Intelligent Blockchain-Based Secure Framework for Transaction in Mobile Electronic Payment System

https://doi.org/10.3991/ijim.v17i04.37671

Adil. O. Y. Mohamed
Department of Computer Science, Qassim University, Buraydah, Saudi Arabia
adi.mohamed@qu.edu.sa

Abstract—The rate of smartphone purchases is rising daily, and mobile payments are now frequently accepted in various areas. It is essential to transfer money completely safe as well as quick. The encrypted distributed ledgers function provides verified real-time transaction confirmation without the necessity for intermediaries like banks and clearinghouses; blockchain provide quick, secure, decentralized, and inexpensive transaction services. Blockchain technology makes money transfer simpler with transparency and financial data security. Through these capabilities, blockchain has attracted interest from around the world. However, some challenges arise while completing some financial security needs. This work proposes a framework for secure mobile payments based on blockchain technology. The advantages of blockchain are discussed and how blockchain technology provides multi-level authentication to secure mobile based financial transactions. Due to the increased safety and confidentiality of users on mobile payment apps, the suggested system takes into account the need of developing a safe application for the mobile transactions. We have also addressed the security related challenges of blockchain based payment applications and provided potential solutions.

Keywords—mobile payment, Blockchain, secure, transaction, fast

1 Introduction

Mobile electronic payment has become the suggested way of payment for several people's day-to-day purchasing as mobile communication networks have quickly gained popularity. Mobile payment employs smart phones to send and receive the amount, which is demanding in developing countries where the maximum number of people just has access to the internet via their phones. The majority of existing mobile payment systems, which rely on a centralized party, such as banks or carriers faces the following challenges [1]: i) The poor penetration rate of financial services is the main impediment to consumers in these locations completely utilizing the benefits of mobile payment. ii) For those who can have a bank account, using a bank to process transactions is not cheap. Financing companies and banks charge a fee for processing payments. iii) The use of bank-based mobile payments also exposes users to potential

inflation risks. This is especially acute in developing and underdeveloped countries [2].

Most internet transactions are performed through applications like PayPal and other mobile payment apps, which let consumers wait while a centralized server verifies their identities. PayPal and other online payment services charge users for online transactions and security issues also arise. For safe and quick mobile payment transactions, blockchain is introduced by many online payment service providers [3]. Unlike typical online payment methods using mobile apps, which require permission and authentication from service providers including networks, payment application service providers, and banks, blockchain work on decentralized servers [4] and doesn't require permission from any additional service providers. A simple architecture of blockchain is shown in Figure 1.

Through the use of the blockchain payment gateway, the blockchain system may carry out a decentralized authentication on a ledger that records agreements and transactions between participating nodes. In order to guarantee transaction integrity and nonrepudiation amongst participating nodes, a blockchain payment system has been developed [5]. A blockchain, which is a continuously growing collection of archives maintained by a peer-to-peer (P2P) system, is broadly used in conjunction with artificial intelligence, cloud computing, big data, mobile banking, and other pieces of machinery in a variety of technological contexts [6].

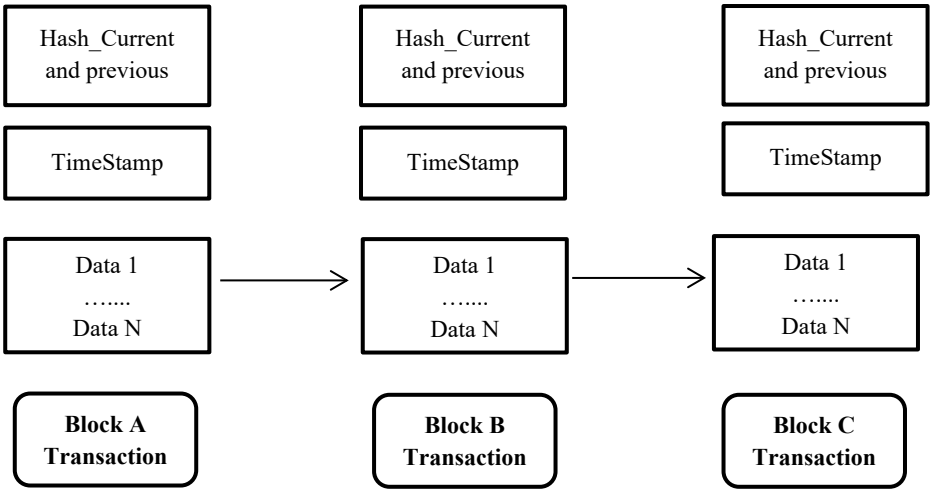

Fig. 1. Blockchain Structure

Blockchain systems are built using network users and protocols like proof of work that are hashed with digital signatures. As seen in Figure 1, each block contains a set of transactions that are digitally signed by the owner and confirmed by the reset users before being added to the block. By utilizing all of the blockchain features and characteristics: a decentralized, digital ledger that is cryptographically secured, unreliable, time-stamped, irreversible, auditable, dispersed, credible, and verifiable—

it removes any central authority or third person between a financial domain and a data exchange [7,8].

2 Advantages of Blockchain in payments

Utilizing distributed ledgers with encryption that provide reliable real-time authorization of transactions without the necessity of mediators like correspondent banks and clearinghouses, blockchain makes it possible to process international payments (and other transactions) quickly, securely, and affordably. Blockchain technology is currently being investigated for a number of non-Bitcoin uses after being initially used to secure the digital currency Bitcoin. Additionally, it provides the following key advantages [9]:

2.1 Automation with smart contracts

For organizations and industrial people, automation with smart contracts is an excellent advantage. Smart contracts can cut the processing time of payment, aid in facilitating immediate payments, and flow payments automatically. One must include all the requirements for payment transactions while designing smart contracts. The involved person is automatically paid once the necessary qualifications are satisfied.

2.2 Eliminates intermediaries

With the present payment structure, mediators and intermediaries are required. For transactions, a person must go through several authorizations and facilitators, such as the payment platform, transfer medium, provider, etc. For ensuring the legitimacy of payments, intermediaries are also responsible, they are charging for transaction service and transaction time is high.

Whereas, blockchain systems do the following: easier transaction settlement, maintain the transactions' validity without the need for middlemen facilitating peer-to-peer payments, securely store the transactional information, create a wallet for cryptocurrencies quickly and use it to make transfers [10].

2.3 Safe and quick cross-border payment

Cross-border payment happens when the sender and receiver reside in various countries. Making this transaction has been difficult for a very long time, and it faces many limitations, like many intermediaries, prolonged processing time, expensive commissions, etc. But with blockchain, cross-border payment can be done quickly. It reduces the processing time of payment, removes intermediaries, and ensures the safety of payment and data.

2.4 Transparency

Transparency is the most important benefit. The details of all transactions are stored in the blockchain, fixed, and everyone can access. Users no need to save any record, the details are automatically stored in the blockchain and are kept safe.

The advantages of blockchain based payments are shown in Figure 2.

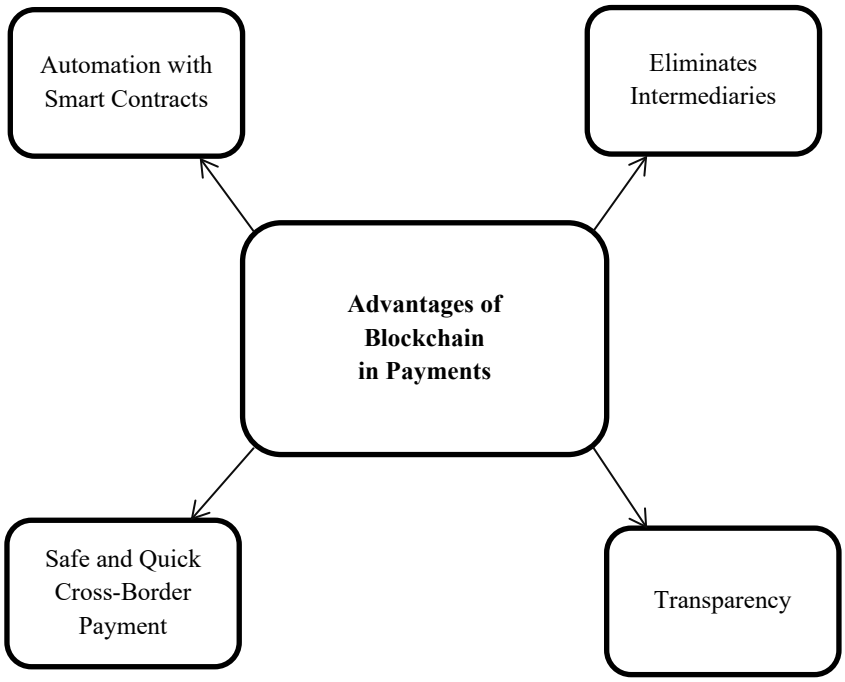

Fig. 2. Advantages of Blockchain

3 Proposed methodology

The block diagram illustrates how blockchain is being used in mobile payments. Each transaction is transformed into a data structure in the diagram, and the data is then separated into blocks. Each block is recognized by a special code, which is confirmed at the time of the transaction. The simple block diagram of the proposed blockchain based payment system is shown in Figure 3.

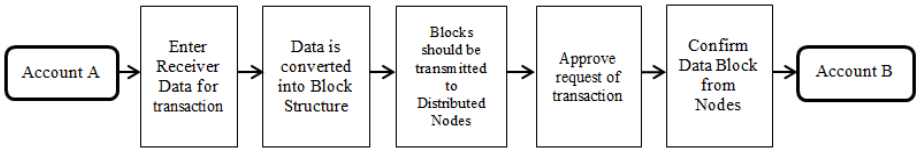

Fig. 3. Block Diagram of the Proposed Blockchain Payment System

Every mobile payment app has a unique blockchain portfolio, which is managed only by the particular app owner. The user of account A (i.e, sender) needs to enter receiver details in the app first, then the payment data is transferred into block structure; these converted blocks should be broadcast to distributed nodes. Data block will be verified from nodes after the acceptance of the transaction request. In the final step, the amount is transferred to Account B (receiver).

4 Addressing challenges of Blockchain in payment system

A few challenges of blockchain in payment systems can be addressed by taking some measures. The four simple ways to deal with the challenges of blockchain in payments in listed in Figure 4.

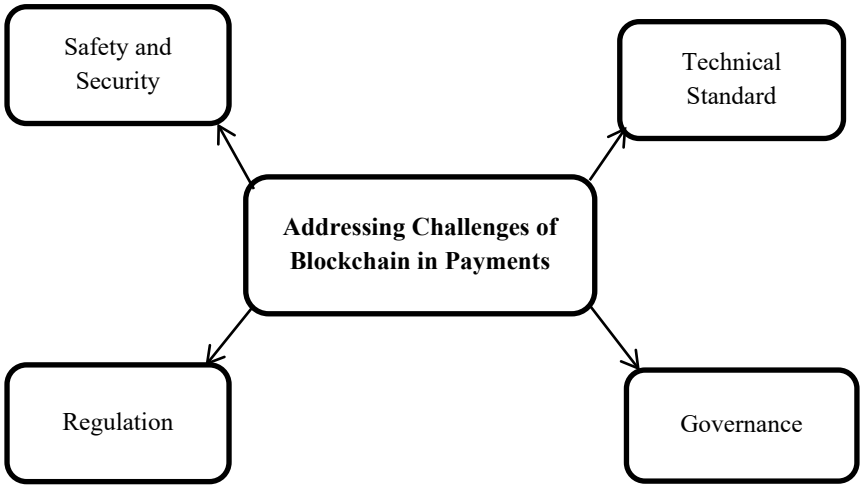

Fig. 4. Addressing Challenges

4.1 Safety and security

As the blockchain method is transparent, it is a concern to a user who doesn't like to share their payment details with everyone. To address this concern, one should set up strong security standards, Users should be made aware of the need to keep their login information safe, check bugs regularly and scan, and apply and adhere to all legal requirements [11].

4.2 Technical standard

Interoperability is essential to ensuring that blockchain payments are effortlessly integrated into existing systems. It is crucial to focus a lot of emphasis on the following components in order to tackle this issue: common technological standards

for the development of interoperability, enhancing network performance across all sizes, implementing a common communication protocol [12], testing to ensure reasonable speed, scalability, and conformity to local requirements.

4.3 Regulation & governance

To ensure full compliance with regulations, one can: Look up all necessary regulatory requirements by geographic region.

To make sure it complies with the requirements, evaluate the technical architecture of its blockchain payment system, and regularly update their blockchain payment system in accordance with the rules established by the relevant government. Provide users with regular updates on the various actions being taken and the laws being observed.

If you notice any violations of the rules, act right away.

Transactions that are not reversible, payment cancellation not possible and accountability of the data-storage ledger on the blockchain challenges can be addressed by establishing governance guidelines to address all issues and creating and implementing methods to enable payment cancellation and reversal.

5 Result & discussion

The payment security, throughput, verification time, and attacks probability result analysis are represented in Figure 5, Figure 6, Figure 7 & Figure 8 respectively. The accuracy of the suggested work (blockchain payment) is compared with previous mobile payment applications such as Googlepay, Phonepay, and Paytm. The result graph analysis shows that the proposed payment system provides the highest accuracy than other base models.

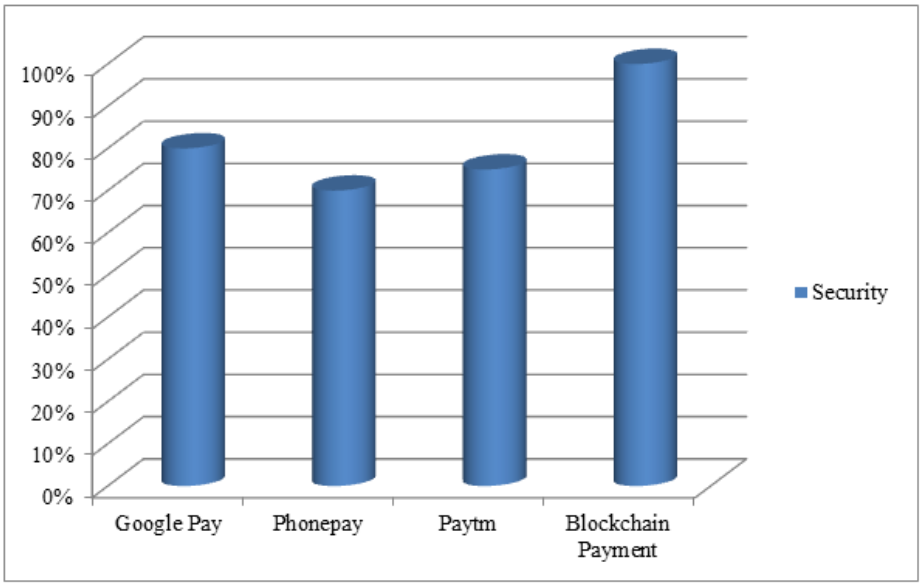

Fig. 5. Payment Security Analysis

The security percentage rate of the proposed technique shows 95% which is better than a compared technique. The quantity of transactions requests for mobile payments are satisfied by linked participants is referred to as throughput. The following graphic compares the throughput of the proposed design to the fundamental paradigm. Compared to the fundamental model, the throughput has increased.

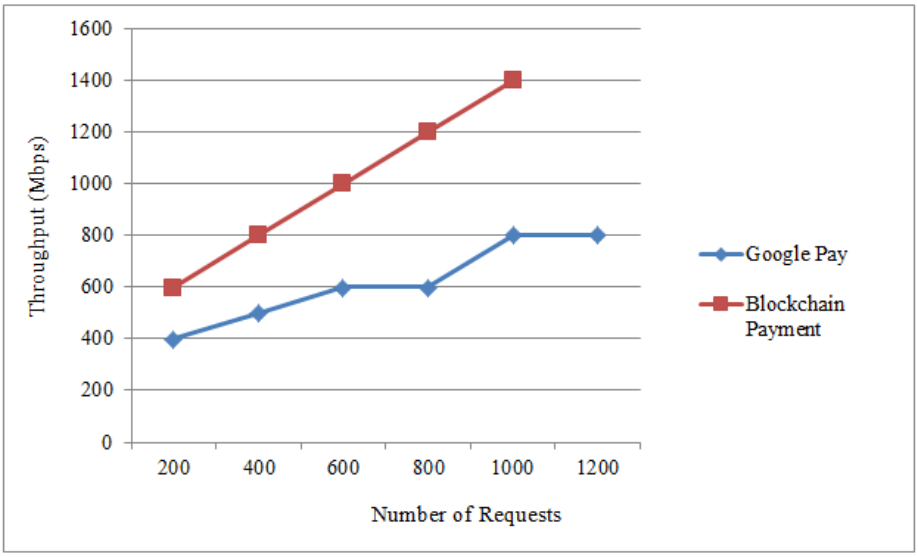

Fig. 6. Throughput Analysis

Time overhead is defined as the time it consumes to finish all verification process. The basic model takes a long time to validate than the proposed model because the previous system needs numerous re-authentication procedures. The proposed design has innovative authentication mechanisms for users, participants, and other personnel, as a result, transmission is quick and effective.

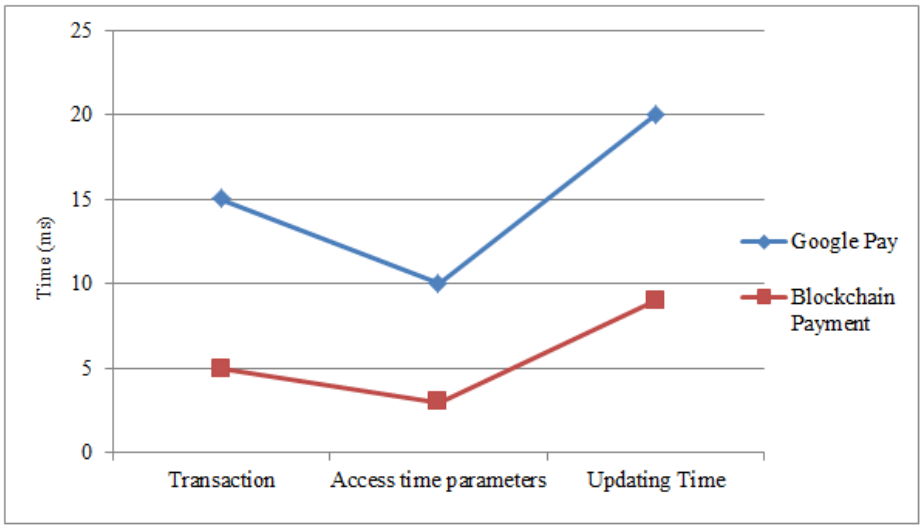

Fig. 7. Verification Period Analysis

The time required to verify each transaction is shown in Figure 7 that clearly shows the blockchain based technique verifies in less time. Each design must take into account security requirements like availability, authenticity, and privacy. Therefore, they must be taken into account in the proposed model for a distributed mobile electronic payment system. Only legal users and stakeholders will have access to the client data on the blockchain, thanks to privacy. Transactions sent to electronic payment management that has not been altered are responsible for the authenticity.

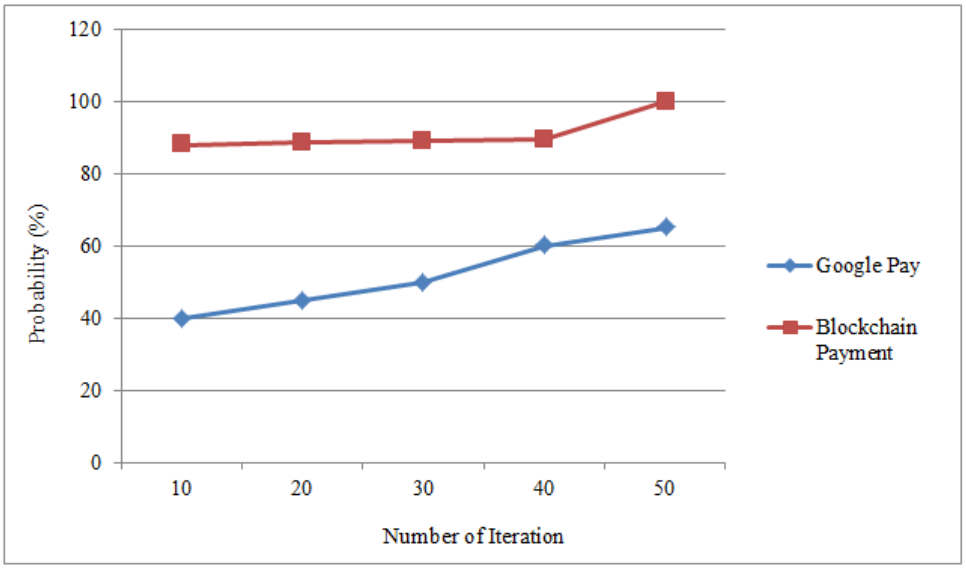

Fig. 8. Attacks Probability Analysis

Figure 8 shows the potential of a connected user to be attacked. The base model and the proposed model are compared during iterations, and the proposed structure has a higher rate of attack detection than the compared model. Attack is very less in blockchain technique as compared to Google pay.

The results shows that the blockchain based payment framework enable secured transaction in a quick manner.

6 Conclusion

Blockchain enabled mobile payments to demonstrate that they can be made digitally quickly, easily, and securely compared to more conventional methods. Blockchain technology has transformed the payments business and continues to deliver improvements. Blockchain based safe mobile payment system is explained in this paper. The proposed blockchain based payment system is compared with various existing payment model and the result shows that the proposed system provides high accuracy, improved throughput, reduced attacks and a minimal verification period. Mobile payment via blockchain is more efficient and convenient for digital payments without additional authorizations, as well as more secure than traditional methods.

7 References

[1] Xu, L., Chen, L., Gao, Z., Carranco, L., Fan, X., Shah, N., & Shi, W. (2020). Supporting blockchain-based cryptocurrency mobile payment with smart devices. *IEEE Consumer Electronics Magazine*, *9*(2), 26-33. https://doi.org/10.1109/MCE.2019.2953734

[2] Briggs, A., & Brooks, L. (2011). Electronic payment systems development in a developing country: The role of institutional arrangements. *The Electronic Journal of Information Systems in Developing Countries*, *49*(1), 1-16. https://doi.org/10.1002/j.1681-4835.2011.tb00347.x

[3] Pillai, B. G., & Madhurya, J. A. A Decentralized Data Privacy for Mobile Payment using Blockchain Technology. *International Journal of Recent Technology and Engineernig, 8*(6), 5260-5264. https://doi.org/10.35940/ijrte.F9426.038620

[4] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, *7*(2), 18-21. https://doi.org/10.1109/MCE.2017.2776459

[5] Kim, S. I., & Kim, S. H. (2020). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, 1-13. https://doi.org/10.1007/s12652-020-02519-5

[6] Joseph Bamidele Awotunde, Roseline Oluwaseun Ogundokun, Sanjay Misra, Emmanuel Abidemi Adeniyi, and Mayank Mohan Sharma. (2020). Blockchain-Based Framework for Secure Transaction in Mobile Banking Platform, *Advances in Intelligent Systems and Computing*, vol. 1375, 525-534. https://doi.org/10.1007/978-3-030-73050-5_53

[7] Obaid, M., AQEL, M, & Obaid, M. (2021). Mobile Payment Using Blockchain Security. *Journal of Applied Science and Engineering, 24*(4), 687-692.

[8] Li, X., & Shen, X. (2022). Blockchain Technology-Based Electronic Payment Strategy for City Mobile Pass Cards. *Mobile Information Systems*, *2022*. https://doi.org/10.1155/2022/4085036

[9] Leeway Hertz, Blockchain in Payments- Transforming the Payments Industry. https://www.leewayhertz.com/blockchain-in-payments/

[10] Ghazi, A., Alisawi, M., Mohammed Wahab, Y., Al-Dawoodi, A., Saber Abdullah, S., Hammood, L., & Yaseen Nawaf, A. (2022). A Systematic Literature Review of Blockchain Technology. *International Journal of Interactive Mobile Technologies (iJIM)*, *16*(10), pp. 97–108. https://doi.org/10.3991/ijim.v16i10.30083

[11] Deng, X., & Gao, T. (2020). Electronic payment schemes based on blockchain in VANETs. *IEEE Access*, *8*, 38296-38303. https://doi.org/10.1109/ACCESS.2020.2974964

[12] Abdulsattar Jaber, T. (2022). Security Risks of the Metaverse World. *International Journal of Interactive Mobile Technologies (iJIM)*, *16*(13), pp. 4–14. https://doi.org/10.3991/ijim.v16i13.33187

8 Author

Dr. Adil Omar Yousif Mohamad is an assistant professor at the department of Computer Science, College of Science and Arts, Al-Bukairiyah, Qassim University, Saudi Arabia from 2015 until now. He taught several courses at the department of computer science. He has been awarded a Master of Computer Engineering, Faculty of Computing and St. Petersburg State University of Railway 2001 St. Petersburg, Russia and a PhD in (Computer Engineering) management and maintenance networks, Mendeleyev University of chemistry and science and technology, Moscow, Russia 2007 (ORCID: https://orcid.org/0000-0003-3918-0128).

Article submitted 2022-10-26. Resubmitted 2022-12-29. Final acceptance 2023-01-05. Final version published as submitted by the author.