IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

Blockchain Enabled Security Framework for Customer Registration in Banking

Deekshitha K [1], Khushi V S [2], Preethi G [3], Kavyashree N M [4],Prof. Dr. Pradeep N[5]

U.G Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[1]

U.G Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India [2]

U.G Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India [3]

U.G Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India [4]

Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India [5]

ABSTRACT: The know your customer or know your client (KYC) is a guideline for the banking system to validate a customer using identity, appropriateness, risk assessment in establishing a banking relationship. With the growing concern of security, the KYC process is complex and involves a high cost for completing for a single customer. In this work, we propose an economical, swift, secure, and transparent platform for KYC document verification for the Banking system through InterPlanetary File System (IPFS) and blockchain technology. The proposed system allows a customer to open an account at one Bank, complete the KYC process there, and generate a hash value using the IPFS network and share it using the blockchain technique. Upon receiving the private key, any Bank/financial organization can retrieve, store customer data (i.e., KYC) securely using IPFS network if the customer wishes to open another account in that Bank/financial organization. The proposed system can save time, money, and repetitive work during the KYC process when someone tries to open an account at multiple Banks.

KEYWORDS: Know your customer, KYC, banking, validation, identity, risk assessment, security, IPFS, blockchain, cost-effective, document verification, hash value, data storage, time-saving, cost-saving.

I. INTRODUCTION

Digital technologies have transformed media content production and distribution in the global entertainment and media industry over the last two decades. Many challenges still remain, though, especially relating to the way in which digital content can be distributed on the Internet, and how content contributors are compensated when their materials are used or bought through legitimate channels. One of the latest experiments in this specific industry involves the use of blockchains and cryptocurrencies for micropayments—payments by consumers of very small sums of money to access specific content. Blockchain technology and cryptocurrencies can provide an ideal, cost-effective framework for payments, preserving privacy, with low commission fees and instant financial transactions without intermediaries.

Blockchain technology become famous following the introduction of blockbuster cryptocurrencies like BitCoin and Ethereum, which are still the sole applications of blockchains at scale. BitCoin and Ethereum have attracted the interest of the financial services industry, while at the same time giving rise to the introduction of additional cryptocurrencies (AltCoins) such as LightCoin, PrimeCoin, NameCoin. Moreover, they have driven the emergence of an entirely new concept for funding innovative ideas and products, namely the Initial Coin Offering (ICO) mechanism. During the last couple of years, there has been a surge of interest in other applications of blockchains beyond cryptocurrencies, notably applications that attempt to exploit the decentralized nature of distributed ledger technologies (DLT), as well as their security, transparency and anti-tampering properties. In many cases applications take advantage of these properties in

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

the scope of permissioned blockchain infrastructures, which offer fine grained authentication and authorization, while at the same time obviating the need for complex and time-consuming Proof-ofWork (PoW) processes. The latter is a key to supporting applications that need to support faster transaction completion than what is supported by conventional public blockchains such as BitCoin and Ethereum. This has given rise to the emergence of platforms destined to support permissioned blockchains such as R3/Corda and Hyperledger Fabric, both of which support hundreds of transactions per second (TPS). Non-cryptocurrencies applications based on permissioned blockchains are currently being explored in many different sectors, such as energy, industry, supply chain management and healthcare. A plethora of such applications are also considered by financial organizations, as part of the wave of FinTech innovations.

The Know your customer (KYC) is a very common term in the banking and financial sector. At this moment, the manual KYC process is outdated and has become a necessity to automate the KYC verification process. Studies around the world have made several attempts to make a better verifi- cation process for KYC. Many academics tried to propose a Blockchain-based solution. Blockchain technology recently draws the attention of the public, as a dispute that leads to the foundation that the trust-free economical transaction is possible with its distinctive method .

II. LITERATURE SURVEY

Blockchains are currently getting a lot of attention as a distributed way of storing data. However, the irreversibility and transparency of blockchains mean they are probably unsuitable for personal data. As far as data privacy is concerned, data stored in blockchains cannot be changed, which means that personal data they contain cannot be removed and so it is very important to design blockchains in order to protect users' privacy. One approach could be to have blockchains used only to provide a timestamp for information held elsewhere. If specific content needs to be taken down from a public source, the fact that the content existed at a given point would still remain in the blockchain but the stored hash would now point to other content that has been changed or simply removed. This approach of using blockchains purely as a time-stamping mechanism and not as a data store has the additional benefit of being more likely to scale in the face of large amounts of data needing to be recorded. Finally, additional encryption of data before it is pushed into the blockchain can be possible. The main problem with this approach is that if the decryption key for encrypted data is ever made public, the encrypted content is readable by anyone with that key; there is no way of encrypting the data with a different key once it is embedded within the blockchain. Regardless of the approach taken to designing blockchains, every blockchain contains transaction data and thus all privacy by design principles have to be taken into consideration before letting any transaction into the ledgers of public/private blockchain implementations.

The underlying technology and ideas behind blockchain have significantly evolved since it was originally proposed as an accounting method for Bitcoin cryptocurrency . Naughton suggests that blockchain technology could be "the most important IT invention of our age", while Mougayar says that it is "at the same level as the World Wide Web in terms of importance". A milestone for the course of blockchain technology was the development of the Ethereum project, offering new solutions by enabling smart contract implementation and execution. It is a suite of tools and protocols for the creation and operation of Decentralized Applications (DApps), "applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference". It also supports a contract-oriented, high-level, Turing-complete programming language, allowing anyone to write smart contracts and create DApps.

III. METHODOLOGY

Blockchain

Blockchain is a purely peer-to-peer version online transac- tion, where a customer directly sends money to others without the help of a financial organization. All transactions will be hashed to an ongoing proof-of-work chain. Each of this called a block; the running block contains the hash of previous all blocks. Therefore, the whole process is tempered proof, as a single peer cannot add a new block without the proof-of-work . Bitcoin was the first fully decentralized cryptocurrency. While the central purpose of DLT was to create digital money and sending and receiving via the Internet, the technology can also be used to authenticate online document sharing using smart contracts. The smart-contract aims to involve them in properties, which are expensive and controlled in a digital manner.

IPFS

The InterPlanetary File System (IPFS) is a peer-to- peer(P2P) file-sharing protocol connecting computing devices for sharing/storing files/data. The content is uniquely recog- nized in the global namespace using the hash code of the file.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

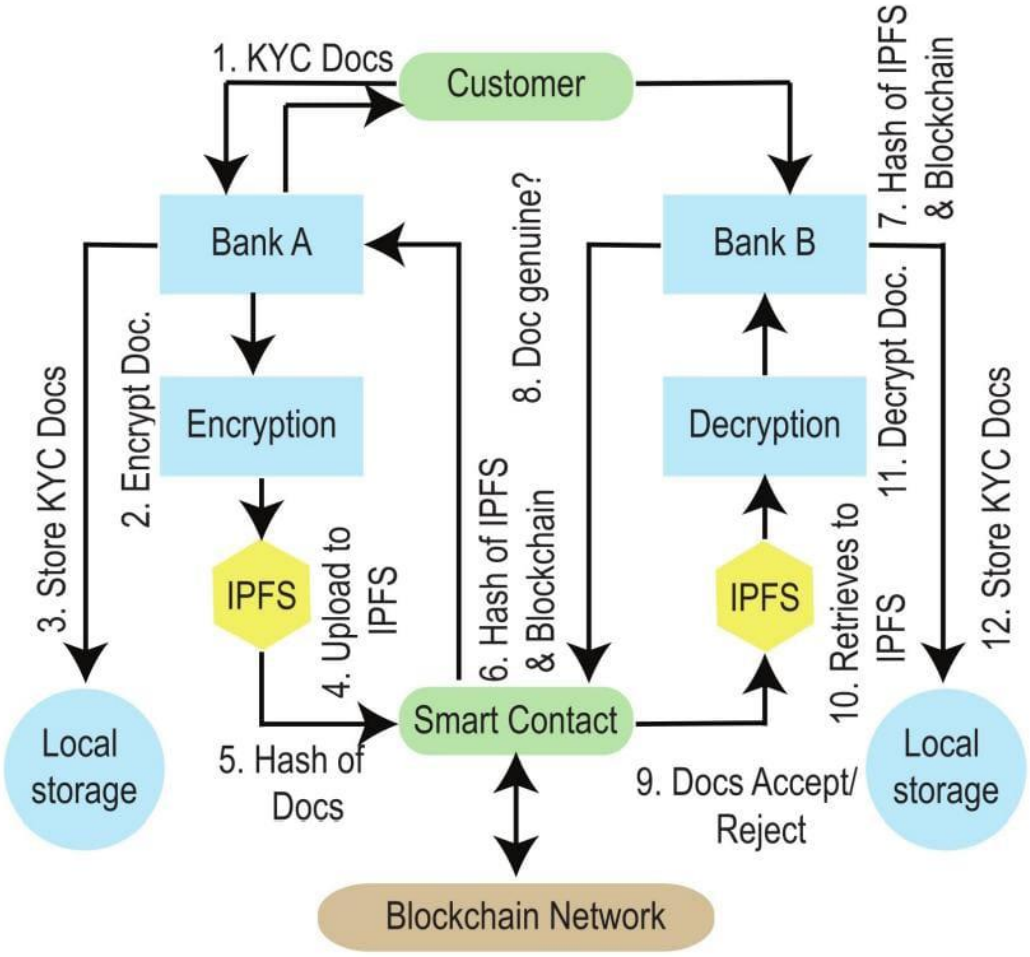
|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

If the hash code is altered, the data can not be verified which will be identified by IPFS. Besides, IPFS identifies duplication if files with the same content are stored.

KYC Verification

We considered a scenario in which, in the first phase, a customer went to Bank A to open an account. The customer submitted the account information along with KYC docs to the Bank. The bank then observed the whole information, which, if found correct, will be encrypted using the system's application (a popular encryption tool, gpg4win, and IPFS in our case) which will be available to all banks to share documents with other bank and store a copy to a local database. Afterward, the encrypted file will be stored in the private IPFS network by bank A. Later, the bank will upload the hash value from IPFS, a very small in-memory size, to the Blockchain network. Bank A also keeps a copy of the customer's KYC docs to the local database of it. Finally, Bank A will share the hash value of Blockchain and IPFS to the customer. Later on, the customer can give access to the KYC doc package by just sharing the hash value to any other institution he intended to work with. However, now the customer can go to another bank to open another account. The customer will share his hash value from IPFS, and Blockchain to Bank B. Since Bank B will be granted access to the hash value of the document package by the customer, the Bank will get access to the Blockchain network for the required hash value. Subsequently, the bank will download the encrypted KYC docs from the IPFS network using the hash value retrieved from Blockchain. Lastly, with the help of the private key of the customer, the Bank will retrieve the KYC docs and keeps a copy of KYC docs to the bank's local database. The regulatory bank defined in the proposed solution in the central bank.

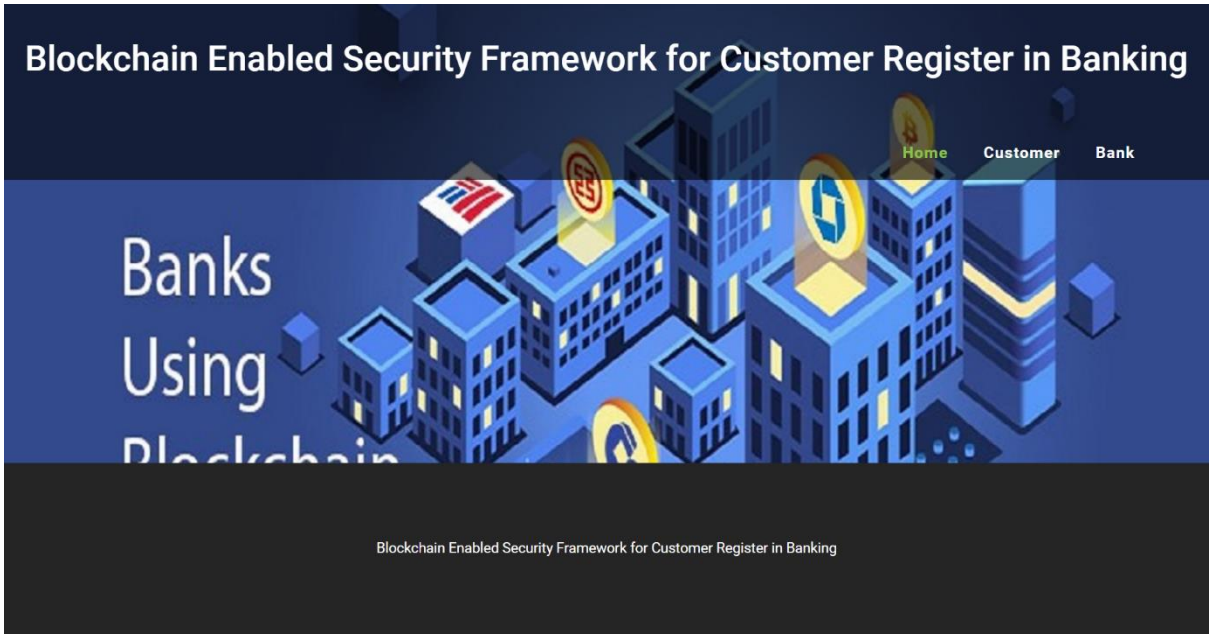


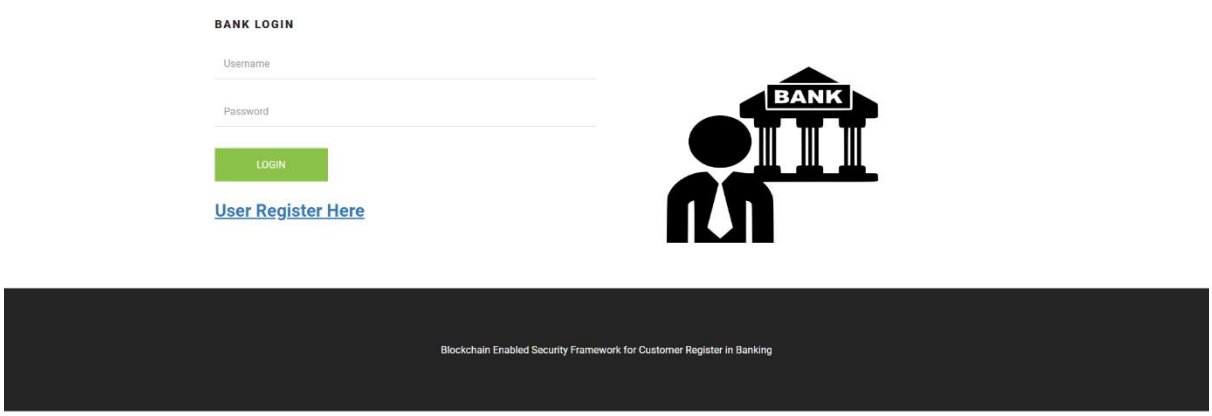
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

IV. EXPERIMENTAL RESULT

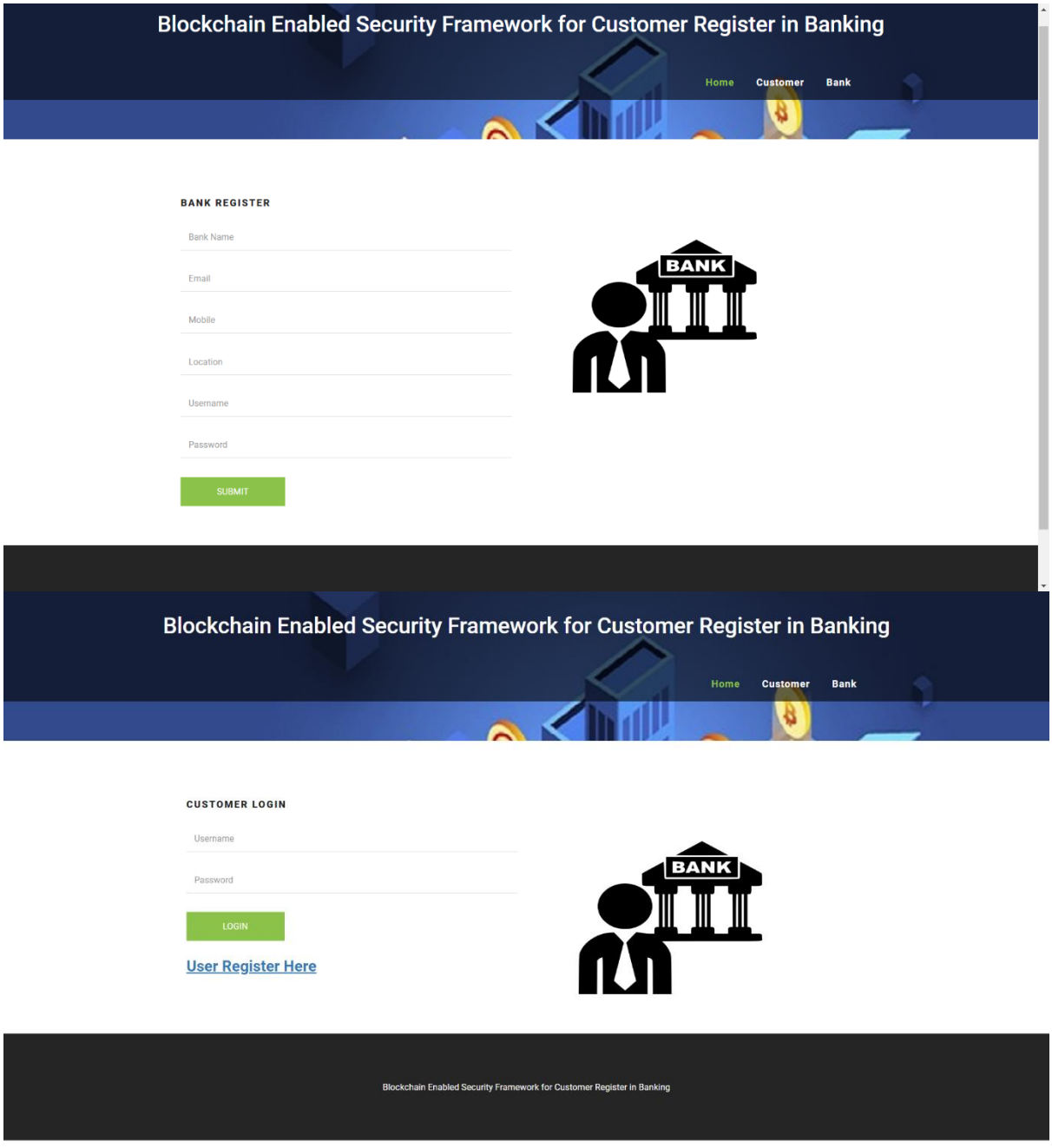




|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

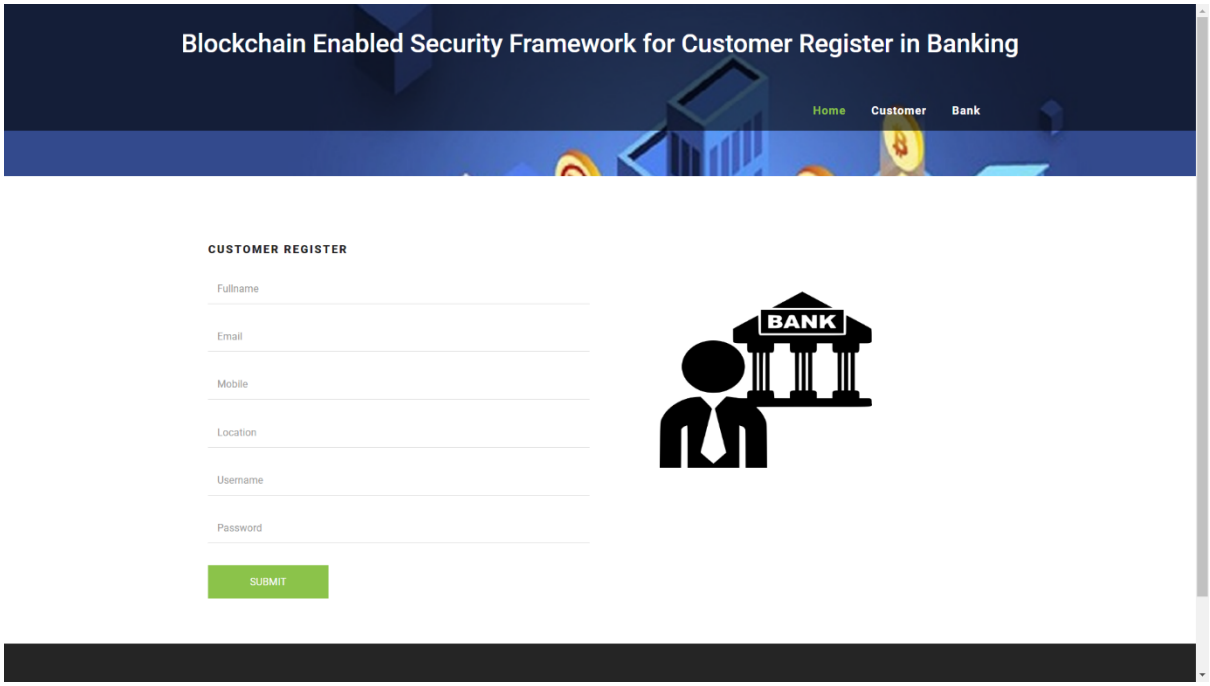
| DOI:10.15680/IJIRSET.2023.1204267 |

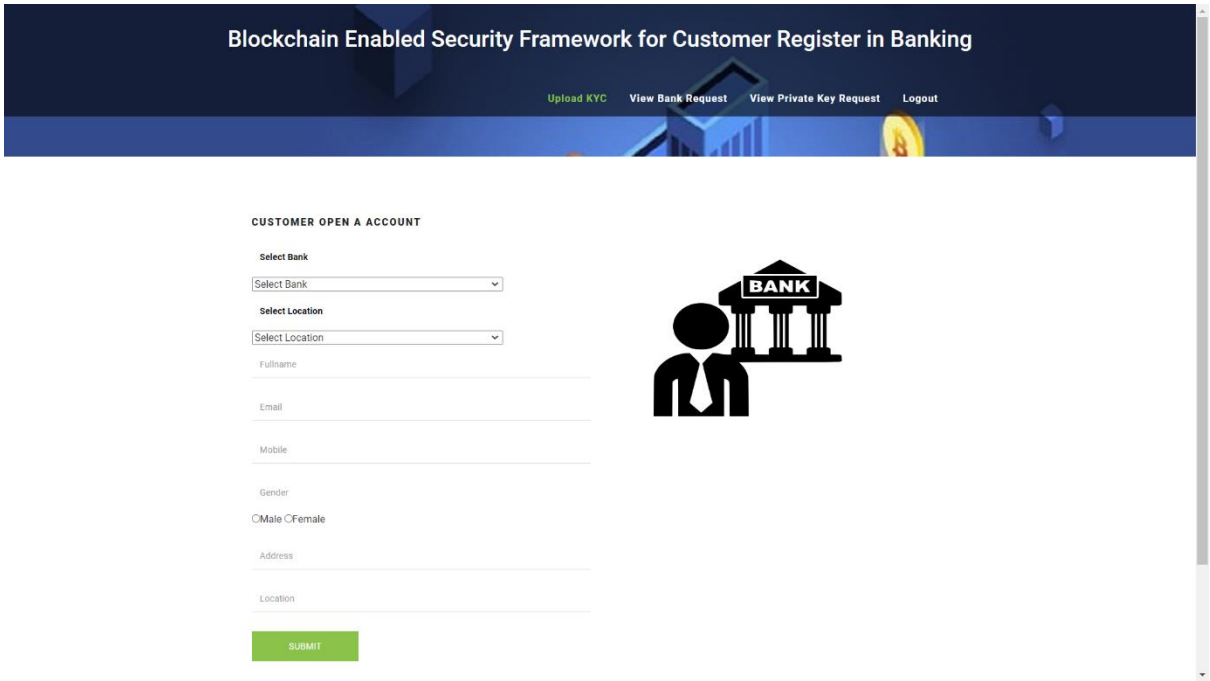


|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

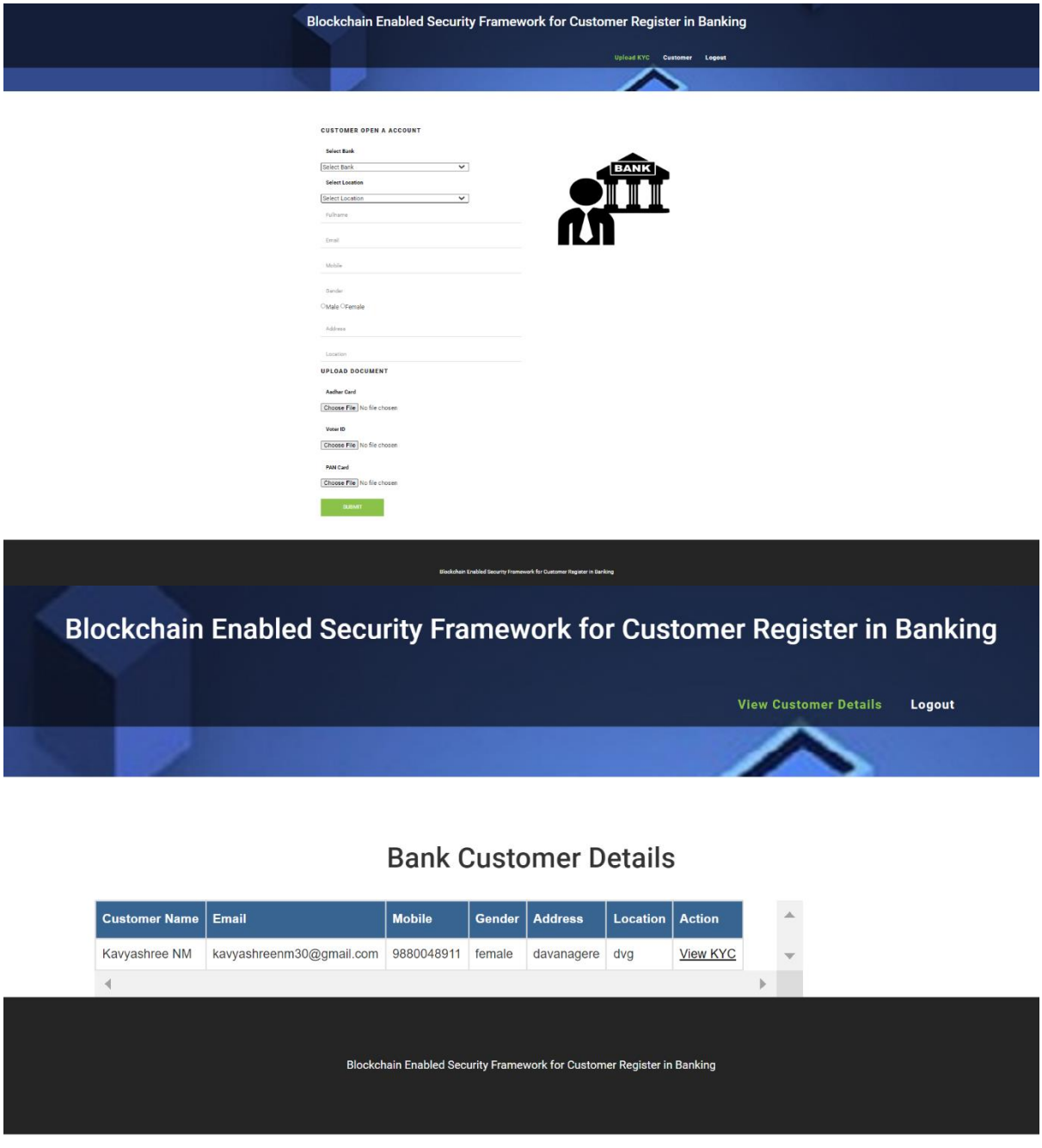




|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

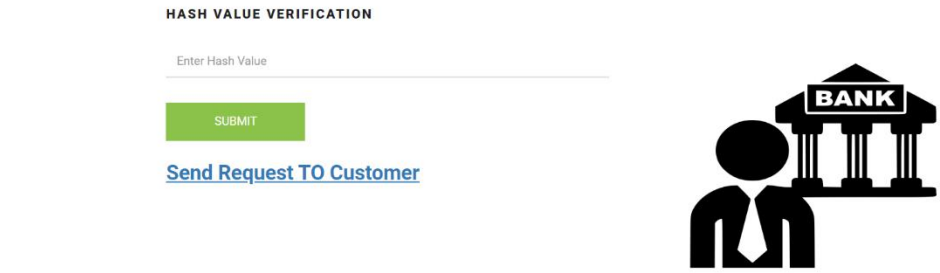
| DOI:10.15680/IJIRSET.2023.1204267 |

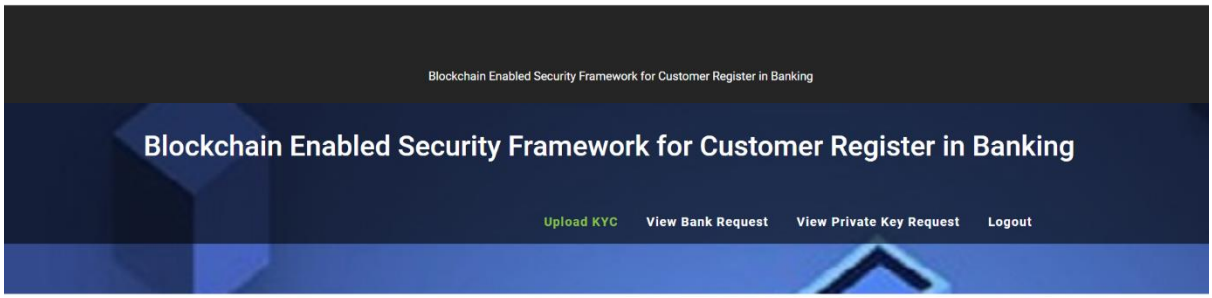


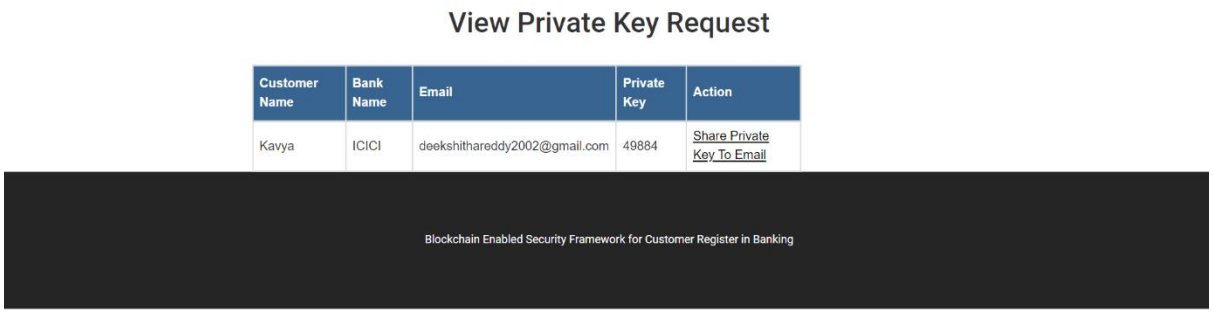
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |



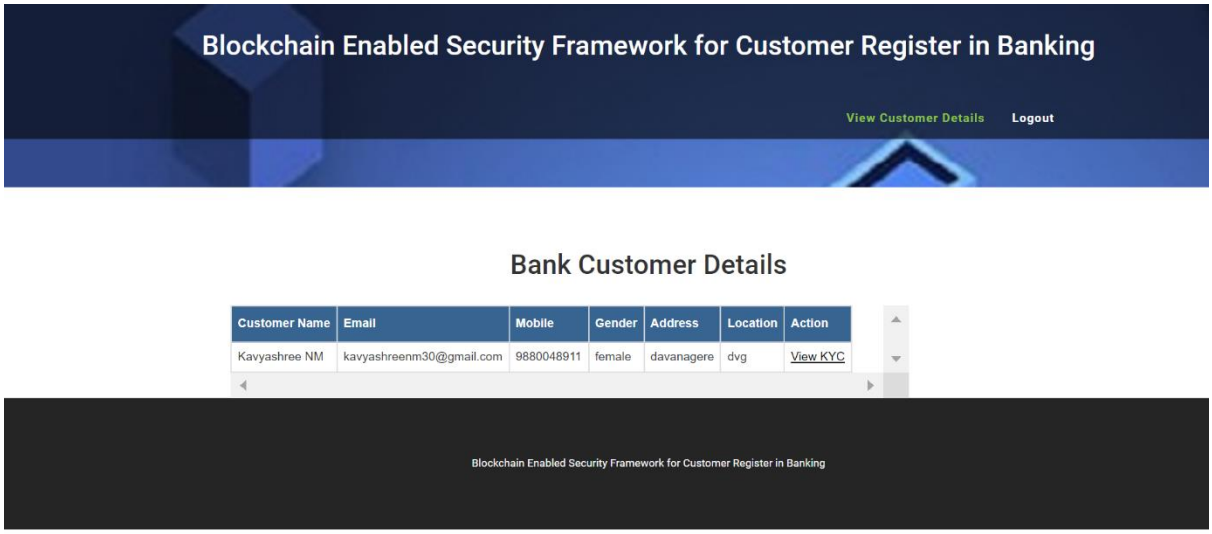


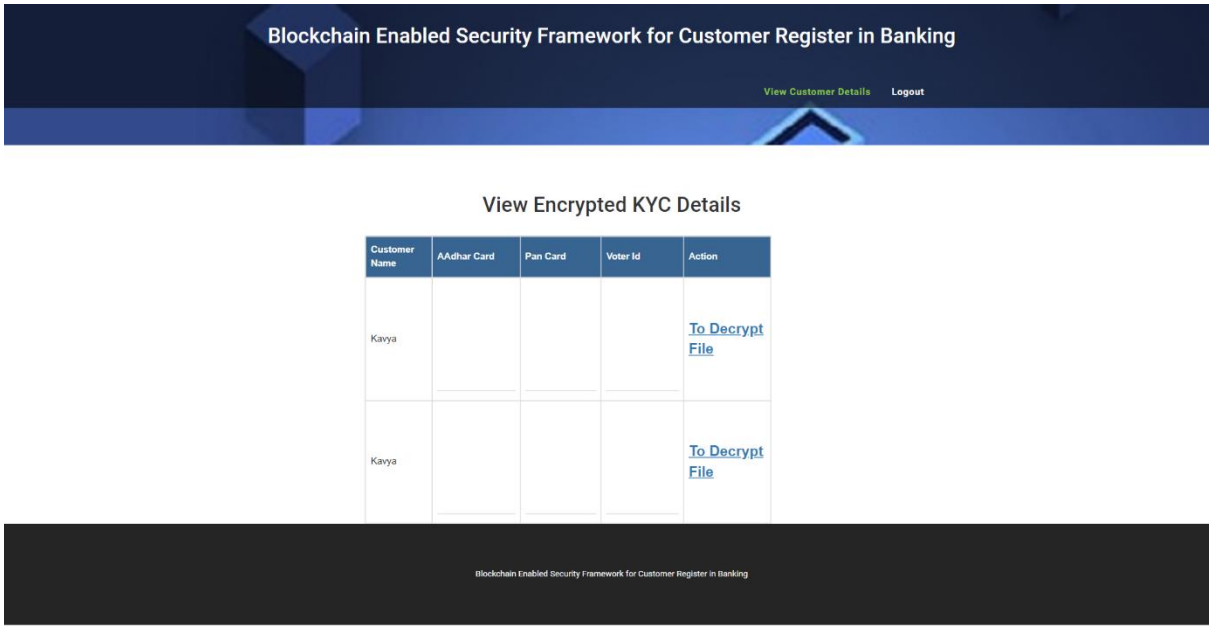


|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

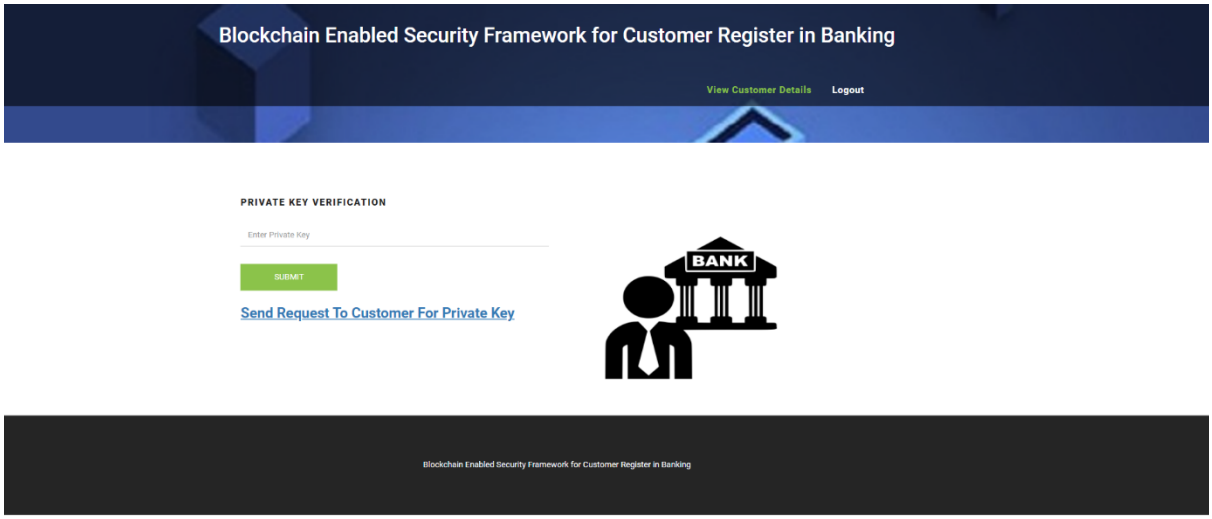


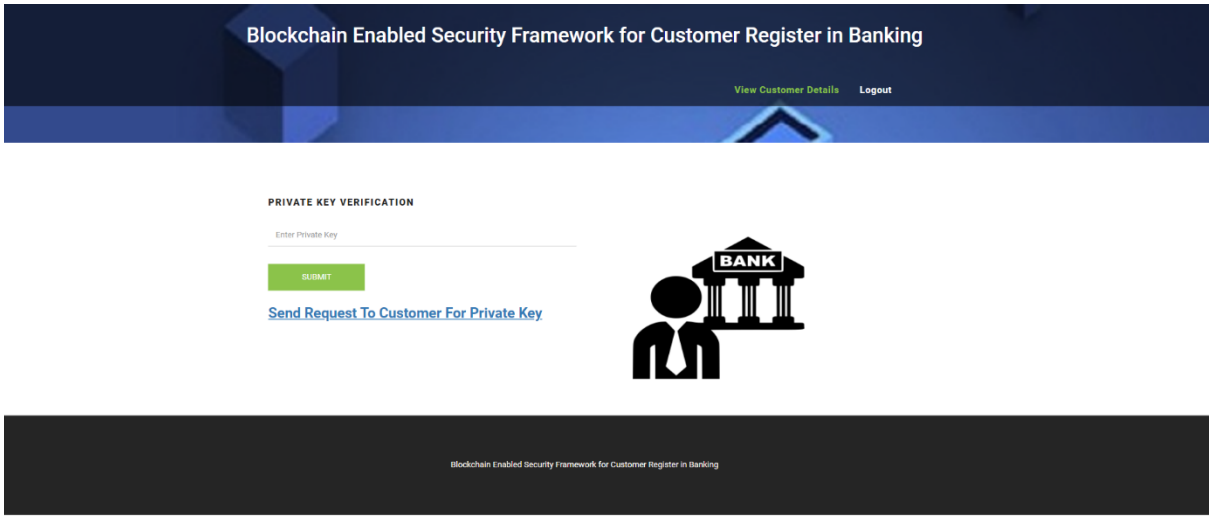


|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

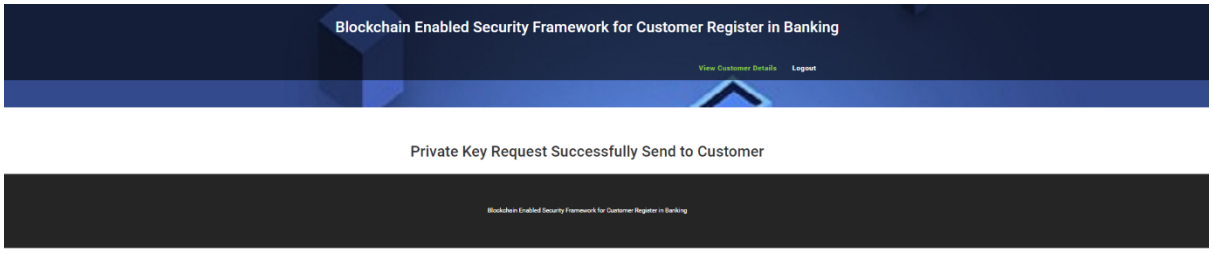


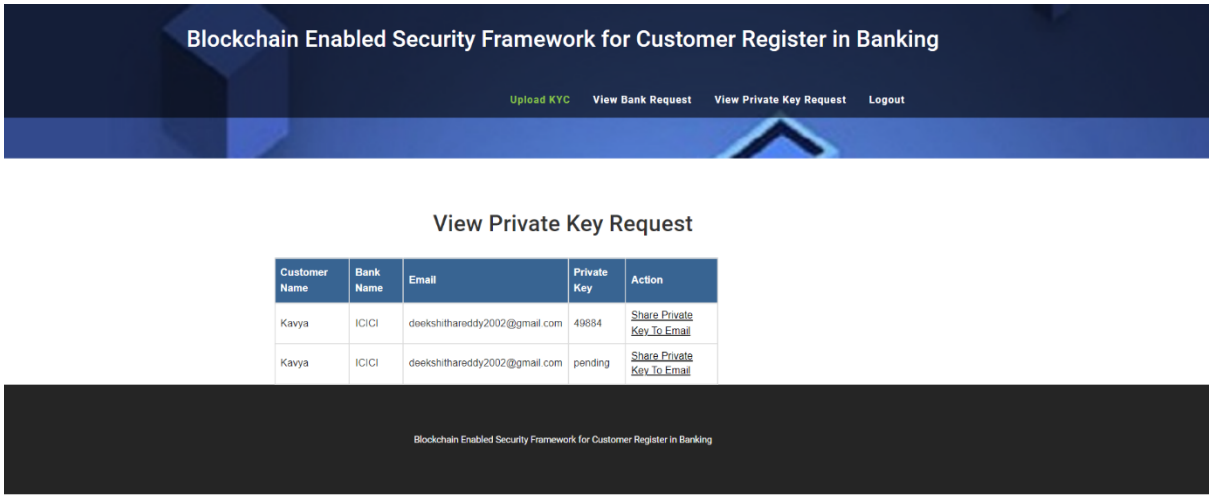


|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

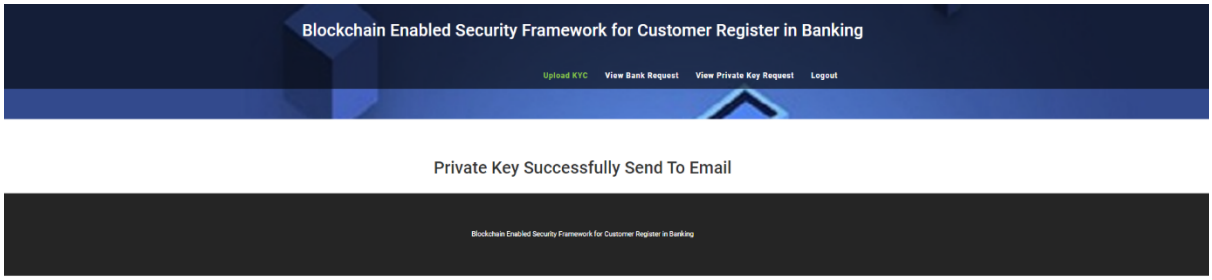


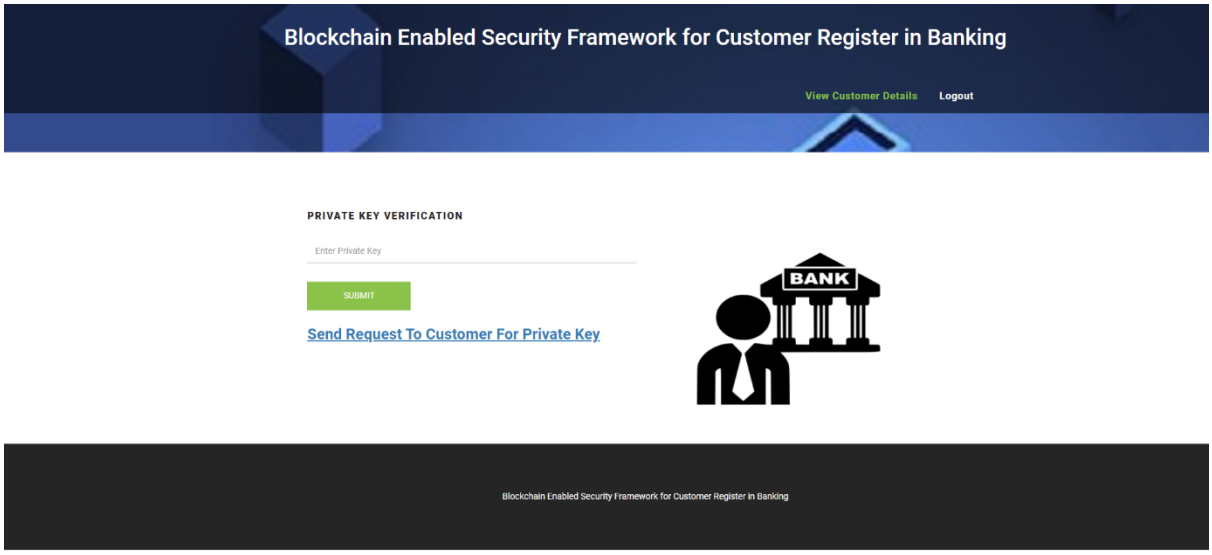


|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

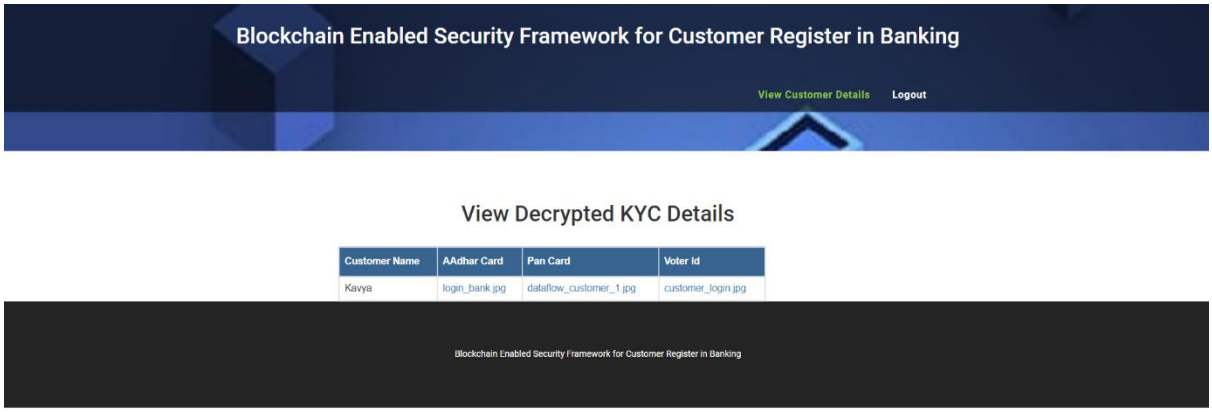




|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |



V. CONCLUSION

To implement a platform for easy KYC document verification through a document-sharing platform called IPFS. We used different operating systems within PCs to test our works. The key generation and encryption processes were very smooth. We easily uploaded the encrypted file using the desktop app of IPFS using the command line interface of Windows Power Shell, and successfully uploaded and retrieved at PC2. Our research focused on a real scenario of a customer going to work with two financial institutions. The paper also showed the way of sharing the KYC docs without many difficulties between financial organizations through the wish of the customer.

REFERENCES

[1] F. Glaser, “Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3052165, Jan. 2017.

[2] A. Rahman, S. Roy, M. S. Kaiser, and M. S. Islam, “A lightweight multi-tier s-mqtt framework to secure communication between low-end ioi nodes,” in 2016 5th International Conference

[3] M. Raikwar, S. Mazumdar, S. Ruj, S. Sengupta, A. Chattopadhyay, and K.-Y. Lain, “A Blockchain Framework for Insurance Processes.” 20/h 9tñ HIP Ititernutionul Conference on New Tec hnc›lc›gies, Mobility und Security (NTMS), 2018.

[4].D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang, “The Blockchain as a Decentralized Security Framework [Future Directions],” IEEE Consumer Electronics Magazine, scd. 7, pp. 18—21, 2018.

[5] M. Mahmud, M. S. Kaiser, M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun, and A. Hussain, “A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications,” Cognitive C‹›myututi‹›n, vol. 10, no. 5, pp. b64—b73, Oct. 201 b. [Online]. Available: [6] l4tt|as://cloi .t / 1 IL I 007/S 1 25 I "9- 0 I S- °)fi43-3 S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2010, library Catalog’ bitcoin.org. Online].

[6] D. Tonin, “Money Button CEO: How to upload large hles to Bitcoin SV blockchain,” Mar. 2019, library Catalog: coingeek.com Section: Tech. [Online].

[7] M. Irvine an‹l D. King, “The Money Laundering Control Act of 19b6: Tainted Money and the Criminal Defense Lawyer,” McGeorpe Law' Review, vol. 19, no. 1, pp. 171—192, Jan. 1987. [Online].

[8]. Kapoor, S. AltCoins: Cryptocurrencies beyond BitCoin. Available online: https://www.itexchangeweb.com/blog/altcoins-cryptocurrencies-beyond-bitcoin/ (accessed on 30 July 2019).

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204267 |

[9]. Guo, Y.; Liang, C. Blockchain application and outlook in the banking industry. Financial Innovation 2016, 2, 24.
[10]. Rosati, P.; Cuk, T. Blockchain Beyond Cryptocurrencies: FinTech and Strategy in the 21st Century. In Disrupting Finance, Lynn, T., Mooney, J.G., Rosati, P., Cummins, M. (Eds.), pp.149-170, 2016.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details