International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 15 (2023) pp. 512-521

Received: 04 July 2022; Accepted: 15 May 2023; Published: 9 July 2023

Smart Card-Based Secured Cloud Banking System Using Smart Contracts

Ankur Biswas[1], Abhishek Roy[2] and Debashis Nandy[3]

[1] Department of Computer Science and Engineering, Adamas University,
Barasat, Kolkata 700126, India
ankur2u@gmail.com
[2] Department of Computer Science and Engineering, Adamas University,
Barasat, Kolkata 700126, India
dr.aroy@yahoo.com
[3] Department of Computer Science, Brainware University,
Barasat, Kolkata 700125, India
debashisnandy99@gmail.com

***Abstract*: By eliminating a few of the operational hurdles that institutions encounter with their very own technology and infrastructure, cloud banking allows them to fulfil expanding requirements and shifting customer expectations. The financial cloud enables banks to acquire on-demand access to different computers and processing capacity, focusing attention on quick scalability whenever the organization encounters unanticipated high-volume activities. The analysis of the article will result in implementing an intelligent, protected cloud-based financial system. The four major topics linked to the cloud as well as blockchain technology in financial systems will be outlined in the paper's introduction. To begin, the disadvantages of the traditional banking system will be explored. Second, the technical advancement of the financial system and the extent to which technology will evolve in the banking industry will be presented. Third, the security of banking transactions will be performed, which will include a description of the security measures that will be implemented by financial organizations. Fourth, the basic idea and applications of blockchain will be thoroughly covered, including the topics of smart contracts as well as the cloud banking system. The whole suggested secure authentication mechanism of something like the cloud financial system will then be defined in-depth in the second section of the research. This section of the study will also include flowchart and GUI depictions of financial transactions among sender and recipient of various banks. As a result, a cloud-based safe web banking system equipped with smart cards will indeed be established.**

***Keywords*:** Cloud Banking, Smart Card, Blockchain, Smart Contract**.**

I. Introduction

In today's economic structure, financial institutions progress depositors' cash as mortgages to industrialists, dealers, entrepreneurs, or businessmen. Whenever a businessman with just 10 crores of their very own investment acquires 90 crores through banking as well as invests in a major project's success, it signifies that 90 percent of the enterprise was generated by depositors' cash, whereas only 10% was developed according to their own investment [1]. If such a huge task generates large profits, just a little percentage, say 8 or 10%, would go to depositors through into the banks, whereas the remainder would go to businesspeople with real role in the company is less than 10% [2-5]. Perhaps this tiny amount approximately 8 or 10 % is returned away by manufacturers since it's included in expense of producing goods.

In a nutshell, every one of the company's current gains is made by those whose personal money doesn't surpass 10% of the invested capital. In contrast, those holding 90% of the invested capital receive nothing other than a set interest rate, which would be frequently recovered via increasing product pricing [6].

On the flipside, if the manufacturers go insolvency in extraordinary situations, whose personal damage is limited to 10%, whereas the other 90% is entirely paid by the banks, and even in some situations, through the depositors. As a result, the real interest rate is indeed the chief reason for inequities in the distribution network, which has a persistent propensity to favor the affluent but also against the poor's interests. In contrast, Islam does have a definite guideline for such financiers. A banker should assess if he is providing a loan to aid the borrower on compassionate grounds or if he wants to distribute his earnings, thus according to Islamic standards. If someone wishes to help the debtors, they must refrain from demanding anything extra on the capital of his debt since their purpose is to help them [7-9].

Nevertheless, if someone wants to partake in their debtor's earnings, they must share equally in their debtor's misfortunes. As a result, the financier's rewards have indeed been linked to the company's current real profitability. The bigger the enterprise's earnings, the larger its rate of interest to that same financier. If indeed the firm makes great earnings, they would not be safeguarded just by the entrepreneur and would be enjoyed by the general public as banking depositors. As just a

result, finance based on principles of Islam tends to favor the normal folks instead of the wealthy [10].

A. Technological enhancement of the banking system

AI, clouds, robots, APIs, and cybersecurity are opening up fresh options for financial firms, allowing banks, community banks, and non-traditional suppliers to launch innovative goods/processes, improve client interactions, and increase efficiencies that could save huge amounts of money [11]. The rising use of e-banking, the advent of technological advances, the weaving of industrial environments, and a greater emphasis on innovation everywhere are producing difficulties and possibilities with in banking business. Clients are gradually flocking to fintech alternatives including huge tech companies providing vital financial products like savings, mortgages, transfers, and investment, fracturing existing ties [12-14]. The necessity of designing and implementing innovative internet products, creating new business opportunities, and shifting from such a product-centric to something like a customer-centric mindset should indeed be emphasized by all community banks in the future. Such activities could no longer be regarded as long-term goals. They must always be completed immediately at electronic speed and strength. Recent gains in online banking acceptability and then use has helped neo-banks, product-focused fintech start-ups, especially major big tech marketplaces. Although younger audience groups continue to favor technological services, the rising usage of different financing organizations as a principal commercial bank should be a worry including all conventional community banks [16].

There seems to be an increasing tendency forward toward a demand for companies which can combine multiple economic services under a unified platform, with such a greater level of personalization than is now seen in most banking firms [17]. As financial instrument inventories spanning numerous firms grow increasingly diversified, so does a need to harness current technology. Regrettably, numerous businesses lack confidence in their capacity to exploit new technologies as well as lack the institutional skills and knowledge to rapidly improve competencies. Whereas the outbreak increased technological advancement that assist online banking transition, the majority of these expenditures were scattered and lacked an overall plan for implementation [18-20]. As a consequence, the performance of these ventures was frequently erratic. According to a Deloitte study, just 11% of banking firms worldwide have automatically patched their basic operations.

When questioned if there are substantial hurdles to implementing technological advances, over 50 % of companies questioned reported difficulties with each key technology required for future success [21]. Alarmingly, despite the abundance of solutions and services eager to assist, more than four out of five enterprises are experiencing difficulty implementing AI [22]. The difficulties in recruiting and creating a more modernized workforce are among the causes of the obstacles to adopting sophisticated technology [23]. According to the Deloitte report, four out of ten credit institutions participants say their staff is still not capable of adapting, re - skilling, or take new tasks, and acquiring new people with unique technical knowledge is more difficult than before. In several circumstances, corporations have worked with third-party services to help improve internal management skill enhancement [24]. Financial firms would need to employ contemporary technologies to facilitate flexibility, productivity, safety, as well as technology in order to be future-ready. Smart requires great, new banking APIs, cloud services, increasing automation, embedded solutions, including security would help financial institutions distinguish themselves in 2022 and even beyond [25]. The goal of every technology diffusion ought to be to improve online customer engagement to such a rapid and large extent.

B. Security of banking transaction

As a component of an eCommerce purchase, everyone does digital/retail transactions online, on handheld platforms, including POS terminals. Online shoppers tend to conduct general financial operations such as local remittances or global cross-border remittances using the Banking / Fintech interface [26]. As part of its promotional banking activities, banking, financial firms, including payments fintech firms present their customers with a variety of money transfers. As they design applications for multiple platforms such as Android, iOS, including specially built to meet the varying demands of customers for transaction commencement. At the very same moment, there really are security breaches and illegal networking activities. Banks want to guarantee that networking transactions are secured since client financial information is at stake. The main issues that banks and financial institutions confront in terms of financial safety are the frauds of online payment and triangulation. Security of banking transactions refers to banks and other financial institutions providing comprehensive safety control over resource transactions done by customers from across networks and access and on any platforms such as Net Banking, Smartphones, and E-commerce [27-29]. As a component of processing transactions, this plays a critical role in verifying that transactions are started by authentic consumers and other entities. Consumers should indeed be warned that they can also experience dangers such as duplicated transactions, fraudulent websites, or transactions failures while using the network connecting their banking institution as well as transaction aggregates. There might be a variety of reasons for system failures, including network problems, slow response out from network infrastructure, and so forth. Banks will wish to record and track the essential information in respect of each and every transaction handled by their customers:

- Transactions inception,
- The medium upon which transactions are carried out.
- Method for Transactions Verification,
- IP address,
- The timeline of the transaction.

As previously said, the above-mentioned data would give crucial information about just the total transaction structure for any further research and investigation in order to determine the actions that occurred so over networks [30]. Banks must combat illegal transactions that occur via the internet. Because deception can come at any stage whenever data is easily accessible to attackers. Continuous monitoring of payment channels, information transfer of consumer Personal information, data protection vulnerabilities, the client often changing mobile number/email for obtaining electronic OTPs and credentials, etc. Banks and other financial institutions should adopt the following measures to improve money transfer safety are [31-34]:

- At periodic intervals, performing of auditing reviews on different tools and procedures.
- Allowing a varying consumer authentication protocol depending on the user's geo-spatial position and the gadget used to begin the transactions.
- VR technology could play a pivotal role in the national economy. Allowing a face recognition system to authenticate consumer authenticity, which would be a tamper-proof system.
- AI / ML system design Organizations can develop numerous data methods to assess consumer transaction patterns and commonly utilised channels.

At conclusion, banking, financial institutions, and fintech companies want to guarantee the safety of any and all monetary operations [35]. Transactions provenance ought to be precise, and openness improves bank management as well as regulation and control. This enables banks to concentrate on key business acumen and customer loyalty, whereas fraudulent financial adherence, as well as management, get to be a key differentiator instead of an expensive charge [36-38].

C. Basic concept and application of block chain

A blockchain consists of discrete chunks of memory that represent a sequence of connected events that are connected together within chronological order. It enables all participants to exchange a digital ledger along with a computer system without requiring a centralised government [39]. A trade may look just like this: A would like to donate cash to B. Blockchain does have the power to change the way people conduct business all over the globe. It offers the potential to boost business productivity by automating as well as simplifying laborious as well as paper-based processes [40-43]. Since it is decentralised and can also be possessed by such a single individual, a blockchain network may be an excellent tool for collaboration. As a result, blockchain is much more than merely the technologies that underpin cryptocurrencies such as Bitcoin as well as Ethereum. The 5 Blockchain usage in the sector of banking are as follows –

- Fund Raising Systems
- Payment in a faster way
- System of clearance and settlement
- Financial Trade
- Credits and Loans

Blockchain must satisfy a range of criteria before it could be considered a widespread innovation in financial services. It is critical first to construct the architecture required to operate a global network utilizing matched technology [44]. Blockchain would only be able to thwart the business if it has been broadly used. Nevertheless, the expenditure would be well worth it. Blockchain, whenever completely deployed, is believed to enable institutions to accept payment very rapidly as well as accurately whilst simultaneously cutting transaction management expenses [45-49].

Smart contracts are electronic agreements which are maintained on even a blockchain and thus are implemented instantly while pre-set criteria as well as circumstances are satisfied. Smart contracts are essentially programmes that run if certain criteria are satisfied and are recorded on a blockchain [50]. These are often used to streamline the implementation of a contract so all stakeholders are instantly confident of the result, even without participation of a middleman or the waste of time. They could also automate a process by initiating the very next operation because certain circumstances are satisfied.

Retail banks reacted with brilliance as well as effectiveness towards the pandemic's immediate and significant service problems [51]. Several institutions were eager to design and implement rapid consumer migrations to remote-based offerings including internet as well as app-based financial services. This advancement is critical for such banking sector since it demonstrates whatever institutions are genuinely able to accomplish technically whenever forced to do something in response to customer demands [52]. The obvious advantages of this approach for banks demonstrate how they can maintain their amazing digital initiatives. Cloud computing has the potential to centralise data collecting, storing, as well as interpreting procedures [53]. It can also bring down the cost involved with any of these important operations while generating significantly richer, more accurate, and quicker data-driven deep insight that institutions can employ to improve success [54]

II. Related Work

In this section, the authors have compared some of the various suggested cloud banking models with existing works to propose the desired solution. In one of the paper by Ankur Biswas et al. [55], authors had proposed Blockchain-based user authentication scheme for Citizen-to-Government (C2G) type of Cloud Governance transaction. Ankur Biswas et al. [56] in their paper had proposed a Multipurpose Electronic Card (MEC)-based Cloud Banking System (CBS) as a part of broader Integrated Electronic Service Delivery System (IESDS), that verifies its user (i.e. Client) through various multilevel architecture. In another paper, Ankur Biswas et al. [57] had studied about the various applications of dynamic authentication techniques over smart card-based electronic transactions. Furthermore, Ankur Biswas et al. [58] with the help of Interplanetary File System (IPFS) over banking and legal datasets had implemented secured electronic file management. In this paper, the authors have used these models as origin of the proposed research work, which has been discussed in the subsequent sections. The motivation of this research is to enhance the existing methods using smart card technology for secured online banking transaction systems.

III. Transactions Using Secured Cloud Banking System

Financial institutions and financial market experts are quickly realizing that perhaps the cloud is far more than technologies; it provides a location for financial institutions to store programs and data and utilize sophisticated hosted services over the internet [59]. Cloud banks provide a variety of advantages to financial firms, notably cost reductions, enhanced flexibility, and better productivity. However, like with any latest tech, there really are hazards involved in using cloud banking [60].

The transaction of the cloud-based online banking system has been discussed in detail. The system has been proposed through the Figure 1 stated showing the flowchart of the cloud-based online banking system.

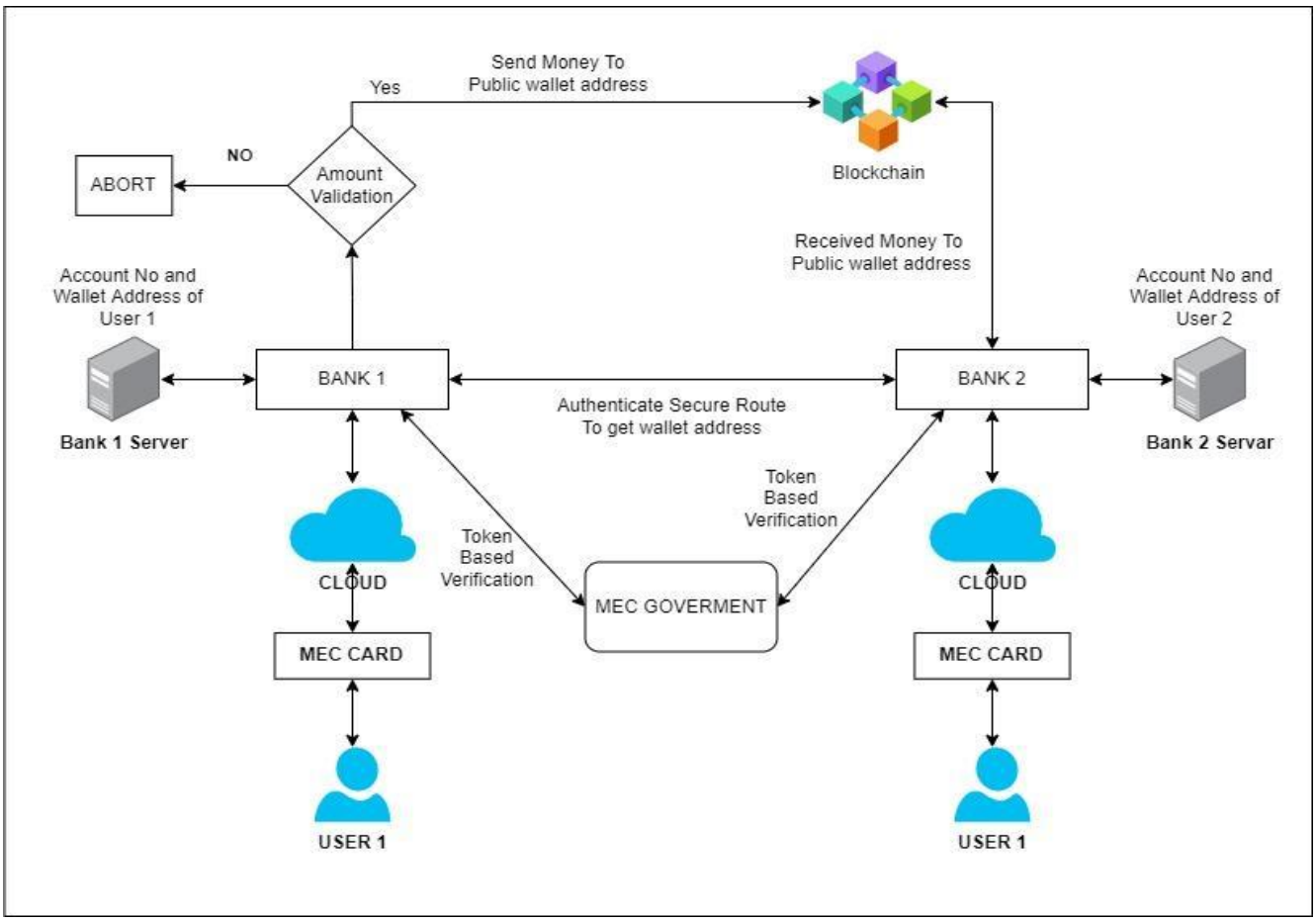

Figure 1. The cloud-based online banking system

According to Figure 1, there are two banks and two users are using the server of two banks. The user 1 and user 2 uses the MEC card for accessing the cloud-based services of the bank 1 and bank 2 respectively using vending machine for swiping or making use of the card. For making a link between the user 1 and the user 2 of bank 1 and bank 2, the MEC governing body came into action to authenticate the routes that are secured for getting the address of the wallet of each bank. This process takes the help of the verification using the tokens to get better access of the customer data and information. The servers of bank 1 and bank 2 store the account number and address of the wallet for user 1 and user 2, respectively. For making the transaction from user 1 of bank 1 to user 2 of bank 2, at first, the amount to be transacted will be validated to see whether the amount is available in the bank of user 1. After validation, if the bank could realize that the amount required by user 2 of bank 2 is available with user 1 of bank 1 then the money is sent to the blockchain by using the wallet address of the public body. The money is then received by user 2 of bank 2 with the help of blockchain.

Blockchain acts as the heart or brain of the system and works as the controlling body for the cloud-based online banking system, which works mainly with blockchains. Systems have the potential to enable financial institutions to process money transfers and trace them more effectively than older techniques like SWIFT. Because of how the financial system is structured, a regular bank transaction takes several days to finalize. Because blockchain is decentralised, there really is no centralised location where it may be maintained. As a result, it is maintained in machines or devices all over the internet. Such devices or machines are referred to as nodes. Every node contains a single copy of blockchain, or the activities that take place on the system. Transactions may be conducted quicker and more effectively by optimising such procedures using blockchain. Supporting documents and transaction data may be recorded on the blockchain, removing such a need to trade hardcopy. Because of no use of hardcopy to balance the various general ledger, trading and settlement may be completed significantly more quickly. If the bank could realize that the amount required by user 2 of bank 2 is not available with user 1 of bank 1 then the whole process will get aborted, and no transactions would be possible between the two banks. The banking system has two users such as the sender and the receiver.

A. Transaction at sender side

Here, user 1 is taken as the sender and user 2 is taken as the receiver. The work of the sender is to send or make transactions of the money to the receiver of another bank having different cloud-based services. The MEC card is used by both the sender and the receiver to access the cloud-based operations of bank 1 as well as bank 2 using a vending

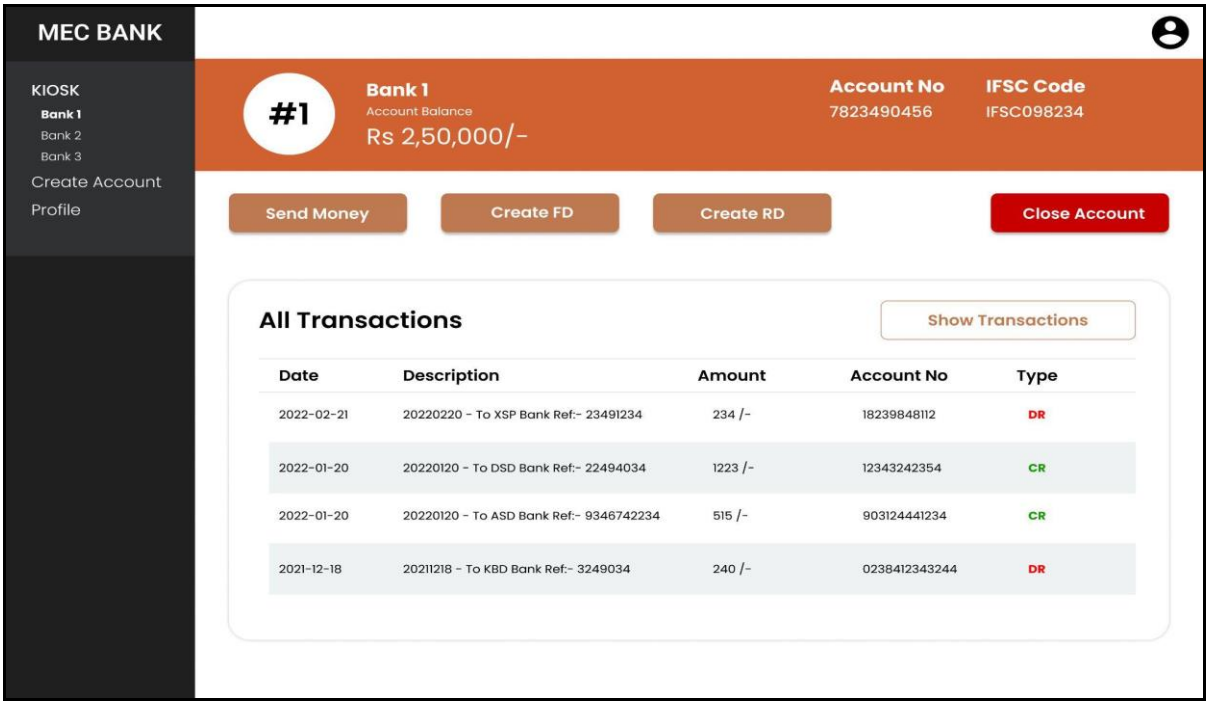

Figure 2. Dashboard for Sender's Side

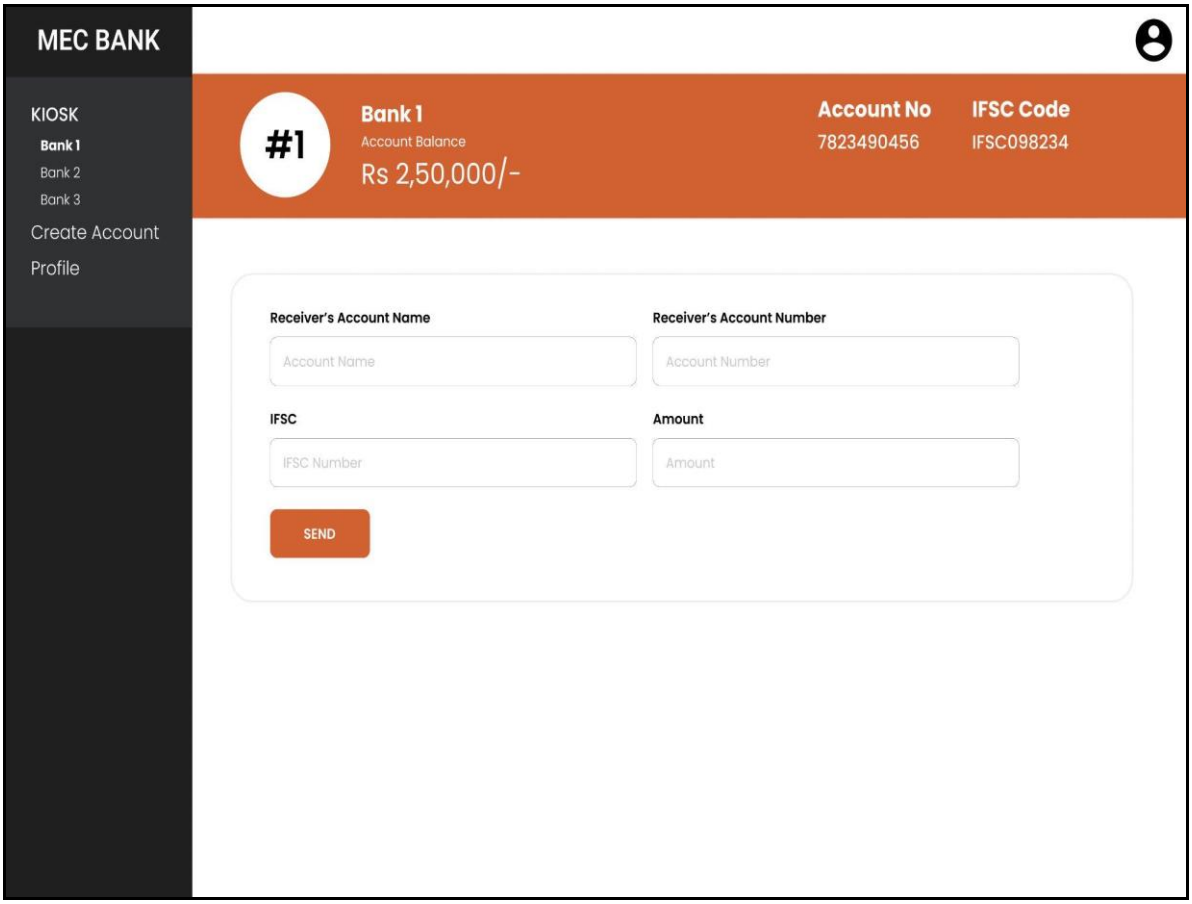

Figure 3. Receiver's information page

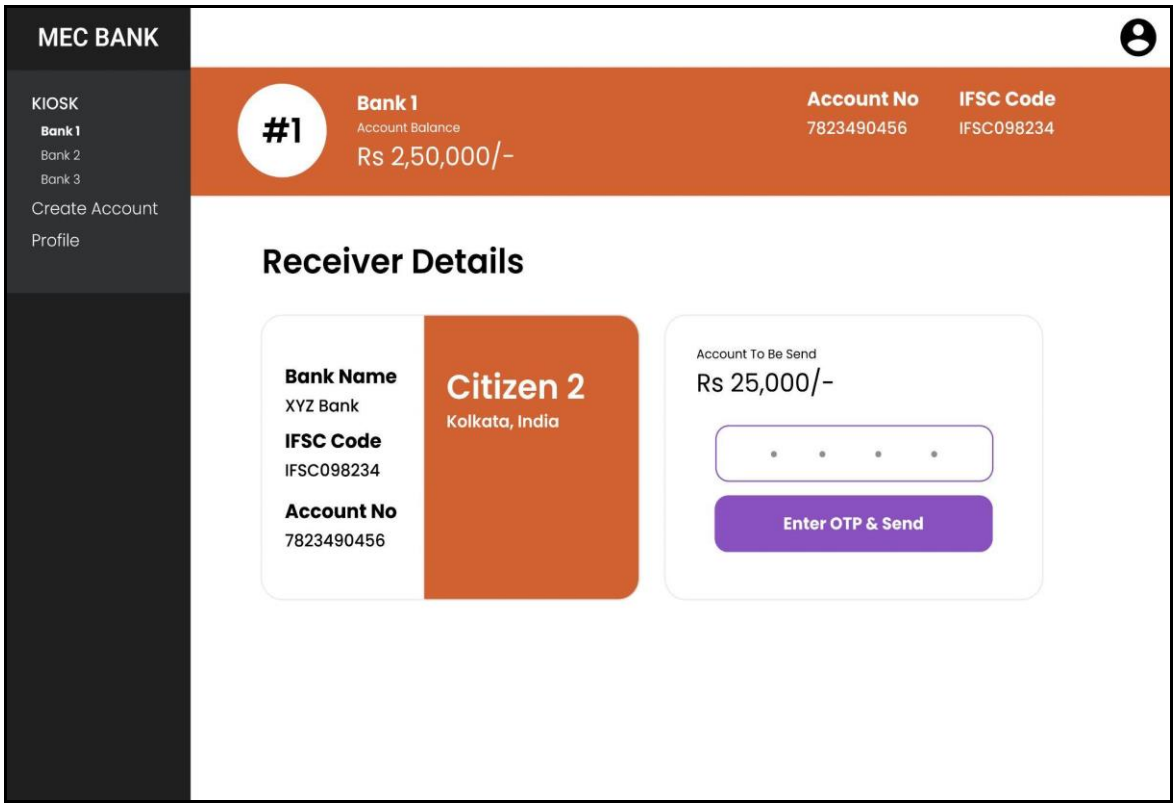

Figure 4. Receiver's verification page

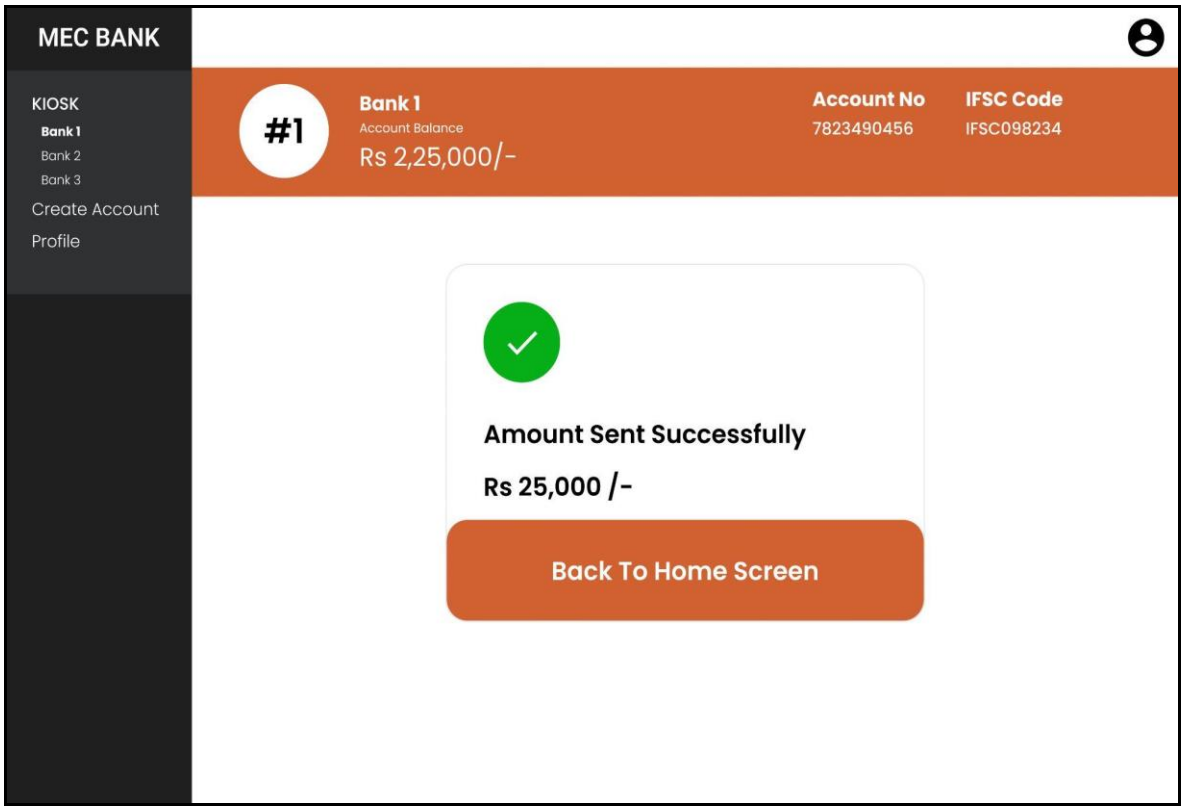

Figure 5. Confirmation Page

machine for swiping or making use of the card. The MEC governing board took measures to authenticate the pathways that are protected for receiving the addresses of every bank's wallet in order to create a connection in between the sender and the recipient of bank 1 as well as bank 2. This procedure makes use of token-based authentication to get greater access to sensitive records/knowledge. The account number and address of such wallets are stored on the databases of bank 1 and bank 2 for such transmitter and recipient, accordingly. To complete the transaction between the sender of bank 1 and the receiver of bank 2, the money to be transacted would first be verified to determine whether the money is accessible in the sender's account. Following confirmation, if indeed the bank determines that perhaps the amount requested by the recipient of bank 2 is accessible well with transmitter of bank 1, the cash is delivered to the blockchain via the governmental body's digital wallet. Bank 2's recipient subsequently receives the cash via the blockchain network. If the bank discovers that perhaps the amount requested by the recipient of bank 2 is just not accessible with the transmitter of bank 1, the entire procedure will indeed be cancelled, and also, no transfers in between both banking institutions will indeed be permitted.

A. Transaction at receiver side

The receiver at first claims money from the sender. On the receiver side, the transaction occurs only if the amount that will be transacted is approved by the sender side. Without that, the receiver side could not get any money from the sender. The receiver will never have the right to force the sender for a money transaction.

IV. Results And Discussions

This section talks about the implementation of banking transactions using MEC card. Here in Figure 2-5, the GUI implementation of the software has been done to make the transactions possible between the users of different banks using MEC card. Figure 2 shows the dashboard for the sender's side in which users can send money to other bank account, can create fixed deposit accounts or recurring deposits. It shows the latest transaction of the user. Latest transaction details include date, description, amount, account no and type (debit/credit). It also shows account balance, account number and IFSC Code of the user's account. When user wants to send money to other account, user clicks on send money button. Figure 3 shows the receiver's information page through which user will put information about receiver's account. It includes receiver's account name, number, IFSC and amount. After entering all the receiver's details and transaction amount, software goes to next step of its application. During this step transaction amount validation happens with the users account balance. Figure 4 shows receiver's details verification page which gives user an authorization of OTP to send money. User receives OTP into users registered mobile. User enters the received OTP to validate the transaction. Figure 5 shows confirmation page, which confirms the transaction of money successfully. It displays the transaction amount and effective new account balance.

V. Conclusion

To conclude, a smart secured cloud-based banking system has been implemented through the study of the paper. The introduction of the paper stated the four different topics related to the cloud and blockchain technology in banking systems. Firstly, the drawbacks of the conventional banking system have been discussed. Secondly, the technological enhancement of the banking system and to what extent the technology has emerged in the sector of the bank has been presented. Thirdly, the security of banking transactions stating the security measures that are taken by the financial institutions is done. Fourthly, the basic concept and application of the blockchain have been discussed in detail saying the topic of smart contracts and the cloud banking system. Then in the second part of the study, the proposed secured transaction mechanism of the cloud banking system is described in detail. This part of the study has also presented the monetary transactions between the sender and receiver of different banks in the form of flowcharts and GUI representations. Hence, a cloud-based secured online banking system has been implemented using smart cards.

References

[1] Roy, A. Object-Oriented Modeling of Multifaceted Service Delivery System Using Connected Governance. In: Jena A., Das H., Mohapatra D. (eds) *Automated Software Testing. ICDCIT 2019. Services and Business Process Reengineering. Springer, Singapore*. pp. 1–25. 2020. https://doi.org/10.1007/978-981-15-2455-4-1

[2] Roy, A.: Smart delivery of multifaceted services through connected governance. In: *3rd International conference on computing methodologies and communication (ICCMC)*. IEEE. India. pp 476—482. 2019. https://doi.org/10.1109/ICCMC.2019.8819851

[3] Pinno, O.J.A., Gregio, A.R.A., De Bona, L.C.E.: ControlChain: blockchain as a central enabler for access control authorizations in the IoT. In: *GLOBECOM 2017–2017 IEEE Global Communications Conference, Singapore* 2017.

[4] Tapas, N., Merlino, G., Longo, F.: Blockchain-based IoT-cloud authorization and delegation. In: *2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina*, pp. 411–416. 2018.

[5] Benhamouda, F., Halevi, S., Halevi, T.: Supporting private data on hyperledger fabric with secure multiparty computation. In: *IEEE International Conference on Cloud Engineering (IC2E)*, April 2018.

[6] Ying, N., Yao, Z., Hua, Z.: The study of multi-level authentication-based single sign-on system. In: *2009 2nd IEEE International Conference on Broadband Network and Multimedia Technology*, pp. 448–452, 2009.

[7] Kansal, S., Kaur, N.: Multi-level Authentication for Internet of Things to establish secure healthcare network. *Int. J. Adv. Res. Ideas Innov, Technol*, 2016.

[8] Peter, S., Gopal, R.K.: Multi-level authentication system for smart home-security analysis and implementation. In: *2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore*, 2016.

[9] Gupta, S., Gabrani, G.: A dynamic two-level priority based authentication system for job scheduling in a heterogeneous grid environment. In: *2016 SAI Computing Conference (SAI), London*, pp. 1100–1106 2016.

[10] Odelu V. IMBUA: Identity Management on Blockchain for Biometrics-Based User Authentication. In*: Prieto J., Das A., Ferretti S., Pinto A., Corchado J. (eds) Blockchain and Applications. BLOCKCHAIN 2019. Advances in Intelligent Systems and Computing, vol 1010. Springer, Cham*, 2020. https://doi.org/10.1007/978-3-030-23813-1-1

[11] Yu, Y., Zhao, Y., Li, Y., Du, X., Wang, L., Guizani, M.: Blockchain-Based Anonymous Authentication With Selective Revocation for Smart Industrial Applications. *IEEE Transactions on Industrial Informatics*. 16, 3290–3300 , 2020. https://doi.org/110.1109/TII.2019.2944678

[12] Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., Salah, K.: A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes. *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*. 2018. https://doi.org/10.1109/AICCSA.2018.8612856

[13] Park, B., Lee, T., Kwak, J.: Blockchain-Based IoT Device Authentication Scheme. *Journal of the Korea Institute of Information Security and Cryptology*. 27, 343–351 2017. https://doi.org/10.13089/JKIISC.2017.27.2.343

[14] Ghosh, A., Das, T., Majumder, S., Roy, A.: Authentication of User in Connected Governance Model. *Data Science and Analytics*. 110–122, 2020. https://doi.org/10.1007/978-981-15- 5830-6_10

[15] Khatun, R., Bandopadhyay, T., Roy, A.: Data modelling for e-voting system using smart card based e-governance system. *Int. J. Inf. Eng. Electron. Bus*. 9, 45–52. 2017. https://doi.org/10. 5815/ijieeb.2017.02.06

[16] Applebaum, B.: Key-Dependent Message Security: Generic Amplification and Completeness. *Advances in Cryptology - EUROCRYPT 2011*, 527–546 , 2011. https://doi.org/10.1007/978- 3-642-20465-4_29 19.

[17] MAGUIRE, M.: A review of user-interface design guidelines for public information kiosk systems. *International Journal of Human-Computer Studies*. 50, 263-286, 1999. https://doi.org/10.1006/ijhc.1998.0243

[18] Haoxiang, W., Smys, S.: Secure and Optimized Cloud-Based Cyber-Physical Systems with Memory-Aware Scheduling Scheme. *Journal of Trends in Computer Science and Smart Technology*. 2, 141–147 2020.

[19] Biswas, S., Roy, A.: An Intrusion Detection System Based Secured Electronic Service Delivery Model. In: 2019 *3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India*, pp. 1316–1321. 2019. https://doi.org/10.1109/ICECA.2019.8822016

[20] Khatun, R., Bandopadhyay, T., Roy, A.: Data Modeling for E-Voting System Using Smart Card based E-Governance System. *International Journal of Information Engineering and Electronic Business*. 9, 45–52 2017. https://doi.org/10.5815/ijieeb.2017.02.06

[21] Roy, A., Karforma, S.: Uml Based Modeling of ECDSA for Secured and Smart E-Governance System. *Computer Science and Information Technology* (CS and IT). 2013. https://doi.org/10.5121/csit.2013.3219

[22] Mohapatra, S., Paul, K., Roy, A.: Object-Oriented Modeling of Cloud Healthcare System Through Connected Environment. *Applications of Internet of Things*. 151–164, 2020. https://doi.org/10.1007/978-981-15-6198-6

[23] Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. Business & Information. *Systems Engineering* 59(3), 183–187 2017. https://doi.org/10.1007/s12599-017-0467-3

[24] Risius, M., Spohrer, K.: A Blockchain Research Framework. *Business & Information Systems Engineering* 59(6), 385–409 2017. https://doi.org/10.1007/s12599-017-0506-0

[25] Beinke, J., Fitte, C., Teuteberg, F.: Towards a Stakeholder-Oriented Blockchain-Based Architecture for Electronic Health Records: Design Science Research Study. *Journal of Medical Internet Research* 21(10), p.e13585, 2019. https://doi.org/10.2196/13585

[26] Batubara, F., Ubacht, J., Janssen, M.: Challenges of blockchain technology adoption for e-government. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. 2018. https://doi.org/10.1145/3209281.3209317

[27] Motta, G., Tekinerdogan, B., Athanasiadis, I.: Blockchain Applications in the Agri-Food Domain: The First Wave. *Frontiers in Blockchain*. 3, 2020. https://doi.org/10.3389/fbloc. 2020.00006

[28] Xie, J., Tang, H., Huang, T., Yu, F., Xie, R., Liu, J., Liu, Y.: A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*. 21, 2794–2830 2019. https://doi.org/10.1109/COMST.2019.289961

[29] I. Gordin, A. Graur, A. Potorac, Two-factor authentication framework for private cloud, in 2019 23rd *International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania*, pp. 255–259 2019. https://doi.org/10.1109/ICSTCC.2019.8885460

[30] A. Mahalle, J. Yong, X. Tao, Ethics of IT security team for cloud architecture infrastructure in banking and financial services industry, in 2019 *IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Porto, Portugal*, pp. 506–511 2019. https://doi.org/10.1109/CSCWD.2019.8791928

[31] M. Singh, K.S. Tanwar, V.M. Srivastava, Cloud computing adoption challenges in the banking industry, in 2018 *International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban*, pp. 1–5 2018. https://doi.org/10.1109/ICABCD.2018.84654129.X

[32] Liao, S. Alrwais, K. Yuan et al., Cloud repository as a malicious service: challenge, identification and implication, in Cybersecurity, vol. 1, 14 2018. https://doi.org/10.1186/s42400- 018-0015-6

[33] J. Gowthami, N. Shanthi, N. Krishnamoorthy, Secure three-factor remote user authentication for E-Governance of smart cities, in 2018 *IEEE International Conference on Current Trends Toward*

Converging Technologies (IEEE, India, 2018), pp. 1–8, 2018. https://doi.org/10.1109/icctct. 2018.8551172

[34] S. Dhal, V. Bhuwan, Cryptanalysis and improvement of a cloud based login and authentication protocol, in 2018 *4th International Conference on Recent Advances in Information Technology (RAIT) (IEEE, Dhanbad, India, 2018)*, 2018. https://doi.org/10.1109/RAIT.2018.8388988

[35] S.P. Tripathi, A. Kumar, R. Astya, Study on secured framework for cloud based online banking, in 2017 *International Conference on Computing, Communication and Automation (ICCCA), Greater Noida*, pp. 853–858 2017. https://doi.org/10.1109/CCAA.2017.8229915

[36] N. Srilatha, G. Mrali, M. Deepthi, A framework to improve E-seva services through E-governance by using DNA cryptography, in 2017 *International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) (IEEE, India, 2017)*, pp. 1–4, 2017. https://doi.org/10.1109/ICAMMAET.2017.8186748

[37] S. Nagaraju, L. Parthiban, Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. *J. Cloud Comp.* 4, 22 2015. https://doi.org/10.1186/s13677-015-0046-4

[38] J. Park, Y. An, K. Yeom, Virtual cloud bank: an architectural approach for intermediating cloud services, in 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, pp. 1–6 (2015). https://doi.org/10.1109/SNPD.2015.7176235

[39] N.E. Madhoun, F. Guenane, G. Pujolle, A cloud-based secure authentication protocol for contactless-NFC payment, in 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), Niagara Falls, ON, pp. 328–330, 2015. https://doi.org/10.1109/CloudNet. 2015.7335332

[40] S.K.S.V.A. Kavuri, G.R. Kancherla, B.R. Bobba, Data authentication and integrity verification techniques for trusted/untrusted cloud servers, in 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, pp. 2590–2596 2014. https://doi.org/10.1109/ICACCI.2014.6968657

[41] U. Habiba, R. Masood, M. Shibli, M. Niazi, Cloud identity management security issues and solutions: a taxonomy, in Complex Adaptive Systems Modeling, vol. 2, 5 2014. https://doi.org/10.1186/s40294-014-0005-9

[42] Sangavarapu, S. Mishra, A. Williams, G.R. Gangadharan, The Indian banking community cloud, *IT Professional*, vol. 16, 6, pp. 25–32, 2014. https://doi.org/10.1109/MITP.2014.97

[43] F. Zhu, H. Li, J. Lu, A service level agreement framework of cloud computing based on the Cloud Bank model, in 2012 *IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie*, pp. 255–259 2012. https://doi.org/10.1109/CSAE.2012.6272592

[44] J. Jiang, D. Yang, A research on commercial bank information systems based on cloud computing, in 2011 *IEEE 3rd International Conference on Communication Software and Networks, Xi'an*, pp. 363–366 2011. https://doi.org/10.1109/ICCSN.2011.6014585

[45] V. Andrianova and D. Efanov, "Cloud-Based Electronic Signature Authentication Issues", 2019 *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2019. https://doi.org/10.1109/eiconrus.2019.8656803 .

[46] S. Qiu, G. Xu, H. Ahmad, G. Xu, X. Qiu and H. Xu, An Improved Lightweight Two-Factor Authentication and Key Agreement Protocol with Dynamic Identity Based on Elliptic Curve Cryptography, *KSII Transactions on Internet and Information Systems*, vol. 13, no. 2, 2019. https://doi.org/10.3837/tiis.2019.02.027 .

[47] S. Yusuf, M. Boukar, A. Mukhtar and A. Yusuf, "User Define Time Based Change Pattern Dynamic Password Authentication Scheme", 2018 *14th International Conference on Electronics Computer and Computation (ICECCO)*, 2018. https://doi.org/10.1109/icecco.2018.8634675 .

[48] S. Sahoo, S. Mohanty and B. Majhi, "An Improved and Secure Two-factor Dynamic ID Based Authenticated Key Agreement Scheme for Multiserver Environment", *Wireless Personal Communications*, vol. 101, no. 3, pp. 1307-1333, 2018. https://doi.org/10.1007/s11277-018-5764-8 .

[49] X. Li, D. Yang, I. Zeng, B. Chen and Y. Zhang, "Comments on "Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model"", IEEE Transactions on Information Forensics and Security, pp. 1-1, 2018. https://doi.org/10.1109/tifs.2018.2866304 .

[50] C. Chen, Y. Deng, Y. Tang, J. Chen and Y. Lin, An Improvement on Remote User Authentication Schemes Using Smart Cards, *Computers*, vol. 7, no. 1, p. 9, 2018. https://doi.org/10.3390/computers7010009 .

[51] S. Sahoo, S. Mohanty, S. Sunny and B. Majhi, An Improved Remote User Authentication Scheme for Multiserver Environment Using Smart Cards, *Advances in Intelligent Systems and Computing*, pp. 217-224, 2018. https://doi.org/10.1007/978-981-10-8639- 7_22 .

[52] S. Shinand and K. Kobara, Security Analysis of PasswordAuthenticated Key Retrieval, *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 5, pp. 573-576, 2017. https://doi.org/10.1109/tdsc.2015.2490064.

[53] A. Goutham Reddy, E. Yoon and K. Yoo, Comment on Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards, *IET Information Security*, vol. 11, no. 4, pp. 220-221, 2017. https://doi.org/10.1049/ietifs.2016.0218

[54] Z. Gao, S. Huang and W. Ding, "Cryptanalysis of three dynamic ID-based remote user authentication schemes using smart cards", *IEEE International Conference of Online Analysis and Computing Science (ICOACS)*, 2016. https://doi.org/10.1109/icoacs.2016.7563046 .

[55] R. Madhusudhan and M. Hegde, "Cryptanalysis and Improvement of Remote User Authentication Scheme Using Smart Card", 2016 *International Conference on Computer and Communication Engineering (ICCCE)*, 2016. https://doi.org/10.1109/iccce.2016.30 .

[56] X. Li, J. Ma, W. Wang, Y. Xiong and J. Zhang, "A novel smart card and dynamic ID based remote user

authentication scheme for multi-server environments", *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 85-95, 2013. https://doi.org/10.1016/j.mcm.2012.06.033 .

[57] Gaharana, S. and Anand, D. Dynamic Id Based Remote User Authentication in Multi Server Environment Using Smart Cards: A Review. 2015 *International Conference on Computational Intelligence and Communication Networks (CICN)*, 2015. https://doi.org/10.1109/CICN.2015.212 .

[58] Hsiang, H. and Shih, W. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. *Computer Standards & Interfaces*, 31(6), pp.1118- 1123, 2009. https://doi.org/10.1016/j.csi.2008.11.002 .

[59] Biswas, A., Roy, A. Blockchain-Based User Authentication in Cloud Governance Model. In: Raj, J.S., Palanisamy, R., Perikos, I., Shi, Y. (eds) *Intelligent Sustainable Systems. Lecture Notes in Networks and Systems, vol 213. Springer, Singapore*, 2022. https://doi.org/10.1007/978-981-16-2422-3_64

[60] A. Biswas and A. Roy, "Multilevel User Verification in Cloud Banking System", *Proceedings of International Conference on Computational Intelligence Data Science and Cloud Computing*, pp. 527-537, 2021.

[61] Biswas, A., & Roy, A. A study on Dynamic ID based user authentication system using smart card. *Asian Journal For Convergence In Technology (AJCT)* ISSN -2350-1146, 5(2), 2019. https://asianssr.org/index.php/ajct/article/view/871

[62] Biswas, A., Sil, R., Roy, A. (2021). A Study on Application of Interplanetary File System. In: Sharma, H., Gupta, M.K., Tomar, G.S., Lipo, W. (eds) *Communication and Intelligent Systems. Lecture Notes in Networks and Systems, vol 204. Springer, Singapore*, 2021. https://doi.org/10.1007/978-981-16-1089-9_79

[63] Elgamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4), pp.469-472, 1985. DOI: https://doi.org/10.1109/TIT.1985.1057074 .

[64] F. Wen and X. Li, An improved dynamic ID-based remote user authentication with key agreement scheme, *Computers & Electrical Engineering*, vol. 38, no. 2, pp. 381-387, 2012. https://doi.org/10.1016/j.compeleceng.2011.11.010

Author Biographies

First Author Ankur Biswas, He is currently pursuing his Ph.D. degree from Dept. of CSE, Adamas University, Kolkata, India. He is Founder and Director of SASLAB Technologies Pvt Ltd, Kolkata, India. He is also member of IEEE, life Member of Cryptology Research Society of India. His research interests include: Cryptography, Cyber Security, Blockchain and E-Governance.

Second Author Abhishek Roy has completed his in Ph.D. (Computer Science), M.Sc. (Computer Technology) and B.Sc. Information Technology Honors from The University of Burdwan, West Bengal, India. His research area includes Artificial Intelligence, Machine Learning and Data Analytics. He is serving as resource person to various international and national research societies, conferences and journals. Currently he is serving in the capacity of Associate Professor and Ph.D. Supervisor (Technology) at Department of Computer Science and Engineering under School of Engineering and Technology at Adamas University, Kolkata 700126, India.

Third Author Debashis Nandy has completed his MCA from the Dept. of CS, Brainware University, Kolkata, India. He is currently working as Software Engineer in SASLAB Technologies Pvt Ltd, Kolkata, India.