ISSN NO : 1006-8341

Trusted Framework for Online Banking in the Public Cloud using Multi-Factor Authentication using Blockchain Technology

Rohit Shendge[1], Indrajit Datar[2], Adwait Shinde[3], Anurag Gulavane[4], Prof. Reshma Kanse[5]

[1,2,3,4] B Tech Students and [5]Asst. Prof of Department of Computer Science and Business Systems,

Bharti Vidyapeeth Deemed University, Department of Engineering and Technology

Navi Mumbai, Maharashtra, India

Abstract: *Blockchain is a distributed database or a decentralized ledger that is most commonly used to exchange digital currency and perform transactions securely. Every participant of the network has access to the ledger which will be updated by every new transaction. The Blockchain ledger is a collection of all transactions executed in the past. The Blockchain ledger is a continuously growing tamper-proof data structure containing blocks that hold batches of individual transactions. The completed blocks are added in chronological order. Blockchain via Bitcoin has had a massive impact on the world in the past decade and it's safe to say that this will continue, especially with many people working tirelessly to remove the various limitations that are prohibiting blockchains from becoming mainstream. One such limitation is the high processing and electrical costs that come from the Proof-of-Work consensus protocol. With ever-evolving technologies, the banking systems can update from their traditional methodologies to a digital, immutable, distributed ledger that can be implemented via Blockchain. Blockchain Technology is a distributed peer-to-peer linked structure that can solve the problem of maintaining and recording transactions in a banking system. Blockchain provides properties like transparency, robustness, suitability and security. This paper aims at giving these functionalities in a distributed banking system using blockchain, which will be at par with the current methodologies. It will also focus on the limitations while implementing blockchain and future scope. In the Proposed work, we propose an alternative proof-by-approval protocol which is a more advanced form of the proof-of-reputation protocol, that offers better security and is a more decentralized approach than the former at the cost of being less performant and harder to setup.*

Index Terms*: *Block chain, Proof-by-Approval, Secure transaction, Blockchain, Bitcoin, Cryptography, Ledger, Distributed Network, Consensus, Smart Contracts, etc.

I. INTRODUCTION

Physical banking haven't solely modified the banking Perspective of the planet, however a general perspective as well. In Private Blockchain network the participants are known and trusted and there is a level of confidentiality. For example, in a conglomerate, many of the mechanisms aren't needed or they are replaced with legal binding contracts making everyone whoever has signed the contract to abide to these rules. It rapidly changes the technical decisions used to build the solution. Blockchain unlike traditional systems is dynamic enough to become a leader in implementation in a mercurial market scenario. In a blockchain the supreme advantage it ensures is that each party has a record which is maintained in a ledger available to each one. It is a ledger widely passed between different users thereby creating a shared database which is replicated to these users and who can access it only after they have the access right for it. Consensus, provenance, immutability, finality are the various aspects into which it works, making sure that all these facets work together into a reasonable amalgamation.

II. NEED OF BLOCKCHAIN FOR BANKING SECURITY

The major question that arises is to why use blockchain when already the market has flourishing plethora of other databases. What substantial importance it holds against the competing products. For this let's understand the problem with the existing systems.

They could be summed up as follows:

- Difficult to monitor and evaluate asset ownership and its transfer in a trusted business network.
- Inefficient, expensive, vulnerable: All these factors extremely hinder the performance and there by destroying the progress.

The below issues basically we facing in banking data security and transaction approach which defined here

- To migrate the centralization of banking transaction into the decentralized approach.
- To create a single platform where user can access all bank accounts using transactional authentication.
- To eliminate all physical things dependency which is must require for banking transaction.
- To implement such approach on global environment using secure time less time consuming manner.
- We notice that the decentralized architecture provides the automatic data recovery from different attacks.

III. PROBLEM DEFINITION

- To design and develop an approach for secure multi banking transaction system using transactional security and blockchain.
- To develop an algorithm for runtime thumb recognition using image processing.
- To design and develop an own blockchain to store all transaction records in secure manner.
- Deploy a dynamic smart contract with consensus algorithm to enhance the transaction clarity to end user.

IV. PROPOSEDSYSTEM

The Anatomy of the Blockchain architecture:

The blockchain architecture consists of a few fundamental concepts like decentralization, digital signature, mining and data integrity.

- **Decentralization:** Rather than one central authority overpowering others in the ecosystem, blockchain explicitly distributes control amongst all peers in the transaction chain.
- **Digital signature:** Blockchain enables an exchange of transactional value using public keys by the mechanism of a unique digital sign i.e. code for decryption known to everyone on the network and private keys known only to the owner to create ownership.
- **Mining:** In a distributed system every user mines and digs deep into the data which is then evaluated according to the cryptographic rules and it also acknowledges miners for confirmation and verification of the transactions.

- **Data integrity:** Complex algorithms and agreement among users ensures that transaction data, once agreed upon, cannot be tampered with and thus remains unaffected. Data stored on blockchain acts as a single version of truth for all parties involved hence reducing the risk of fraud.

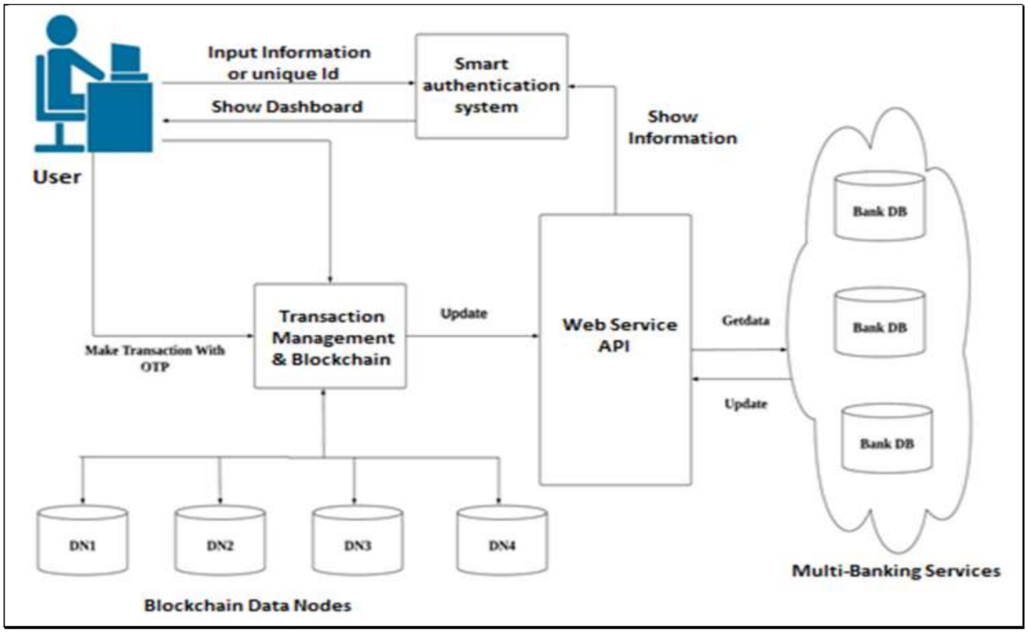

Fig. 1: Proposed System Architecture

1. Data Set

The gas pipeline dataset is taken on real time environment with around 2 years duration. The data set contains some values which is continuously monitor to the pipeline thickness according to specific time interval. In a single day for reading has been taken in 6 hours interval which basically measures thickness, internal temperature, external temperature, pressure etc. Basically this parameters can we show thickness reduction into the specific reading. Basically the data set has converted training and testing according to standard as a 70%-30% respectively. The overall system works like reinforcement learning which continuously train according to current generated data and predict the result for future scenario.

2. Data Exploration

Data exploration is the first step in data analysis and typically involves summarizing the main characteristics of a dataset. It is commonly conducted using visual analytics tools, but can also be done in more advanced statistical software, such as java. In data exploration includes various steps such as Variable Identification; Univar ate Analysis, Bi-variety Analysis, Missing values treatment Outlier treatment

3. Data Pre-processing

Data preprocessing is a data mining technique that involves transforming raw data into an understandable format. Real-world knowledge is usually incomplete, inconsistent, and/or lacking in bound behaviors or trends, and is probably going to contain several errors. Knowledge preprocessing could be a proved technique of resolution such problems.

In real world information are usually incomplete: lacking attribute values, lacking bound attributes of interest, or containing only mixture information. Noisy: containing errors or outliers. Inconsistent:

containing discrepancies in codes or names. In Data Preprocessing includes various steps such as Import the libraries, Import the data-set, Check out the missing values, See the Categorical Values, Splitting the data-set into Training and Test Set, Feature Scaling.

V. IMPLEMENTATION

This paper seeks to present an application similar to the banking app (a Bank-Bank payments application by banking system) but one which uses Blockchain. The main objective of the paper is to create an application where one could use a decentralized network to make transactions between centralized systems. So, the intention isn't to start the next race towards decentralization but rather to build a practical blockchain application that could be implemented in the present time.

In the application, two characters are considered, a user (the one who would use the app to make payments or transfer money to other people directly via their bank accounts) and a bank (who would approve of such transactions). The working of the app would go as:

Whenever a user wants to make a transaction, he/she would create a block with details of the transaction as described in the working of the protocol above, (Only the user's username would be visible to everyone who has a copy of the blockchain. The user would have his/her personal details separately shared to his/her bank via KYC for example verification done by bank) and send it to the bank where his/her account is present (or optionally it could also be setup in such a way that banks communicate limited information to each other via encryption for security in order to make it possible for transactions to be made via any approver).

The bank would receive details of the transaction from the block. The bank then after validating, approves of the transaction (but doesn't go through with it yet) if it is not fraudulent and sends the block back to the user. The user would then validate the block and add it to the blockchain where the block's data essentially acts like a receipt on a permanent unhackable ledger compelling the concerned banks to process and complete the transaction.

In a Proof-of-Reputation consensus protocol (PoR) version of the same, the banks would also put the block into the blockchain which for this context would probably work just as fine but our intention was to try and give users a bit more control over their transactions and this would also force banks to be a bit more careful with the transactions they will be handling.

VI. RESULT

Thus, this system would be able to implement a distributed system as well as the banking nodes could be semi-automatized so as to reduce work. We can further have additional banking facilities integrated in the system. And as the finances are involved not all the power is given to the user node i.e. the customers.

A Cryptographically linked Immutable Ledger (Similar to the one used by Bitcoin, see Literature Review section for details)

- A Peer-to-Peer Network (Again similar to the one used by Bitcoin which uses DNS Seeding) There are two types of user entities in this protocol:

- Users: Read and Write-after-approval to the Blockchain
- Approvers (Bank): Reads and Approves writes to the blockchain. But cannot directly write to the Blockchain.

Attribute	**Public**	**Private**	**Consortium**
Nature	De- centralized	Centralized	Semi-centralized
Homogeneity	Anonymous user.	Identified users Verified	Verified users
Administration	All nodes can mine	Centralized nodes can mine	Permissioned nodes can mine
Consensus Mechanism	All miners	Organization owners	Only Authorized nodes
Consensus Cost	Expensive	Inexpensive	Inexpensive
Time for verification	Few minutes	Few milliseconds	Few milliseconds
Protocol Efficiency	Low	High	High
Intrusion	Impossible	Possible	Possible

Table.1: Contrast of Different Types of Blockchain

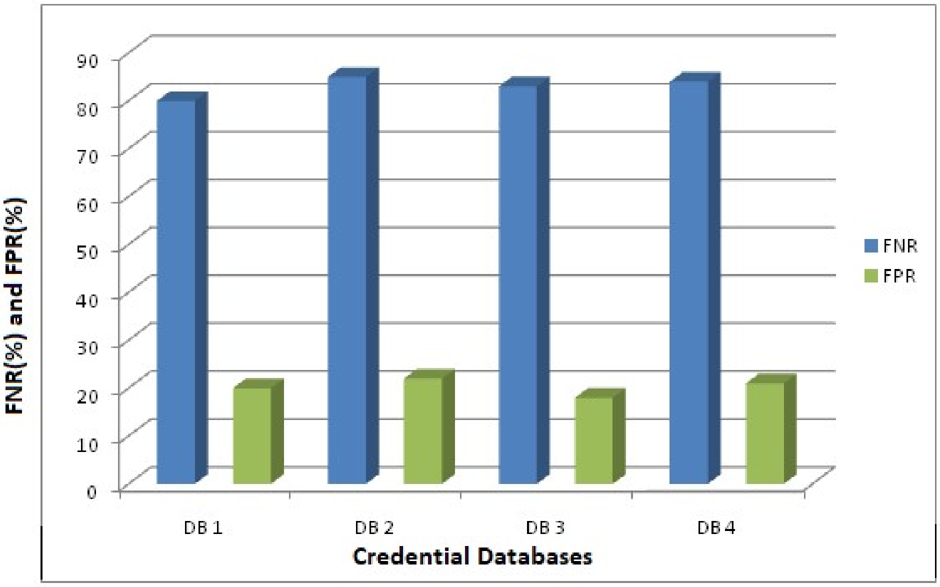

Fig.2: Performance of our proposed multi-factor Authentication

We set a time window bound in minutes for validating user login and authentication credentials in terms of False Negative Rate (FNR) and False Positive Rate (FPR). FNR means the rate of input credentials matched correctly and calculated as tp/(tp + fn), where fn is false negative and tp is true positive. FPR means the rate of input credentials matched incorrectly and computed as tn/(tn + fp), where tn is considered as true negative and fp taken as false positive.

VII. CONCLUSION AND FUTURE WORK

This paper suggests a secure and efficient way to store data on the cloud. Blockchain-based cloud storage with data encryption gives data security in a decentralized structure. The proposed framework for security model is suitable for measures initially used in banking transactions included blockchain technology. The algorithms used to implement the system model are efficient and required less time and give high security for the data which is being stored on the cloud. This kind of architecture makes the system more robust and resistant to different security attacks which are performed by unauthorized users who try to steal and disclose the information in the data files of the user for their benefit. Finally, we conclude that the security level of banking transactions has considerably increased, thus making the overall process of banking much more convenient.

ACKNOWLEDGMENT

We would prefer to give thanks the researchers likewise publishers for creating their resources available. We are conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

[1] Sabout Nagaraju and LathaParthiban, “Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway,” Open Access Journal of Cloud Computing: Advances, Systems and Applications (2015)

[2] Dorri, S. S. Kanhere and R. Jurdak, “Blockchain in internet of things: Challenges and Solutions,” arXiv: 1608.05187 [cs], 2019.

[3] Sukhodolskiy, Ilya, and Sergey Zapechnikov. “A blockchain-based access control system for cloud storage.” Young Researchers in Electrical and Electronic Engineering (EICon- Rus), 2018 IEEE Conference of Russian IEEE, 2018.

[4] Yang, Huihui, and Bian Yang. “A Blockchain-based Approach to the Secure Sharing of Healthcare Data.” Proceedings of the Norwegian Information Security Conference. 2020.

[5] Goyal, Vipul, et al. “Attribute-based encryption for fine-grained access control of encrypted data.” Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006.

[6] Wang, Hao, and Yujiao Song. “Secure cloud-based EHR system using attribute-based crypto-system and blockchain.” Journal of medical systems 42.8 (2018): 152.

[7] Michalevsky Y, Joye M. “Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy”.

[8] Wu, Axin, et al. “Hidden policy attribute- based data sharing with direct revocation and keyword search in cloud computing.” Sensors 18.7 (2018): 2158.

[9] Khan S, Khan R. “Multiple authorities’ attribute-based verification mechanism for Blockchain micro-grid transactions”. Energies. 2018 May; 11(5):1154.

[10] Guo, Rui, et al. “Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems.” IEEE Access 776.99 (2018): 1-12.

[11] Monika D. Rokade, Dr. Yogesh Kumar Sharma, “Deep and Machine Learning Approach’s for Anomaly based Intrusion Detection of Imbalanced Network Traffic.” IOSR journal of Engineering (IOSR JEN), _ISSN (e): 2250-3021, ISSN(p): 2278-8719

[12] Monika D. Rokade, Dr. Yogesh Kumar Sharma, “MLIDS: A Machine Learning Approach for Intrusion Detection for real time Network Dataset.” 2021 International Conference on Engineering Smart Computing and Informatics (ESCI), IEEE.

[13] Monika D. Rokade, Dr. Yogesh Kumar Sharma. (2020) “Identification of Malicious Activity for Network Packet using Deep Learning.” International Journal of Advance Science and Technology, 29(9s), 2324-2331.

[14] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin.org, 2008.

[15] D. J. Hwang and K. Lee, “Analysis of security threats and solutions in payment systems,” Information Security Journal: A Global Perspective, vol. 25, no. 2, pp. 50–58, 2016.

[16] T. Dierks and C. Allen, “The TLS Protocol Version 1.3,” Internet Engineering Task Force, 2018.

[17] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin.org, 2008.

[18] P. Koshy, D. Koshy, and P. McDaniel, “An Analysis of Anonymity in Bitcoin Using P2P Network Traffic,” in Financial Cryptography and Data Security, 2014, pp. 469–485.

[19] T. Elgamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.

[20] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[21] A. Shamir, “How to Share a Secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

[22] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[23] B. A. Forouzan, Cryptography and Network Security: Principles and Practice, McGraw-Hill Education, 2015.

[24] B. C. Neuman and T. Ts'o, “Kerberos: An Authentication Service for Computer Networks,” IEEE Communications Magazine, vol. 32, no. 9, pp. 33–38, 1994.

[25] J. Salowey et al., “The Secure Sockets Layer (SSL) Protocol Version 3.0,” Internet Engineering Task Force, 1996.

[26] M. C. Rosu, M. Danubianu, and M. V. Rosu, “Blockchain Solutions for the Digital Banking Revolution,” Procedia Economics and Finance, vol. 23, pp. 200–204, 2015.

[27] P. Koshy, D. Koshy, and P. McDaniel, “An Analysis of Anonymity in Bitcoin Using P2P Network Traffic,” in Financial Cryptography and Data Security, 2014, pp. 469–485.

[28] V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum.org, 2014.

[29] D. J. Hwang and K. Lee, “Analysis of security threats and solutions in payment systems,” Information Security Journal: A Global Perspective, vol. 25, no. 2, pp. 50–58, 2016.

[30] C. N. Chuang, Y. C. Liao, and Y. C. Chen, “A Privacy-Preserving Cloud-Based Electronic Health Record System Based on Blockchain Technology,” Journal of Medical Systems, vol. 42, no. 8, p. 139, 2018.