

Trusted Framework for Online Banking in Public Cloud Using Multi-Factor Authentication Using Block-Chain Framework

Nikita Dhakad¹, Himanshu Jagtap², Vedant Bhosale³, Prof. Prakash Kshirsagar⁴

¹Student, Bachelors in Engineering, Department of Computer Engineering, Nutan Maharashtra Institute of Engineering and Technology Talegaon, Maharashtra, India.

²Student, Bachelors in Engineering, Department of Computer Engineering, Nutan Maharashtra Institute of Engineering and Technology Talegaon, Maharashtra, India.

³Student, Bachelors in Engineering, Department of Computer Engineering, Nutan Maharashtra Institute of

Engineering and Technology Talegaon, Maharashtra, India.

⁴Professor, Department of Computer Engineering, Nutan Maharashtra Institute of Engineering and Technology Talegaon, Maharashtra, India.

Abstract - There are always potential hazards from hackers, adware, malware, and viruses. Many big international corporations have experienced hacking and security breaches in the previous few years. In certain instances, this has resulted in the leakage of private and confidential information, such as bank account information, addresses, and transactions, but there are security measures in place that can block these things before they get too close to the company's private data. This is crucial for both secrecy and to avoid paying the steep fines levied on businesses that fail to adequately safeguard customer information. The project is a verification mechanism that only allows users with the proper input credentials to access the system. The project involves modules or user certificates. Security credentials come in a variety of forms. Thus, we incorporate a unique blockchain for banking security and user authentication in this proposed methodology. This degree of authentication reduces the possibility of hacking and the loss of sensitive data. Also, in the current environment, safer bank transactions are necessary due to advancements in security technologies. They have also made advances into industries, healthcare, telecommunications, and home automation, among others. A distributed ledger is basically what a blockchain is. It can keep information about who owns a certain piece of property or, for example, a bond. A permanent record of ownership can be maintained using technology, which also makes it possible for parties with a low level of trust to exchange the asset.

Key Words: Custom Blockchain, Distributed Ledger, Authentications, Confidentiality, Transactions, Security System, Credentials, Banking Security, etc.

1. INTRODUCTION

A blockchain system can be compared to an unbreakable encrypted database that will be used to store private user information. Everybody who is utilizing the software has access to the computer network that runs the system. Blockchain works as a pseudo-anonymous system, but despite the fact that it is tamper-proof in terms of data integrity, all transactions are accessible to everyone, and it still has privacy problems. To manage diverse users' confidential records across a few MNC establishments and devices, the access control had to be properly designed. Blockchain was not designed to be a solution for storing enormous volumes of data. In terms of the basis for secure banking, a decentralized storage solution would significantly strengthen the blockchain's weak spot. As a decentralized system, the blockchain network is more resistant to attack or failure than centralized systems because there isn't a single point of failure or attack. Yet, because all bitcoin transactions are public and open to everyone, there is currently analytics software that can identify community members based solely on transaction records [2]. The two types of records that make up the blockchain implementation's most crucial module are blocks and transactions. The secure hash technique provides a connection to a previous block for each block that includes a timestamp. Several algorithms, including SHA for hash creation, mining for producing a valid hash, smart contracts for system policy, and consensus for confirming the current blockchain across all Peer to Peer nodes, are executed while the transaction information is being stored in the blockchain system. As a result, banking applications are safer. Data accessibility and storage come in second. Use both content-based cryptography methods and the Secret Shamir hashing technique for this point.

2. LITERATURE REVIEW

Smart Contracts [1] also called crypto-contract, it is a computer program used for trans-ferring / controlling the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy / agreement. These smart contracts are stored on block-chain and BC is an ideal technology to store these contracts due to the ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred / returned or since the transaction actually happened.



Currently CSIRRO team has proposed a new approach to integrate Block on IOT with [2]. In its initial endeavor, he uses smart-home technology to understand how IOT can beblocked. Block wheels are especially used to provide access control system for Smart- Devices Transactions located on Smart-Home. Introducing BC technology in IOT, this search again provides some additional security features; however, every mainstream BCtechnology must have a concept that does not include the concept of comprehensive algorithms. Moreover, this technology cannot provide a general form of block-chain solutionin case of IOT usage.

According to Ilya Sukhodolski. The Al [3] system presents a prototype of multi-user sys-tem for access control over datasets stored in incredible cloud environments. Like other unreliable environments, cloud storage requires the ability to share information securely.Our approach provides access control over data stored in the cloud without the provider's investment. Access Control Mechanism The main tool is the dynamic feature-based encryption scheme, which has dynamic features. Using Blockchain based decentralized badgers; our systems provide an irrevocable log for accessibility requests for all meaningful security incidents like large financing, access policy assignment, alteration or cancellation. We offer a set of cryptographic protocols that make the secret or secret key of cryptographic operation confidential. The hash code of the sifter text is only transmittedby the block on laser. Our system has been tested on prototype smart contracts and tested on Iterium Blockchain platforms.

According to Sarmadullah Khanet. Al [9] embedded power transactions in blockchain are based on their defined characteristics through the signature of many manufacturers. These signatures have been verified and customers are satisfied with the features that do not open any information that meet those features. The public and private key manufacturershave been created for these customers and using this key ensures that the support process is authorized by customers. There is no central authority required in this perspective. To protest against collision attacks, the makers are given secret pseudo-functional workseeds. Comparative analysis shows the efficiency of the proposed approach to existing people.

3. METHODOLOGY

Today, security is a top priority. Data processing is carried out online and stored on a dependable server in 99% of cases. Yet when the user puts their data on the permitted server and has to send and receive data over a secure communication channel, security issues appear. The most data is currently processed by the following sectors or applications: healthcare, e-commerce, internet baking, education, and business applications. Because all of these services are used online, there are several potential for various attacks against them. To overcome these difficulties, we created a trusted framework for online banking on the public cloud using multi-factor authentication and blockchain framework services as security against various attacks. As demonstrated in this article, all of the solutions depend on creating a unique (custom) blockchain to store all transaction records insecurely. Only a software-based system

Step 3 : CurrentHash= SHA256(d)

Algorithm 2: Hash Generation:

Input: Genesis block, Previous hash, data d,

Output: Generated hash H according to givendata

Step 4 : Retrun CurrentHash

Step 1 : Input data as d

Algorithm 3: Mining Algorithm for valid hash creation:

Input: Hash Validation Policy P[], Current Hash Values hash Val



Fig-1: System Architecture

4. ALGORITHM

Algorithm 1: Protocol for Peer Verification

Input: User get IP address, User Transaction TID,

Output: Enable IP address or current queryif any connection is valid

Step 1 : User generate the any transaction DDL, DML or DCL query

Step 2 : Get current IP address For each (read IP into IP address) If (connection(IP) equals(true)) Flag true Else Flag false End for Step 4 : if (Flag == true) Peer to Peer Verification valid Else Peer to Peer Verification Invalid End if End for



ISSN: 2582-3930

Output: Valid hash Step 1: System generate the hash Val for ith transaction using Algorithm 1 Step 2 : if (hash Val.valid with P[]) Valid hash Flag =1 Else Flag=0 Mine again randomly Step 3: Return valid hash when flag=1

5. RESULTS AND DISCUSSIONS

This technology would be able to construct a distributed system and semi-automate the banking nodes to decrease workload. Additionally, we can integrate more banking services into the system. Additionally, not all of the authority is provided to the user node, or the customers, because finance is involved.

A cryptographically connected, immutable ledger and a peerto-peer network that employs DNS seeding, much like the one employed by Bitcoin. In this protocol, there are two categories of user entities:

Users: Read and Write to the Blockchain after Approval Authorizers (Bank): Reads and approves blockchain writing. but is unable to write directly to the Blockchain. Some of the screenshots are as follows:

The database design of project:

ping funnin	Carl and a second contraction of the second s									
A 2 8 0 4	E BAANDA SK SHACK	·	states a	meant as export	in mport 2º operations it	instand in the	Ibora			
	✓ Showing cost 0 - 5 (-6 t	nd 😖 , Query took S	Cost 1708							
(entrates)										
ne_bara_apporation V	SELECT'									
cc_ditaits	LIMIT 0 .00									
ang_counts							C. Problem Instead 1 (1) (1) (1)	star for H	Create Part of	and 11
pcodethie										
iaccountbank										
insurance	Show : That one 0	Number of row	s 31.	Heathers meny 100	1295					
Insurance in the	South a local Manage	101								
nafaretpcede	section in the section of the sectio									
	+ Options		Constant of the local division of the local					-	the second	-
Ovian's	and the second sec	the second second							the second	
indunts Br_dechalts	*-T-*	w at uname	passene.							
, delark ar, delark Rhdrawolpcode	• T •	+ d unates	Pp@123	Your First School Name	PC	pute	strilligmeil com	888668866	5 0	Active
_detain ar_distats thdrawotycode mate table	+. T + □ J Ent H Cary © De □ J Ent H Cary © De	 d uneme bele 1 pc1 bele 2 allocit 	Pp@123 An@123	Your First School Name Your First School Name	r r	pune june	str@gmail.com alice@gmail.com	0400-04000	1	Active Active)
i ostars ner dedats ethdrawotpcode Xeate lable	Tre JEan Ja Casy @ De	d united total t	Pp@123 Ap@123 1122	Your First School Name Your First School Name Favorite Color Name?	K E Bue	pane june Pane	sp@gmail.com abco@gmail.com re@gmail.com	8886688899 8886688999 9876543270	6 8 6 8 6 9	Астия Астия Астия
Losters or Schalts Bharawolpcole mate lable	Tre for process of	d uname durame det 1 pc1 det 2 dect durame duram	Po@123 Aa@123 1122 M@1120	Your First School Name Your First School Name Faverile Color Name? Your Car Netsber?	IK JK Bive MHDAT234	pune june Pune Pane	pp@gmail.com alcoldgmail.com na@gmail.com hutsync.sulabors@gmail.com	8805083800 8805083800 9876543270 7666282455		Астия Астия Астия Астия
Louist or fistan Midravopcolo mate table		di unaces deter 1 pc1 deter 2 albot deter 4 Raj deter 7 Major deter 8 Nikto Dhatac	Po@123 Aa@123 1122 M@1122 M@1122 Nk@16	Your First School Name Your First School Name Faverile Color Name? Your Car Namber? Your First School Name?	pt pt Blue MHYDAT234 CMS English Modum High School	pune pune Pune Pune chinai pradhiwaan	pp@gmail.com alcol@gmail.com na@gmail.com hartype: salabora@gmail.com nacdhakart?s@gmail.com	8800088000 880008800 9870543230 7666282450 986729340	6 0 6 0 0 0 0 7 7 6	Астия Астия Астия Астия Астия
Loues ar dealt drawopcole ceals table	For provide the former of	d uname d uname pc1 pc1 una pc1 pc1 una pc1	Po@123 Aa@123 1122 M@1122 M@1122 Nek@16 H@1122	Your First School Name Your First School Name Favorite Color Name? Your Câr Namber? Your First School Name? Favorite Color Name?	PC gic Brue Merc2A1234 CMS English Modum High School Red	pune pune Pune Pane chistel predhikaran chistel predhikaran	pp@gmail.com abcdggmail.com ne@gmail.com nutrync:subdoss@gmail.com nikodhailart?3@gmail.com himambu@gmail.com	840008000 94008090 9470543270 7446202435 9467203437 9465527004		Астия Астия Астия Астия Астия Астия
, oxanı nızdedin dirdiniyotycolo Zwala table	The Corry Office Fort Jac Corry Office Corrock All Uncertails	de unaces inte 1 pc1 inte 2 alcol inte 4 llag inte 7 Mayor inte 8 Ninte Chalae inte 8 Ninte Chalae inte 8 Firmanute inte 8 Minte poinchet	Pp@123 Aa@123 1122 M@1122 M@1122 Nkg16 H@1122 Charge	Tour First School Name Your First School Name Fairmit Color Name? Your Car Nember? Your Car Nember? Your First School Name? Fairmit Color Name?	pc BC Dive MHIDAT234 CMS English Medium High School Bail	pune june Para Para chinat pratikaran chinat pratikaran	pp@gmail.com allco@gmail.com ne@gmail.com httpps://subbone@gmail.com ninamhs@gmail.com	8485084950 948564595 9476545295 9455729540 9465522500	8 9 8 8 9 9 9 9 9 9 9 9 1 8 8 8	Астич Астич Астич Астич Астич Астич
onan ur.don drawopcode zwale table	The Server of the Construction of the Con	de Lunames lette 1 pc1 latte 2 alloch lette 4 Ray latte 2 Marpor latte 9 Nikta Dhasas Nikta Dhasas Mitta Statue Nikta Dhasas Nikta Statue Nikta Statue	Pp@123 Aa@123 1122 M@1122 Ne@1122 Ne@1122 Change 0 30	Tau Fini School Name Your Fini School Name Faurtie Color Name? Your Fini School Name? Taurtie Colo Name? Delete Depot Headers serve 100	PC p1 Bise MetOACOH CoACOH Bad Inne	pane (une Pane Pane chânal prachéanas chânal prachéanas	pp@gmail.com allcd@gmail.com w@gmail.com autyper: usadors.@gmail.com desttalaat?2@gmail.com bimanthu@gmail.com	64255626000 0426542245 246522656 045720340 0685562100	8 0 6 0 0 0 2 1 7 6 5 0	Астия Астия Астия Астия Астия Астия
outen estatati thdrawopcolo mate table	Tore Tore Tore Tore	de unareas lette 1 pc1 lette 2 décé lette 4 Ray lette 2 Mayor lette 3 Nakte Ohiere lette 9 Nakte Ohiere Na Billin seinchel Namber of rom	Pp@123 Aa@123 1122 M@1122 M@1122 Nok@36 H@1123 Charge 1 3	Tau Fini School Name Your Fini School Name Faurtie Color Name? Your Fini School Name? Taurtie Color Name? Delete	pc pc Store MetroCAT204 CASE English Medium High School Dadi	pone pune Pune Pane chihai pradhikanan chihai pradhikanan	ph@gmail.com atlcd@gmail.com red.gmail.com turtyre:saladors@gmail.com headmaarth@gmail.com	640008000 94008000 9475543270 7466283456 9457293457 9465521007	5 0 6 0 0 0 7 5 5 8	Астин Астин Астин Астин Астин Астин
johan Markan Indrawotocode wate table	T + T + T + T + T + T + T + T + T + T + T + T + T + T + T + T + T + T + T +	d uname d uname fert fort une fort une fort une fort une fort fort	Pp@123 Aa@123 1127 M@1122 Neg1122 Neg1122 Charge 2 1 21	Sur Fini School Name Your Fini School Nami Faceria Color Name? Your Fini School Name? Faceria Color Name? Delete Prot Handles serve 100	ec pi Dee sectoAr224 CMIS English Medium High Echool Red	pure pure Pure Pare chinai problema chinai problema	atodymeticen atodymeticen exglyneticen okotrustert (gynaticen nenensegynaticen	040008000 040068000 047654220 746028240 0465720540 0465522500	5 0 6 0 0 0 7 5 5 8	Астин Астин Астин Астин Астин Астин
onani <u>u Stani</u> Indrawopcodo wala tuble	Tri Tell Ji Cary D D Tell Ji Cary D	de unaces entre 1 port entre 2 doct	Pp@123 Aa@123 1123 M@1122 Na@16 H@1122 Charge 6 s 21	Tour First School Name Haar First School Name Favertie Color Name? Nam Cale Nontbar? Tour First School Name? Date: Date Papet Headlers server 100	IC III III III III III III III III III	pure pure Pure Pure chinai padhisan chinai padhisan	pp@gmel.com atcdgumet.com ex@gmel.com totyper.suidoos@gmel.com himandw.@gmeit.com	610008000 818008000 04795432% 7490282450 946522450 946522450 946522450	6 0 0 0 2 1 7 8 6 8	Астия Астия Астия Астия Астия

Code Implementation:



Sign In Page:

(8) Bitbank		Home Bigs in Bigs Lip (Jow)	Star Gr
	Sign In to B	itBank	
	- Select Roll -		
	Erral		
	Paseword		
	SIGN IN		
	New in this site ? Create New Account For	rget Password	

Fig-4: Sign In Page

Sign in OTP Authentication Page:

(B)Bitbank	Create Account	Deposite Do V	Vithdraw Get Balan	ce Transfer Amount	View Report Add Insu	nance LogOut	
		Si	gn In to Bi	tBank	_		
		Customer Login					
		0	Start				
		1	2	3			
		4	5	6			
		7	8	9			
			Submit				

Fig-5: OTP Authentication Page

6. CONCLUSIONS

A safe and effective method of cloud data storage is suggested or summarized by the proposed system. A decentralized structure that uses blockchain-based cloud storage and data encryption provides data security. The proposed framework for the security model is appropriate for security measures that initially used blockchain technology in financial transactions. The techniques utilized to create the system model are efficient and required little time and give great security for the data which is being saved on the cloud. This type of architecture increases the system's robustness and resistance to various security assaults carried out by unauthorized users who attempt to steal and divulge the information contained in the user's data files for their own gain. Finally, we draw the conclusion that banking transactions are now a lot more secure, making the entire banking procedure much more convenient.

ACKNOWLEDGEMENT

We would also like to show our gratitude to, Prof. Prakash Kshirsagar (professor, department of computer engineering, Nutan Maharashtra Institute of Engineering and Technology, Talegaon, Maharashtra, India) for sharing their pearls of wisdom with us during the course of this research. We are also immensely grateful to him for his comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons



REFERENCES

- 1. SaboutNagaraju 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, Systemsand Applications (2015)
- Dorri, S. S. Kanhere and R. Jurdak, "Blockchainin internet of things: Challenges and Solutions," arXiv: 1608.05187 [cs], 2019.
- 3. Sukhodolskiy,Ilya, and Sergey Zapechnikov. "A blockchain-based access control systemfor 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.
- Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of en- crypted data." Proceedings of the 13th ACM conference on Computer and communica- tions security. Acm, 2006.
- 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 withReceiver Privacy".
- 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 forBlockchain micro-grid transactions". Energies. 2018 May;11(5):1154.
- 10. Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities forBlockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.