

**A FRAMEWORK FOR IDENTITY MANAGEMENT SYSTEM USING
BLOCKCHAIN TECHNOLOGY**

BY

Razve Khan Tanmoy

ID: 191-15-12393

Nahian Siddique

ID: 191-15-12443

Md. Mujahidul Islam

ID: 191-15-12628

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Syada Tasmia Alvi

Lecturer

Department of CSE

Daffodil International University

Co-Supervised By

Sharmin Akter

Sr. Lecturer

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

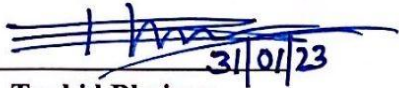
DHAKA, BANGLADESH

JANUARY 2023

APPROVAL

This Project/internship titled “A framework for Identity management system using blockchain technology”, submitted by Razve Khan Tanmoy ID: 191-15-12393, Nahian Siddique ID: 191-15-12443 and MD. Mujahidul Islam ID: 191-15-12628 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfilment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on *date*.

BOARD OF EXAMINERS



31/01/23

Dr. Touhid Bhuiyan

Professor and Head

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



Md. Abbas Ali Khan

Assistant Professor

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Ms. Aliza Ahmed Khan

Senior Lecturer

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Md. Sazzadur Rahman

Associate Professor

Institute of Information Technology
Jahangirnagar University

External Examiner

DECLARATION

We hereby declare that this project has been done by us under the supervision of **Syada Tasmia Alvi, Lecturer, Department of CSE Daffodil International University**. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

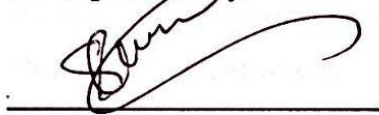
Supervised by:



Syada Tasmia Alvi

Lecturer
Department of CSE
Daffodil International University

Co-Supervised by:

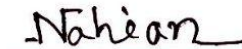


Sharmin Akter
Sr. Lecturer
Department of CSE
Daffodil International University

Submitted by:



Razve Khan Tanmoy
ID: -191-15-12393
Department of CSE
Daffodil International University



Nahian Siddique
ID: -191-15-12443
Department of CSE
Daffodil International University



MD. Mujahidul Islam
ID: -191-15-12628
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to **Syada Tasmia Alvi, Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “*Blockchain*” to carry out this project. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Professor Dr. Touhid Bhuiyan, Head Department of CSE**, and Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

Identification is important for a person and country. Identity contains valuable information. It contains fingerprints, Name, Date of Birth etc. By using this we can identify someone. So, it is very important to secure this data. Nowadays we are using a server to store the database. But somehow the unethical people managed to modify this data. And there they managed to get unauthorized access. This is a threat for a country. By using this they can easily get passports and other facilities. That's why the security of a person's identity is very important. Blockchain technology facilitates greater assurance in the data being shared across a network, providing enhanced security, improved transparency, and allowing for easier tracking of the information. If we use this technology in our identity system, this will increase trust. And the system will be secure enough. To ensure security of the identity system is our main purpose of our research-based project.

In our system we use Ethereum smart contract. We performed comprehensive testing in a variety of scenarios and conditions with a wide range of users using Remix IDE. Using Remix IDE, we can simulate a realistic situation that has an owner and multiple users by having access to multiple Ethereum wallets. Some security properties are anonymity, integrity, privacy, security, authenticity, trust, immutability, decentralization. Our system can ensure all those security properties. There are some security properties such as immutability which are ensured by our proposed system.

Table of content

CONTENTS	Page No
Board of examiners	i
Declaration	ii
Acknowledgements	iii
Abstract	iv
CHAPTER	
CHAPTER 1 : INTRODUCTION	1-3
1.1 Introduction	1-2
1.2 Motivation	2-3
1.3 Objective	3
1.4 Report layout	3
CHAPTER 2 BACKGROUND	4-5
2.1 Related work	4-5
CHAPTER 3: METHODOLOGY	6-13
3.1 Proposed Model	6
3.2 List of Notation	7-8
3.3.1 User data verification	8-10
3.3.2 Storing data in Blockchain	10-11
3.3.3 Authentication of valid user	12-13
CHAPTER 4: IMPLEMENTATION AND TESTING	14-24
4.1 Implementation	14-15
4.2 Gas cost function in our smart contract	15-22
4.3 Security property analysis	22-25

CONTENTS	Page No
4.4 Comparative analysis of property	26
CHAPTER 5: CONCLUSION AND FUTURE SCOPE	27
5.1 Discussion and conclusion	27
5.2 Scope for further developments	27
REFERENCES	28-29

LIST OF FIGURES

FIGURES

PAGE NO

Figure 3.1: Identity management model using Blockchain	6
Figure 4.1: Data input for new user	16
Figure 4.2: Successful user data entry	16
Figure 4.3: Get all user data	17
Figure 4.4: Gas value of get all data	17
Figure 4.5: get Specific data	17
Figure 4.6: user data index	18
Figure 4.7: user data visualization	19
Figure 4.8: Storage	20
Figure 4.9: Solidity state	20
Figure 4.10: Storing single user record	21
Figure 4.11: insert records in code	21
Figure 4.12: Function to get specific user data	22
Figure 4.13: function to get all the records	22

LIST OF TABLES

TABLES PAGE NO

Table 1: List of Notation	7-8
Table 2: Gas cost function in our smart contract	15
Table 3: Comparative Analysis of Property	26

CHAPTER 1

Introduction

1.1 Introduction

A government-issued number that is used to track citizens, permanent citizens and temporary residents for purposes such as education, work, tax, health care, etc. is referred to as a national identification number, national identity number, or national insurance number. A national identity system serves to associate a set of information with an individual, for example through the use of an identity card which can be used to verify someone's membership of a particular group. Having a national ID card is intended to make public and private transactions, school enrollment, and bank account openings simpler. It is hoped that this will lead to better efficiency, especially when dealing with government services, as people will only need to present one ID. However, due to international privacy regulations such as the General Data Protection Regulation, the security and privacy of the ID must be carefully taken into account to avoid data leaks or identity fraud, which can cause economic losses and reduce trust in identity providers. Therefore, it is necessary to explore new identity management solutions that meet these requirements. A centralized management and validation system is prone to disruption from a single point of vulnerability, leaving it vulnerable to cyberattacks like DDoS, DoS, and malicious software. Blockchain technology has emerged as a viable option for creating a secure and distributed platform for exchanging data. Blockchain is a type of database that is shared and maintained by a network of computers. It was first introduced through the Bitcoin ledger, however now many more exist globally. Each block consists of data such as transaction records, user information, and unique identifiers. Blockchain is appealing due to its features of being immutable, secure and transparent. Blockchain is a system of digital blocks linked together in a chain, each of which contains records of transactions. The connections between the blocks make it difficult to alter a single record, as a hacker would need to alter the block containing the record and the ones linked to it to avoid detection. Sadly, for those aspiring cyber criminals, blockchain technology is decentralized and spread through peer-to-peer networks that are constantly updated and kept in sync. As there is no centralized location, blockchain does not have a single point of vulnerability and cannot be modified from a single computer. It would

take an enormous amount of computing power to be able to control a large portion of a blockchain, so we have incorporated blockchain technology into our system to avoid this situation. In this research, our aim is to create an Identity Management System based on Blockchain technology that ensures maximum transparency and control for users regarding their personal data. We evaluate the safety features of the system to show that it can accurately link real-world data to the information stored on the blockchain. The cryptographically secure Ethereum blockchain is used in combination with distributed data storage systems to store data securely, while maintaining a decentralized system. This allows us to remove the need for centralized data storage systems while still ensuring data integrity and trust among users. Additionally, techniques such as hashing and encryption provide anonymity, privacy, and authenticity. Finally, immutability and decentralization further guarantee the security of the system.

1.2 Motivation:

We are Living at the age of modern technology. Everywhere we are using these technologies to make our life easy. Our goal is to make the world a better place for everyone, particularly those in need, through the implementation and utilization of blockchain technology. We anticipate that governments and companies will become more competent, effective, and reactive, and that individuals will be the major beneficiaries of these changes. After using technology in the identity sector, we can identify very effectively. Identity is very important for a person and a country. Identity contains valuable information. It contains fingerprints, Name, Date of Birth etc. By using this we can identify someone. So, this is very important to secure this data. Nowadays we are using a server to store the database. But somehow the unethical people managed to modify this data. And there they managed to get unauthorized access. In Bangladesh some Rohingyas got NID cards. This is a threat for a country. By using this they can easily get passports and other facilities. That's why the security of Identity is very important. And we will secure this total system. Here we have used Blockchain technology. This blockchain technology is the safest technology that has been invented yet. Blockchain technology facilitates greater assurance in the data being shared across a network, providing enhanced security, improved transparency, and allowing for easier tracking of the information. This will result in a reliable, unfilterable, and no consumable source of data and information

that can be accessed from any place on the globe. Blockchain technology is driven by the desire to decentralize, which is accomplished by sharing the computing tasks among the various nodes in the blockchain network. This decentralization eliminates some of the issues that are inherent in traditional systems, such as being prone to a single point of failure. Blockchain technology could be used to safeguard the interests of both consumers and creators of digital works by tracking the ownership of digital assets and potentially enforcing digital rights.

1.3 Objective

- To provide a method to secure the Identity system using blockchain technology.
- To validate the system to ensure only the legitimate users are allowed to use the system
- To increase trust between citizens about sharing their data.
- To analyze the system's performance based on different security properties

1.4 Report Layout

Chapter 1: Introduction

Motivation, objectives

Chapter 2: Background

Related works, comparison, scope of the problem and challenges.

Chapter 3: Methodology

Business process modeling, requirement collection and analysis, use case model, logical relational database model and design requirements.

Chapter 4: Implementation and

Implementation, Gas Cost, Figure of system, Security properties analysis, Comparative analysis of property.

Chapter 5: Conclusion and Future Scope

Discussion and Conclusion and Scope of further Development

Chapter 2

Background

2.1 Related Works:

They suggested a decentralized blockchain network, a decentralized approach for managing personal data that guarantees data ownership and control by people. Develop a system that transforms a blockchain into an automatic access-control manager without needing third-party trust. This platform uses standard cryptographic building blocks: a symmetric encryption method, a system for digital signatures, and an encryption hash function.

They offer a means of protecting the security of smart card data, which will benefit the government in ensuring the privacy of citizens' personal information and increasing information management openness. If citizens want access to third-party information, it will give them access control capabilities. Instead of a private network, suggest an open one. It uses an asymmetric cryptography algorithm to supply protection during the information exchange. To verify transactions and create new blocks for the chain, the PoW algorithm is utilized. For a blockchain calculation, a hash is a function that satisfies the encrypted requirements.

They provide a system that is constructed using smart contracts based on the Blockchain (qualities of decentralization and high security). By use of a smart contract, the attribute data is kept on the Blockchain. Here attributes (Hash, Value, Reputation, Grantee, Certificate) and services are two key ideas. They primarily categorize their services into two categories: authentication and authorization services.

They Make a Blockchain-based decentralized identity management system suggestion. Suggest a mechanism for managing identities based on the operative mechanism and the Ethereum Blockchain in this system's anarchism. The system comprises two components: an identification verification module (allowing a person's identification to match their Ethereum public key address), and a module for reputation management (trying to capture how an identity behaves inside the system).

They create a blockchain-based national identity management methodology and architecture. They used Blockchain in the smart city to quickly identify people and

deliver various government services. For this concept, use the Consortium blockchain. Where to provide the required assistance on a big scale, nodes are distributed and linked. As a result, the end user will have secure access to and control over their personal information.

They claimed that biometric technology, which automates the identification of people based on their biological and behavioral characteristics, provides better security and ease than traditional personal identification techniques. Specific biometric measurements are distinctive and reliable enough for identity management systems to use them as identifiers. Biometrics establish a one-to-one link between physical individuals and identity records and limit individuals to one document or set of records; biometrics have particular appeal in digital identity management. One frequently mentioned issue with biometrics is that some characteristics, even when gathered as verifiers, might serve as universal identifiers, enabling the data owners to link identity records.

They provide an identity management system, which enhances usability. Customers save their identities and login credentials from several service providers in a piece of hardware impervious to tampering, such as a smart card or other portable personal devices (personal authentication device). Protocol adaptability can be achieved by using a PAD (personal authentication device) that supports various authentication protocols and technologies without the need to update existing identity management systems.

Chapter 3

METHODOLOGY

The general architecture of the proposed system is shown in figure 3.1. We present a framework using Ethereum Blockchain via smart contracts for identity management of a user.

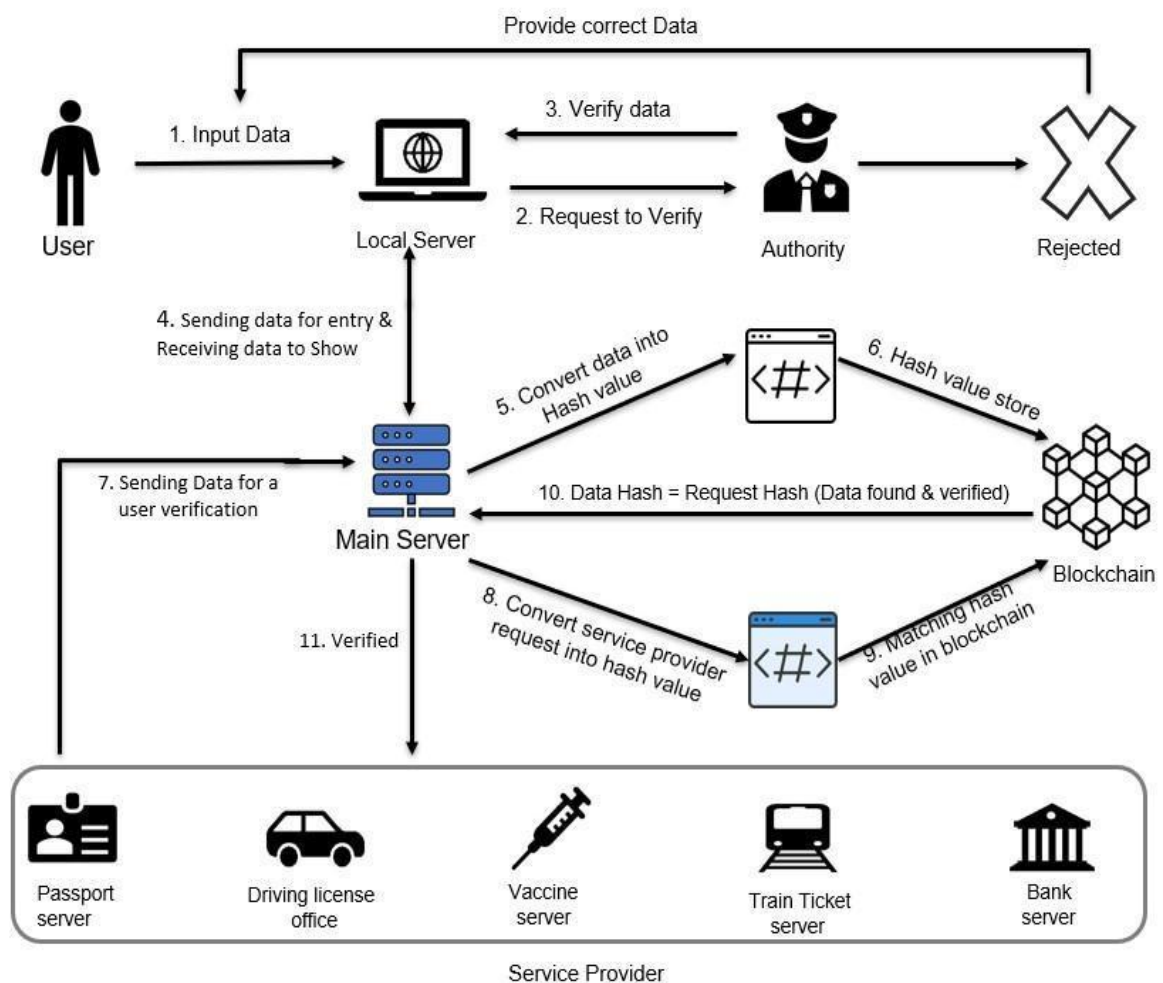


Fig 3.1: Identity management model using Blockchain

In our system, users should first input their credentials into the local server. The information will be verified by the authority who is assigned by the government. Verified data is sent to the main server from the local server. This data will be converted into hash value & stored in the Blockchain. In order to validate a user's data, service providers such as the passport office, driving license authority, vaccine server, train ticket server, bank server, etc. submit requests to the main server. The

main server transforms the request into a hash value and compares it to data hashes which are stored in the blockchain. If the requested hash and the data hash match, the blockchain will transmit the data to the main server for verification, and the main server will notify the service provider that the requested data has been validated.

There are three steps in our system

1. User data Verification
2. Storing data in Blockchain
3. Validate user data.

List of notation

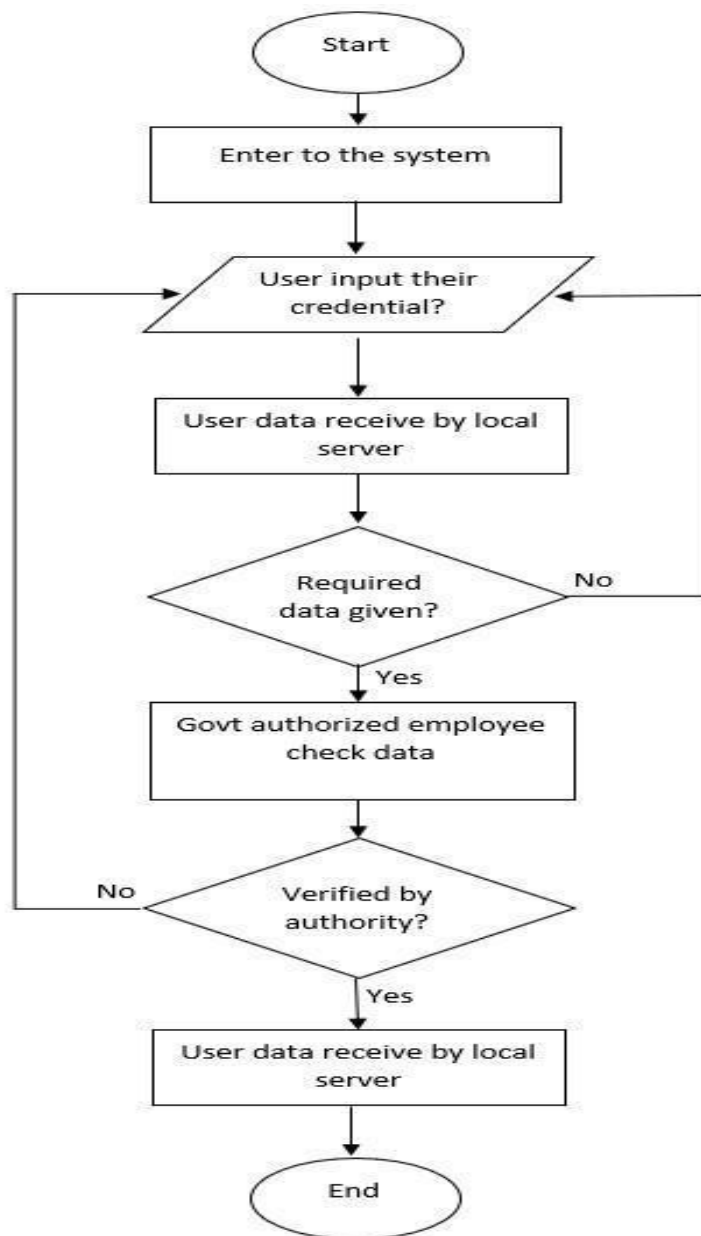
Table: 1

Notation	Definition
u	User
nm _U	User name
age _U	User age
gnd _U	User Gender
dob _U	User date of birth
ct _U	User contract number
hma _U	User home address
nid _U	User National identity number
U _C	User credential

VC_u	Verified user Credential
AU	Authority of system
LS	Local Server of the system
rjt	Rejected data by authority
MS	Main Server of the system
BC	Blockchain
D_{hv}	User Data converted to hash value
R_{hv}	Requested Data converted to hash value
SP	Service Provider
req_{SP}	Service Provider Request for data to main server
rec_{SP}	Service Provider receiving data from main server

3.1 User data verification

A user is the owner of the identity. The user needs to obtain a digital identity from the Authority, which can be used to identify him/herself. The user is not trusted, he/she may try to use others' digital identities. Authority verifies the user data. The user data verification process is shown in flowchart 1.



Flowchart 1: User data verification

Algorithm 1: User Data Verification

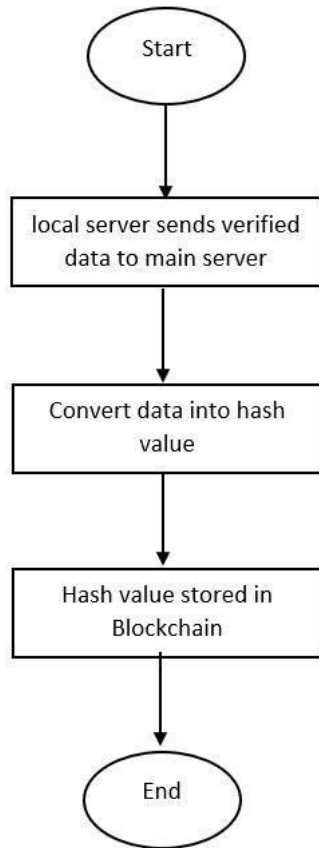
Input: $nm_U, age_U, gnd_U, ct_U, hma_U, nid_U$
Output: VU_C

- 1 Input $nm_U, age_U, gnd_U, ct_U, hma_U, nid_U$
- 2 **if** $GetRequiredData(nm_U, age_U, gnd_U, ct_U, hma_U, nid_U)$ **then**
- 3 send all U_C to the AU
- 4 **if** $VerifyUserCredential(U_C)$ **then**
- 5 Return "Verification of User Complete Successfully"
- 6 **else**
- 7 "Rejected"
- 8 goto step 1
- 9 **else**
- 10 go to step 1

Algorithm 1 illustrates the data verification process. In step 1, users have to input their credentials as input such as user name, user age, user date of birth, user contract number & most importantly, user national identity number, to the local server. The local server receives all information about a user and checks whether all the necessary information is given or not at step 2. If all information is given according to system requirements, the local server sends data to the authority at step 3. Verified data checked by the authority, if data is correct authority notifies the local server "verification of user successfully" at step 5. If all given data are not correct, then the authority rejects the request at step 7 and gets back to the user that gives correct and relevant information according to the requirement at step 8. Also, if required data is not given to the system re-enter user credential input at step 10.

3.2 Storing data in Blockchain

Blockchain has decentralized and strong security attributes. In our proposed system blockchain is used to store the hash value of user verified credentials.



Flowchart2: Storing data in Blockchain

Algorithm 2: Storing Data in Blockchain

Input: VC_u

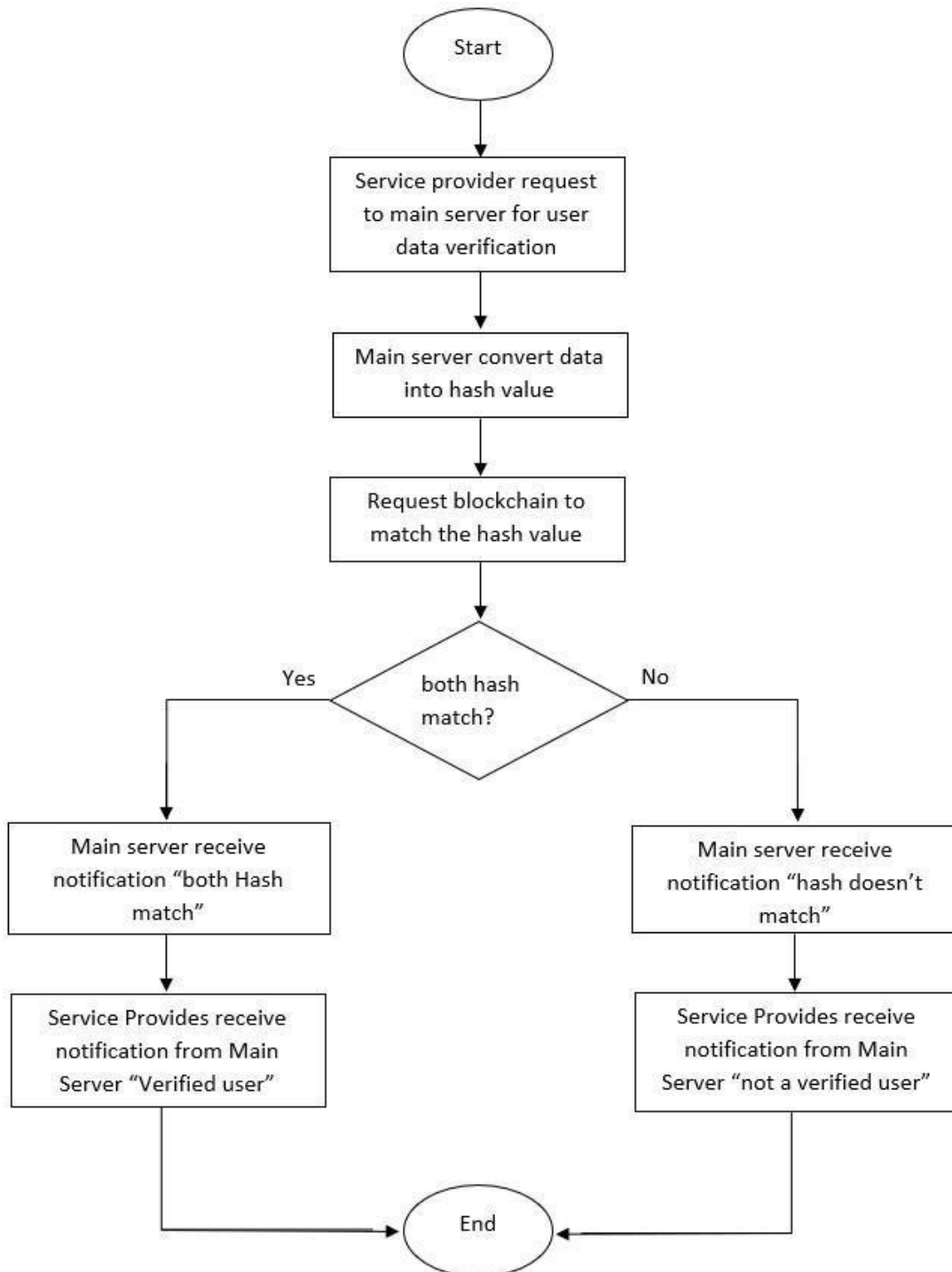
Output: D_{hv}

- 1 LS send VC_u to the MS
 - 2 $D_{hv} = \text{generateHash}(VC_u)$
 - 3 Store D_{hv} in BC
-

The local server sends all verified data to the main server as input at step 1. The main server receives all verified data from the local server and converts verified data into a hash value at step 2, which includes the user name, age, date of birth, contact number, home address, and national identity number. Blockchain stores hash data about a user for further verification or other using purposes at step 3.

3.3 Authentication of valid user

A Service Provider wants to verify the user authentication. Here service providers are: Passport Office, Vaccine server, Driving license authority, Train ticket server, Bank server.



Flowchart 3: Authentication of valid user

Algorithm 3: Authentication of valid user

Input: U_C, D_{hv}

Output: R_{hv}

- 1 SP submit U_C to MS
 - 2 $R_{hv} = \text{generateHash}(U_C)$
 - 3 **if** ($D_{hv} == R_{hv}$) **then**
 - 4 Return "Valid User"
 - 5 **else**
 - 6 Return "Not a Valid User"
-

Whenever a service provider needs to check a user data that the user is valid or invalid, they need to send a request to the main server by giving information about the user at step 1. Receiving the request from the service provider, the main server converts this request into hash value. This requested hash is sent to the blockchain, and the blockchain checks this request hash with a stored data hash at step 3. If the request hash matches with the stored data hash of a user, then the blockchain notifies the main server data is matched and the main server sends a message that requested user is valid at step 4. If the requested hash does not match the stored data hash, then the blockchain notifies the main server that the requested data is not found and the main server sends a message that requested user is not a valid user at step 6.

Chapter 4

IMPLEMENTATION AND SECURITY PROPERTY

4.1 IMPLEMENTATION:

We used the Remix IDE from <http://remix.ethereum.org/> to build and test our smart contract. Here, we put the Ethereum smart contracts through their paces to ensure proper operation across the board. The broad feature set provided by the Remix IDE makes it easy to test and troubleshoot smart contracts before putting them into production. The availability of several Ethereum wallets within Remix IDE enables us to mimic a real-world scenario that involves an owner as well as a number of users. In addition, there is a debugger that can be used to investigate different transactions and check that the contract is behaving as expected. This is made possible by the fact that the debugger is made public.

We used Remix IDE to conduct extensive testing on a number of different scenarios and conditions with a number of different users in order to guarantee that the contract would produce the expected logical functionality and execution outcome. These tests also guaranteed that the correct behavior would be exhibited, including access to function setters and modifiers, as well as the generation of an access token.

The authority and the service provider make up the two primary participating entities in our decentralized smart contract. Each of the entities has an Ethereum address, and they all have the ability to participate in the smart contract by making function calls at the appropriate times. Since direct function calls are handled by authority, it is forbidden for an entity to make any direct function calls. Because of the modifiers, the functions can only be called by certain individuals or organizations. To begin, as was covered in the preceding part of this article, one of the registered authorized persons is responsible for the creation of the smart contract. This contract contains information regarding the document, such as the document's name and its 256 hash. During this time, a registered authorized person creates and uploads a document. The hash value for this document is then stored in the contract.

After that, the authorized person will submit a request for permission by supplying the hash in order to update the new version of the chain. The version reference is only saved in the smart contract if it has been given the go-ahead for storage by at least two-thirds of all the approvers. This process is ongoing, with each authority uploading a new version of the software. In addition, the intelligent contract is used to oversee the registration of any new authority.

All registered authorized users need to accept and consent to the request before a "new" registration can be considered successful. The message sequence diagram for a new registration that was requested by either a developer or an approver. In this scenario, the new entity that wants to get registered will send a request to the smart contract by the main server. The request for fresh registration would only be accepted if it was supported by all of the participants who were actively taking part in the activity. If not 51% of the approvers provide their consent, the registration request made by a new participant approval will be turned down.

4.2 Gas cost function in our smart contract

(GAS PRICE = 2.4 WEI, 1 ETH '=1247\$)

Table: 2

Algorithm	Gas used	ETH	USD
Add new user	20438	0.00002526	0.0316
Get all data	41992	0.00005190	0.0649
Get specific data	4342	0.00000537	0.0067
Update data	10067	0.00001244	0.0155

User have to input their valid information to the system such as user name, user age, user date of birth, user contract number & most importantly user national identity number shown in figure 4.1

The image shows a web form titled 'newUser'. It contains seven input fields, each with a label on the left and a text box on the right. The labels and their corresponding values are: '_name: Mujahid', '_age: 23', '_gender: Male', '_dateOfiBrth: 07.03.2000', '_contact: 01626609516', '_homeAddress: Dhaka', and '_numNID: 6284589963'. At the bottom right of the form is an orange button labeled 'transact'. Below the button are two links: 'Calldata' and 'Parameters', each with a document icon.

Figure 4.1: Data input for new user

User given their required data and the data are verifying by authority. Then this data goes to main server as a successful new user entry which shown in figure 4.2.

```

[vm] from: 0x583...eddC4 to: identityManagement.newUser(string,uint256,string,string,uint256,string,uint256) 0xd91...39138 value: 0 wei data: 0xf61...00000 logs: 1 hash: 0x34c...2f858
transact to identityManagement.newUser pending ...

[vm] from: 0x583...eddC4 to: identityManagement.newUser(string,uint256,string,string,uint256,string,uint256) 0xd91...39138 value: 0 wei data: 0xf61...00000 logs: 1 hash: 0xa58...577cb
transact to identityManagement.newUser pending ...

[vm] from: 0x583...eddC4 to: identityManagement.newUser(string,uint256,string,string,uint256,string,uint256) 0xd91...39138 value: 0 wei data: 0xf61...00000 logs: 1 hash: 0x09c...3e81f
transact to identityManagement.newUser pending ...

[vm] from: 0x583...eddC4 to: identityManagement.newUser(string,uint256,string,string,uint256,string,uint256) 0xd91...39138 value: 0 wei data: 0xf61...00000 logs: 1 hash: 0x286...512ce
transact to identityManagement.newUser pending ...

[vm] from: 0x583...eddC4 to: identityManagement.newUser(string,uint256,string,string,uint256,string,uint256) 0xd91...39138 value: 0 wei data: 0xf61...00000 logs: 1 hash: 0xb7e...fe1b8
transact to identityManagement.newUser pending ...

[vm] from: 0x583...eddC4 to: identityManagement.newUser(string,uint256,string,string,uint256,string,uint256) 0xd91...39138 value: 0 wei data: 0xf61...00000 logs: 1 hash: 0xc8a...7bb6b
transact to identityManagement.newUser pending ...

[vm] from: 0x583...eddC4 to: identityManagement.newUser(string,uint256,string,string,uint256,string,uint256) 0xd91...39138 value: 0 wei data: 0xf61...00000 logs: 1 hash: 0xf79...ef13d

```

Figure 4.2: Successful user data entry

Get all data and provide the information about how much data is in the system. It shows all data which are already stored in the system shown in figure 4.3

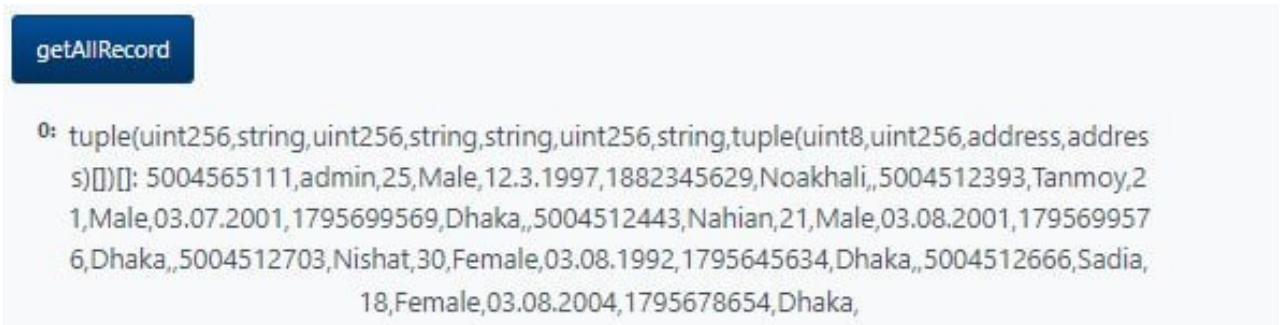


Figure 4.3: Get all user data

4.6

Total Gas consumes to store 6 data in the system shown in figure 4.4. This gas number depends on the number of data in the list. If the number of user data is increased so the gas value for getting all data also increases.

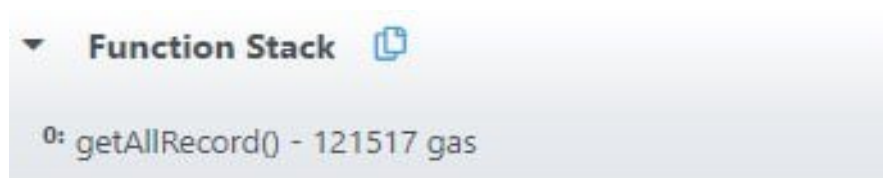


Figure 4.4: Gas value of get all data

If the main server wants to check if a user data is validated or not. Using NID number as the primary key, the Main server can search specific users shown in figure 4.5. If the user is already stored show the data else show empty data.

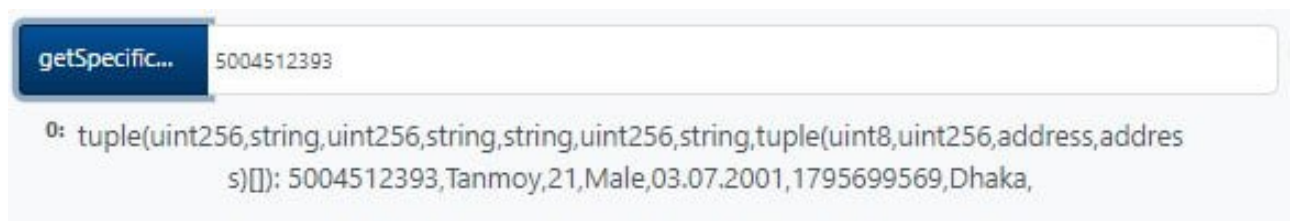


Figure 4.5: get Specific data

Owner can see the all data index list of users which have already been verified by the authority which is shown in figure 4.6.

```

owner:
0x5B38DA6A701C568545DCFCB03FCB875F56BEDDC4
address
▼ userRecord: struct identityManagement.User[]
length: 6
▶ 0: struct identityManagement.User
▶ 1: struct identityManagement.User
▶ 2: struct identityManagement.User
▶ 3: struct identityManagement.User
▶ 4: struct identityManagement.User
▶ 5: struct identityManagement.User
▼ userRecordIndex: mapping(uint256 => uint256)

0000000000000000000000000000000000000000000000000000000000000000
000000000ba6f37169: 2 uint256

0000000000000000000000000000000000000000000000000000000000000000
000000000ba6f3729f: 4 uint256

0000000000000000000000000000000000000000000000000000000000000000
000000000ba6f37254: 1 uint256

0000000000000000000000000000000000000000000000000000000000000000
000000000ba6f3719b: 3 uint256

0000000000000000000000000000000000000000000000000000000000000000
000000000ba6f3727a: 5 uint256

```

Figure 4.6: user data index

Owner can see the all data index list of users which have already been verified by the authority and every index has all information about user input user name, user age, user date of birth, user contract number & most importantly user national identity number shown at figure 4.7.

```
▼ 1: struct identityManagement.User
  numNID: 50045612628 uint256
  name: Mujahid string
  age: 22 uint256
  gender: Male string
  dateOfiBrth: 03.07.2000 string
  contact: 1626609516 uint256
  homeAddress: Noakhali string
  ▶ bT: struct identityManagement.UpdateData[]
▼ 2: struct identityManagement.User
  numNID: 50045612393 uint256
  name: Tanmoy string
  age: 21 uint256
  gender: Male string
  dateOfiBrth: 24.09.2001 string
  contact: 1795699569 uint256
  homeAddress: Dhaka string
  ▼ bT: struct identityManagement.UpdateData[]
    length: 0
▼ 3: struct identityManagement.User
  numNID: 50045612443 uint256
  name: Nahian string
  age: 21 uint256
  gender: Male string
  dateOfiBrth: 03.08.2001 string
  contact: 1795699576 uint256
```

Figure 4.7: user data visualization

Storage address of the system as an object which is shown in figure 4.8.

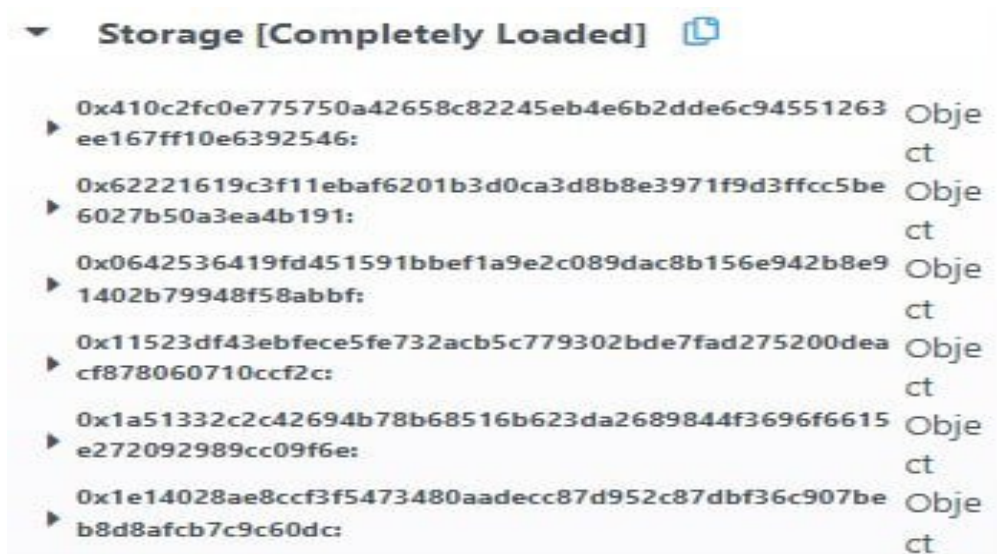


Figure 4.8: Storage

Solidity state is where owner can see the index of user list shown at figure 4.9



Figure 4.9: Solidity state

Storing a single user record in code where we recorded NID number, name, ages, gender, date of Birth, contact, home address shown in figure 4.10.

```

// Used for storing single user records
struct User {
    uint256 numNID;
    string name;
    uint256 age;
    string gender;
    string dateOfiBrth;
    uint256 contact;
    string homeAddress;
    UpdateData[] bT;
}

```

Figure 4.10: Storing single user record

We inserted name, age, gender, date of birth, contact, home address, nid number by using this code which is shown in 4.11.

```

// insert records
userRecord.push();
userRecord[index].name = _name;
userRecord[index].age = _age;
userRecord[index].gender = _gender;
userRecord[index].dateOfiBrth = _dateOfiBrth;
userRecord[index].contact = _contact;
userRecord[index].homeAddress = _homeAddress;
userRecord[index].numNID = _numNID;

```

Figure 4.11: insert records in code

This portion of code show the function for get user data of a specific user which is shown in 4.12

```
// function to get specific user data
function getSpecificUserData(uint256 _numNID)
  external
  view
  returns (User memory)
{
  uint256 index = userRecordIndex[_numNID];
  return userRecord[index];
}
```

Figure 4.12: Function to get specific user data

This portion of code will show the full record of user data which shown in 4.13

```
// function to get all the records
function getAllRecord() external view returns (User[] memory) { PUSH1 costs 3 gas - this line costs 174540 gas - 2978779 gas left
  return userRecord;
}
```

Figure 4.13: function to get all the records

4.3 Security property analysis

This section examines the security and privacy capabilities of a blockchain-based identity system from a theoretical perspective.

4.3.1 Authentication:

physical data and the system address is needed to establish an identity. This combination of information cannot be used to create a second identity. To validate the identity authentication, we employ three sets of input data. If someone attempts to

create an account with different identity information but with the same system address as an existing user, that attempt will be unsuccessful. [21] In our proposed system, users must enter their information into the local server. The local server then verifies the user's identity before sending the data to the main server. This way, the integrity of the data is secured.

4.3.2 Immutability:

Blockchain is characterized by immutability, meaning that data stored on it cannot be altered without the agreement of all participating nodes, leading to an extremely secure level of data integrity. [22] The blockchain system being proposed will keep the user data secure by hashing the pointers and storing them on external repositories. The trust that comes with blockchain technology will be incredibly useful in protecting data privacy.

4.3.3 Transparency:

Blockchain offers complete visibility and verifiable evidence about various transactions associated with user information and identity management, which will strengthen the faith and security of the system for all users and providers. Our proposed system utilizes blockchain technology to ensure transparency. Every individual connected to the network can track the transactions registered on the blockchain, making it impossible for anyone to tamper with the data.

4.43 Anonymity:

Blockchain's anonymity feature permits users to hide their identity and details when it is needed. Furthermore, the decentralized and distributed consensus protocols of blockchain make it difficult for malicious actors to take control of the system. Unless someone has more than a majority of the network's power (51%), any false entries or changes to the data will not be accepted. The hash function offers anonymity, so this system allows for users to enter their information into the blockchain without revealing their identity. In this system, data is encoded into a unique code (hash) which guarantees that user privacy is protected and users can verify their identity without having to reveal who they are. In the blockchain network, the public key serves as an identifier for the user, while the hash value is a representation of the user's data.

4.3.5 Privacy:

Privacy preservation is the safeguarding of users' sensitive data, including personal details, locations, movements, and habits, from unauthorized access by third parties. [20] Our proposed model suggests the use of privacy-enhancing encryption and destruction techniques to safeguard an individual's privacy rights, such as hashing data or applying other forms of data transformation to personal information, as well as revoking access rights to a blockchain application.

4.3.6 Trust:

Users and service providers within the same security domain trust and depend on the same identity provider, ensuring that their personal data is safe from exploitation or misuse by the identity provider or any other external parties. Numerous times, devices are vulnerable, leaving personal information repositories open to theft by malicious intruders. When it comes to maintaining privacy and being sustainable in the IoT era, where everything is connected, the implicit faith in identity providers is called into question, rendering the centralized identity paradigm outmoded. The growing number of online service providers and identity suppliers isolates and fragments digital identities across the Internet, despite the fact that businesses (like Google or Facebook) aim to provide uniform identity providers for all cyber-users and service providers. Unquestionably, blockchain-based identity management systems remove the need for superfluous information to be disclosed to other parties and offer numerous positive attributes including immutability, impartiality, and secure timestamping that can be utilized to establish confidence. Decentralized applications that operate on their own should be created by redesigning the applications. [20] No unauthorized individuals are able to access user records in the system we offer. Furthermore, no one is permitted to alter user data without consent. Additionally, we are protecting the user's privacy. Thus, this will guarantee the user's trust.

4.3.7 Decentralization:

The fundamental concept of decentralization has become increasingly popular as blockchain technology has advanced. Blockchain is a decentralized network where

users retain identical data replication while exchanging data with other node members. Blockchain technology offers features including data accuracy, privacy, and distribution. A trustworthy and secure Identity management system can be created with the use of blockchain technology. [5] Access is spread among several environments via decentralized identity management. Individuals can keep identification-related information in a digital wallet thanks to the decentralized identity concept. The implementation of blockchain in our system has made our data decentralized.

4.3.8 Integrity:

To protect critical identity attributes or to spot any tampering with the identity attributes, an identity system's integrity is crucial. Anytime a user needs to be verified, he must give some identifying information to a third party. Diffie and Hellman's concept of public key cryptography was put forth in order to protect the integrity. The authors asserted that it might not be adequate in terms of identification, nevertheless. Identity theft may potentially result from careless message security. [26] Merkle trees are a feature of blockchain technology that guarantee data integrity. Ethereum has implemented the Merkle tree concept to enable a condensed and effective verifiable proof that guarantees a transaction is included in a block. [5] Users should not be altered, falsified, or secretly eliminated. The integrity of the results is a key idea during the identification process. A component of blockchain technology that ensures data integrity is the Merkle tree. The blockchain has a predetermined number of transactions in each block. Every transaction that takes place on the blockchain is documented in a data structure called the Merkle tree. Because the data is permanently saved and cannot be altered or erased, the technology satisfies the primary criteria for data integrity. We can ensure integrity by employing this.

4.4 Comparative Analysis of Property

The comparison between the known works and our suggested mechanisms is shown in Table 4.2. We can observe from this comparison that [10, 11,17,19] do not offer anonymity. Integrity is not provided by [6,11,19]. It doesn't offer privacy, [19]. Authenticity is not provided by [10]. [6,10] don't inspire confidence. Both Decentralization and Immutability are absent from [6,11,19]. Our proposed system provides anonymity, integrity, privacy, security, authenticity, trust, immutability, and decentralization in order to achieve a fair and democratic result. Based on the analysis, we can see that none of the existing works provide all the security properties together in their systems.

Comparative Analysis of Property

Table: 3

Properties	[6]	[10]	[11]	[17]	[19]	Proposed methodology
Anonymity	✓	X	X	X	X	✓
Integrity	X	✓	X	✓	X	✓
Privacy	✓	✓	✓	✓	X	✓
Security	✓	✓	✓	✓	✓	✓
Authenticity	✓	X	✓	✓	✓	✓
Trust	X	X	✓	X	✓	✓
Immutability	X	✓	X	✓	X	✓
Decentralized	✓	✓	X	✓	X	✓

Chapter 5

CONCLUSION AND FUTURE SCOPE

5.1 Discussion and Conclusion

Identity management is crucial for both an individual and a nation. Almost all of our crucial tasks are completed with the help of this ID card. We rely on this in our daily lives. We use this identity in the banking, ticket, passport, shot, and driver's license industries. Security is being ensured by our blockchain. Blockchain identity management that is implemented well can raise the bar for security and privacy. Third parties can validate the user's data without wasting time or money thanks to the immutable and decentralized ledger. Blockchain is decentralized, making it impossible for unauthorized parties to alter the dataset. If some unauthorized individuals attempt to alter the database, they must alter the entire blockchain dataset. Thus, it is practically impossible for unauthorized individuals to update.

5.2 Scope for Further Developments

Any development project has no end to develop. So, we have also to develop this project

in the future. Here some of the plans are given below:

- We wish to integrate it with the present data server for our nation.
- Make it accessible across various industries
- Assures that all users of the network have access to the same reliable data.
- Increase both internal and external trust in the organization.
- We'll work to keep it affordable.

References:

- [1] Md Anisur Rahman Tonu, Sharfuzzaman Hridoy, M Ameer Ali, and Salahuddin A Azad. Block-nid: A conceptual secure blockchain based national identity management system model. In 2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), pages 1–7. IEEE, 2019.
- [2] AR Khan. National identity card: The dilemma between social opportunities and threats. *International Journal of Multidisciplinary Studies*, 5(1), 2018.
- [3] Andreea-Elena Panait, Ruxandra F Olimid, and Alin Stefanescu. Identity management on blockchain–privacy and security aspects. arXiv preprint arXiv:2004.13107, 2020.
- [4] Noe Elisa, Longzhi Yang, Fei Chao, and Yi Cao. A framework of blockchain-based secure and privacy-preserving e-government system, *Wireless networks*, pages 1–11, 2018.
- [5] Alvi, S.T., Uddin, M.N., Islam, L. and Ahamed, S., 2022. DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *Journal of King Saud University-Computer and Information Sciences*, 34(9), pp.6855-6871.
- [6] Kaaniche, N., Laurent, M., Kaaniche, N., Laurent, M., 2018. A blockchain-based data usage auditing architecture with enhanced privacy and availability to cite this version Availability. In: In Network Computing and Applications (NCA), 2017 IEEE 16th International Symposium on IEEE, pp. 1–5.
- [7] Datta, P., Bhowmik, A., Shome, A. and Biswas, M., 2020, November. A secured smart national identity card management design using blockchain. In 2020 2nd international conference on advanced information and communication technology (ICAICT) (pp. 291-296). IEEE.
- [8] Zhao, Z. and Liu, Y., 2019, September. A blockchain based identity management system considering reputation. In 2019 2nd International Conference on Information Systems and Computer Aided Education (ICISCAE) (pp. 32-36). IEEE.
- [9] Liu, Y., Zhao, Z., Guo, G., Wang, X., Tan, Z. and Wang, S., 2017, August. An identity management system based on blockchain. In 2017 15th Annual Conference on Privacy, Security and Trust (PST) (pp. 44-4409). IEEE.
- [10] B. Shahzad and J. Crowcroft, “Trustworthy electronic voting using adjusted blockchain technology,” *IEEE Access*, vol. 7, pp. 24 477–24 488, 2019.
- [11] Jøsang, A. and Pope, S., 2005, May. User centric identity management. In AusCERT Asia Pacific information technology security conference (Vol. 22, p. 2005).
- [12] Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R.R. and Avital, M., 2021. Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, 2(2), p.100014.
- [13] Khan, A.R., 2018. National Identity Card: The Dilemma between Social Opportunities and Threats. *International Journal of Multidisciplinary Studies*, 5(1).
- [14] Panait, A.E., Olimid, R.F. and Stefanescu, A., 2020. Identity Management on Blockchain–Privacy and Security Aspects. arXiv preprint arXiv:2004.13107.
- [15] Elisa, N., Yang, L., Chao, F. and Cao, Y., 2018. A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless networks*, pp.1-11.

- [16] Rana, R., Zaeem, R.N. and Barber, K.S., 2019, October. An assessment of blockchain identity solutions: Minimizing risk and liability of authentication. In 2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI) (pp. 26-33). IEEE.
- [17] Buccafurri, F., Lax, G., Russo, A. and Zunino, G., 2018, October. Integrating digital identity and blockchain. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"* (pp. 568-585). Springer, Cham.
- [18]] Zyskind, G. and Nathan, O., 2015, May. Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.
- [19] Volner, R. and Boreš, P., 2009. Biometric Techniques in identity management systems. *Elektronika ir Elektrotechnika*, 95(7), pp.55-58.
- [20] Zhu, X. and Badr, Y., 2018, July. A survey on blockchain-based identity management systems for the Internet of Things. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1568-1573). IEEE.
- [21] Amujo, O., Ebelogu, C.U., Agu, E.O. and Hammawa, M.B., 2019. Development of a National Identity Management System using Blockchain Technology.
- [22] Faber, B., Michelet, G.C., Weidmann, N., Mukkamala, R.R. and Vatrappu, R., 2019. BPDIMS: A blockchain-based personal data and identity management system.
- [23] Rathee, T. and Singh, P., 2021. A systematic literature mapping on secure identity management using blockchain technology. *Journal of King Saud University-Computer and Information Sciences*.

Identity Management

ORIGINALITY REPORT

15%

SIMILARITY INDEX

10%

INTERNET SOURCES

9%

PUBLICATIONS

5%

STUDENT PAPERS

PRIMARY SOURCES

- | | | |
|---|--|----|
| 1 | Submitted to Daffodil International University
Student Paper | 3% |
| 2 | repository.uwl.ac.uk
Internet Source | 2% |
| 3 | Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, Sajib Ahamed. "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system", Journal of King Saud University - Computer and Information Sciences, 2022
Publication | 1% |
| 4 | Submitted to Heriot-Watt University
Student Paper | 1% |
| 5 | Zhimin Gao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, Weidong Shi. "Blockchain-based Identity Management with Mobile Device", Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock'18, 2018 | 1% |