbai during the academic year 2021-2022.

Prof. Sulochana
Bishnoi
Supervisor/Guide

Prof. Meena Ugale **Dr. Y.D Venkatesh**
Head of Department **Principal**

PROJECT REPORT APPROVAL FOR B.E.

This project report entitled “DIGITAL IDENTITY MANAGEMENT USING BLOCKCHAIN”

By

SHRINEETH KOTIAN (XIEIT181925)

MANISH KUMAVAT (XIEIT181926)

DIXIT PATEL (XIEIT181936)

is approved for the degree of BACHELOR OF ENGINEERING.

Examiners

1. ______________________

2. ______________________

Supervisors

1. ______________________

2. ______________________

Date:

Place: MAHIM, MUMBAI

DECLARATION

I declare that this written submission represents my ideas in my own words and where others' Ideas or words have been included; I have adequately cited and referenced the original sources.

I also declare that I have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which thus have not been properly cited or from whom proper permission have not been taken when needed.

Shrineeth Kotian (XIEIT181925) -------------------------------

Manish Kumavat (XIEIT181926) --------------------------------

Dixit Patel (XIEIT181936) --------------------------------

Date:

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Abstract

Digital Identity Management is a new identity management model in which the identity holder really have the ownership of their identity data and have control over it without involving any intermediary.Every user has multiple identities that he creates and maintains, to use on different applications, as per the set rules of that application. This has generated in large amount of user's private data with the service providers, resulting in two problems which include, the private data which is owned by the user is saved and left to the discretion of such 3rd party applications and the ownership of the user's data is no longer with him. Maintenance of such multiple identities will only become more difficult as the digital era unfolds. We attempt to solve this problem by using the Blockchain technology for digital identities. Blockchain is an enabling technology for building Digital Identity that offers a decentralized and secure environment. A blockchain's data is cryptographically connected and distributed across multiple computers, making them nearly impossible to temper with. Hence, Blockchain technology is the best and the secured platform to build Digital Identity. The identity management system which is present right now is neither secure nor reliable. Thus, blockchain technology can make the path to Digital Identity through decentralized networks, which assures the user's privacy, trust and security.

Acknowledgement

We would like to thank Fr. Dr. John Rose S.J (Director of XIE) for providing us with such an environment so as to achieve goals of our project and supporting us constantly.

We express our sincere gratitude to our Honorable Principal Dr. Y.D.Venkatesh for encouragement and facilities provided to us.

We would like to place on record our deep sense of gratitude to Prof. Meena Ugale, Head of Dept Of Information Technology, Xavier Institute of Engineering, Mahim, Mumbai, for her generous guidance help and useful suggestions.

With deep sense of gratitude we acknowledge the guidance of our project guide Prof. Sulochana Bishnoi. The time-to-time assistance and encouragement by her has played an important role in the development of our project.

We would also like to thank our entire Information Technology staff who have willingly cooperated with us in resolving our queries and providing us all the required facilities on time.

Shrineeth Kotian (XIEIT181925) ----------------------------

Manish Kumavat (XIEIT181926) ----------------------------

Dixit Patel (XIEIT181936) ----------------------------

Introduction

An identity of an individual or an organisation can be represented using a set of attributes association with the entity such as name, address, etc. Identity management consists of maintaining the identity data and the control over its access. There are three main actors in the Identity management system viz. Holder, Issuer and Verifier.

The identity issuer is basically a trusted party such as local government, can issue personal credentials and documents for an identity holder i.e. an legal individual / organisation. By issuing these credentials, the identity issuer attests to the validity of the personal data in that credential for example the user's last name and date of birth. The holder can store those credentials in their personality identity wallet and use them later to prove statements about his or her identity to a third party, the verifier. A Credential is a set of multiple identity attributes and an identity attribute is a type of information about an identity for example it can be a name, an age, a date of birth, etc. A credential is a verifiable claim, which comprises of some facts that is attested and digitally signed by the identity issuer about the identity holder. These credentials are issued by second parties which attest to the validity of the data inside the credential. The adequacy and reliability of any credential document totally depends on the reputation or trustworthiness of the issuer i.e. how much the issuer can be trusted. A credential can anything like the holder's identity data, for example date of birth or other types of factual data, for example a GPA. After there builds a good trust relationship with an issuer, anyone can be a verifier for example an employer of a claim. A verifier requests for a specific credential for example passport, and verifies the validity of the credential via the issuer's signature.

Identity management becomes challenging if the identity holders do not have a full control over their own identity data, since the data are usually maintained at sites such as Government institutes, Banks, etc which are considered the vulnerable point in the current identity management system as they are vulnerable to theft of user data. Thus, the blockchain comes with the possibility of discarding the intermediaries while allowing citizens to manage identity independently. This concept of digital identity management allows holders or users to retain his/her ownership of their identities or credentials and control over how their identity data is used.

1.1 Problem Definition

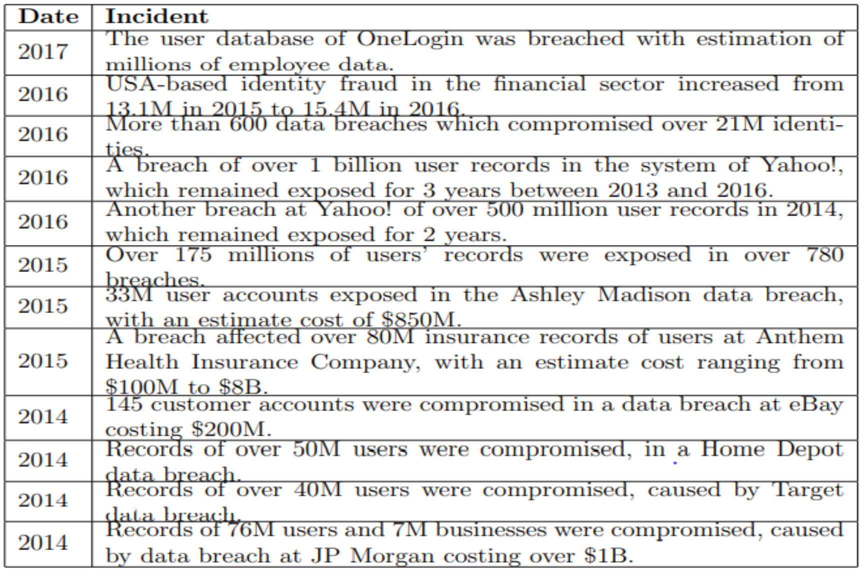
Identity management includes maintaining the identity data and their access control. The identity of an individual or an organisation are the set of attributes associated with them. Identity management is nothing but the maintenance of this identities and their access control. In today's digital world, for an individual or an organisation it becomes difficult to handle all the identity which they have. And also user do not have a full control over their identity data, because their identity data are usually maintained at the third party sites. To overcome this, we proposed a Digital Identity management using Blockchain technology, which manages the identity of the users. Blockchain allows everyone on the network to have the same source of truth about what credentials are valid and who has verified the validity of the data within the credentials without revealing the actual data.

Literature Review:

1. **Mehmet Aydar, Serkan Ayvaz , Salih Cemil Cetin, "Towards a Blockchain based digital identity verification, record attestation and record sharing system"- June 2020**

   Individuals can identify themselves using various identity documents such as their name, national identity number and passport number,etc. The traditional methods of identity management are open and susceptible to data breaches, identity theft and frauds can also occur. A solution to this is blockchain, where blockchain enables identity owners to have control over their identity and identity based personal documents, control access to their records i.e. they can manage to whom they share their details and for what purpose their data is used, and allows identity owners to share minimum amount of information while totally ensuring integrity and trust. This particular study focuses on things such as using the Blockchain technology for identity sovereignty purpose. The paper contains the followings which explains current problems in traditional identity management methods, and then tells about Blockchain technology, explains why the technology fits for a digital identity management system, and the concepts that are used in Blockchain based identity management systems.

   There were many problems in the traditional system which included problems like privacy, security, usability, globalization, etc.



Date	Incident
2017	The user database of OneLogin was breached with estimation of millions of employee data.
2016	USA-based identity fraud in the financial sector increased from 13.1M in 2015 to 15.4M in 2016.
2016	More than 600 data breaches which compromised over 21M identities.
2016	A breach of over 1 billion user records in the system of Yahoo!, which remained exposed for 3 years between 2013 and 2016.
2016	Another breach at Yahoo! of over 500 million user records in 2014, which remained exposed for 2 years.
2015	Over 175 millions of users' records were exposed in over 780 breaches.
2015	33M user accounts exposed in the Ashley Madison data breach, with an estimate cost of $850M.
2015	A breach affected over 80M insurance records of users at Anthem Health Insurance Company, with an estimate cost ranging from $100M to $8B.
2014	145 customer accounts were compromised in a data breach at eBay costing $200M.
2014	Records of over 50M users were compromised, in a Home Depot data breach.
2014	Records of over 40M users were compromised, caused by Target data breach.
2014	Records of 76M users and 7M businesses were compromised, caused by data breach at JP Morgan costing over $1B.

Figure 2.1: Problems in traditional system

Blockchain is basically a distributed ledger which is immutable by anyone, which stores the ownership of digital documents in the form of transactions and blocks. In this, the asset owners are identified by asymmetric cryptographic i.e. public-key cryptography which means the user's public key, It uses asymmetric cryptography concept in order to assign digital identity to the documents added.

2. E. Bertino, "Digital Identity Management Techniques and Policies" - CS Department and ECE School, CERIAS, Purdue University.

Digital identity is basically the digital representation of the information known about some specific individual or sometimes an organization. It can be defined as a distinguishing character or a personality of an individual which makes him stand apart from a crowd of people. This identity of an individual can be stolen which is termed as Identity Theft which is in turn defined as usage of someone's credentials like personal information credentials without that particular person knowing about it and using it for other purposes mainly fraud. The main idea behind verification of a user is that it will require additional identity information for example mother's name or it can be a SSN too which can be used as a proof to qualify to be the owner of the documents that are stored like credit card or pan card or any other documents. This two factor authentication can be carried out with the help of the zero knowledge proof method which is basically a method mostly a mathematical method which is used to verify an individual without even sharing or revealing any of their data.

The functional view of the system consists of the registration process where identity record will be uploaded and stored and then its usage. There is a way to detect duplicacy of documents which consists of putting the strong identifiers in a hash table and look for collisions to occur, and it should be a distributed hash table. The advantages of this system include that the actual values of the registered documents used as proofs for multi-factor authentication and privacy is provided security using ZKP. There is assurance that the information provided is totally valid. It allows a flexible approach to authentication and a validation approach to information. Thus, Identity Management and Theft Protection are major areas of concern and active work which is drastically growing . This Identity Management system has potential to provide an environment which is secure and collaborative by providing a solution to the problem of Identity Theft with the help of privacy preserving multi-factor authentication.

3. Akash Takyar, CEO LeewayHertz, "Blockchain Identity Management: Enabling Control Over Identity"- 2021

In this system we saw the benifits of blockchain in digital identity management. The challenges like identity theft, kyc and the major problems of the IDs and passwords that can be easily solved by it. Uploading the documents on a decentralised servers which is backed up by IPFS. And using Blockchain identity management backed up by IPFS doesn't allow any hacker to steal the personal information of the user. And mainly without the consent of the user no third party can get the access of the users data.

4. **Zhimin Gao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, Weidong Shi, "Blockchain-based Identity Management with Mobile Device"- June 2018**

In todays world identity management plays an very important role for getting any of our work done. Whether a small scale or a large scale company everyone needs to show their identity. But in our existing system everywhere we have to submit the copies of our data and many more. And it is possible the submitted data can be manipulated. So there rises a risk in identifying the right data. And to verify all this it would consume much time and money. This technique is neither reliable nor secure. Blockchain Identity Management offers a complete reliable and secure environment for everyone around the world. Keeping the ID's and documents on a decentralized application and can be used whenever necessary. This technology will help to keep our important data safe and allows us to share the data only to the consent person. All the transactions made are clearly visible to the users thereby giving a trust to the users of their confidential data. And will make the path easier for all the users.

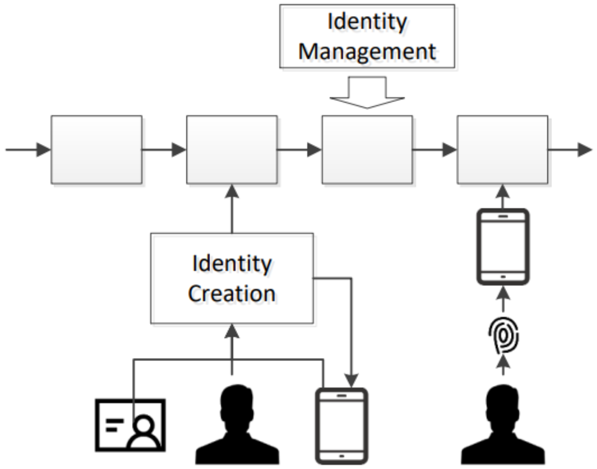


Figure 2.2: Overview of Identity Management using Biometric security

Blockchain based identity management is a powerful and uses decentralized method for storing data and keeping the records of a transaction for every user. Blockchain is a secure and relaiable method for keeping the transactions securely. It is very much indeed to use such technologies because in the current system the confidential data which we submit to the third party can even leak our data. There are many cases of data leaks nowadays. And this shared data can even be used by frauds in illegal ways. Digital Identity management keeps a track with whom we share our documents and confidentials.

5. **Benedict Faber , Georg Michelet , Niklas Weidmann , Raghava Rao Mukkamala, Ravi Vatrapu, "BPDIMS:A Blockchain-based Personal Data and Identity Management System"- 2019**

   In this paper, the authors proposes a conceptual design and high-level architecture for a Blockchain-based Personal Data and Identity Management System (BPDIMS), a human-centric and GDPR-compliant personal data and identity management system based on the blockchain technology. In this paper they discuss about the concept of MyData which was published by the Finnish government. MyData facilitates the idea that users should have a better idea of where their data is stored, who uses it, and be able to change this. It is a humanistic approach to people's data and aimed at giving full control over the personal data back to the users. The main objectives of the MyData from the user perspective are right to know what personal information exists, right to see the content of personal information, right to rectify false personal information, right to audit who accesses personal information and why, right to obtain their personal information and access it freely, right to share/sell personal information to others., and right to remove or delete personal information. The key stakeholders in the proposed system, BPDIMS are User : end users utilizing the system, Service provider : company providing a service to user, either paid or free, Data purchaser : an entity (company or person) purchasing the user data for a specific stated purpose, Data validators : entities who validate the user data to check that it belongs to that particular user or not. The system consists of several components, namely three blockchain layers that is basically smart contract blockchain, access blockchain and identity blockchain, the Off chain data storage, and the User interface. In which the first layer i.e. the Smart Contract Blockchain is used to store conditions for data exchanges between : User and Service Providers, User and Data purchaser. Now, the second layer i.e. an access blockchain will be implemented as a tool to ensure privacy, this framework enables users to control and own their personal data, user can set automatically enforced time limits for the access of the data. After the time limit, the consent is automatically revoked. The third layer is used for storing hashes of data. These hashes are created, when personal data of the user is verified by certain trusted authorities and the hash of the verified data stores on this layer. The Off-chain repository are the storages where the user data will be stored in the online data storage spaces which could be cloud storage database systems. All the user data will be stored in an encrypted manner with the encryption keys that are owned by the respective user who is the owner of the data. Here encryption proposed are symmetric-key algorithms like Rijndael AES, Diffie-Hellman key exchange algorithm or even public key infrastructure. Lastly, the User interface to give an overview over all personal data of the user and to be able to manage all the data and system functionalities. In our system consent appears in three ways : Consent for processing per- sonal data in return for services, Consent for storing personal data, and Consent for selling/access to per- sonal data. All user's consents are stored on the Access Blockchain of the system. The second and third type of consent regarding monetization and storage is linked to the Smart Contract Blockchain. Then the paper depicts the benefits of this blockchain based user-centric personal data management system in detail. The system is benefited with all the secured features of blockchain technology, trusted and fully-automated self-enacting smart contracts technology, implementation of storing data using various secured encryption and hashing methods i.e. cryptography.

6. **Puneet Bakshi, Sukumar Nandi “Privacy Enhanced DigiLocker using Ciphertext-Policy Attribute-Based Encryption”- Dec 2020**
In this paper, the authors propose a scheme to implement Privacy Enhanced DigiLocker with CP-ABE. Although DigiLocker ensures traditional security such as data integrity and secure access to data, the data protection of electronic documents has yet to be regulated. According to the authors, encryption based on ciphertext policy attributes (CP-ABE) can improve data protection. In DigiLocker, documents of subscribers are hosted on public cloud which is assumed to be a trusted entity. However, cloud storage can be unreliable and prone to insider attack. CP-ABE (Ciphertext Policy Attribute-Based Encryption) is a newer cryptographic mechanism that can improve data protection. However, correct implementation and efficiency are still a major concern for the overall implementation. Attribute-based encryption (ABE) is the encryption method in which the encryption is carried out under a number of attributes. ABE is classified in Key-Policy ABE (KP-ABE) and CP-ABE. In KP-ABE, the access policy is encoded in the subscriber’s private key and a number of attributes are encoded in the ciphertext. In CP-ABE, the access policy is encoded in ciphertext and a number of attributes are encoded in the subscriber’s private key. In CP-ABE, the recipient can only decrypt the ciphertext if the set of required attributes encoded in the recipient’s private key meets the access guidelines encoded in the received ciphertext. Finally the scheme proposed to prepone part of the encryption process to increase performance. This preponed process creates a token which can be reused later. The proposed system has been shown to be safe and secure against IND-sAtt-CPA games. According to the authors, the proposed scheme can be further improved by using homomorphic encryption that enables encrypted computing and post-quantum ABE schemes to be used for both, although schemes exist, but they are not yet trivial or practical.

7. **Dr. Vinay Kumar “A Solution to Secure Personal Data When Aadhaar is linked with DigiLocker”- May 2018** Digilocker is basically a digital document wallet where you can store your documents. It is used to store documents such as government issued documents, academic certificates etc., so that the documents can be shared easily on the web or wherever it is required. It provides access to the user to their stored documents for various public and private purposes. As it is a government made software and as a key initiative of the Digital India program, there was a beta version of DigiLocker launched. It basically works around Aadhar card number so it is a Aadhaar linked facility. But there are always security reasons related to Aadhaar card number and One Time Password generated which provides access to DigiLocker stored documents. There have been many such cases where OTPs has also been illegally accessed. And as of Aadhaar card numbers, they would be more easily known . The problems with the traditional system was that a citizen of India need to show their personal documents everywhere before they can enjoy privilages to avail any kind of services depending upon the services they want to avail. In some cases it might happen that the required documents might not be physically present at that time. The documents required can be anything ranging from personal identity card to any personal or academic documents or important documents. There has been many such cases where it has been experienced by many people they were not able to present the required document at that required moment of time. The problems that exists in the traditional systems can be broadly enlisted as the document is not properly verified so proper verification or the authenticity of the documents by government agencies can cause difficulties, there may be difficulties faced

during submission of multiple copies of physical document periodically and there maybe a very high chances that the original documents can be lost or stolen or the chances of the original documents being damaged due to wear and tear from usage since a long long time. There are some benefits of Aadhaar linked DigiLocker too. DigiLocker holds two types of certificates, one of which is educational and the second one is life time. There is an alert one month prior to the expiry date to some documents such as a driving license or a passport, and it may prompt to change it or update it and upload a updated document. The process being very transparent, once it gets logically linked with UIDAI and then PAN card, it can then verify more accurately by matching uniqueness of the user's first name, parent's name or relative's or guidance's name. But at the same time last name can be failure. There have been many security disadvantages of the system which includes the key security concerns of authentication, authorization at client-server both end and secure communication at the time of data traversal. Any data transfer should be done in an encrypted form with significantly high level of encryption standards and there should be maintenance of data integrity, and verification of trust between both parties and exchange of trust certificates so that trust should be maintained.

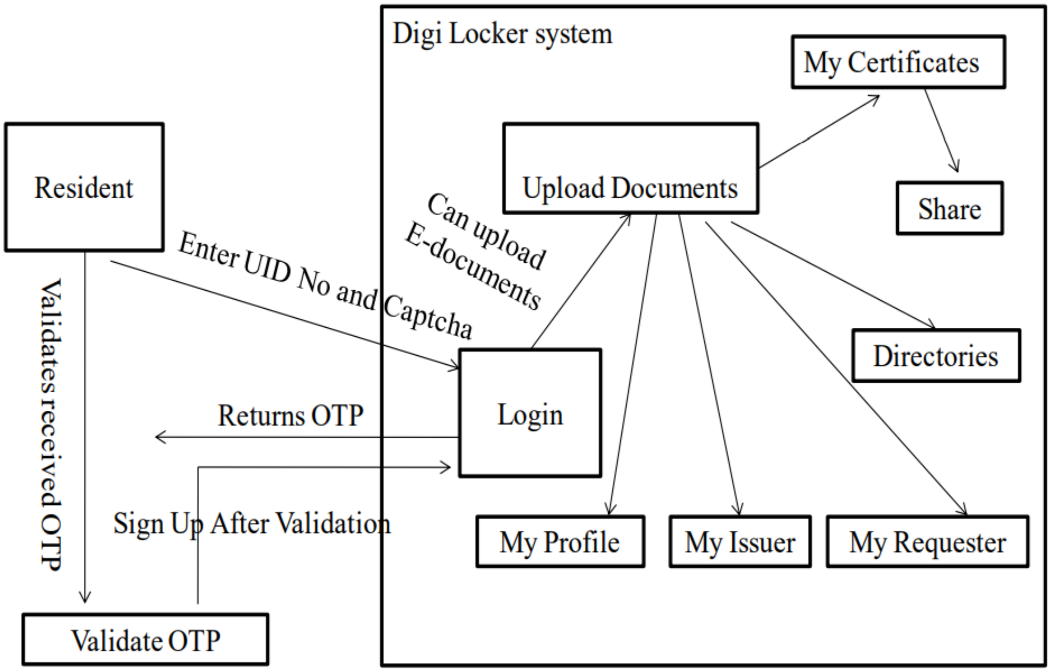


Figure 2.3: Working of DigiLocker System

Table 2.1 Summary of Papers

Sr. No	Year	Name of Paper	Author	Content
1	2020	Towards a Blockchain based digital identity verification, record attestation and record sharing system	Mehmet Aydar, Serkan Ayvaz , Salih Cemil Cetin	The study focuses on using the Blockchain technology and it explains current problems in traditional identity management methods, and then tells about Blockchain technology, explains why the technology fits for a digital identity management system, and the concepts that are used in Blockchain based identity management systems.
2	2019	Digital Identity Management Techniques and Policies	E. Bertino	In this paper, the author has briefed about the techniques and the policies used for the authentication purpose like zero-knowledge proof , multi-factor authentication,etc.
3	2021	Blockchain Identity Management: Enabling Control Over Identity	Akash Takyar	In this paper, the author has discussed about the benefits of Blockchain in digital identity and also addresses about challeneges in maintaining digital identity.
4	2018	Blockchain-based Identity Management with Mobile Device	Zhimin Gao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, Weidong Shi	In this paper, the author discussed about how the security of the digital ID can be improved using biometric authentication and face recognition.
5	2019	BPDIMS:A Blockchain-based Personal Data and Identity Management System	Benedict Faber , Georg Michelet , Niklas Weidmann	In this research work, we propose a conceptual design and high-level architecture for a Blockchain-based Personal Data and Identity Management

			, Raghava Rao Mukkamala, Ravi Vatrapu	System(BPDIMS), a human-centric and GDPR compliant personal data and identity management system based on the blockchain technology
6	2020	Privacy Enhanced DigiLocker using Ciphertext-Policy Attribute-Based Encryption	Puneet Bakshi, Sukumar Nandi	In this paper, the authors propose a scheme to implement Privacy Enhanced DigiLocker with CP-ABE. Although DigiLocker ensures traditional security such as data integrity and secure access to data, the data protection of electronic documents has yet to be regulated. According to the authors, encryption based on ciphertext policy attributes (CP-ABE) can improve data protection
7		A Solution to Secure Personal Data When Aadhaar is linked with DigiLocker	Dr. Vinay Kumar	In this paper, the author has enlisted various disadvantages of the usage of Aadhar card linkage and a Solution to secure personal data when Aadhaar is linked with DigiLocker.

IMPLEMENTATION STRATEGY

3.1 Proposed System:

3.1.1 Overview Of Digital Identity Management:

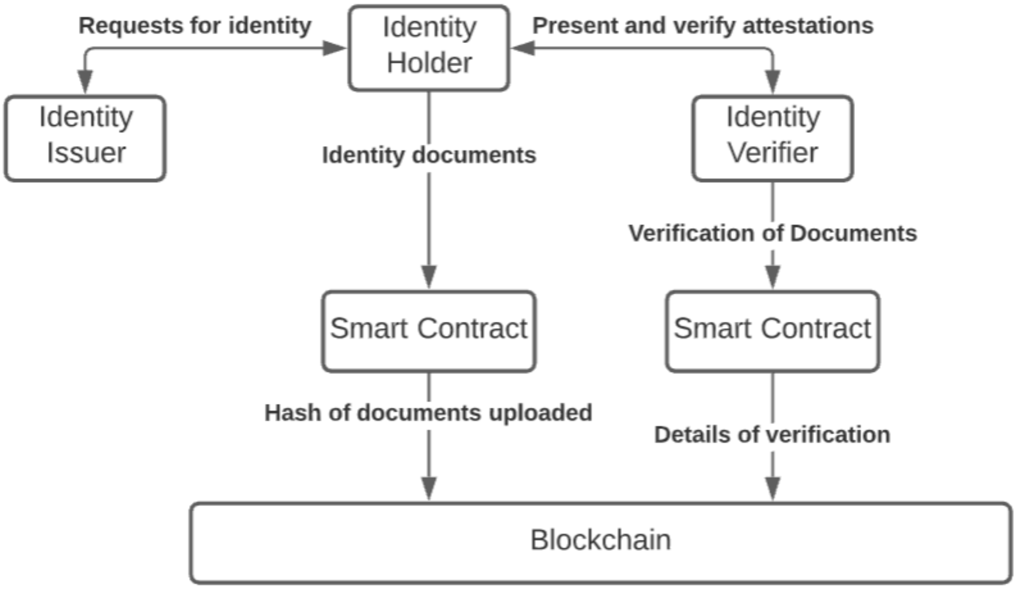


Figure 3.1: Overview Of Digital Identity Management

In the system, the identity issuer, a trusted party such as Government or any Organisation issues the trusted personal identity or important credentials to the holder as per the request. Then later the holder can present this credentials to the verifier, here verifier can be anyone such as bank employer,etc can verifies the validity of the credential via the issuer's signature.

3.1.2 Working Of Digital Identity Management:

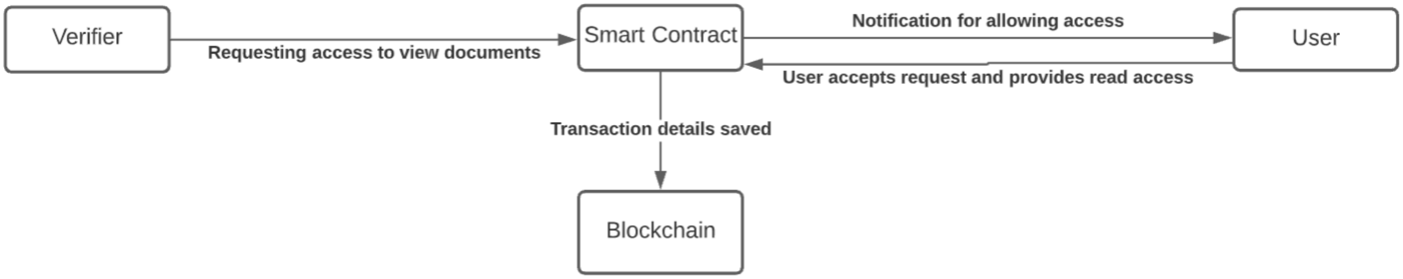

Verifier
Requesting access to view documents
Smart Contract
Notification for allowing access
User
User accepts request and provides read access
Transaction details saved
Blockchain

Figure 3.2: Working Of Digital Identity Management

This is the detailed view when verifier request to holder for identity verification and then holder gets notification and allows verifier to read the credentials which are required for verification. The whole transaction is stored in blockchain network with time stamps.

3.2 Hardware Requirements:

- Device Name:Lenovo IdeaPad S145-14API

- Processor: AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx 2.10Ghz

- RAM:8.00 GB

3.3 Software Requirements:

- Platform:
  Ethereum Virtual Machine

- Languages Used:
  Front End: Android App Development
  Ethereum Blockchain / Smart Contracts: Solidity

- Test Environment:
  Smart Contracts: Truffle IDE
  Blockchain Framework: Truffle IDE

3.4 Implemetation Details:

3.4.1 Methodology :

Firstly we will make the application in which the user sign ups and submits atleast one required details like their personal details, any supporting credentials, legal proofs, attestations for authentication of the user. This information would then be processed through various algorithms to generate the unique identification number for that user. This identification number is different and unique to every user. And the unique block is created for each user. This unique identification number is cryptographically hashed to ensure protection from any unauthorised access. Only this hashed and signed unique identification number would be recorded on that user's block in blockchain network. System does not store any user's private identity data on blockchain.

User wants to use some services then firstly verifier asks for authentication of user through sending request to user, then user gets notification on the app and allows verifier to read the credentials which are required for verification. This event gets stored as consent proof of data sharing i.e. transaction details happened between the identity owners and the verifying parties with time stamps.

Between all this transaction we will implement Smart Contracts which omits the need for a third party in each and every transaction. Smart Contracts increase the level of trust and security from both sides at reduced costs and also requires less time, as the conditions are stored in blockchain and executed through immutable program code. The access management is based on this Smart Contracts, so that the user can set automatically enforced time limits for the access of the data to the verifier. After the time limits over, the consent is revoked automatically from the verifying party.

3.4.2 List of Algorithms :

A) Hashing Algorithm : SHA-256 (Secure Hash Algorithm) hashing algorithm.

3.4.3 Implementation:

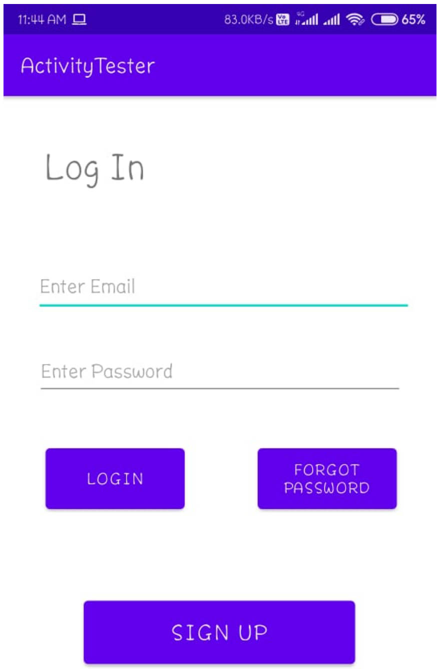


Figure 3.3: Login Page Design

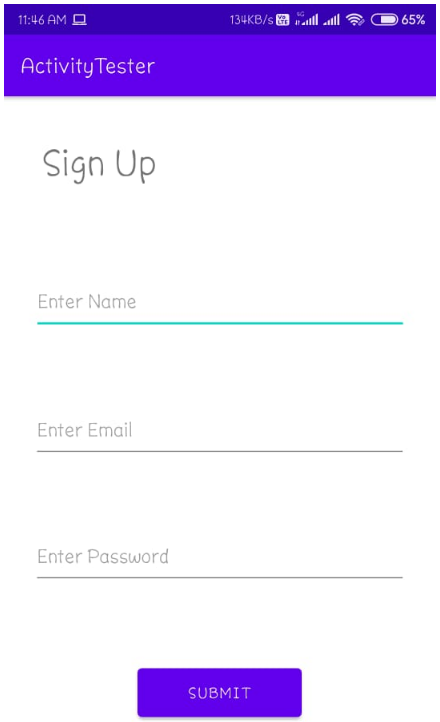
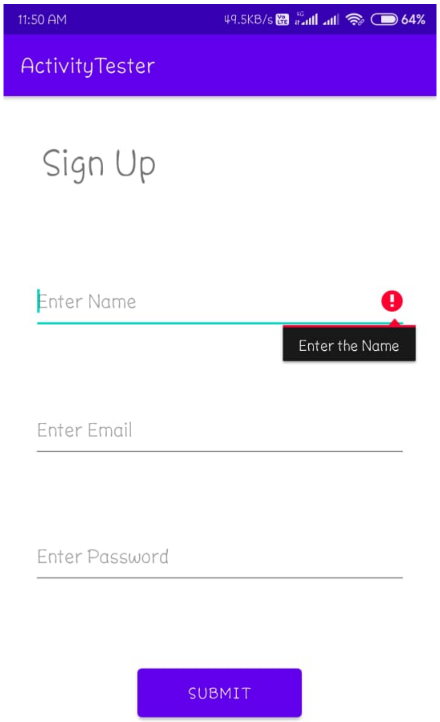
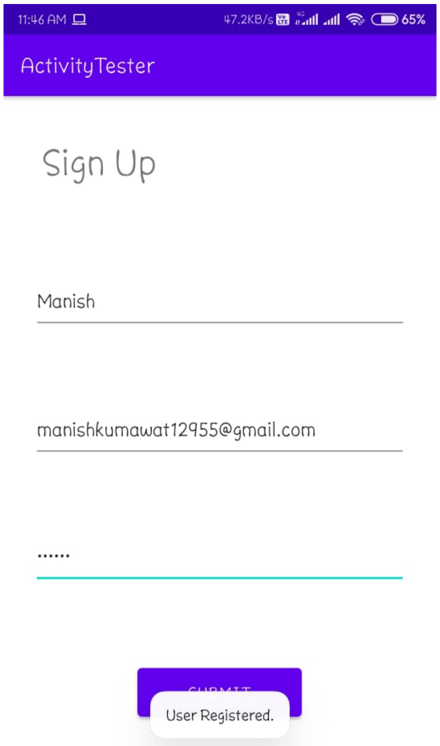


Figure 3.4: Sign up Page



Enter the Name

Figure 3.5: Sign up Page Validation



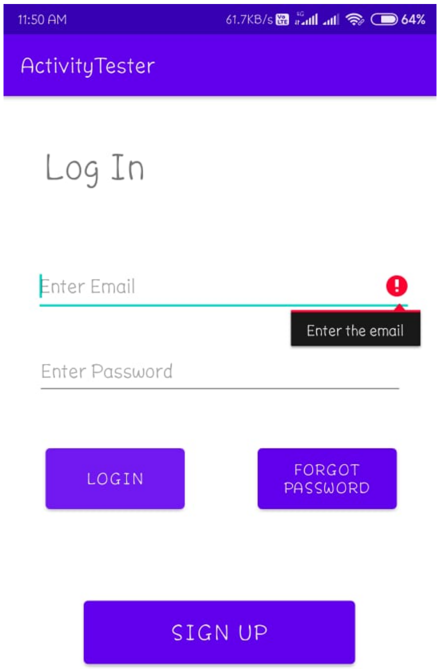
Manish

manishkumawat12955@gmail.com

......

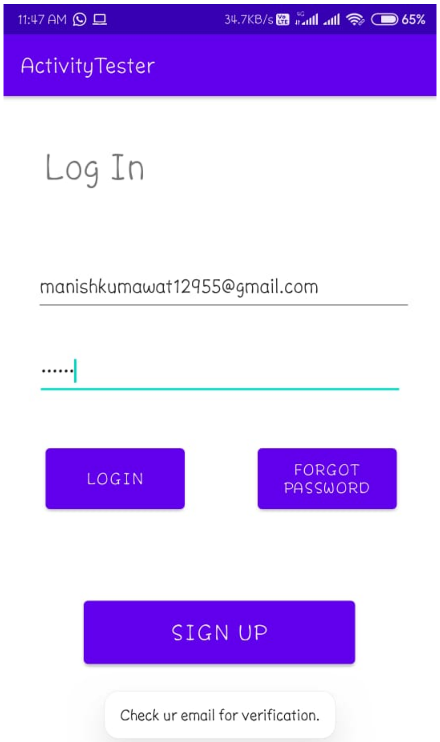
User Registered.

Figure 3.6: User Signing up



Enter the email

Figure 3.7: Login Page Validation

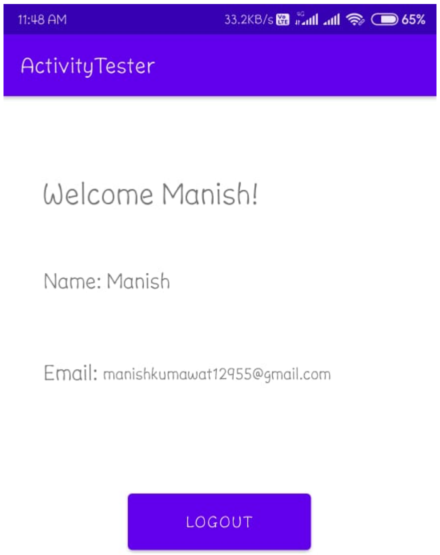


manishkumawat12955@gmail.com

••••••

Check ur email for verification.

Figure 3.8: User Logging in

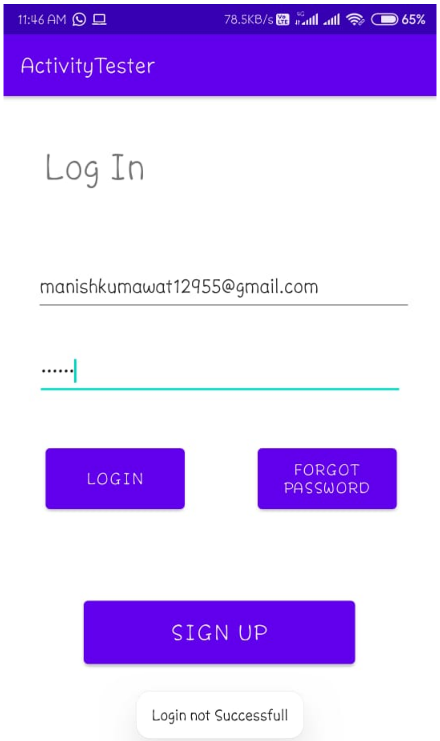


Welcome Manish!

Name: Manish

Email: manishkumawat12955@gmail.com

Figure 3.9: User Logged In

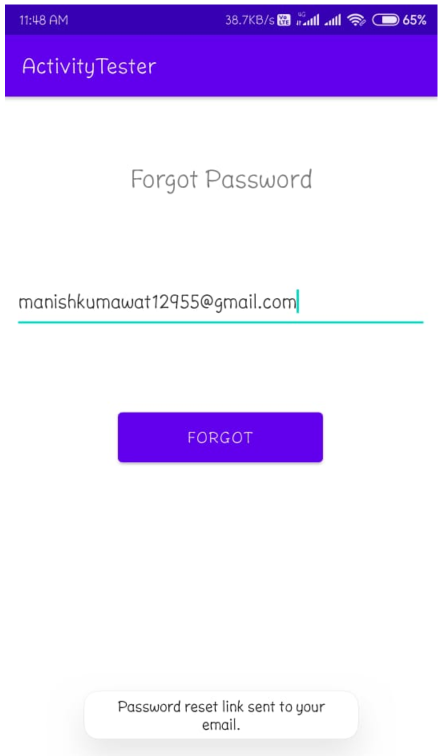


manishkumawat12955@gmail.com

••••••

Login not Successfull

Figure 3.10: Login Not Successful



manishkumawat12955@gmail.com

Password reset link sent to your email.

Figure 3.11: Forgot Password Page

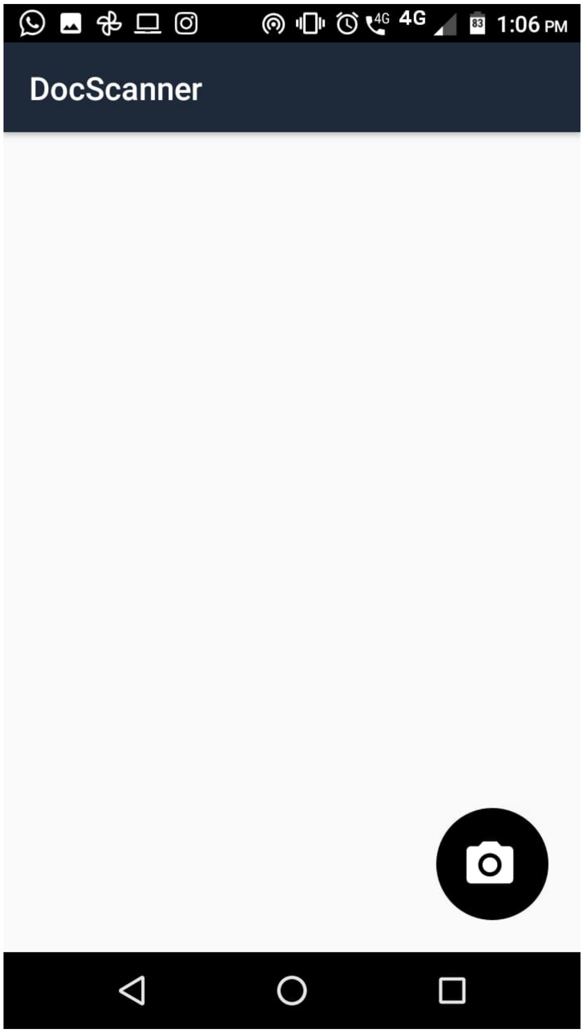
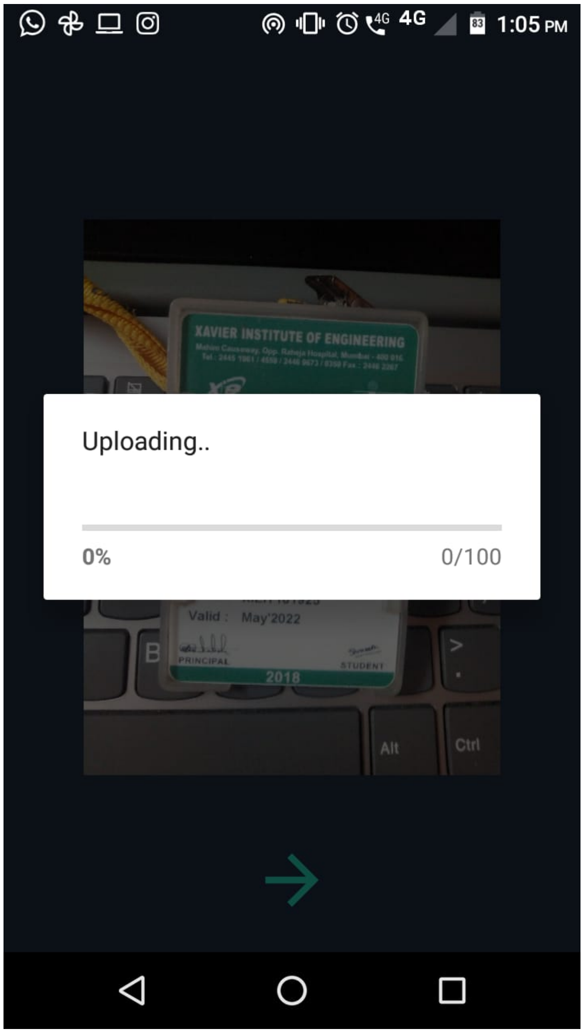


Figure 3.12: Scanning the documents



Uploading..

0%

0/100

Figure 3.13: Uploading the documents

PLAN FOR NEXT SEMESTER

Our Project “Digital Identity Management Using Blockchain” has been divided into 4 modules namely Front end development, Back end development, Blockchain module and Testing.

1. Front End Development: Firstly we will start building with the basic designs of the app, then start making the front end of our system containing every part of the system discussed and try completing it before the first month of the 7th semester and then move onto coding for the back end of our system.

2. Back End Development: Then we will move onto designing the back end of the app which will conclude the designing of the app. We will try completing this module before the second month of the 7th semester ends. And then we will move to implementing blockchain in our system. Further addition related to designing of the app will be done simultaneously.

3. Blockchain: In Blockchain , hashing will be utilized in hashing transaction and block data. A Digital signature refers to digitally signing a message in order to certify its authenticity and ensure the integrity of the message in peer-2-peer communication, which is achieved using the public key cryptography and hashing. As per the planning, we will be using the SHA256 algorithm for hashing purpose . Furthermore, all the user data will be stored in an encrypted manner with the encryption keys that are owned by the respective user who is the owner of the data. We will study and implemeted either of these symmetric-key algorithms like Rijndael AES, and the algorithm Diffie-Hellman key exchange can also be implemented. With this our system will be ready for testing purpose.

4. Testing: Lastly we will be using Truffle IDE for testing of the system.

REPORT OF INVESTIGATION ON THE EXISTING SYSTEM

Digilocker is basically a digital document wallet where you can store your documents. It is one of the main initiatives under the Programme Digital India . This was launched by the Information Technology and the Department of Electronics. It is used to store documents such as government issued documents, academic certificates etc., so that the documents can be shared easily on the web or wherever it is required. It provides access to the user to their stored documents for various public and private purposes. As it is a government made software and as a key initiative of the Digital India program, there was a beta version of DigiLocker launched. It basically works around Aadhar card number so it is a Aadhaar linked facility. But there are always security reasons related to Aadhaar card number and One Time Password generated which provides access to DigiLocker stored documents. There have been many such cases where OTPs has also been illegally accessed. And as of Aadhaar card numbers, they would be more easily known.

DigiLocker holds two types of certificates, one of which is educational and the second one is life time. There is an alert one month prior to the expiry date to some documents such as a driving license or a passport, and it may prompt to change it or update it and upload a updated document. The process being very transparent, once it gets logically linked with UIDAI and then PAN card, it can then verify more accurately by matching uniqueness of the user's first name, parent's name or relative's or guidance's name. But at the same time last name can be failure. There have been many security disadvantages of the system which includes the key security concerns of authentication, authorization at client-server both end and secure communication at the time of data traversal.

Despite that DigiLocker ensures traditional security like data integrity and secure data access, privacy and protection of e-documents is yet to made. As Digilocker makes use of the cloud storage to store the personal data of the users, but the cloud storage may not be safe and trustworthy and it may be susceptible to various kinds of attacks. Another drawback was the security while transferring of the documents to the requesting organizations and security while uploading of the documents by the resident

CONCLUSION

Thus we have planned on laying a foundation for a decentralized digital identity using Blockchain as Self-sovereign identity, including modern cryptography and verifiable digital credentials. We enlisted the problems and challenges that exists in the traditional identity management methods in terms of security, privacy, usability and globalization. We reviewed existing solutions in the literature, and proposed a blockchain system which leverages features of Blockchain to realize a protected, private, secure and globally usable digital identity system, in which identity owners have full control over their portable stored identity in the form of documents and identity based records or files. For future work, we intend to explore possibilities of integrating our solution on mobile applications, and try making it totally secured and make it usable to every range of age group and by any nation with ease.

REFERENCES

1. Mehmet Aydar, Serkan Ayvaz , Salih Cemil Cetin, “Towards a Blockchain based digital identity verification, record attestation and record sharing system”- June 2020

2. E. Bertino, “Digital Identity Management Techniques and Policies” - CS Department and ECE School, CERIAS, Purdue University

3. Akash Takyar, CEO LeewayHertz, “Blockchain Identity Management: Enabling Control Over Identity”- 2021

4. Zhimin Gao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, Weidong Shi, “Blockchain-based Identity Management with Mobile Device”- June 2018

5. Benedict Faber , Georg Michelet , Niklas Weidmann , Raghava Rao Mukkamala, Ravi Vatrapu, “BPDIMS:A Blockchain-based Personal Data and Identity Management System”- 2019

6. Puneet Bakshi, Sukumar Nandi “Privacy Enhanced DigiLocker using Ciphertext-Policy Attribute-Based Encryption”- Dec 2020

7. Dr. Vinay Kumar’ “A Solution to Secure Personal Data When Aadhaar is linked with DigiLocker”- May 2018

8. Xiwei Xu, Yue Liu, Hye Young Paik, Qinghua Lu, “Design Patterns for Blockchain-based Self-Sovereign Identity” - June 2020