Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

Enhancing the Speed of Response in Digital Money Transactions using Distributed Blockchain System

Joy Iong-Zong Chen[1], Lu-Tsou Yeh[2]

[1]Professor, Department of Communication Engineering, Da-Yeh University, Chang-Hua, Taiwan
[2]Professor, Department of Electrical Engineering, Da-Yeh University, Chang-Hua, Taiwan

Email id: [1]jchen@mail.dyu.edu.tw

Abstract

Waiting for anything is undesirable by most of the human beings. Especially in the case of digital money transactions, most of the people may have doubtful thoughts on their mind about the success rate of their transactions while taking a longer processing time. The Unified Payment Interface (UPI) system was developed in India for minimizing the typographic works during the digital money transaction process. The UPI system has a separate UPI identification number of each individual consisting of their name, bank name, branch name, and account number. Therefore, sharing of account information has become easier and it reduces the chances of typographic errors in digital transaction applications. Sharing of UPI details are also made easy and secure with Quick Response (QR) code scanning methods. However, a digital transaction like UPI requires a lot of servers to be operated for a single transaction same as in National Electronic Fund Transfer (NEFT) and Immediate Payment Services (IMPS) in India. This increases the waiting time of digital transactions due to poor server communication and higher volume of payment requests on a particular server. The motive of the proposed work is to minimize the server communications by employing a distributed blockchain system. The performance is verified with a simulation experiment on BlockSim simulator in terms of transaction success rate and processing time over the traditional systems.

Keywords: Distributed blockchain, digital transaction, UPI, transaction speed, secure information, server optimization

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

1. Introduction

Safe money transaction is a primary motive of all the banking applications. To ensure that several encryption and decryption steps are enforced in most of the applications on their back end algorithm [1, 2]. One time password, 2 step authentication and biometric recognition are some of the common front end steps involved in securing the money transaction applications. Certain advanced applications are using Google authenticator for generating a Time-based One Time Password (TOTP) for the security purpose. Figure 1 indicates a simple architectural view of TOTP system, where the time is considered as a changing factor of generated passwords. The traditional OTP systems are also called as Hash-based Message Authentication Code (HMAC) OTP, where the changing factor of password is about the counter connected to the algorithm. The change in HMAC-OTP occurs with respect to the count of requests made by a user [3, 4].

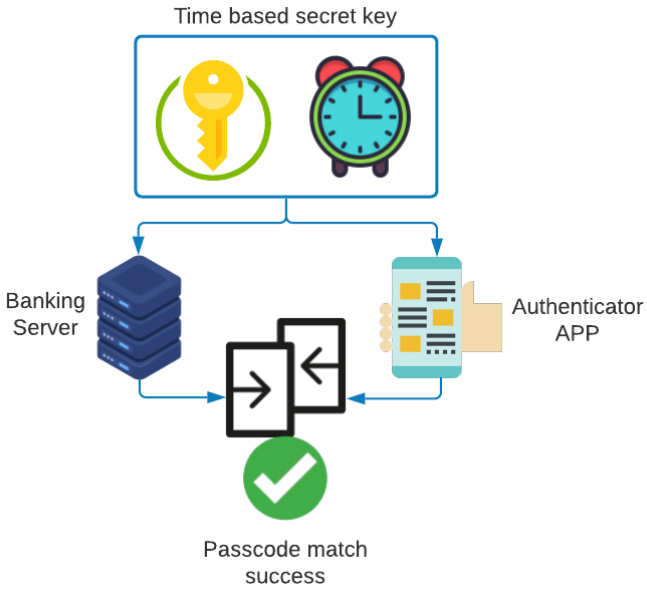

Figure 1. Architecture of TOTP system

Most of the banking applications in India are using the 2 step authentication model for their transaction process. The HMAC-OTP is forwarded to the user through mobile SMS [5].

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

The user must need a separate third party application on their mobile like Google authentication, when the bank is using a TOTP mode [6]. In certain recent banking applications the authentication systems are included with a biometric scan for ensuring the originality of the user. However, the biometric authentication models are not widely used in the present scenario due to its poor accuracy in the prediction process. The computational speed of biometric authentication also seems very less when comparing it to the OTP kind of logins [7, 8].

The payment services provided by the banks are usually operated with a centralized server of National Payments Corporation of India (NPCI) monitored by the Reserve Bank of India (RBI). The NPCI server has the responsibility of digital money transactions in all the mediums like NEFT, IMPS and UPI [9]. To improve the operational efficiency of the NPCI server, several transaction mediums were introduced. Table 1 represents the primary operating differences among the different payment services available in India. The change in operational time of the different transaction medium reduces the computational stress happening over the NPCI server at a single time [10].

Table 1. Operation differences among the digital transactions

Transaction Type	NEFT	IMPS	UPI
Transaction Frequency	Batch model (30 minutes minimum)	Instant	Instant
Transaction Timing	Bank working hours	24/7	24/7
Primary Requirement	Internet Banking	Internet Banking	Smartphone UPI app
Transaction Requirement	Account No. IFSC code	Account No. IFSC code	UPI ID/Mobile No./ Account No. IFSC code
Maximum Transaction Limit	No	Rs. 2 Lakhs	Rs. 1 Lakhs
Transaction Servers	Bank and NPCI	Bank and NPCI	PSP, Bank and NPCI

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

The NEFT and IMPS transactions accompany bank's server in its operation for money transaction and confirmation process. The NPCI server acts like a mediator and monitoring sever in between the two different bank servers for ensuring a secure payment process [11]. The UPI model includes a Payment Service Provider (PSP) server to their operation to facilitate the user to communicate with the bank server through a mobile application. The PSP server also has the primary information of the user for accessing their accounts from the bank server [12]. Due to the involvement of a third party server (PSP), the transaction limits are enabled in the UPI model as rupees 1 lakh per day. The following literature work section explores the attainments of various algorithms on secure money transaction process in a limited processing time.

2. Literature Work

Machine learning techniques are widely implemented for fuzzy logic based prediction and classification process on several applications. In banking systems, the machine learning models are implemented for detecting the suspicious transactions. It detects the suspicious transactions by analysing the Anti-Money Laundering (AML) typologies, link analysis, anomaly detection, geographic capability, risk score and behavioural modelling of the transaction requests [13]. The banking sectors are usually employed with an AML software for screening every transactions made online along with a watch list monitor for identifying any unusual transactions made by forbidden people. Know Your Customer (KYC) systems were also implemented in the banking sector for identifying the communications with forbidden business models. A machine learning component technique was developed to integrate with the watch list monitoring system for finding out the unusual activities in digital transactions. The work was verified with various machine learning algorithms like support vector machine, naïve bayes and decision tree. The experimental work found that the SVM model performs better than the other two algorithms. The maximum attained accuracy of SVM is found to be 84.8%. The technique was also extended to block the abnormal transactions [14].

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

A Deep Convolution Neural Network (DCNN) based technique was designed to observe the abnormal activity in credit card transactions. The training process of the DCNN was made with a real time dataset on credit card fraud actions. The testing accuracy of the work was found to be more than 99% with the computational speed of 45 seconds per transaction [15]. An optimal geometric transformation technique was proposed to secure the data that needs to be forwarded to the digital transaction analysis applications. The technique will also act as an attack resistance medium to avoid loss of information at the time of analysis. The proposed model was verified with various dataset and machine learning algorithms and found successful in all the scenarios [16]. In some cases, the critical details available in the transaction data are forwarded to a machine learning algorithm in an encrypted format. This improves the secrecy of the data transmission and avoid hacking of information. A hybrid encryption technique was developed for such application to encrypt the data in the speed of 2630 KB/S. The hybrid model was developed by combining the traditional Advance Encryption Standard (AES) system with a customized cipher key [17].

A user layer protection system was proposed with a chaotic biometric authentication for delivering the secret information in a secure manner to a destination. The work equips fingerprint biometrics for the operation with a N-stage Arnold Transform for ensuring the settlement claim of information [18]. A Secure Socket Layer (SSL) was introduced to data security and privacy protection in the cloud data transmission network. The system has prediction based encryption model for data encryption in a secure transmission. The suitability of the developed algorithm is verified with sensitive medical data and e-commerce data. The experimental analysis found that the proposed work requires 44.4 seconds for a 64Mb file [19]. A decentralized blockchain technique was developed to secure health care data on the cloud environment. The system is equipped with an efficient cryptographic algorithm for securing the data on the cloud surface. The decentralized system is found better in securing process, as the centralized security system has a single node to be operated for the cyber-attacks [20].

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

The Distributed Denial of Service (DDOS) attacks are quite common in recent days on the centralized cloud system. A soft computing based autonomous detection approach was developed to find out the low rate DDOS attack in the centralized cloud system. The work utilizes a hidden Markov model for analysing the change in flow process of the network and a random forest classifier is equipped for categorizing the attack and its nature in the cloud architecture. The experimental projection of the verified model gives accuracy of 97.34%, which is comparatively better than the existing artificial bee colony ANN and the adaptive threshold-based attribute selection systems [21]. A Federated Access Control Reference Model (FACRM) was formulated to secure the big data information in the Apache Hadoop cloud stack. The model was successful in addressing certain limitations of the cloud architecture like access control complexity, security auditing, data integrity and node adaption [22].

A blockchain based communication network was designed to make connection between the smart vehicles. The system is also designed to share information from the vehicle to the roadside units for tracking purpose [23]. An enhanced soft computing technique was developed by combining the fuzzy logic system with the decision tree and K means algorithm for observing the intrusions in the social media networks. The developed model was verified with DARPA and KDD-NSL datasets and observed to have better detection rate with minimum complexity when comparing it with various SVM algorithms [24]. A Dijkstra-based optimal algorithm was designed to make routing connection from the IoT sensors to its destinations. The algorithm was framed to utilize minimum energy consumption with least transmission distance. The algorithm was also further extended to secure the network connection from the attackers to maintain the consistency. The simulation analysis of the developed algorithm explores the attainments of both energy efficiency and route stability to 16% [25].

A real time fire detection approach was developed with a cloud network communication and IoT sensors. The collected information from the primary source areas are forwarded to the prediction algorithm via cloud communication. The simulation work analysis, reports that the analysing speed of the proposed model is not affected with respect to the huge data forward to

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

the cloud servers. A prediction accuracy of 98% was also observed in the verified network [26]. An artificial bee colony optimization algorithm was proposed to make an efficient communication between the wireless networks. The nature inspired algorithm was verified with a MATLAB simulation along with a machine learning based network traffic analyser. The experimental analysis shows that the proposed work has the ability in predicting multiple short routes for communication with lesser complexity [27]. A comparative work was performed in finding the efficiency of soft computing techniques in wireless sensor network route selection process. The experiment was performed with genetic algorithm, particle swarm optimization and ant colony optimization techniques. The simulation process explores a betterment in terms of network lifetime, energy and packet delivery ratio in ant colony optimization technique [28]. From the literature analysis, it has been found that an efficient routing algorithm along with a secured network are the primary essentials for making communication in the cloud architecture. The upcoming section explores a new technique for making an efficient routing process with minimum computational speed in UPI payments.

3. Proposed Work

A PSP system consists of distributed blockchain setup developed in the proposed model for reducing the computational complexity in the traditional blockchain less transaction system. The architectural view of the traditional digital transaction process using UPI is shown in Figure 2, where the primary user has a mobile application connected with the PSP server for enabling the transaction request. The motive of the PSP server is to forward the UPI information from the user's mobile application to the sub server of NPCI named as UPI server. The UPI server forwards a request to the beneficiary PSP server for collecting the account number and branch details of the bank. After successful receipt of the bank details the UPI server will send a request to the remitter bank server for money transaction. The remitter server verifies the primary user account for its balance statement and make corrections to the digital ledger according to the request made by the primary user. A confirmation message with money transaction token will be forwarded back from the remitter bank server to the beneficiary bank

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

server through UPI server. The UPI server will make a note of this transaction in the centralized NPCI server and confirms the primary user about the successful completion of the transaction.

The number of server included in the traditional UPI transactions are very high and that improves the computational complexity to certain extent. A failure or information loss in any of the server may affect the whole transaction process and it may lead to unusual transaction speed on certain circumstances. Therefore a blockchain based PSP server is introduced in the proposed work to minimize the number of transactions from the available present digital transactions.

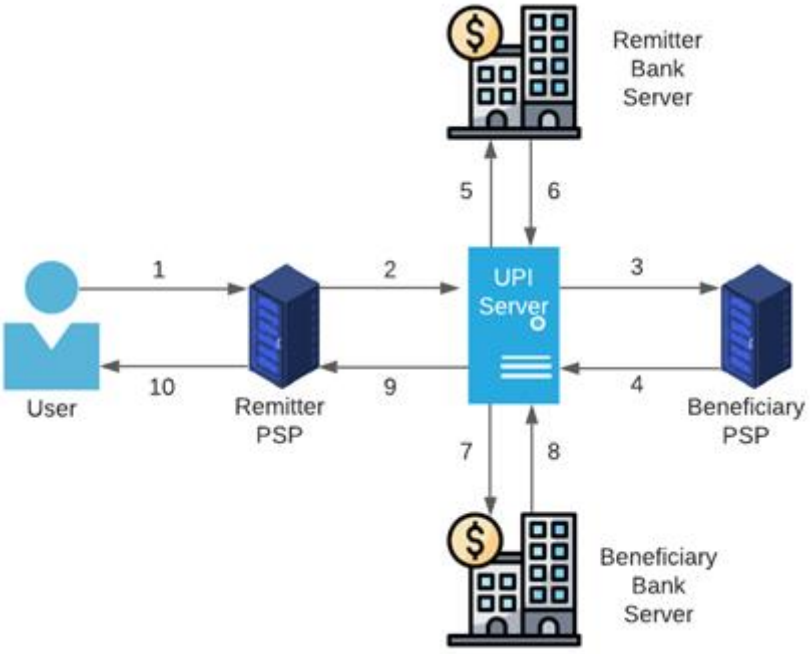

Figure 2. Architecture of traditional UPI transaction

The architectural view of the proposed UPI transaction model is shown in Figure 3. The role of beneficiary PSP server is avoided in the proposed approach by employing a blockchain setup to the remitter PSR server. The role of the blockchain model included in the remitter PSP is to store the account and branch information after the successful completion of the first transaction. The proposed system gathers the account information from the remitter PSP itself

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

rather than contacting the beneficiary PSP server. In this way the number of communications made between the servers are minimized. Table 2 compares the number of steps involved in the proposed work over the traditional UPI model.

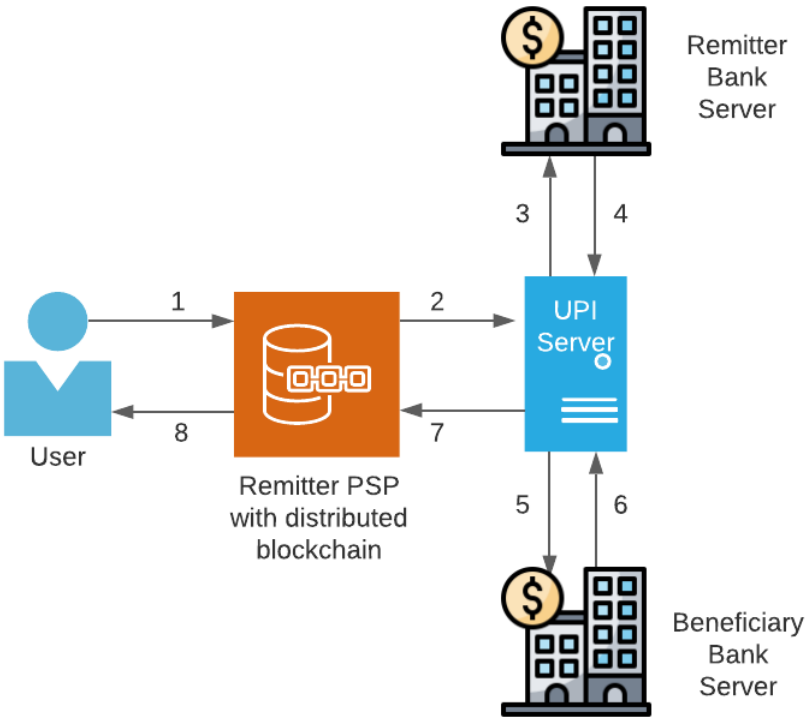

Figure 3. Architecture of the proposed UPI transaction

Table 2. Comparison of steps involved in the proposed model over the traditional model

Steps	Process in traditional UPI model	Process of the proposed distributed blockchain model
1	Initiating transaction request	Initiating transaction request
2	UPI details forwarded	UPI details with account information forwarded
3	Request to collect beneficiary account details	Debit details forwarded to remitter bank

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

4	Beneficiary details forwarded to UPI server	Remitter bank responds to the request
5	Debit details forwarded to remitter bank	Amount credited to beneficiary account
6	Remitter bank responds to the request	Confirmation forwarded to UPI server
7	Amount credited to beneficiary account	Success message forwarded to the PSP
8	Confirmation forwarded to UPI server	Transaction completed
9	Success message forwarded to the PSP	-
10	Transaction completed	-

The distributed blockchain is very popular in recent days due to its resistive nature to a common hacking algorithm. All distributed blockchains are having a separate secret code for enabling the data available in it. Therefore a common hacking tool or algorithm may not work all the time in every distributed blockchain network. However, the cost for maintaining the distributed blockchain systems are comparatively higher than the centralized blockchain systems.

4. Experimental Analysis

A network model based on the proposed architectural flow is compared with the traditional network flow in a blocksim blockchain simulator for observing the transaction performances for a same set of data. The transaction performances considered in the work for evaluation are transaction per second, transaction throughput and transaction latency. The transaction per second analysis indicates the maximum number of transaction requests that can be submitted to the network for the operation. This will explore the scalability and volume of the developed network in the transaction process. The block size created in the PSP server is fixed to 1MB and the average transaction data request utilized in the work is about 124.5 bytes,

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

whereas the transaction data size of traditional PSP server is 51.2 bytes. The change in request data size is about the information change from the proposed method to the traditional method. Figure 4 represents the comparative analysis among the existing and proposed model on transactions per second.

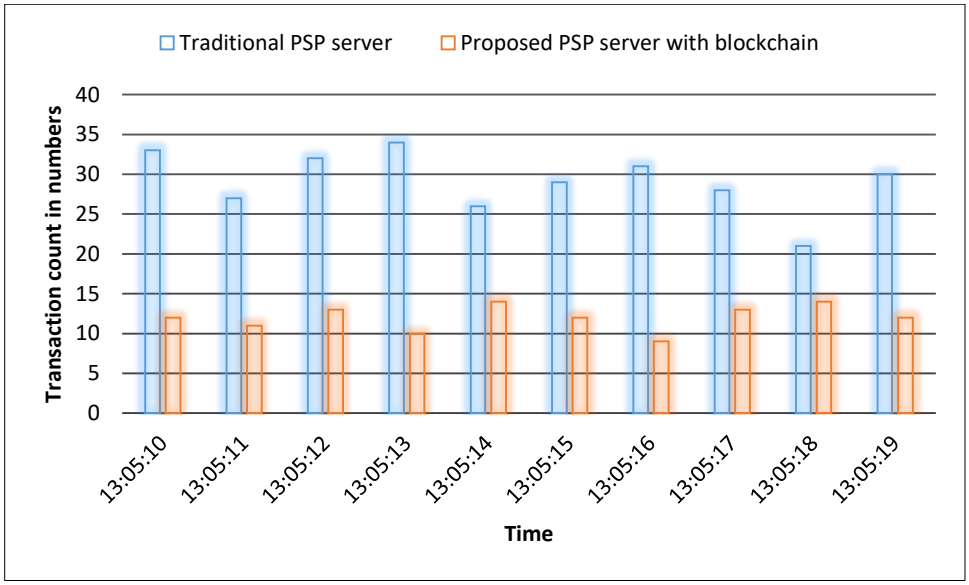

Figure 4. Comparative analysis of transactions per second

The maximum transactions per second that a block can do is calculated with respect to the equation given below. It explores the total number of transaction a block can do for every 600 seconds.

$$Transaction\ count\ per\ block = \frac{Block\ size\ in\ bytes}{Average\ transaction\ size\ in\ bytes} = \frac{1048576}{124.5} = 8422.29$$

Therefore the maximum transactions a PSP block can do for a second is limited to approximately 14 numbers in the proposed system. Figure 4 indicates the performances betterment in the traditional model. However, the data size in traditional model is very limited with UPI ID, where as in proposed PSP blockchain model it is extended to complete account information. Figure 5 and 6 compares the performances of the transaction latency that explores the acceptability of the given requests by both the algorithms in UPI server.

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

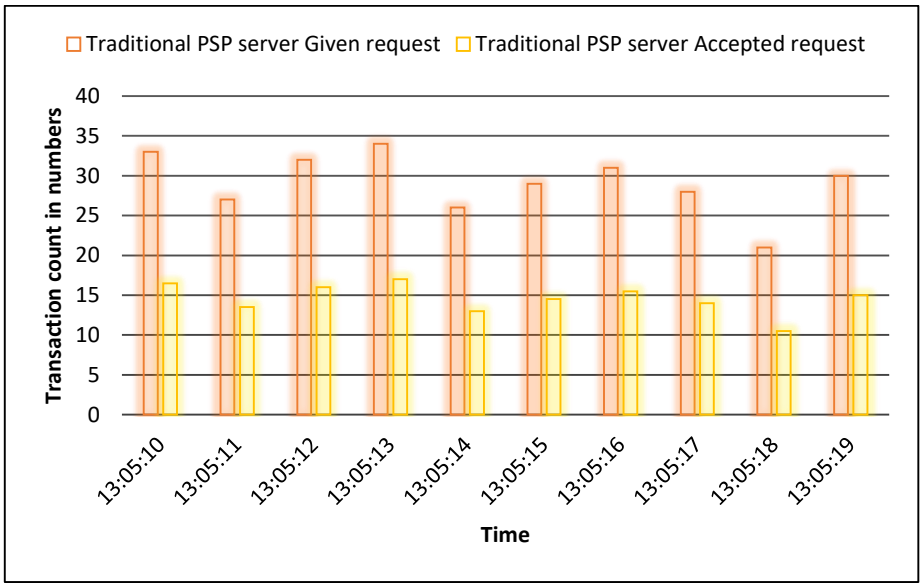

Figure 5. Acceptability of the given requests in the UPI server – Traditional model

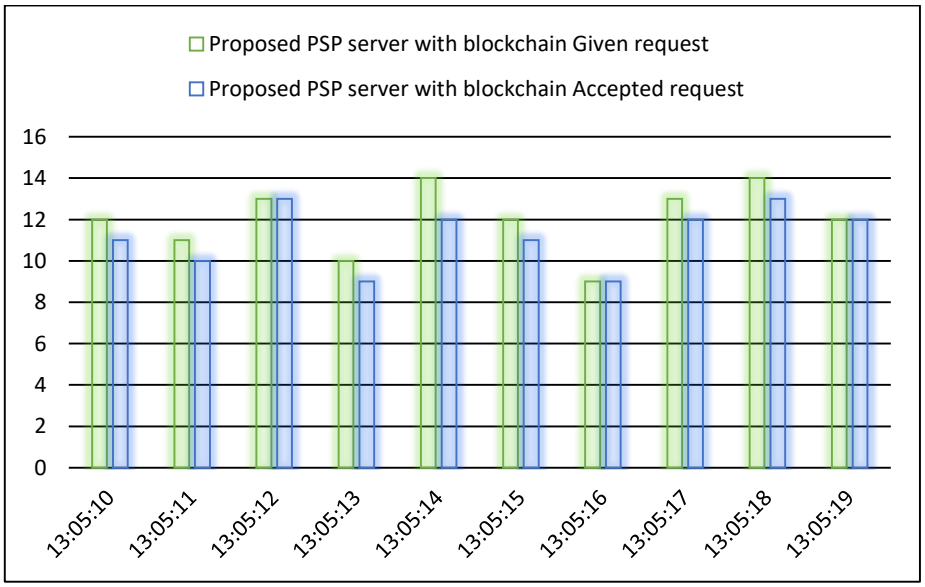

Figure 6. Acceptability of the given requests in the UPI server – Proposed model

The acceptability of the given requests by the proposed model are comparatively better than the traditional model's with respect to time. The time taken to give acceptance by the UPI server is completely minimized in the proposed approach, as it has the total required

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

information of the transaction. It is achieved by eliminating the connection of beneficiary PSP server for beneficiary data collection. Figure 7 indicates the comparative time requirement for completing the transaction process by both models.

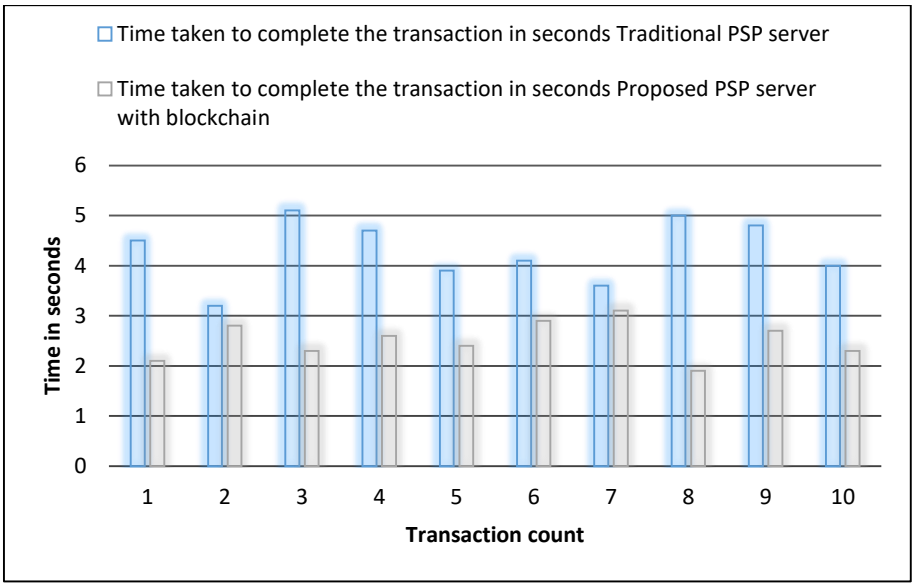

Figure 7. Performance comparison of the proposed model with the traditional model to complete the transaction

The experimental analysis projected in Figure 7 indicates that the overall time requirement for completing the digital transaction is minimized up to a certain extent in the proposed method. The average time required for completing the given 10 transactions in the traditional model is 4.29 seconds, whereas in the proposed approach it is limited to 2.51 seconds.

5. Conclusion

Instant digital money transaction is a primary expectation of many people in the last few years. It has been started with the use of debit and credit cards. However, the security in utilization of debit and credit cards are not up to the mark when compared to the traditional NEFT and IMPS transactions. In order to make secure instant transaction, the UPI payments

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

were introduced. As people are more convenient in using smartphones, the UPI payments have become popular. Though, the response time of the UPI payments are not quite satisfying for many people in several circumstances, a distributed blockchain based PSP server is employed in the proposed work to minimize the service requests made by the UPI server among the various secondary servers. The experimental analysis of the proposed model indicates that the overall transaction speed is improved by 49.4%.

References

[1] Gao, Juntao, Tong Wu, and Xuelian Li. "Secure, fair and instant data trading scheme based on bitcoin." *Journal of Information Security and Applications* 53 (2020): 102511.

[2] Rajathi, N., and Meghna Praveen. "Practical Implementation and Analysis of TLS Client Certificate Authentication." In *Proceedings of International Conference on Intelligent Computing, Information and Control Systems*, pp. 695-703. Springer, Singapore, 2021.

[3] Lu, Yuefeng, Kaimin Yu, and Xiang Lv. "Image encryption with one-time password mechanism and pseudo-features." Multimedia Tools and Applications 80, no. 10 (2021): 15041-15055.

[4] Rathi, Nikhil, Rohith Srivathsav, Rishabh Chitlangia, and V. K. Pachghare. "Automatic selenium code generation for testing." In International Conference on Intelligent Computing, Information and Control Systems, pp. 194-200. Springer, Cham, 2019.

[5] Das, Debashis, Sourav Banerjee, and Utpal Biswas. "A secure vehicle theft detection framework using Blockchain and smart contract." *Peer-to-Peer Networking and Applications* 14, no. 2 (2021): 672-686.

[6] Patel, Shikhar Singh, Akarsh Jaiswal, Yash Arora, and Bharti Sharma. "Survey on Graphical Password Authentication System." *Data Intelligence and Cognitive Informatics* (2021): 699-708.

[7] Bal, Prasanta Kumar, and Sateesh Kumar Pradhan. "Multi-level authentication-based secure aware data transaction on cloud using cyclic shift transposition algorithm."

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

In *Advances in Intelligent Computing and Communication*, pp. 384-393. Springer, Singapore, 2020.

[8] Pimple, Kshitij U., and Nilima M. Dongre. "Biometric Authentication in Cloud." In *International Conference on Intelligent Data Communication Technologies and Internet of Things*, pp. 245-254. Springer, Cham, 2019.

[9] Mohapatra, Somanjoli. "Unified Payment Interface (UPI): A cashless Indian e-transaction process." *International Journal of Applied Science and Engineering* 5, no. 1 (2017): 29-42.

[10] Gupta, Ambika, Priti Dimri, and R. M. Bhatt. "An Optimized Approach for Virtual Machine Live Migration in Cloud Computing Environment." In *Evolutionary Computing and Mobile Sustainable Networks*, pp. 559-568. Springer, Singapore, 2021.

[11] Yuan, Shunbo, Lei Liu, Baoduo Su, and Hai Zhang. "Determining the antecedents of mobile payment loyalty: Cognitive and affective perspectives." *Electronic Commerce Research and Applications* 41 (2020): 100971.

[12] Wang, Hao, Hong Qin, Minghao Zhao, Xiaochao Wei, Hua Shen, and Willy Susilo. "Blockchain-based fair payment smart contract for public cloud storage auditing." *Information Sciences* 519 (2020): 348-362.

[13] Chen, Zhiyuan, Ee Na Teoh, Amril Nazir, Ettikan Kandasamy Karuppiah, and Kim Sim Lam. "Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review." *Knowledge and Information Systems* 57, no. 2 (2018): 245-285.

[14] Alkhalili, Mohannad, Mahmoud H. Qutqut, and Fadi Almasalha. "Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering." *IEEE Access* 9 (2021): 18481-18496.

[15] Chen, Joy Iong-Zong, and Kong-Long Lai. "Deep Convolution Neural Network Model for Credit-Card Fraud Detection and Alert." Journal of Artificial Intelligence 3, no. 02 (2021): 101-112.

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

[16] Haoxiang, Wang, and S. Smys. "Big Data Analysis and Perturbation using Data Mining Algorithm." Journal of Soft Computing Paradigm (JSCP) 3, no. 01 (2021): 19-28.

[17] Viswanath, G., and P. Venkata Krishna. "Hybrid encryption framework for securing big data storage in multi-cloud environment." *Evolutionary Intelligence* 14, no. 2 (2021): 691-698.

[18] Manoharan, J. Samuel. "A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits." Journal of Innovative Image Processing (JIIP) 3, no. 01 (2021): 36-51.

[19] Shakya, Subarana. "An efficient security framework for data migration in a cloud computing environment." Journal of Artificial Intelligence 1, no. 01 (2019): 45-53.

[20] Pandey, Prateek, and Ratnesh Litoriya. "Securing and authenticating healthcare records through blockchain technology." *Cryptologia* 44, no. 4 (2020): 341-356.

[21] Mugunthan, S. R. "Soft computing based autonomous low rate DDOS attack detection and security for cloud computing." J. Soft Comput. Paradig.(JSCP) 1, no. 02 (2019): 80-90.

[22] Awaysheh, Feras M., Mamoun Alazab, Maanak Gupta, Tomás F. Pena, and José C. Cabaleiro. "Next-generation big data federation access control: A reference model." *Future Generation Computer Systems* 108 (2020): 726-741.

[23] Smys, S., and Haoxiang Wang. "Security Enhancement in Smart Vehicle Using Blockchain-based Architectural Framework." Journal of Artificial Intelligence 3, no. 02 (2021): 90-100.

[24] Sathesh, A. "Enhanced soft computing approaches for intrusion detection schemes in social media networks." Journal of Soft Computing Paradigm (JSCP) 1, no. 02 (2019): 69-79.

[25] Haseeb, Khalid, Soojeong Lee, and Gwanggil Jeon. "EBDS: An energy-efficient big data-based secure framework using Internet of Things for green environment." *Environmental Technology & Innovation* 20 (2020): 101129.

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 193-209
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.004

[26] Sungheetha, Akey, and Rajesh Sharma. "Real Time Monitoring and Fire Detection using Internet of Things and Cloud based Drones." Journal of Soft Computing Paradigm (JSCP) 2, no. 03 (2020): 168-174.

[27] Jacob, I. Jeena, and P. Ebby Darney. "Artificial Bee Colony Optimization Algorithm for Enhancing Routing in Wireless Networks." Journal of Artificial Intelligence 3, no. 01 (2021): 62-71.

[28] Haoxiang, Wang, and Smys Smys. "Soft Computing Strategies for Optimized Route Selection in Wireless Sensor Network." Journal of Soft Computing Paradigm (JSCP) 2, no. 01 (2020): 1-12.

Author's biography

Joy Iong-Zong Chen is currently a full professor in the Department of Communication Engineering Dayeh University at Changhua Taiwan. Prior to joining Dayeh University, he worked at the Control Data Company (Taiwan) as a technical manager from Sep. 1985 to Sep. 1996. His research interests include wireless communications, spread spectrum technical, OFDM systems, and wireless sensor networks. He has published a large number of SCI Journal papers on the issues addressed by the physical layer for wireless communication systems. Moreover, he also majors in developing some applications of the IOT (Internet of Thing) techniques and Dr. Joy I.-Z. Chen owned some patents authorized by the Taiwan Intellectual Property Office (TIPO).

Lu-Tsou Yeh works as a Professor in the Department of Electrical Engineering, Da-Yeh University, Chang-Hua, Taiwan. His major area of research are semiconductor materials, computer science, nano electronics, object/web technologies, microelectronics, quantum electronics, VLSI, electronic system design, IT integrated manufacturing, fabrication, and analysis which remains as the backbone for developing next generation electronic devices and information technology applications.

ISSN: 2582-418X
Submitted: 16.08.2021
Revised: 30.09.2021
Accepted: 18.10.2021
Published: 29.10.2021