Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

PROTECTING DATA PRIVACY PERMISSIONED BLOCK CHAIN USING IDENTITY BASED ENCRYPTION

Mr. D. KRISHNA JAYANTH[1], Ms. P. LAVANYA LAHARI[2], MR. P. PREM KUMAR[3],Mr. G. VENKATA KALYAN[4], Ms. Dr. J. KAVITHA[5]

1.BTECH, COMPUTER SCIENCE AND ENGINEERING, SANKETIKAINSTITUTE OF TECHNOLOGY AND MANAGEMENT, P.M.PALEM, VISAKHAPATNAM, ANDHRA PRADESH, INDIA-530041
2.BTECH, COMPUTER SCIENCE AND ENGINEERING, SANKETIKAINSTITUTE OF TECHNOLOGY AND MANAGEMENT, P.M.PALEM, VISAKHAPATNAM, ANDHRA PRADESH, INDIA-530041
3.BTECH, COMPUTER SCIENCE AND ENGINEERING, SANKETIKAINSTITUTE OF TECHNOLOGY AND MANAGEMENT, P.M.PALEM, VISAKHAPATNAM, ANDHRA PRADESH, INDIA-530041
4. BTECH, COMPUTER SCIENCE AND ENGINEERING, SANKETIKAINSTITUTE OF TECHNOLOGY AND MANAGEMENT, P.M.PALEM, VISAKHAPATNAM, ANDHRA PRADESH, INDIA-530041
5.Assitant Professor COMPUTER SCIENCE AND ENGINEERING, SANKETIKAINSTITUTE OF TECHNOLOGY AND MANAGEMENT, P.M.PALEM, VISAKHAPATNAM, ANDHRA PRADESH, INDIA-530041

ABSTRACT
Governments, financial institutions, and high-tech companies have recently focused heavily on blockchain, a developing decentralised architecture and distributed public ledger technology that underpins Bitcoin. Blockchain is thought to increase productivity, save costs, and improve data security, but there are still significant privacy concerns that could prevent blockchain from being widely used. In this research, we introduce a practical technique that significantly enhances data privacy for non-transaction applications by incorporating the Identity-Based encryption system. Analysis demonstrates that our concept is functional, effective, and practicable in many applications for non-transactional scenarios, and that it has a high security level that can avoid both disguise and passive assaults.

1 INTRODUCTION

Blockchain is a distributed public ledger system that operates on a peer-to-peer network and is distinguished by its decentralisation and lack of trust. It is gaining popularity across a variety of industries and use cases. A distributed network of peer nodes that maintains an immutable transaction log is known as a blockchain. By applying transactions that have been verified by a consensus procedure and arranged into blocks with a hash that links each block to the one before it, these nodes each keep a copy of the ledger. Figure 1 depicts the usual structure of a blockchain. Figure 1. The fundamental design of a blockchain A distributed ledger that keeps track of all network transactions serves as the brain of a blockchain network. A blockchain also uses cryptographic techniques to ensure that the data is append-only, which ensures that once a transaction is added to the ledger, it cannot be changed. It is simple to verify that data has not been altered after the event thanks to this immutability attribute. The blockchain's earliest and most well-known application is the Bitcoin money, but Ethereum took a different tack by including many of Bitcoin's fundamental traits while also including smart contracts to build a platform for distributed applications. A category of public permissionless blockchain technology includes Bitcoin and Ethereum. In essence, these are public networks that are accessible to everyone and allow for anonymous communication. Almost anyone can participate in a permissionless blockchain, and each participant is anonymous. Permissionless blockchains often use transaction fees or a native cryptocurrency that is "mined" to offset the prohibitive costs of taking part in a byzantine fault-tolerant consensus system based on "proof of work" in order to reduce the lack of trust.

2. LITERATURE SURVEY AND RELATED WORK

1 D. D. Detwiler, This study deals about “One nations move to increase food safety with blockchain” Although the spinach on the grocery store shelf is a vibrant green and appears delectable, how can you be sure it is safe to consume? What if your retailer could verify every stop that spinach took on the way to the store, as well as where it was cultivated, handled, kept, and inspected, with absolute certainty? Blockchain, a shared, distributed ledger technology, gives your retailer access to this data. By directly integrating growers, processors, distributors, suppliers, retailers, and regulators with a common, immutable view of their transaction history, blockchain-based solutions

have the potential to change the food business.

2 Boneh, D., Franklin, M. Identity, based encryption from the Weil pairing. In: Kilian, We suggest an identity-based encryption system that is fully operational. (IBE). In the random oracle model, the system has chosen ciphertext security while assuming a special case of the computational Diffie- Hellman problem. The foundation of our system is a bilinear map between groups. One such map is the Weil pairing on elliptic curves. We provide clear definitions for safe identity-based encryption techniques and list many uses for these systems.

3 Boneh, D., Boyen, X. Efficient, elective-ID secure identity based en- cryption without random oracles. We provide an identity-based encryption method that is 100 percent secure and whose security proof does not rely on the random oracle heuristic. The decisional bilinear Diffie-Hellman assumption underlies security. The security reduction from the underlying complexity assumption resulted in a significant penalty factor for prior designs of this sort. The current system's security reduction is polynomial across all parameters.

4 Boneh, D., Boyen, X. Secur identity based encryption without random oracles Using no random oracles, we introduce the first effective Identity-Based Encryption (IBE) technique. We initially discuss our IBE construction before reducing the decisional Bilinear Diffie-Hellman (BDH) problem to describe the security of our system. Additionally, we demonstrate that a new signature scheme that is secure without random oracles under the computational Diffie-Hellman assumption can be created using our techniques.

5 R. S. Wahby, I. Tzialla, A. Shelat, J. Thaler and M. Walfish, Cluster computing in zero knowledge, EUROCRYPT. For scalability and economic considerations, large computations that may be conducted in distributed parallel are frequently carried out on computer clusters. Such calculations are employed in a variety of applications, including, but not limited to, statistical machine translation, webgraph mining, and machine learning. But frequently, just the output of the computation can be published because the input data is secret. In these circumstances, zero-knowledge proofs would enable the verification of the output's validity without disclosing (extra) information about the input. We examine theoretical and applied elements of zero-knowledge proofs for cluster computations in this paper. We design, construct, and test zero-knowledge proof systems where: (i) a proof verifies that a cluster computation was carried out correctly; and (ii) creating the proof involves a cluster computation identical in complexity and structure to the initial one. We specifically concentrate on MapReduce, a beautiful and well-liked cluster computing method. A monolithic NP statement that accounts for all mappers, all reducers, and shuffling can theoretically demonstrate the soundness of a MapReduce computation using previous zero-knowledge proof techniques. However, it is unclear how to produce the evidence for such monolithic claims using distributed systems' parallel execution. Our study provides theoretical and practical evidence that the structure and complexity of proof production might resemble those of the original cluster computation. Our primary method is a bootstrapping theorem for succinct non-interactive arguments of knowledge (SNARKs), which demonstrates how, through recursive proof construction, sition and Proof-Carrying Data, it is possible to convert any SNARK into a distributed SNARK for MapReduce that proves each individual computation's global consistency as well as its correctness piecewise and over a distributed network.

3 Implementation Study

It is vital to utilise encryption technology to convert plaintext to ciphertext in order to improve data privacy in blockchain. However, the encryption algorithm must be properly constructed in order to prevent compromising the consensus process. However, all procedures under consensus don't include mathematical operations in the non-transaction situation. So long as the key management issue is resolved, we can ensure that sensitive data is encrypted while being recorded on the blockchain. In this part, we build a straightforward ID-based encryption privacy protection solution that works well in permissioned blockchain non-transaction contexts. Encryption based on an ID.

Shamir requested a public key encryption method in 1984 in which the secret key could be generated by the PKG, a reputable third party, and the public key may be any string. (Private Key Generator)

3.1 MODULES:

3.1.1 Block chain generator: - by using we generate the block chain here it will generate the 10 block chain users and 10 block chain private keys after that we use the master key to connect to the solidarity to store the data in the form of blocks

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

3.1.2 User login: - user has to first register and after registration the user can upload a document and message where these data will be stored in the block chain and the image will be only visible to the user after the validation of the IBE private key is validated and then the user can view the information which was shared to the user only the permissible users can see the data.

4 PROPOSED WORK AND ALGORITHM

The master key is the most crucial component of the suggested scheme. The system is destroyed as soon as the master key is compromised. It needs to be properly saved as a result. The management of the master key by a single PKG in many systems causes issues with centralization and security. A threshold secret sharing mechanism can now be applied. The issue of centralization and security is resolved by creating a (t, n) threshold scheme in which the master key is managed by multiple trustworthy PKGs rather than a single PKG. This prevents any single PKG from being able to recover the master key. Here, we use IBE cryptography to implement private key creation.

ADVANTAGES OF PROPOSED SYSTEM:

1. GREAT ACCURACY
2. STRONG EFFICIENCY

Proposed System Architecture

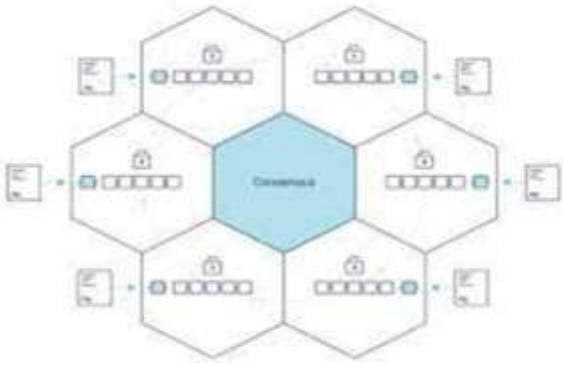

Fig-1: Proposed System Architecture

5 METHODOLOGIES

We suggest a version-based, fine-grained, and privacyprotected data structure with five sections, as illustrated in Figures 2 and 3. These sections are KeyID, Subject data, Attachments, Data trajectory, and Privacy and authentication. For each data transmission activity on the blockchain, the KeyID component represents the specific identifying code. The transmitted data's metadata are contained in the Subject data portion. The information about attachment files is kept with the primary data in the Attachments portion.

Step 1: -The private keys in the IBE are integers (in the range of the curve's field size, typically 256-bit integers). Example of 256-bit IBE private key (hex encoded, 32 bytes, 64 hex digits) is:

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

0x51897b64e85c3f714bba707e867914295a1377a7463a9dae8ea6a8b9 14246319

Step 2: - The key generation in theIBE cryptography is as simple as securely generating a random integer in certain range, so it is extremely fast. Any number within the range is valid IBE private key. Step 3: - The public keys in the IBE are EC points - pairs of integer coordinates {x, y}, laying on the curve. Due to their special properties, EC points can be compressed to just one coordinate + 1 bit (odd or even). Thus, the compressed public key, corresponding to a 256-bit IBE private key, is a 257-bit integer. Example of IBE public key (corresponding to the above private key, encoded in the Ethereum format, as hex with prefix 02 or 03) is: 0x02f54ba86dc1ccb5bed0224d23f01ed87e4a443c47fc690d7797a13d 41d2340e1a. In this format the public key actually takes 33 bytes (66 hex digits), which can be optimized to exactly 257 bits

6 RESULTS AND DISCUSSION

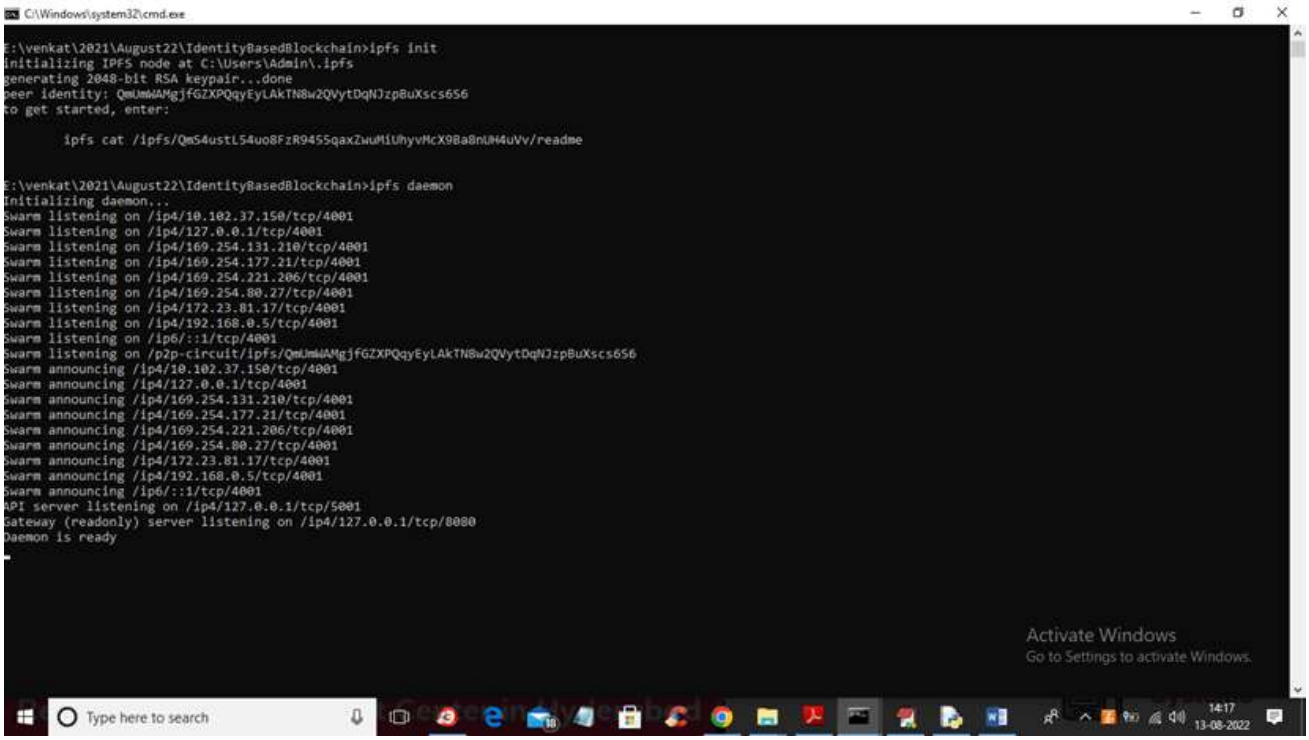

Fig-2 running Django server

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

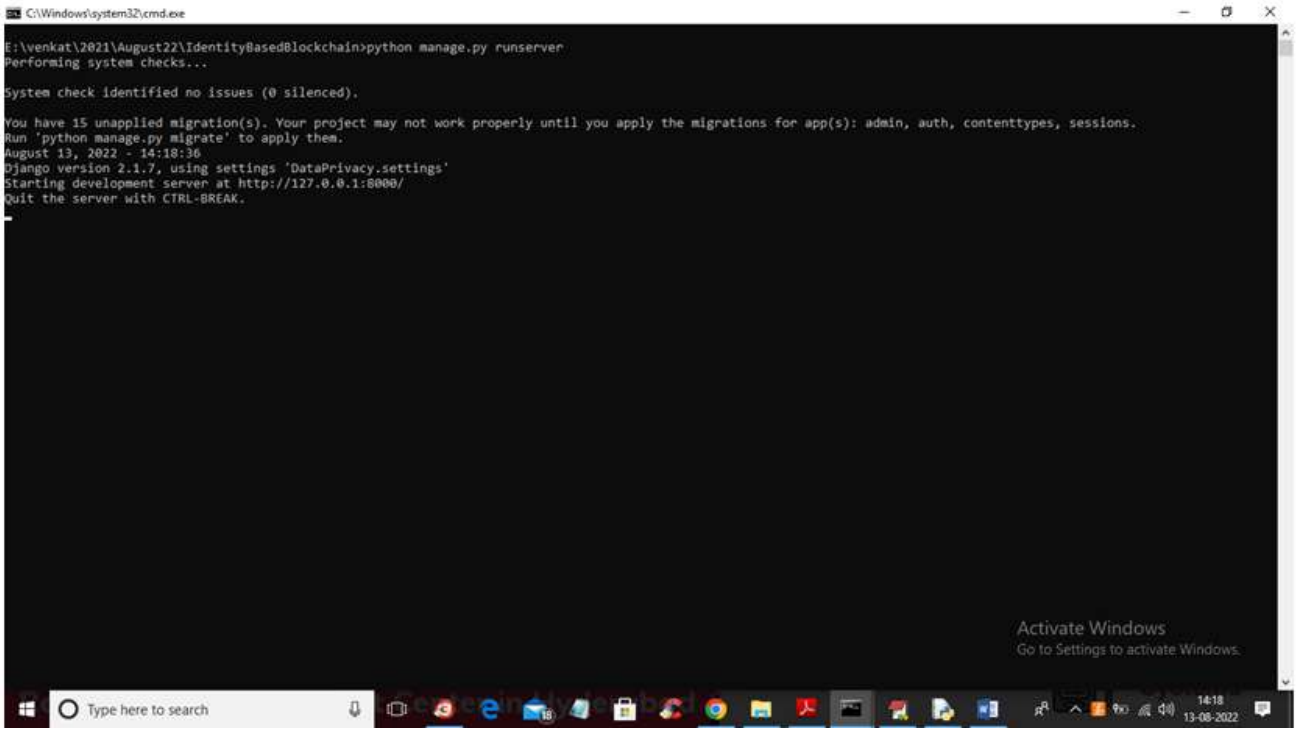

Fig-3 server url

Fig-3: click on 'New User Signup Here' link to signup user

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

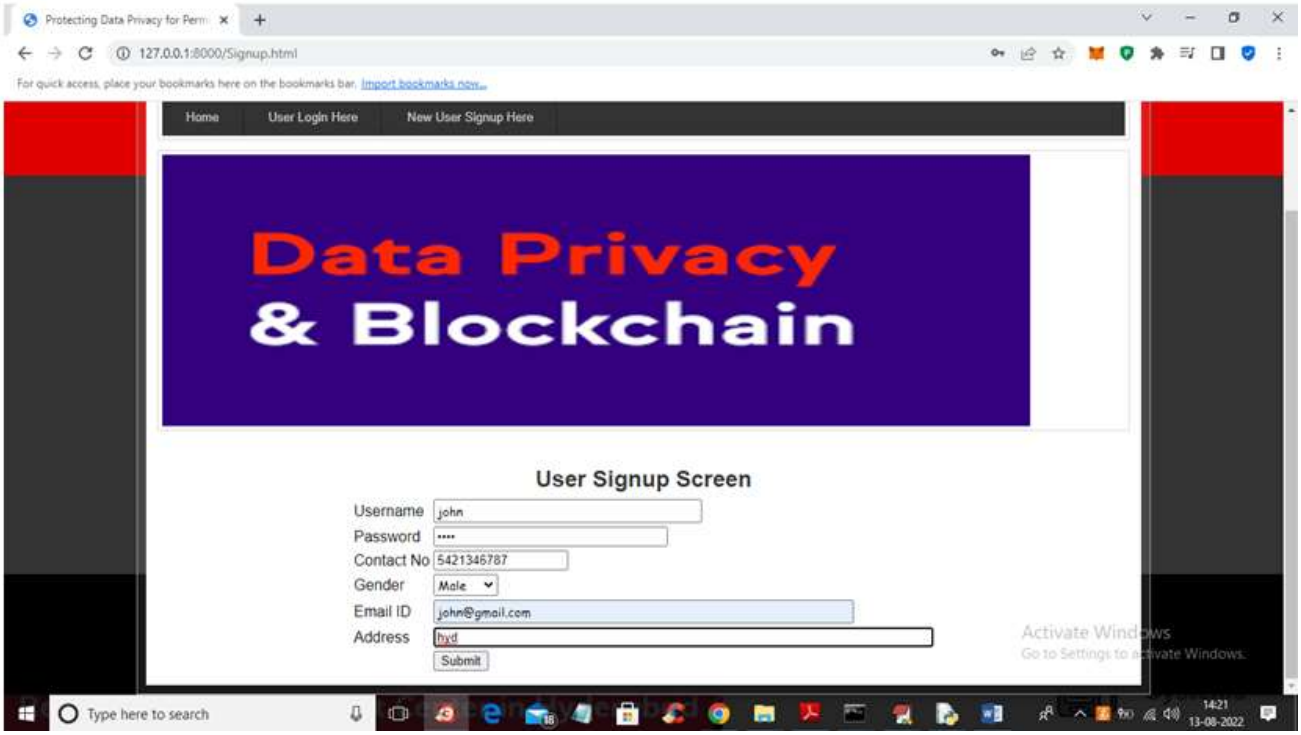

Fig-4: user is entering signup details and press submit button to store details in Blockchain and get below output

Fig-5: user signup completed and details saved in Blockchain and now click on 'User Login' link to get below screen

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

Fig-6: user is login and after login will get below screen

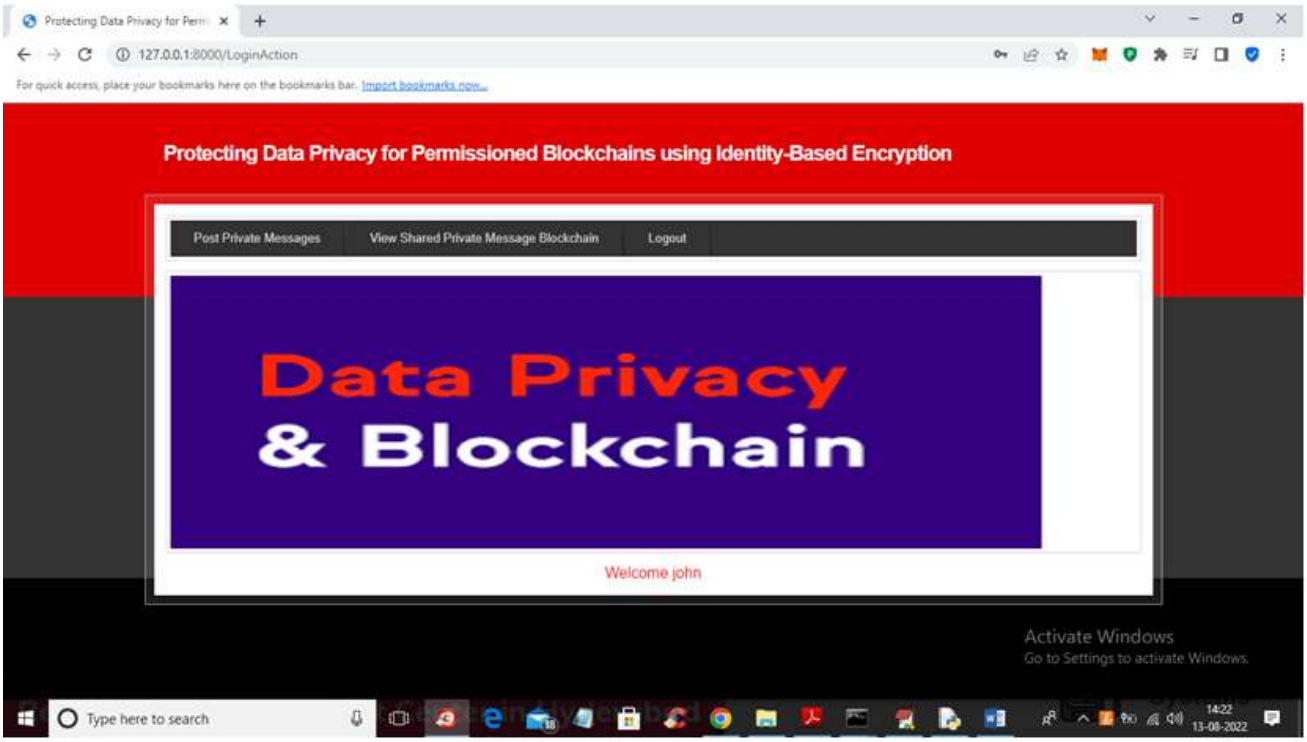

Fig-7: user can click on 'Post Private Messages' link to upload message

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

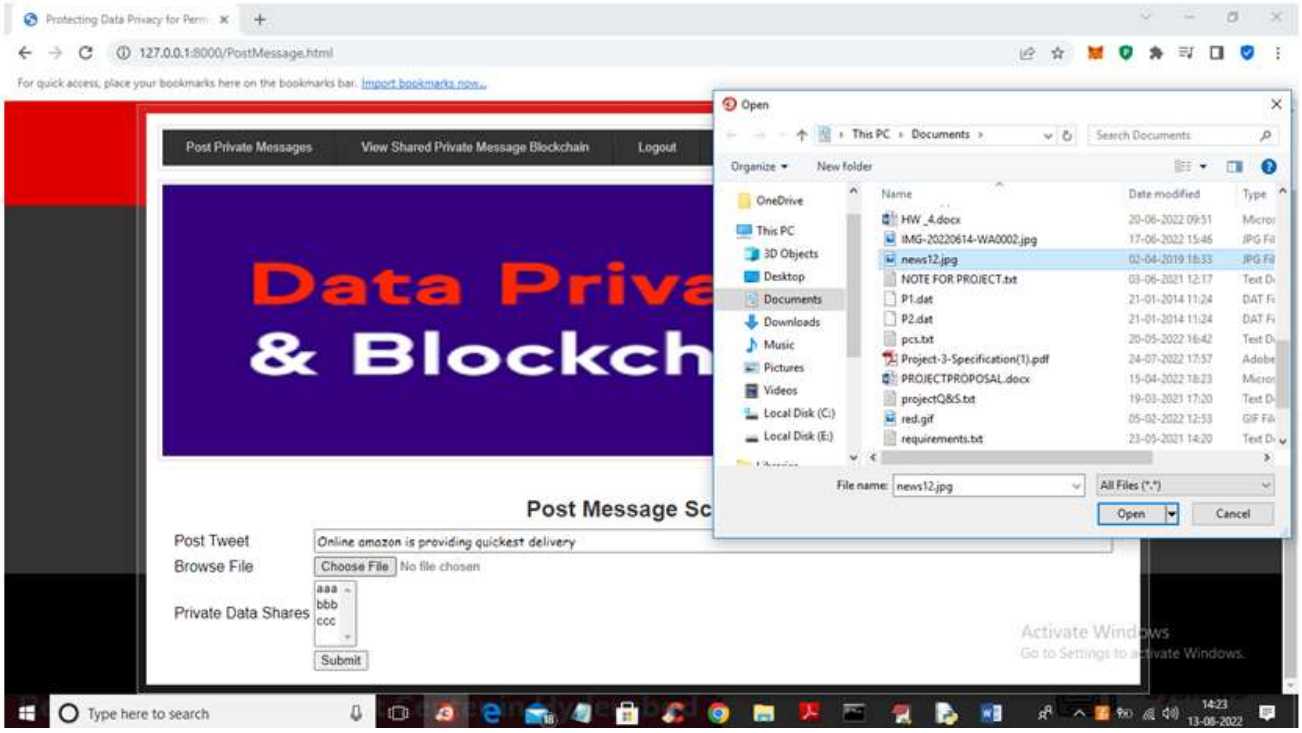

Fig-8: user type some message and then uploading image and then select list of users to share with and you can select multiple users by holding CTRL key like below screen

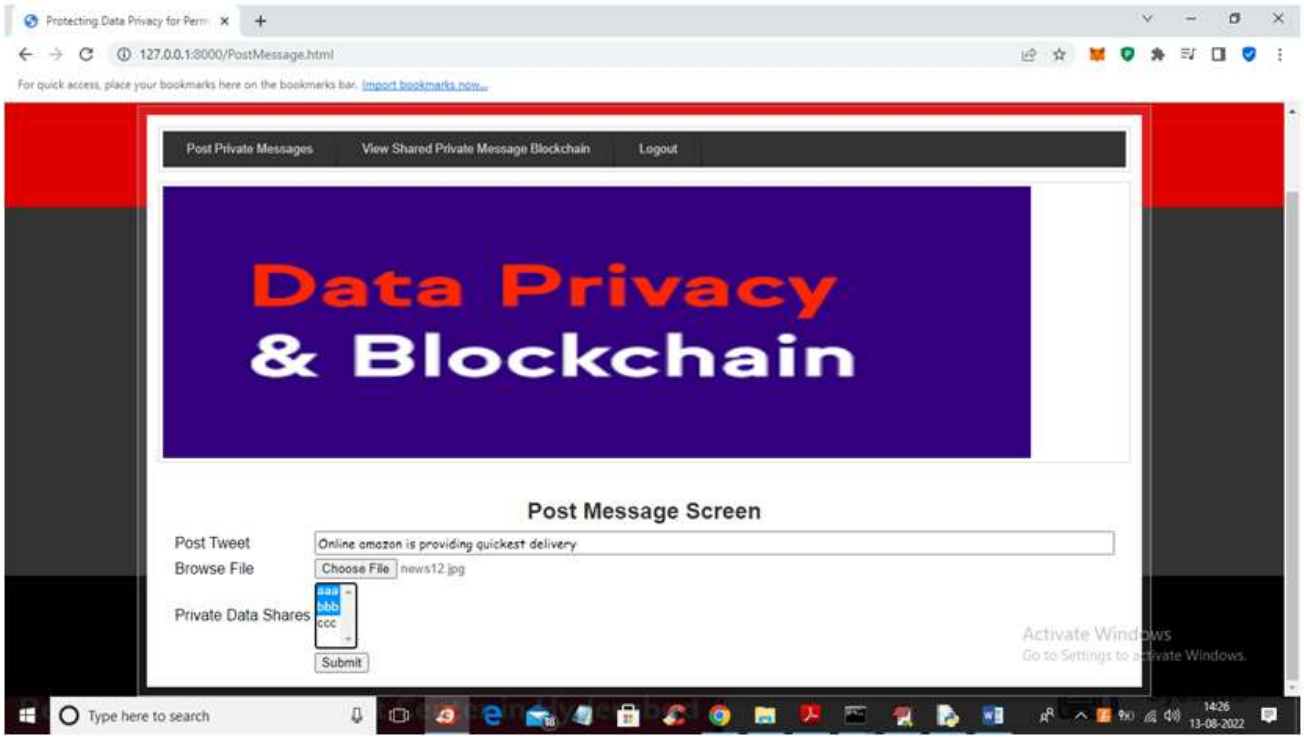

Fig-9: user John is uploading some post and then giving share access to user 'aaa and bbb' and user 'ccc' cannot access and now press 'submit' button to save post in Blockchain and get below output

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

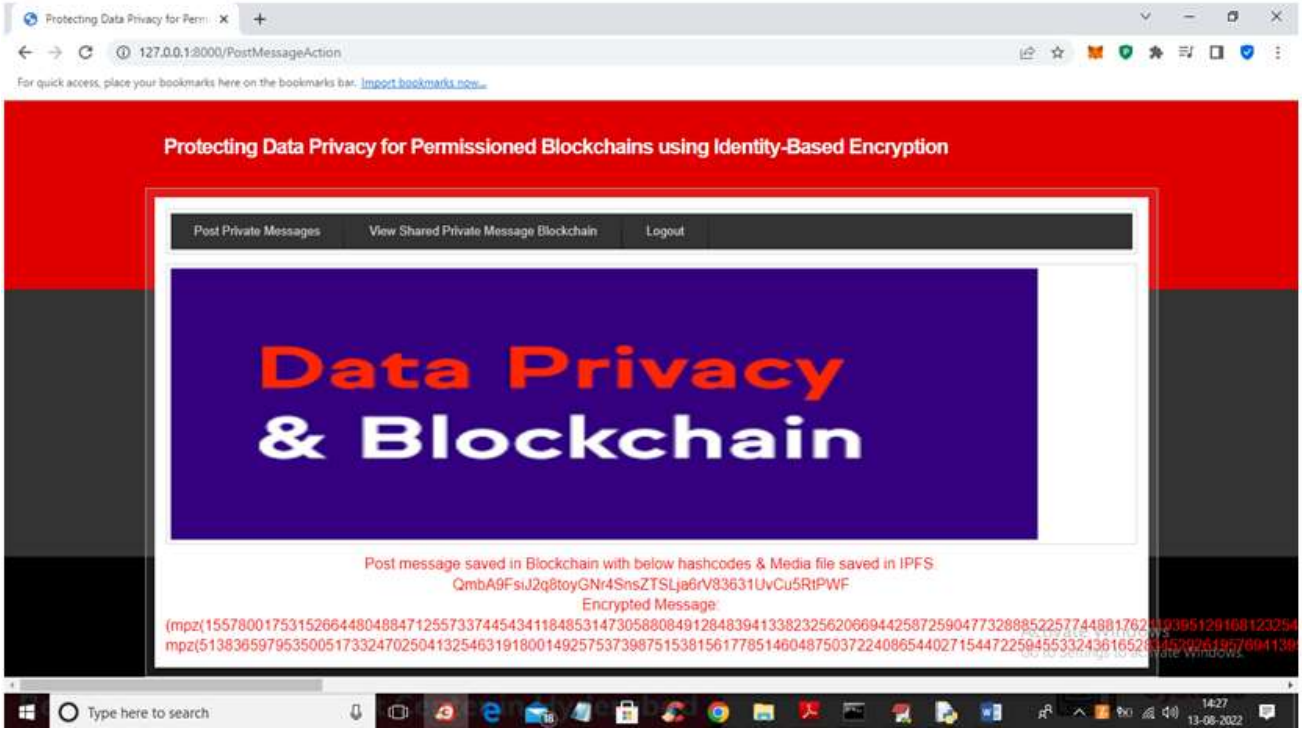

Fig-10: we can see message in red colour as POST MESSAGE saved in Blockchain and with Hashcode and we can see IBE encrypted message and now click on 'View Shared Private Message Blockchain' link to view message in decrypted format

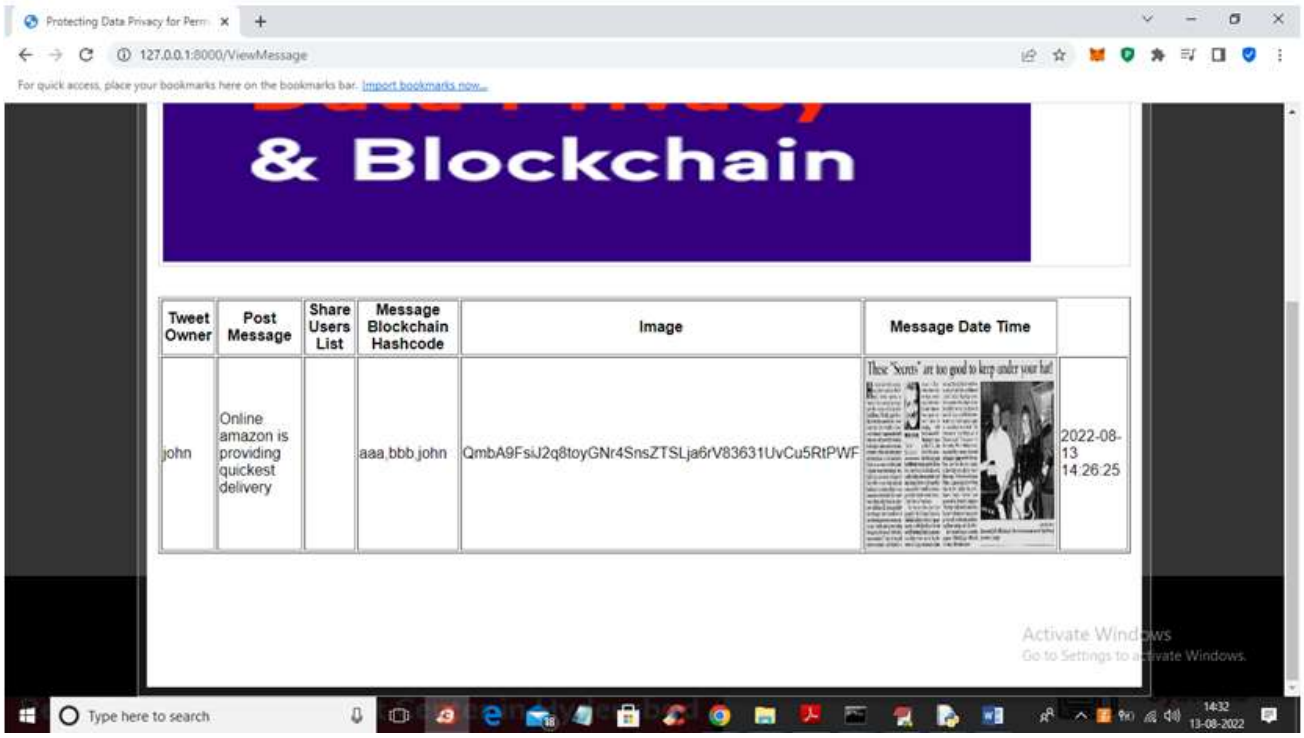

Fig-11: user can view decrypted message with image and hashcode and this user has shared post with user 'aaa' and now we login as 'aaa' and check message

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

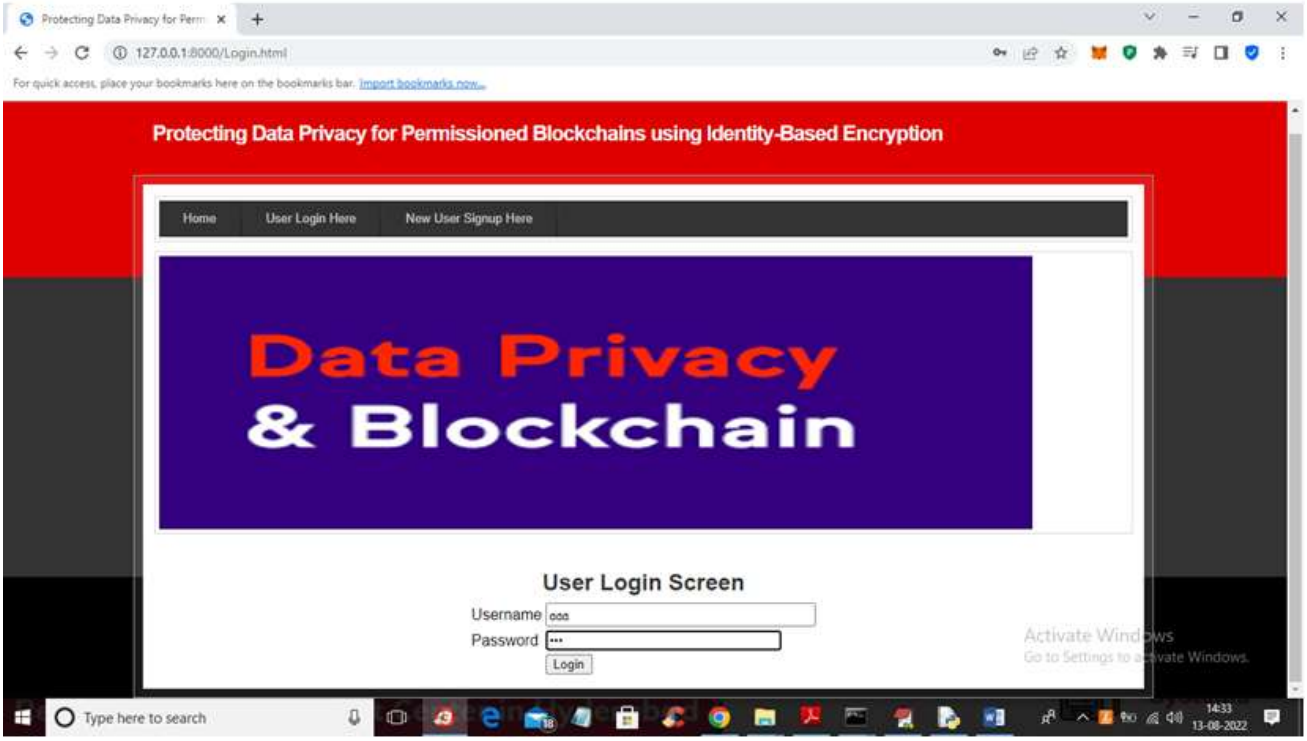

Fig-12: user 'aaa' is login and after login will get below screen

Fig-13: click on 'View Shared Message' link to get below output

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

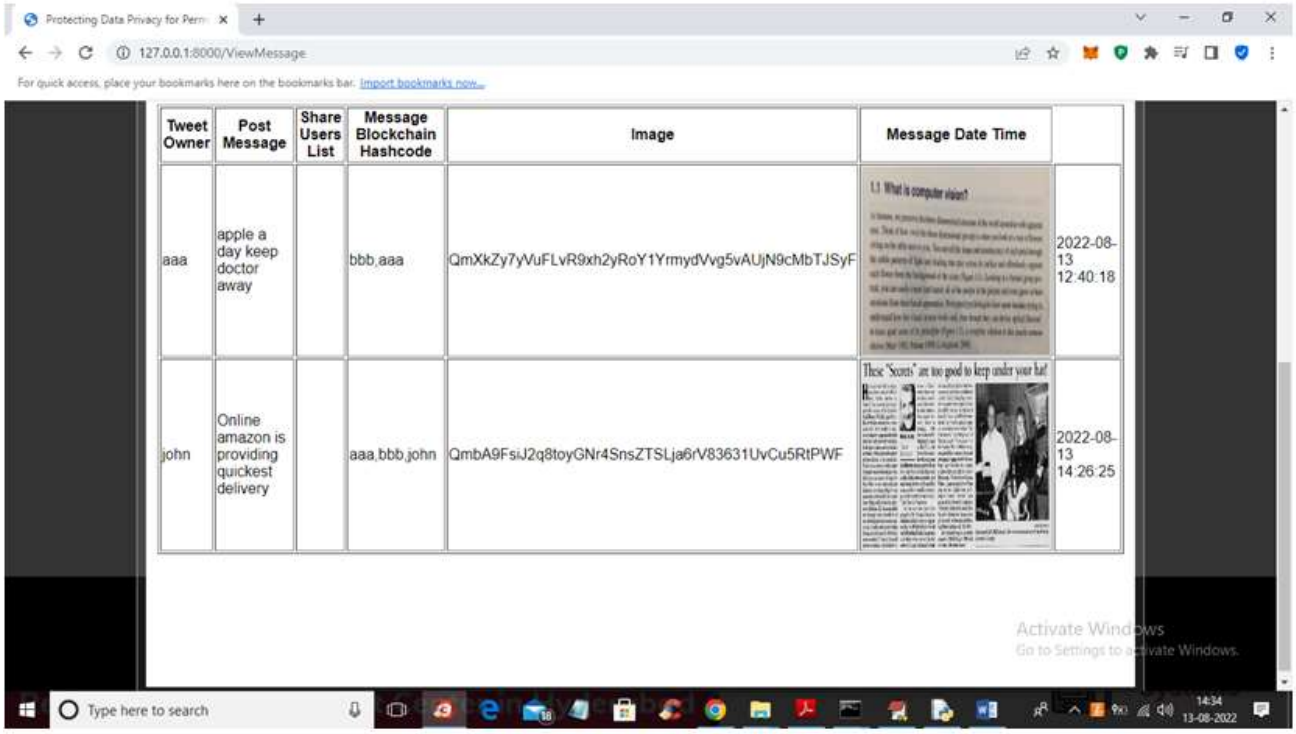

Fig-14: user aaa can view all his and shared messages and now we will login as user 'ccc' and check message as this user has no sharing permission

Fig-15: user 'ccc' is login and after login will get below output

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 4, April 2023

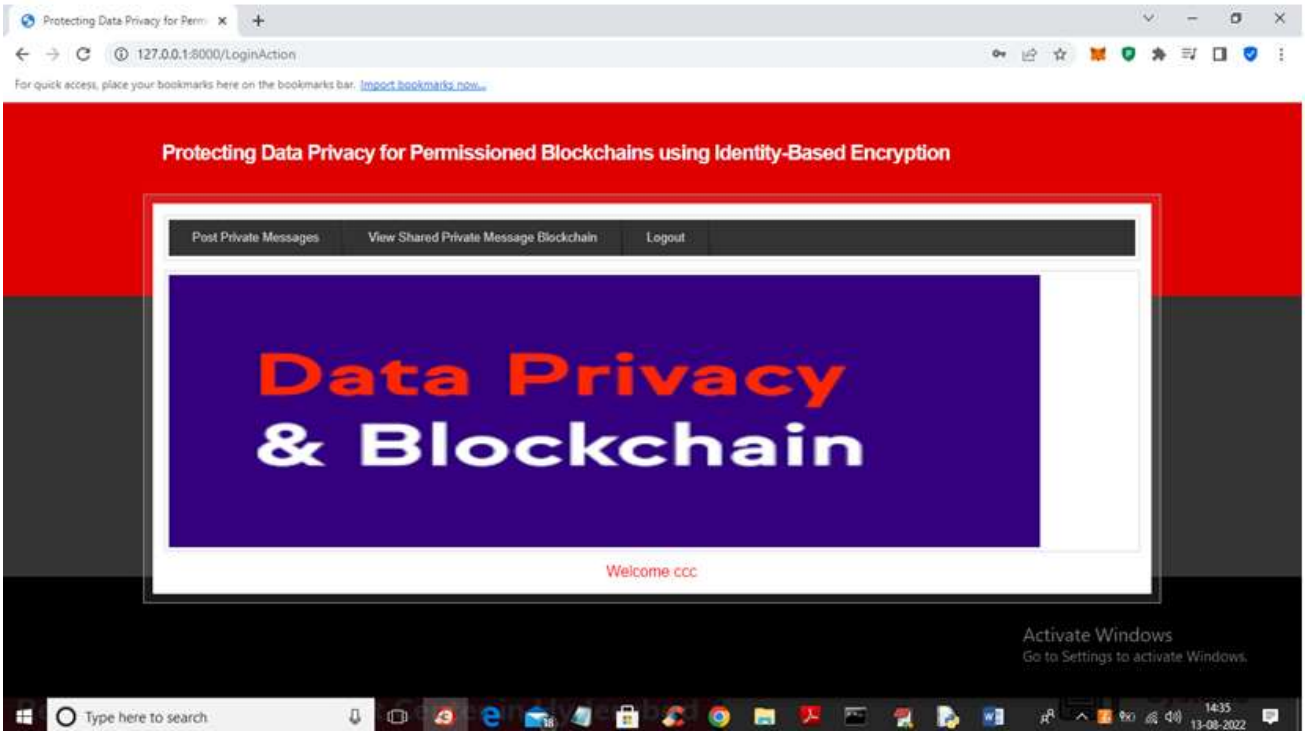

Fig-16: user can click on 'View Shared Message' link to view messages

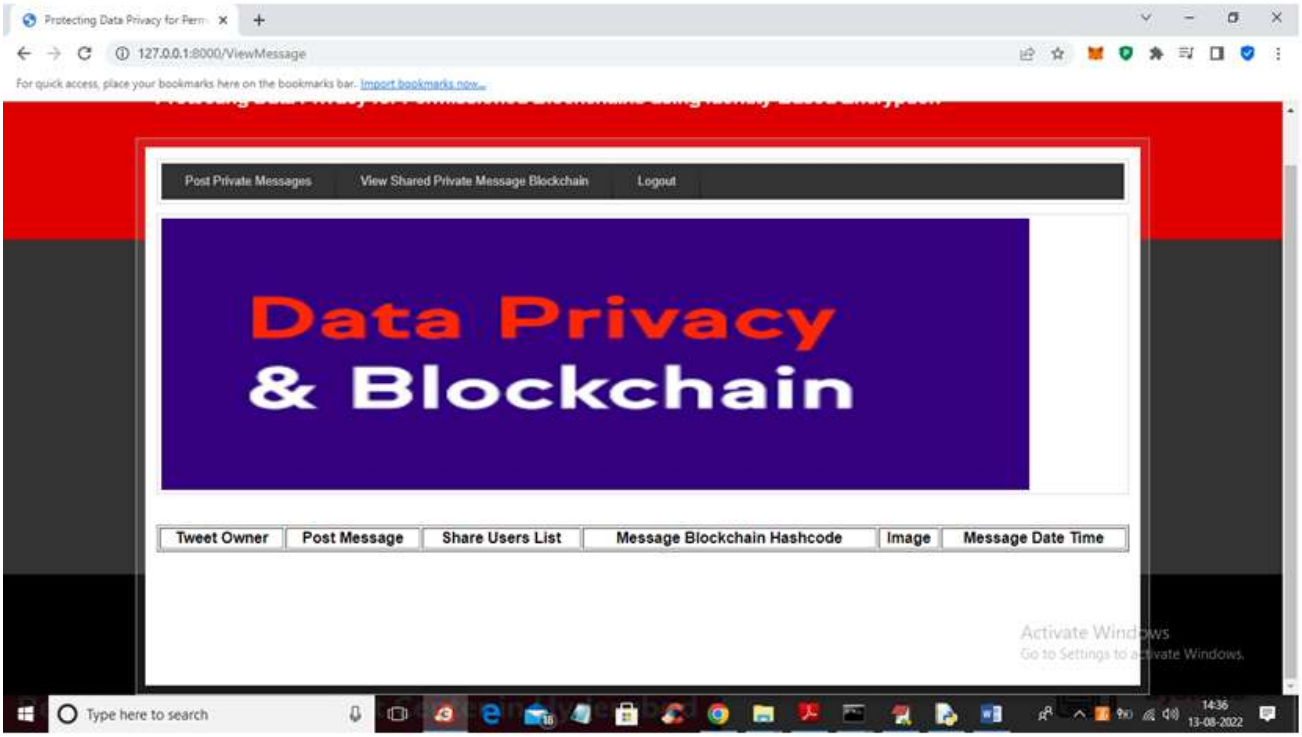

Fig-17: can see user CCC has no share permission so he cannot decrypt and view messages and privacy will be achieved

7. CONCLUSION AND FUTURE WORK

To further demonstrate the privacy, we have suggested an enhanced delicately scheme on top of non-transactional circumstances in permissioned blockchain. Without the use of cutting-edge technologies like ring signature, homomorphic encryption, or zero-knowledge proofs, our approach may conceal the information by converting the plaintext into the ciphertext. Our approach not only eliminates the challenging certificate issuing and management seen in the conventional PKI system, but it also offers a high level of security that can thwart passive and disguised attacks and is functional, efficient, and useful for applications. This system offers an innovative method for maintaining sensitive transaction confidentiality in numerous applications for non-transactional contexts.

8. REFERENCES

1. The Linux Foundation Helps Hyperledger Build the Most Vibrant Open Source Ecosystem for Blockchain. http://www.linuxfoundation.org/.
2. S. Omohundro. Cryptocurrencies, smart contracts, and artificial intelli- gence. AI Matters, 1(2):19C21, Dec. 2014.
3. D. D. Detwiler. One nations move to increase food safety with blockchain. https://www.ibm.com/blogs/blockchain/2018/02/one-nations- move-to-increase-food-safety-with-blockchain/,2018. [Online; accessed 1-May-2018].
4. Shamir, A. Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47C53. Springer, Heidelberg (1985)
5. Boneh, D., Franklin, M. Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213C229. Springer, Berlin, Ger- many (2001)
6. Boneh, D., Boyen, X. Efficient selective-ID secure identity based en- cryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223C238. Springer, Berlin, Germany (2004)
7. Boneh, D., Boyen, X. Secure identity based encryption without random oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, Springer, Berlin, Germany (2004).
8. Gentry, C. Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445C464. Springer, Berlin, Germany (2006).
9. Labs, Shen Noether Mrl. Ring confidential transactions. 2016.
10. R. S. Wahby, I. Tzialla, A. Shelat, J. Thaler and M. Walfish. Doubly- Efficient zkSNARKs Without Trusted Setup. 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 926-943.
11. B. Bnz J. Bootle D. Boneh A. Poelstra P. Wuille G. Maxwell. Bullet- proofs: Efficient range proofs for confidential transactions", IEEE S&P May 2018.
12. A. Chiesa E. Tromer M. Virza. Cluster computing in zero knowledge, EUROCRYPT Apr. 2015.
13. A. Chiesa M. A. Forbes N. Spooner. A zero knowledge sumcheck and its applications. CoRR abs1704.02086 2017.
14. T. P. Pedersen et al. Non-interactive and information-theoretic secure verifiable secret sharing. in Crypto, vol. 91, pp. 129C140, Springer, 1991.
15. P. Paillier et al. Public-key cryptosystems based on composite degree residuosity classes. in Eurocrypt, vol. 99, pp. 223C238, Springer, 1999