A Decentralized Data Privacy for Mobile Payment using Blockchain Technology

Beena G Pillai, Madhurya J A

***Abstract:** Mobile payments today have become the most preferred method of transaction for an increasing number of customers. To provide robust security mechanism for mobile payment in public network is challenging task for device manufacturing companies and network service companies. Most of the mobile payment apps make payment easy and fast, but users have to face new security challenges. Because users have to do payment transaction in an open network this makes users sensitive data put at risk, where advisories launch attack and theft of user's identity information. Resent payment apps like Google-pay and phone-pay successfully address the security issues, but these apps might suffer from internal attacks, because data is centralized where apps should accept permission from bank server to do the transaction. In the proposed system we introduce a protected transaction pattern using blockchain technology which overcomes the limitation from the existing system. Our money transformed in the form of cryptocurrencies and it stored in the separate wallet. The particular wallet is installed in the mobile devices. Payment or transaction through two consumers lacking any prior permission. The proposed System uses decentralized data server to preserve data privacy from adversaries. While transaction we directly transfer through the blockchain wallet without any interference from the Bank. The proposed system proven to be secure and efficient for online payment transaction. It secured from cyber attackers or intruders hence data can be stored in separate blocks and its difficult to find out exact data. This overcomes the negative aspect of usual mobile payments.*

***Keywords:** Blockchain, cryptocurrency, decentralized server, online payment, security.*

I. INTRODUCTION

Mobile Application plays an important role in user's life, where thousands of mobile applications come to market every day which makes users work smooth and fast. Recent mobile payment apps make payment transaction simple and fast for users, but app users and app service suppliers have to face new date privacy challenges. Because of large number of app services and online communications applications comprising app users' confidential data put at risk of individuality stealing and mis-uses of personal data. Almost all online transaction are made using application like 'PayPal' and other mobile payment apps, which force users wait to complete the verification process from centralized server. Also online payment apps like PayPal make charger to customers for online transaction. These apps increase the risk each time app users route confidential data by payment application in open network with no privacy guard systems. The traditional payment transaction schemes, such as Google-Pay and Phone-Pay have protected sensitive data from adversaries to launch attacks. Modern data protection schemes are not efficient enough for preserving data privacy and uprightness during the accomplishment of online payment process.

Current mobile payment apps give customers fast, free checkouts and multiple layers of security mechanism which makes customers feel free transaction. These payment apps don't send vendor's and user's original card number where users doing online transaction, apps enable a method called tokenization, where generated token is represented as user's actual credit card and debit-card number. To accomplish user's transaction app should work with mobile manufacturers, payment network and bank authorities, these organizations together work to generate token and verify token while transaction and provide security for each token generated at the time of transaction.

Mobile payment apps request a token to identify the card for transaction, after token is distributed now the user's card is tokenized, where card now has distinctive number which encrypts by mobile app and it is ready to use for payments. To do payment mobile apps verifies tokenized number and a cryptogram (one-time-password), if given input is valid then only payment network validates actual card number. This paper addresses the privacy issues customer face when customer uses online payment services apps. These applications collect sensitive individual data of which the customer has no idea or to control. In our research, we accept that the available services are honest-but-curious. Where these apps collect sensitive data can be shared with intermediary app package contributors, and online transaction is controlled by many service providers like network service provider, bank service provider, third party app service provider, this might cause internal attack where these services providers can compromise to launch attack and mover over users depends on network to do the transaction. Mobile payment using Blockchain. Blockchain is a circulated catalogue structure so as to files the number of transactions taking place in real time and also maintains in highly reputed database.

Manuscript received on March 15, 2020.
Revised Manuscript received on March 24, 2020.
Manuscript published on March 30, 2020.
***** Correspondence Author

Beena G Pillai*, Dept. of CSE, Gitam University, Bangalore, India. Email: beenagpillai.pradeep@gmail.com

Madhurya J A, Dept. of CSE, Gitam University, Bangalore, India. Email: madhurya72@gmail.com

*Retrieval Number: F9426038620/2020©BEIESP
DOI:10.35940/ijrte.F9426.038620
Journal Website: www.ijrte.org*

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

Blockchain records are time-stamped and making it tampers proof. Online payment service providers find blockchain as most advanced technology for secure and contactless payment. By trusting the technology, blockchain provides users to transfer money to untrusted parties.

Blockchaining work on de-centralized server, and no need to agreement or permission from other service providers unlike that we need to do in traditional online payment using mobile apps, which seeks permission and verification from service providers like network, payment app service provider, bank service provider.

II. OUR CONTRIBUTION

A. Blockchain Mobile-wallet app:

Implementation of blockchain Mobile-wallet is required to bypass permission from multiple services providers, where blockchain app will do the transaction to untrusted users without seeking any permission from service providers.

B. Single authorization for transaction: user account information should be maintained by user himself and should not be maintained by any other service providers.

C. Blockchain with Private and Public Key: Every user has public and private key using which users can do the payment transaction.

III. LITERATURE WORK

To understand the reality of existing payment services, Lacmanovi., address the uses of radio frequency based payment techniques it supporting many type of payment methods like Visa, MasterCard, and others etc.

The authors also addressed several type of contactless payment transaction such as merchant card and other new technologies and furthermore talk about precautions distress, together with exploitation of stolen cards, identity theft protection and also focused on strong security system, strong data security and a trusted and strong security device, and other support for biometric authorization and information privacy.

Most of online payment system using third-party payment network to do the transaction which might rise security issues, where transaction are made through third-party network there might be possibility of identity-theft, where third-party network service providers can break into the network and launch attack and misuse of sensitive information.

As stated the third-party service providers are untrusted [1], because third-party service providers have complete control over transaction they can mislead users and to do the identity theft this might be the major drawback why online payment can't be done by trusting third-party service providers.

Current mobile payment apps are very successfully implemented, where security issues are addressed properly and advanced security protocol are upheld secure and fearless transaction with these protocols. These applications work under the control of three modules network service providers, payment app service providers, bank service providers, the entire transaction is depending on these modules and chance of identity theft is very low. These apps don't not receive customers original card number instead it sends transaction request to server, where will generate a token it will be represented as unique identification number that represents card number, by authentication of token transaction can be completed. In spite of data privacy some of the limitations can be found in current online payment application, where third-party apps require bank details which app need to do the transaction, bank service provides token for each user's request, using token app should do the transaction process, and also need network service to complete the transaction, this could be the drawback of the application, where each transaction need permission from minimum three service providers app service provider, network, and bank service provider some time user's might dependent on network services it will take time to verify generated token from bank server even with these security parameters still user's has to face identity theft problem, because if these service providers are compromise with each other there might be a chance of users lost his/her sensitive data.

Blockchain is mostly support to the tools as the functional support: (1) Uniqueness recognition and protection: Recognition and anti-counterfeit are executed using a public key communications. Every description in the blockchain has a public key and a private key familiar with forward to accept the communications. Later than the private key encrypt the operation significance, the recipient subsequently makes use of the sender's public key to decrypt the significance, and the uniqueness of the dispatcher be able to established.

Advancement in digital online payment introduces blockchain for mobile payment in the world business which makes online payment easy and safe. A blockchain wallet application made of two keys explicitly public and private keys. The public key is united through one and all, whereas the private key is reserved as top furtive. These keys effort in a especially related approach to the perception of blocking and key: the block (private key) and the keys (public key).

Development of blockchain wallet-application overcomes the limitation of traditional method drawbacks, where wallet contains private key and public key using which user's can securely do the transaction without taking permission from any third-party services unlike traditional methods.

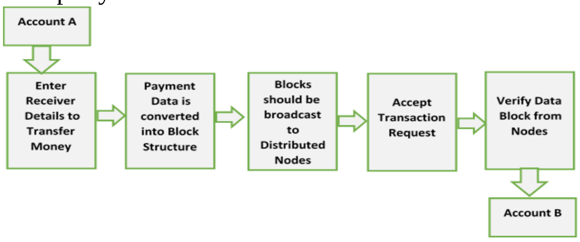

Account A
Enter Receiver Details to Transfer Money
Payment Data is converted into Block Structure
Blocks should be broadcast to Distributed Nodes
Accept Transaction Request
Verify Data Block from Nodes
Account B

Fig. 1 the flow chart for blockchain payment

IV. RESEARCH IDEA

Introducing of blockchain in mobile payment makes mobile payment secure and there is no chance of theft of identity where transaction is being made between two users.

Online digital payment is made through cryptocurrencies and payment information is hidden form hackers.

Cryptocurrency: A cryptocurrency is considered to effort as an intermediate that use to protected financial transactions, it uses de-centralized server system instead of centralized server system unlike banking servers. Using Cryptocurrencies payment can be done through two users without any permission.

V. PROPOSED SOLUTION

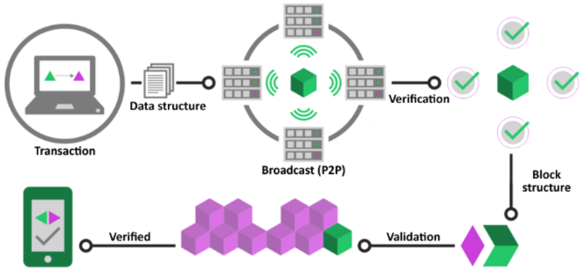


Fig. 2 Blockchain Payment Transaction

The architecture shows the implementation of blockchain in mobile payment, where each Transaction is converted as data structure and Data will be divided into block, where for each block is identified with a unique code that will be verified at time of transaction.

Fig2 shows the authentic implementation of the blockchain wallet app, every app has it's its own blockchain portfolio and that will be operated only by the concerned owner. We must link an id to which we need to send money. The given 'id' is difficult to understand (as 9kiTKEbdeD54cboRWQde). There after creating id users can send money to respective users in cryptocurrency format. The projected revelation proposal is deliberated and executed for the real-world digital money operation connecting consumers and provisions that are by means of Bitcoin.

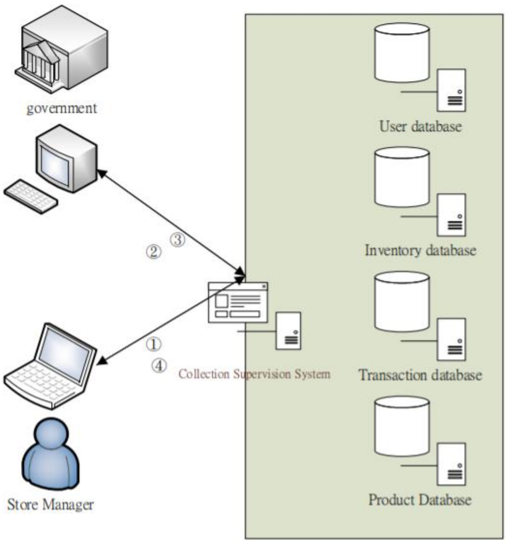


Fig3. Structural design of DBMP and Vendor registration stream.

In the projected DBMP organization, the blockchain-based compensation gathering administration is practiced on Bitcoin digital currency, the DBMP consist of three secondary structure which are SMIMSS (Store and Merchandise Information Management Sub-System), SMCTSS(Store Mobile payment Collection and Transaction Sub-System), CMPTSS(Client Mobile Payment and Transaction Sub-System) and we will illustrate these sub systems later. Furthermore, DBMP be relevant four cloud catalogues which are production in sequence, production creation, register and operation catalogue. The task of these cloud databases are illustrate in this way:

1) Vendor database: supplies in sequence of the business which are less than reassess or contain previously be inspected by government. The accumulate sequence consist of the vendor ID, production name, production locality, vendor's digital currency address, and GPS synchronizes. 2) Product database: simply the approved customers be able to log in to append or amend the in sequence regarding commodities for operating. The artefact database comfortable contains artefact detection number, artefact name, artefact description, dates, prices and one-time associated in sequence. 3) Inventory database: together with artefact number, vendor number, artefact catalogue quantity and current associated in sequence. 4) Operational database: it accounts values together with the operation serialized number, the artefact recognition quantity, artefact operates amount, vendor's digital currency payee address, the consumer's digital currency imbursement address, the vendor ID, and last to be inveterate pasture.

In the meantime, in projected DBMP design, vendors require towards listing to the Collection Supervision System (i.e SMIMSS) 1). The dealer be required to schedule a description with DBMP with a verification of industry record from government systems. 2) DBMP will repeatedly agree to the industry function to the equivalent government economic management item for re-examine the store up digital money operation dealing. 3) If the government accepted the submission from the store's digital money dealing, the server will trigger the store's description formed by the vendor in this gathering management organism. 4) Then, the vendor without charge to sign in to the description and put in the commodities to facilitate the vendor requests to retail and ensure their digital money operation statistics for instance artefact register and artefact operation accounts.

Security Properties of Block Chain

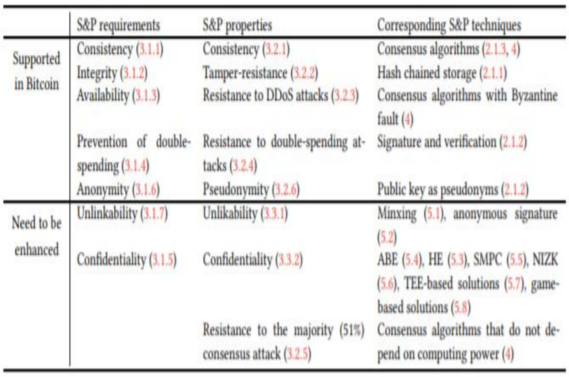
The essential protection possessions of blockchain branch on or after both cryptography continue and Bitcoin recommend and performance. Supposedly, the first protected chain of blocks was put together by means of cryptography in 1991. An application to progress the effectiveness of the cryptographic chain of blocks was put presumptuous in 1993, by integrate Merkle trees and introducing numerous permissions into one block. The blockchain is assembled to make certain a number of intrinsic protection features, such as reliability, corrupt-challenging, resistance to a Distributed Denial-of-Service (DDoS) assault, pseudonymmity, and confrontation to double-expenditure assault.

VI. VI RESULT

Nevertheless, to use blockchain for protected dispersed storage space, further protection and solitude possessions are essential.

Table 1 recapitulate the set of essential and supplementary protection and isolation belongings that want to be ensuring for gathering the information. In the upper part, the set of the protection and isolation requirements that can be assured by the safety and solitude belongings and the procedure make available in the innovative blockchain system, i.e., Bitcoin. In the inferior measurement, we show the protection and confidentiality needs and belongings that necessitate to be strengthening by some further protection and confidentiality belongings and methods. We illustrate the essential safekeeping and seclusion belongings and the further belongings for a short time declared the set of essential protection and isolation system and to converse the supplementary procedure that can be leveraged to advance development the sanctuary and isolation of blockchains.

Table1. Summarization of protection and isolation needs.



	S&P requirements	S&P properties	Corresponding S&P techniques
Supported in Bitcoin	Consistency (3.1.1)	Consistency (3.2.1)	Consensus algorithms (2.1.3, 4)
	Integrity (3.1.2)	Tamper-resistance (3.2.2)	Hash chained storage (2.1.1)
	Availability (3.1.3)	Resistance to DDoS attacks (3.2.3)	Consensus algorithms with Byzantine fault (4)
	Prevention of double-spending (3.1.4)	Resistance to double-spending attacks (3.2.4)	Signature and verification (2.1.2)
	Anonymity (3.1.6)	Pseudonymity (3.2.6)	Public key as pseudonyms (2.1.2)
Need to be enhanced	Unlinkability (3.1.7)	Unlikability (3.3.1)	Minxing (5.1), anonymous signature (5.2)
	Confidentiality (3.1.5)	Confidentiality (3.3.2)	ABE (5.4), HE (5.3), SMPC (5.5), NIZK (5.6), TEE-based solutions (5.7), game-based solutions (5.8)
		Resistance to the majority (51%) consensus attack (3.2.5)	Consensus algorithms that do not depend on computing power (4)

Table2. Online Payment Security Analysis

Payment Mode	Security
Blockchain Wallet	100%
Google Pay	80%
Phonepay	70%
Paytm	75%
Applepay	90%

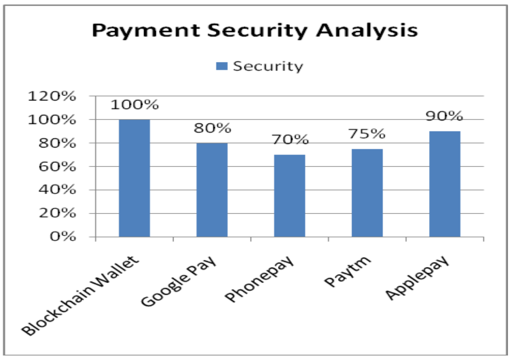


Fig4. Payment Security

Table3. Cryptocurrency works Analysis

Block chain Technology	Number of Exits
Cryptocurrency exchange	100
Cryptocurrency data	80
Cryptocurrency financial services	60
Block chain innovations	75
Cryptocurrency Payment	65
Cryptocurrency wallets	60
Cryptocurrency infrastaructure	50
Block chain Trust	100
Block chain services	100

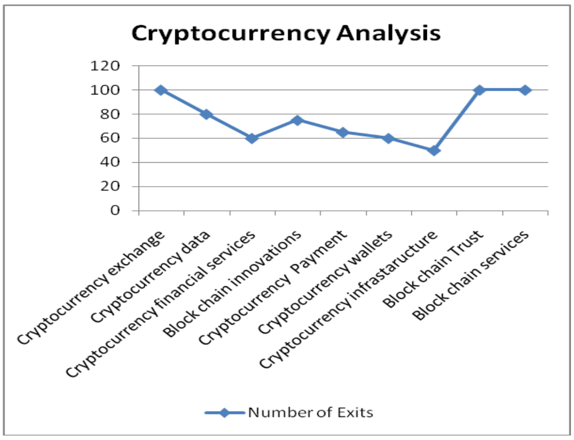


Fig5. Graph Representation of Cryptocurrency Analysis.

VII. CONCLUSION

Mobile Payment using Blockchain proves efficient and easy for digital payment without multiple authorizations and more secure compared to traditional methods. Here we don't have any direct interaction with the Bank. The cryptocurrencies are secured with blockchain wallet-app. The intruders may know about the bank details but they didn't know the Blockchain wallet details. These apps are keep doing all complex operation in background and safe guard the transaction.

REFERENCES

1. Kuo-Hui Yeh , Senior Member, IEEE "A Secure Transaction Scheme With Certificateless Cryptographic Primitives for iot-Based Mobile Payments "IEEE SYSTEMS JOURNAL, VOL. 12, NO. 2, JUNE 2018
2. S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security*, 2003, pp. 452–473.
3. En Wang , Yongjian Yang, Jie Wu, Fellow, IEEE, Wenbin Liu, and Xingbo Wang "An Efficient Prediction-Based User Recruitment for Mobile Crowdsensing" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 17, NO. 1, JANUARY 2018
4. Ke Huang , Xiaosong Zhang , Yi Mu , Senior Member, IEEE, Xiaofen Wang, Guomin Yang , Senior Member, IEEE, Xiaojiang Du , Senior Member, IEEE, Fatemeh Rezaeibagha , Qi Xia , and Mohsen Guizani , Fellow, IEEE "Building Redactable Consortium Blockchain for Industrial Internet-of-Things" IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 15, NO. 6, JUNE 2019
5. PengCheng Wei a , Dahu Wang b,∗ , Yu Zhao a , Sumarga Kumar Sah Tyagi c , Neeraj Kumar d "Blockchain data-based cloud data integrity protection mechanism" 0167-739X/© 2019 Elsevier
6. Harry Halpin, Marta Piekarska "Introduction to Security and Privacy on the Blockchain", 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)
7. Sachchidanand Singh, Nirmala Singh,2016," Blockchain: Future of Financial and Cyber Security ", 2nd International Conference on Contemporary Computing and Informatics (ic3i), pp 463-467.

8. Anjum, Ashiq, Manu Sporny, and Alan Sill. "Blockchain standards for compliance and trust." IEEE Cloud Computing 4.4 : 84-90, 2017.
9. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, ``Where is current research on blockchain technology?_A systematic review,"PLoS ONE, vol. 11, no. 10, 2016, Art. no. e0163477. doi: 10.1371/journal. pone.0163477.
10. T. Aste, P. Tasca, and T. D. Matteo, ``Blockchain technologies: The foreseeable impact on society and industry," Computer, vol. 50, no. 9, pp. 18_28, Jan. 2017. doi: 10.1109/mc.2017.3571064.
11. K. Petersen, S. Vakkalanka, and L. Kuzniarz, ``Guidelines for conducting systematic mapping studies in software engineering: An update," Inf. Softw. Technol., vol. 64, pp. 1_18, Aug. 2015. doi: 10.1016/j.infsof.2015.03.007.
12. Gang Cao and Jie Chen Practical electronic auction scheme based on untrusted third party. In computational and Information Sciences(ICCIS), 2013 Fifth International Conference on, pages 493-496 IEEE, 2013
13. llichetty S Chandrashekar, Y Narahari Charles H Rosa, Devadatta M Kulkarni, Jeffrey D Tew, and Pankaj Dayama. Auction based mechanisms for electronic procurement. IEEE Transactions on Automation science and engineering. A(3): 297- 321, 2007
14. Wen Chen Feiyu Lei. A simple efficient electronic auction scheme. In parallel and Distributed Computing, Applications and Technologies, 2007 PDCAT'07 , Eighth International Conference on, pages 173 – 174. IEEE, 2007
15. Mobile Payment procedures: Scope and characteristics Klaus Turowski.

AUTHORS PROFILE

Beena G Pillai received the B.Tech degree in Computer Science & Engineering from Acharya Nagrajuna University, Guntur, in 2012, the M.Tech degree in computer science and Engineering from Jawaharlal Nehru Technological University, Anantapur, in 2015. She is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Gitam University, Bangalore. Her current research focuses on the security in Block chain technology, Cloud Computing and Cyber Security

Madhurya J A received the B.E degree in Information Science & Engineering from Visvesvaraya Technological University, Belgaum in 2011, the M.Tech degree in computer science and Engineering from Visvesvaraya Technological University, Belgaum, in 2017. She is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Gitam University, Bangalore. Her current research focuses on the security in Cloud Computing, Cyber Security, IoT.