IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

SECURE PERSONAL DATA SHARING USING BLOCKCHAIN

MRS.G.PRANITHA[1] ,KATARI JAHNAVI[2] ,THOTA NARENDRA NADH [3] ,BOGICHANDINI[4] ,GUDIVADA VENKATA SAI CHANDRA SEKHAR [5],PATTHIGIDI NAGARAJU [6]

[1]Assistant Professor , Dept of Computer Science and Engineering , Anil NeerukondaInstitute Of Technology and Sciences , Visakhapatnam, India

[2,3,4,5,6]Students, Dept of Computer Science and Engineering , Anil NeerukondaInstitute Of Technology and Sciences , Visakhapatnam, India

Abstract:

The sharing of personal data poses a significant security risk, especially when using traditional centralized systems. The use of blockchain technology can provide a solution to this issue by creating a decentralized system that ensures the security and privacy of personal data.

To further enhance the security of personal data, identity-based encryption (IBE) can be used. IBE permits users to encrypt data using their identity information, such as their email address, instead of using a public key. This method ensures that the designated recipient alone can decipher the data, providing an added layer of security.

The use of Interplanetary File System (IPFS) for storing image files also provides a more secure way of sharing personal data. IPFS is a decentralized file storage system that uses content addressing instead of location addressing. This means that the files are stored across the network, making it almost impossible for anyone to tamper with or delete them.

Overall, the combination of blockchain technology, IBE, and IPFS provides a highly secure and decentralized system for sharing personal data.

IndexTerms:

Block chain, Identity based encryption, public key, private key, Interplanetary file system, encryption, decryption. ,CocksPKG

I. INTRODUCTION

With the increasing digitization of our lives, personal data has become a valuable asset. However, the existing data sharing systems often fail to protect user privacy and provide transparency, trust, and security. Blockchain technology has emerged as a promising solution to these challenges by offering decentralization, immutability, and transparency. Identity-based encryption (IBE) is a cryptographic technique that utilizes user identities instead of traditional public-private key pairs to encrypt and decrypt data, enhancing security and privacy. In this project, we propose a blockchain-based personal data sharing system that utilizes IBE to provide secure and transparent data sharing.The proposed system enables users to have control over their personal data and eliminates the need for a central authority to manage encryption keys, enhancing privacy protection. We aim to demonstrate the feasibility and effectiveness of our approach through a prototype implementation and experimental evaluation. The results of this project have the potential to contribute to the development of secure and transparent personal data sharing systems that can be applied to various use cases, including healthcare and financial industries

II. RELATED PAPER WORK

Identity-based encryption (IBE) was proposed by Adi Shamir in 1984, but the first practical instantiation of IBE was given by Boneh-Franklin scheme and Cocks's encryption scheme in 2001. Dr. Dan Boneh and Dr. Matt Franklin were the researchers who proposed the Boneh-Franklin IBE scheme, which is one of the most widely used IBE schemes today.

Shamir[1] proposed that recipient public key be calculated mathematically from their individual identities like name,mail,phno etc and the key server calculate the private key which leads to an advantage of overcoming the need for public key queries or certificates. Initially when sender wants to send message to reciever he signs with private key in smart card and encrypt using reciever public key and add his own name. When receiver receives the message he decrypts using his own private keyin smart card and view the message.However, while Shamir constructed an Identity Based Signature which has the drawbacks of single point failure and share revocation.

Boneh and Franklin's[2] Identity-Based Encryption (IBE) from the Weil Pairing is a cryptographic scheme that enables a user to encrypt and decrypt messagesusing their email address or any other unique identifier, instead of using a complex public key. The scheme is based on the Weil pairing, which is a mathematical construct that allows two different groups to be paired together.However, it also has some limitations, such as higher computational requirements and the lack of a straightforward method for key revocation.

Gagné [3] explains Authenticated ID-Based Encryption, where message authentication is given without incurring any extra computational costs. To put it another way, the recipient confirms the sender's identification and whether the message has been tampered with, negating the need for digital signatures in situations where verification is necessary. Secure verified communication is thus feasible.

"A Blockchain-Based Privacy-Preserving Data Sharing Scheme forHealthcare" by R. Ranjan and A. K. Das[4] , in IEEE Access (2020). This paper proposes a blockchain-based privacy-preserving data sharing scheme for healthcare that uses identity-based encryption to protect the privacy of sensitive data. The authors evaluate the proposed scheme using a simulation, and the results demonstrate that it is effective in protecting the privacy of sensitive data.

"A Blockchain-Based Privacy-Preserving Personal Health Record Exchange System" by Yong Liu et al[5]. This paper presents a blockchain-based system for exchanging personal health records with privacy-preserving features using identity- based encryption. The authors use a permissioned blockchain to store encrypted data and smart contracts to manage access control. They also propose a novel identity- based encryption scheme that enables efficient encryption and decryption of personal health records.

Venkatesh and Karthik [6](2021) proposed a framework for secure and privacy-preserving personal data sharing in healthcare using blockchain and identity- based encryption. They used a modified version of the Cocks-Pinch identity-based encryption scheme to protect the privacy of sensitive personal data.

Huang et al. [7](2019) presented a blockchain-based secure personal health record sharing system using attribute-based encryption. They used Ethereum as the blockchain platform and ciphertext-policy attribute-based encryption to control access to personal health records.

Li et al.[8] (2019) proposed a decentralized personal data management system based on blockchain. They used attribute-based encryption to encrypt personal data and control access. Their system also used smart contracts to automate data access management.

Chen et al.[9] (2019) proposed a blockchain-based personal data management system using attribute-based encryption. They used the elliptic curve variant of the BSW scheme for attribute-based encryption and a consortium blockchain platform fordata management.

Kumar et al.[10] (2019) proposed a blockchain-based secure personal data sharing system using identity-based encryption. They used the Boneh-Franklin identity-based encryption scheme and Ethereum as the blockchain platform.

Dan Boneh and Matthew Franklin[11] proposed a new cryptographic primitive called Identity-Based Encryption (IBE) which allows encryption and decryption using a user's identity instead of a public key. The authors introduce a method for constructing IBE systems using elliptic curve pairings.

Victor Shoup[12] presented a general framework for constructing Identity- Based Encryption (IBE) schemes. The author provides a construction for IBE based on bilinear maps, and proves its security under the Decisional Bilinear Diffie-Hellman assumption.

Benoit Libert, Damien Vergnaud, and Romain Vuillemot[13] (2013) introduced a new framework for Identity-Based Encryption (IBE) that allows for flexible and fine-grained control over the decryption policy. The authors propose a construction based on the concept of predicate encryption, which enables a wide range of decryption policies to be expressed.

Amit Sahai and Brent Waters[14] proposed a new variant of Identity-Based Encryption (IBE) called Fuzzy Identity-Based Encryption (FIBE). FIBE allows for the decryption of ciphertexts by a set of users whose identities satisfy certain fuzzy predicates. The authors propose a construction based on bilinear maps and prove its security under the Decisional Bilinear Diffie-Hellman assumption.

Jan Camenisch and Anna Lysyanskaya[15] proposed a new digital signature scheme that allows for efficient revocation of signatures. The authors propose aconstruction based on Identity-Based Encryption (IBE) and show how it can be usedto revoke signatures issued to a particular identity. They prove the security of the scheme under the Decisional Bilinear Diffie-Hellman assumption.

III. MOTIVATION

To address the challenges of existing data sharing systems and develop a secure and transparent approach to personal data sharing, leveraging the benefits of blockchain and IBE technologies. The proposed system has the potential to provide users with control over their personal data, enhance privacy protection by removes the dependence on third parties for key generation(public key,private key), and contributeto the development of secure and transparent data sharing systems that can be applied to various use cases.

IV. PRELIMINERIES

4.1 Blockchain:

Blockchain is a decentralised digital ledger technology that makes it possible for numerous parties to securely and openly record, keep, and exchange information. It is built on a distributed network of nodes that cooperate to confirm and check transactions, guaranteeing the accuracy and immutability of the data recorded on the blockchain.

The main usage of blockchain are:

1. Decentralization: Blockchain eliminates the need for intermediaries such as banks or other financial institutions, allowing for direct peer-to-peer transactions. This reduces costs, increases efficiency, and improves transparency.
2. Security: Blockchain uses cryptographic techniques to secure transactions and prevent tampering, making it virtually impossible to alter or manipulate the datastored on the blockchain.
3. Trust: Blockchain enables trust between parties, as it provides a shared record of data that cannot be altered or manipulated without consensus from the network.

4.2 Identity Based Encryption:

Identity-based encryption (IBE) is a form of public-key encryption in which the public key is a user's distinctive identifier, such as an email address or username. The private key in IBE is created by a trustworthy third party known as the private key generator (PKG), who maps the user's identifier to a private key, eliminating the need for sharing public keys, which can be a complicated process.

The main usage of IBE are:

1. Improved accessibility: IBE makes it easier for users to participate in securecommunication by removing the need for public key distribution.
2. Simplified key management: IBE eliminates the need for users to generate andmanage public key pairs, making key management simpler and more efficient.
3. Flexibility: IBE allows for flexible access control, enabling users to encrypt databased on various attributes such as job title or department.

4.3 Cocks Cryptography:

Cocks cryptosystem is a public-key cryptosystem that is based on the subset- sum problem, which is a hard computational problem that involves finding a subset ofa given set of integers that sums to a specified value. The Cocks cryptosystem uses a matrix of random integers to generate the public and private keys, and encryption and decryption involve matrix operations.

Encryption :

```
cocks_pkg = CocksPKG()
public_key, private_key = cocks_pkg.extract(user) #generate public and private keyusing 'user' identity
cocks = Cocks(cocks_pkg.n)
enc = cocks.encrypt(post_message.encode(), private_key) #encrypt data by usingprivate key data will be encrypted and store in Blockchain
enc = str(enc[0])
```

Decryption:

```
enc = int(enc)
cocks_pkg = CocksPKG()
private_key = cocks_pkg.extract(user) #extracting private key from user identitycocks = Cocks(cocks_pkg.n)
decrypted_bytes = cocks.decrypt((enc,), private_key) decrypt data by using privatekey and encrypted message
decrypted_message = decrypted_bytes.decode()
```

4.4 Interplanery File System:

InterPlanetary File System (IPFS) is a distributed file system that allows users to store and access files from a decentralized network of computers. IPFS uses a content-addressed system, which means that each file is given a unique hash based on its content, making it easy to retrieve and verify files.

4.5 Smart Contracts:

Here smart contract is used to save the details of the user in the block chainand to retrieve the details of the user from the block chain. A smart contract is a computer programme that autonomously executes the conditions of a deal between two parties. A blockchain is a decentralised and distributed digital ledger that documents activities across a network of machines. Smart contracts work by automatically executing the terms of an agreement when certain predefined conditionsare met. The conditions and actions of the smart contract are encoded into the program code and stored on the blockchain.

4.6 Truffle:

Truffle is a development framework that makes it easier to create and implement smart contracts on blockchain networks like Ethereum. The Truffle architecture includes a set of tools for developing, testing, and deploying smart contracts.

V. METHODOLOGIES

The proposed system enables users to have control over their personal dataand eliminates the need for a central authority to manage encryption keys, enhancing privacy protection. We aim to demonstrate the feasibility and effectiveness of our approach through a prototype implementation and experimental evaluation. The results of this project have the potential to contribute to the development of secure andtransparent personal data sharing systems that can be applied to various use cases, including healthcare and financial industries.

5.1 System Architecture:

Based on the literature survey, we finally decided to implement this project by using identitybased encryption and making use of the cocks cryptography algorithm for generating public and private keys. Not only that this method is efficient, but italso provides better results in terms of data privacy.

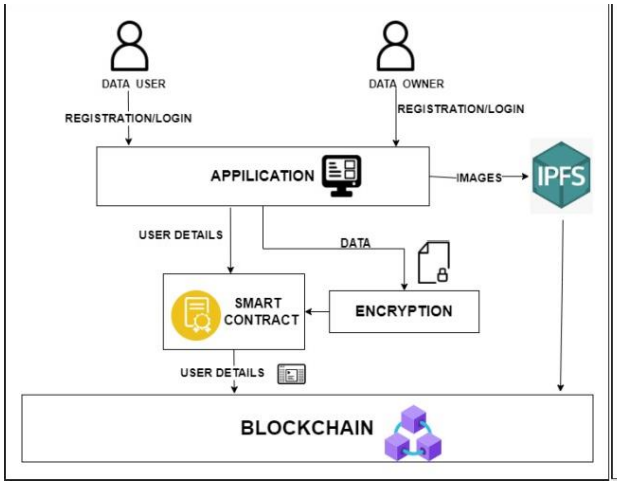

Fig 1

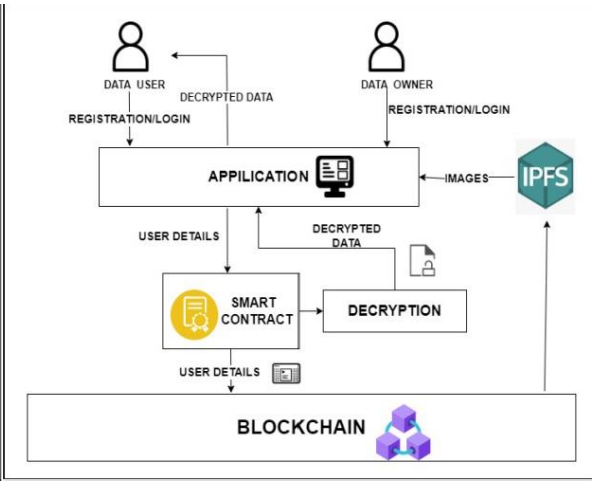

Fig 2

This approach has the following steps:

Encryption:

1. The user provides their address and plaintext message to a smart contract on theblockchain.
2. The smart contract extracts the user's public-private key pair from the CocksPKGsystem parameters using the extract() method.
3. The smart contract uses the private key and the Cocks encryption algorithm toencrypt the plaintext message.
4. The ciphertext is returned to the user.

Decryption:

1. The user provides the ciphertext to the smart contract on the blockchain.
2. The smart contract converts the ciphertext string to an integer.
3. The smart contract uses the public key and the Cocks decryption algorithm todecrypt the ciphertext.
4. The original plaintext message is returned to the user.

5.2 Modules:

5.2.1 Registration:

As shown in Fig1 Intially the sender registers/ login to the appilication by giving his details like name,phone number,mail,password etc to share the data similary receiver register/login to the appilication in order to view the shared data shown in Fig2.

5.2.2 Creating a contract:

As shown in Fig 1,After providing the details the smart contat will be executedand the records will be saved in blockchain that get never get tampered.

5.2.3 Encryption:

The encryption is done on sender's side(Data Owner) where after generating the keys (private and public keys) the data will be encrypted with private key using identity based encryption and converts to cipher text.(Shown in Fig1).

5.2.4 Ipfs Tmage Storage:

The shared image is sent to decentralised interplanery file system as shown in Fig 1 and converts to hash address and that is stored in blockchain.

5.2.5 Testing:

When the data user registers/login to the appilication if the details match with details of the user that the data owner wants to send then that particular data user can get the records of transaction else he cannot access the data.(Shown in Fig2).

5.2.6 Decryption:

As shown in Fig 2 ,From the records the details will be decrypted and the data users gets the message and image securely.

VI. RESULT AND ANALYSIS:

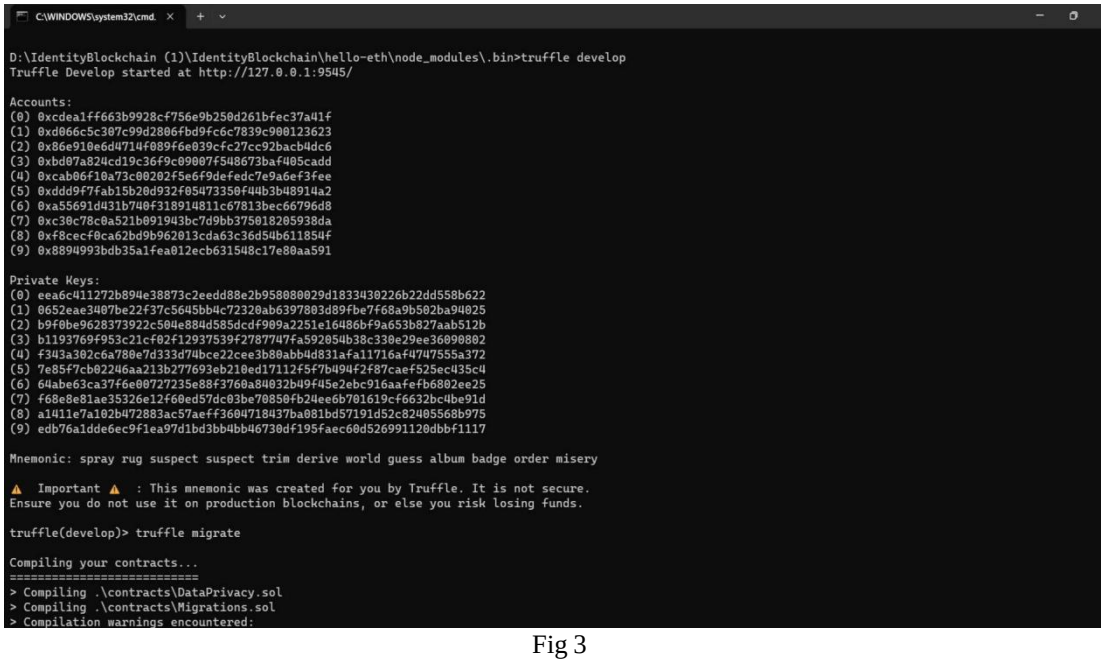

Fig 3

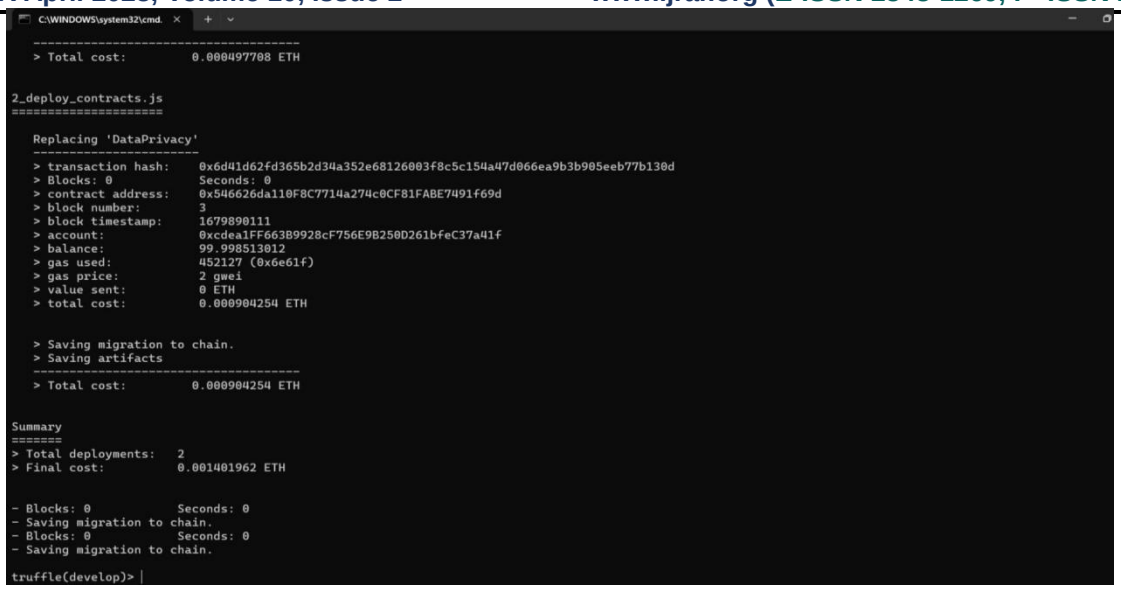

Fig 4

The above figures (Fig 3 and Fig 4) shows the execution of smart contracts using truffle platform which gives Accounts, private keys, blocks, addressess,balance as output in the command prompt.

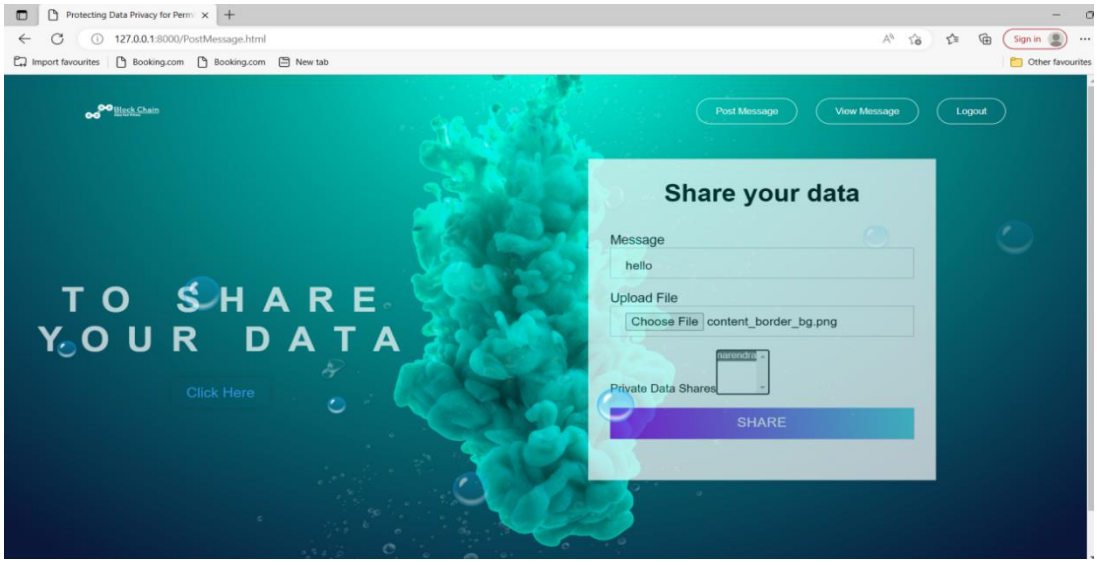

Fig 5

The above Fig 5 is the page to share the data to particular receiver. Asmentioned the sender need to provide the message, upload the file(image) and choose the reciever to whom you want to send and click on share .

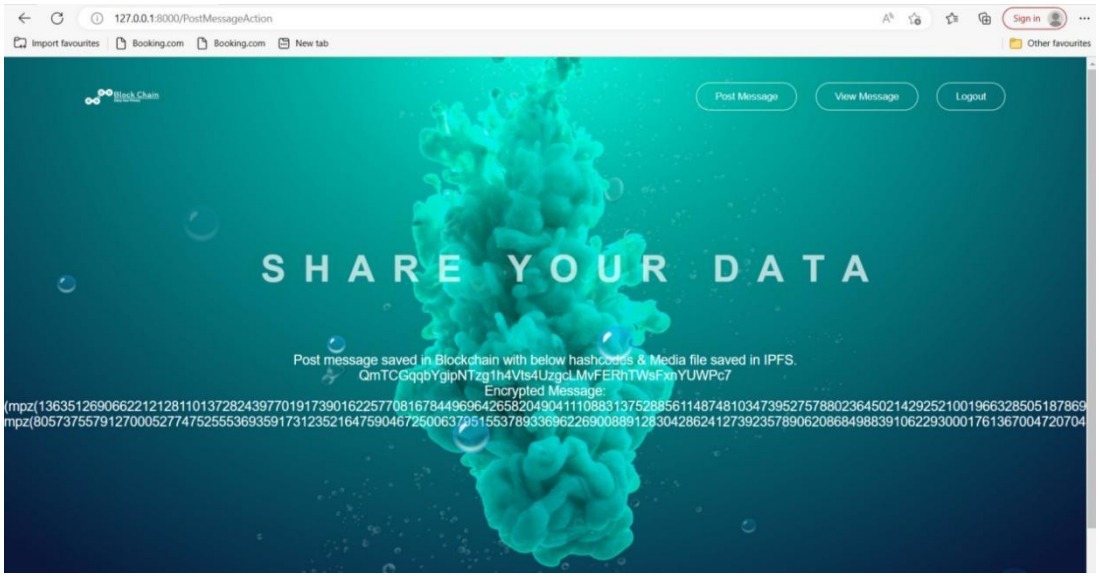

Fig 6

After sending the data the message will be encrypted and image will be saved in blockchain with hashcode as shown in the Fig 6. This shows that the data is successfully encrypted and stored in blockchain.

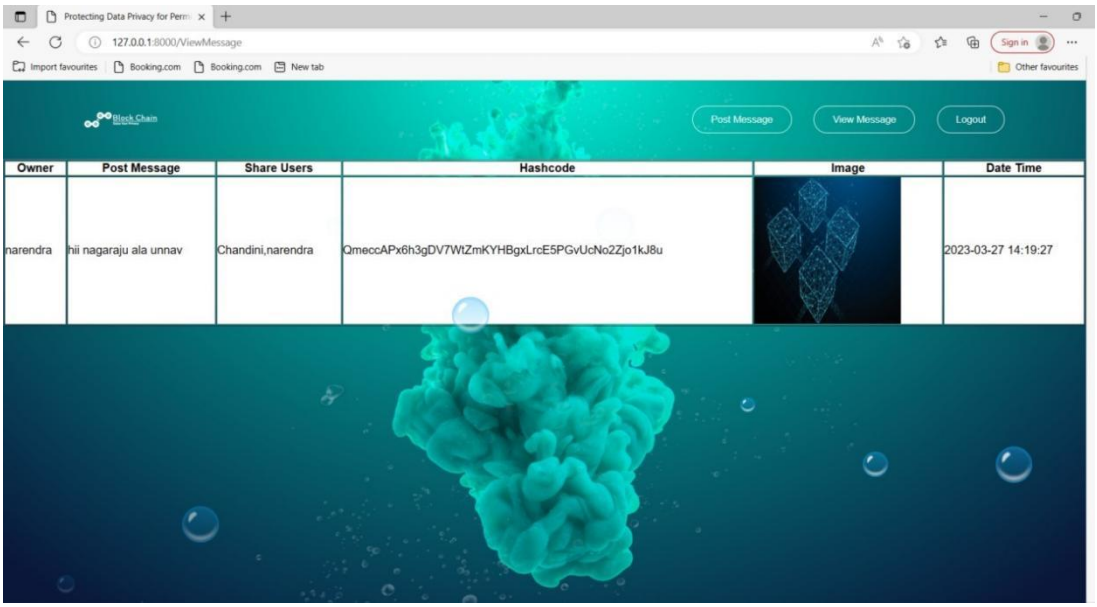

Fig 7

The page that is shown in Fig 7 is from the receiver's side . When receiver login with the correct credentials and if sender mentioned his name in the 'private data share'(Fig 5) then he receives the data which contains Data owner name,Message,Share users,Hashcode,Image and Date Time.

In this way we provide secure sharing of data between sender and receiver in a flexible way such that there will be no tampering of data.

VII. CONCLUSION:

In conclusion, the Identity-Based Encryption (IBE) project, which uses blockchain technology, has the ability to completely change how personal data is shared and kept. By offering a secure and decentralized platform for data sharing, the project seeks to address the increasing concerns about data privacy and security.

Users can share their confidential information with approved organizations using IBE while ensuring that the information is encrypted and secure. The initiative also makes use of blockchain technology to offer immutability, transparency, and security for shared data.For the future work, The project can be made more efficient by integrating it with current systems and programs to enable seamless data exchange and archiving.

VIII. REFERENCES:

[1]. Adi Shamir, ―Identity-based cryptosystems and signature schemes‖, Advances in Cryptology—Crypto 1984, Lecture Notes in Computer Science, vol. 196, Springer- Verlag, pp. 47-53, 1984.

[2]. D. Boneh and M. Franklin , ―Identity based encryption from the Weil pairing‖, SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003. Advances in Cryptology - Crypto 2001, Springer-Verlag, pp. 213-229, 2001.

[3]. M. Gagné, ―Identity Based Encryption: A Survey‖, RSA Laboratories Crypto bytes Volume 6, No.1 — Spring 2003

[4]. R. Ranjan and A. K. Das, "A Blockchain-Based Privacy-Preserving Data Sharing Scheme for Healthcare," in IEEE Access, vol. 8, pp. 82860-82869, 2020, doi: 10.1109/ACCESS.2020.2990661.

[5]. Y. Liu, Y. Zhao, H. Wang, J. Yang and X. Liu, "A Blockchain-Based Privacy- Preserving Personal Health Record Exchange System," in IEEE Access, vol. 7, pp. 85554-85563, 2019, doi: 10.1109/ACCESS.2019.2921574

[6]. Venkatesh, K., & Karthik, S. (2021). Secure and Privacy-Preserving Personal Data Sharing Framework for Healthcare using Blockchain and Identity-Based Encryption.IEEE Access, 9, 38150-38162. doi: 10.1109/access.2021.3066060.

[7]. X. Huang, Y. Zhang, X. Du, and Z. Liu, "Blockchain-Based Secure Personal Health Record Sharing Using Attribute-Based Encryption," in IEEE Access, vol. 7, pp.86966-86976, 2019, doi: 10.1109/ACCESS.2019.2922743

[8]. L. Li, X. Huang, Y. Zhang and X. Du, "A Blockchain-Based Decentralized Personal Data Management System," in IEEE Access, vol. 7, pp. 159528-159540, 2019, doi: 10.1109/ACCESS.2019.2949417.

[9]. X. Chen, W. Jia, L. Chen and H. Chen, "Blockchain-Based Personal Data Management with Attribute-Based Encryption," in IEEE Access, vol. 7, pp. 106397- 106405, 2019, doi: 10.1109/ACCESS.2019.2937676.

[10]. R. Kumar, S. S. S. S. V. Gudla and V. Varadharajan, "Blockchain-Based Secure Personal Data Sharing using Identity-Based Encryption," in IEEE Access, vol. 7, pp. 106998-107008, 2019, doi: 10.1109/ACCESS.2019.2937583.

[11]. Dan Boneh and Matthew Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586-615, 2003.

[12]. Victor Shoup, "Identity-Based Encryption," in Advances in Cryptology -- EUROCRYPT 2001, Springer-Verlag, pp. 453-469, 2001.

[13]. Benoit Libert, Damien Vergnaud, and Romain Vuillemot, "A New Framework for Identity-Based Encryption," in Advances in Cryptology -- EUROCRYPT 2013, Springer-Verlag, pp. 475-492, 2013.

[14]. Amit Sahai and Brent Waters, "Fuzzy Identity-Based Encryption," in Advances in Cryptology -- EUROCRYPT 2005, Springer-Verlag, pp. 457-473, 2005.

[15]. Jan Camenisch and Anna Lysyanskaya, "A Signature Scheme with Efficient Revocation," in Advances in Cryptology -- EUROCRYPT 2004, Springer-Verlag, pp. 93-110, 2004.

[16]. Dan Boneh and Xavier Boyen, "Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles," in Advances in Cryptology -- CRYPTO 2004, Springer-Verlag, pp. 223-238, 2004.

[17]. Ron Steinfeld, "Identity-Based Encryption with Efficient Revocation," in Progress in Cryptology -- AFRICACRYPT 2011, Springer-Verlag, pp. 41-58, 2011.

[18]. Junqing Gong, Kefei Chen, and Jian Weng, "An Efficient Identity-Based Encryption Scheme with Tight Reductions," in Cryptography and Coding -- IMACC 2013, Springer-Verlag, pp. 295-313, 2013.

[19]. Yu Chen and Zhenfu Cao, "A New Efficient Identity-Based Encryption Scheme with Tight Security Reductions," Journal of Computer Research and Development, vol. 51, no. 3, pp. 647-654, 2014.

[20]. Luca Maria Aiello and Claudio Orlandi, "On the Security of Identity-Based Encryption with Efficient Revocation," in Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12), ACM, pp. 899-910, 2012.

[21]. Dan Boneh, "The Decision Diffie-Hellman Problem," in Proceedings of the Third Algorithmic Number Theory Symposium (ANTS-III), Springer-Verlag, pp. 48- 63, 1998.

[22]. Mihir Bellare and Gregory Neven, "Multi-Receiver Identity-Based Encryption," in Proceedings of the 12th International Conference on Cryptology in India (INDOCRYPT 2011), Springer-Verlag, pp. 212-228, 2011.

[23]. Eike Kiltz, Krzysztof Pietrzak, and David Cash, "Efficient Authentication from Hard Learning Problems," in Proceedings of the 2010 IEEE Symposium on Foundations of Computer Science (FOCS 2010), pp. 294-303, 2010.

[24]. Adam O'Neill and Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), ACM, pp. 89-98, 2006.

[25]. Sanjit Chatterjee, Palash Sarkar, and Swaroop Sahoo, "New Identity-BasedProxy Re-Encryption Schemes with Constant-Size Ciphertexts," in Proceedings of the10th International Conference on Cryptology in India (INDOCRYPT 2009), Springer-Verlag, pp. 355-370, 2009.