Sybil Attack Prevention Algorithm That Makes Blockchain Network More Secure

1Azeem ul din Siddiqi,2Zulfikar Ali, 3Shahid Aziz
[1]Punjab University College of Information Technology, Lahore
[2,3]Muhammad Nawaz Sharif university of agriculture, Multan

Abstract: - Research is experiencing exponential growth through blockchain network applications, but it still faces potential challenges in terms of privacy and security. For safe and secure bitcoin transactions blockchain technology is the best-known besides powering cryptocurrencies, trying to make safe and secure transactions from one person to the other. In this paper, the proposed system primarily focuses on delivering security to blockchain Networks by providing a Sybil attack prevention technique. This paper proposed the Sybil attack prevention technique during which the node formation process generates a node's id, the timestamp at which a node is created, password, and encryption code. The code is formed with RSA (Rivest-Shamir- Adleman) mechanism the goal is to allow user authentication in the blockchain framework. To store this information regarding each node we use Routing Protocol (RPC). By using this method, we identify the Sybil nodes from other normal nodes. A Sybil node is identified initially through the data communication process, with no data loss, which results in minimum time and low energy loss which enhances network performance. This approach demonstrates data communication inside the blockchain system and increases the throughput as well.

Keywords: Blockchain, Sybil attack, security, attack prevention algorithm, data security and privacy, routing protocol

1 Introduction

Blockchain is known as the distributed ledger which contains approaches such as cryptography, peer-to-peer(P2P), consensus algorithm, and networks of subscribers and the communications transaction are transparent between the parties which are involved [1]. Blockchain-based systems security has converted a key problem [2]. Sybil's attack is posing a massive risk to the built blockchain systems. This was the major security challenge while evolving cryptocurrencies working to complete the Net [3]. A Sybil attack was first presented in a comprehensive Sybil attack technique. In the Sybil attack, the attacker generates numerous pseudonymous identities in peer-to-peer (P2P) networks by hijacking an insecure computer that threatens user privacy [4].

A single hostile peer can perform the Sybil attack by generating loads of false identities to cheat the organization and break down its trust and redundancy system. A Sybil attack is an extremely potential risk in wireless sensor networks (WSN) that a distributed system [3]. In blockchain systems, this kind of attack is used to isolate a goal node from an honest network, which is used to present the varieties of attacks. As an example, Sybil attacks can block the distributed anonymity procedures and will rise the opportunity to find the manipulator's original identities [5].

The Sybil attack occurs mainly through transmitting, and it can work with no separate authentication and uniqueness assessment of the communication bodies [6]. The main attacker node can get numerous identities. The entity in the association knows how to try to affect the Sybil attacker due to the alertness to each entity through the message in the communication network. The fault and attacker nodes are initiated outside and inside the path and in WSN. The monitoring node can especially recognize the attacker node in a unicast and a multicast situation. The attacks in blockchain systems are 51% [7].

2 Literature Review

Most of the researchers have worked on several attack prevention systems where they are using fuzzy logic design [19, 25], machine learning approaches [21-24, 26-30, 33-37, 41-47] like CNN [32], soft computing [20], computational approaches [38-40], and the fusion approaches [31] as well. In the investigation of a Sybil attack, different methods have been projected to stop or alleviate this attack. Different Algorithms known as Sybil Guard and Sum-up offer confrontation in contradiction of almost 115 Sybil by examining the Sybil social graph [8]. The other blockchain framework named Trust Chain handles this issue by generating using an immutable chain. This chain is the creation of connections

among separate users that is temporally and well-ordered. It calculates the trustworthiness of the agents in online communal created on the previous history. They also used a technique called NetFlow [9] that confirms that each user that is consuming the resources is sharing a few resources with other nodes in the network [10]. Every interaction between two agents is supported with a track record in the data structure.

A limited number of agents, a limited number of connections, a task mapping every communication to the agents engaged in it, the main function that defines the role of an agent in the interaction. Trust Chain computes the trustworthiness of agents in the operational communal with the Sybil attack challenge by utilizing it as the input to a previous transaction. It proves that agents that utilize the available resources from society can also pay back. Every transaction is cryptographically contracted by both participating parties which are using any secure authorization mechanism. This confirms that the contribution of every user involved in a transaction is indisputable [11]. In another research, the Sybil attack resistance system built on Prove of work (PoW) is helpful for the privacy-preserving machine learning mechanism that is a PoW. There are applications to create an additionally accessible blockchain. Bitcoin NG is another protocol of blockchain that is considered to calculate the Byzantine fault-tolerant, vigorous to the risky churn, and which reveals the roughly same trust-based template removing qualitative deviations to the system. Improving the block creation rate has been talked about by employing using the GHOST law, change to the technique of bitcoin nodes 130 re-organize, and constructing the blockchain network. Otherwise, one can reorganize the chain to make a focused acyclic grid of building blocks and drop the transaction recognition instructions which integrate deals at the same time from the contradictory block. Although models offer an important rise in the potential speed, that did not permit limitless scalability and need complicated information 135 consensus mechanisms [12].

Data confidentiality is reached with statistical data and information perturbation, this technique preserves confidentiality even though even letting for effectual model learning by numerous mutual ML procedures. The effort talks about two keyboard encounters meant for blockchain consensus structures and data mining and privacy-preserving information. It offers the method of reducing energy waste characteristic to the blockchains generated on the Nakamoto consensus and lays the basis for a distributed two-way marketplace for the ML versions. The main rewards of the plan are threefold this one reduces energy waste, that offers a distributed market for ML models, and attaches the complete computing capacity of the blockchain systems [13].

In another study lightweight Sybil attack discovery system for a central clustering-based ranked system. The grouping method knowingly extends network life by evading immediate communication among nodes and the basis station. They planned a Sybil attack discovery structure that needs the associate the two available nodes. Secondly, we execute our system for the central clustering-based classified system to stop Sybil nodes after contributing to cluster top choice and these nodes are proficient in creating several virtual clusters with their fake identities [14].

This research shows that it is almost difficult for every node to provide full complex network membership information, as individual nodes hold limited association data termed as local view. Under that premise, a series-based one-to-one interaction system may be used to relay or aggregate messages. A node selects f neighbors at each round and interacts in the pull, push, or push-pull mode with neighbors. It forms a pattern of contact that is recognized as gossip. The Sybil node generates different fake identities between nodes that monitor the system by using unlimited processing resources. Identifying Sybil nodes and protecting them from Sybil attacks in the cloud computing domain should satisfy these properties.

Security: If a regular node named Nodei comes across a Sybil node such as Nodej executing a Sybil attack via creating multiple fake node identities, the Nodei can detect that this Nodej is the Sybil attack node in the network.

Aliveness: If the Sybil node such as Nodej initiates the Sybil attack, the regular nodes can ultimately detect that this Nodej is the Sybil node.

The main ideas of the protection and liveliness in delivered architectures are not anything bad that happens and ultimately a little positive happens. More precisely, the protection and safety function in this algorithm is to make sure that when a regular node that is Nodei checks a Sybil node Nodej, the Nodei always verifies that the Nodej is the Sybil node [15].

In this paper, the Random Password Generation (RPC) methods focus mainly on different traffic phases and protection throughout the information broadcast in WSN. The RPC algorithm creates the routing table that understands data about the implemented nodes. The middle nodes in the route are recognized among the source and the destination. The middle node's information is then compared with the RPC database through interaction between nodes, which are built on assessment results that decides whether they are Sybil node or regular node. The RPC also creates a complete route by adding an honest node in the pathway from the source to the destination node by numerous sub-techniques [16]. A technique for preventing and detecting a Sybil attack in WSN is proposed. They define the message passing and an authentication algorithm. The formation of Sybil's activity using personal identities is known. Existing research tackles the discovery of the Sybil attack through the verification of fake identities. Various nodes are positioned in the network arbitrarily by administrator control. They are well-arranged, promising, and cost-effective nodes in that network. Throughout the node formation process, every node receives a message that indicates the node creation time and starts time in the network. The complete node responds to the BS with location, RES communication message with the ID, and time. This information is kept under network administrator management [3].

Table 1: A literature review of the Sybil attack

Reference	**Year**	**Methodology used**	**Gap**	**Outcomes**
Kumari et al. [17]	2020	the proposed model used RFID technology. The data from the system can be only retrieved by the users who are permitted. That provides the first level of security and when the customer is verified, he can then gain access to the transaction system.	Authentication is carried out using biometrics and that limits users by calculating the amount of data needed to avoid invading IoT requests.	Various security systems improve the confidentiality of the created hash, and validation rate but also satisfy the needs of data security
D. Dasgupta et al. [11]	2019	In this study, they analyze and apply the security problems surrounding blockchain template-related technologies. We have tried to identify the blockchain safety issues based on our latest research papers survey.	Security challenges in blockchain domains.	The study tries to figure out the current trends of blockchain development.
Zhang, R et al. [18]	2019	Bitcoin-like cryptocurrency systems are followed by supplying the additional protection and privacy properties that are desired in lots of blockchain programs.	Privacy and Security Challenges	They analyze the blockchain bitcoin and it consists of consensus processes, hash enclosed garage, linking protocols, secret signatures, and noninteractive zero-knowledge evidence.

S. Zhang et al. [3]	2019	In this paper, Sybil attacks are discussed and raise the possibility of getting into first in the mining race, this	challenges in the prevention of the Sybil attack.	They analyze the Sybil attack.
		effectively initiating the Sybil attack.		
P. Otte et al [8]	2017	This paper introduces a new methodology that presents scalability, openness, and Sybil resistance while replacing proof-of-work with a mechanism to verify the validity and integrity of operations.	Sybil attacks the method that calculates trustworthiness which needs a lot of time and decreases overall performance.	The throughput of the Trust Chain exceeds that of conventional blockchain designs like Bitcoin. This shows up by using obtained data from the live network that Trust Chain has enough information to identify the Sybil attack.
J. Lim et al. [15]	2017	The paper proposes the Sybil attack safety function in our algorithm they guarantee that a regular node tests a Sybil node; a regular node always verifies that the false identity is the Sybil node.	They compare every time the new node takes processing times and resources.	Provide algorithm for Sybil attack detection
M. A. Jan et al. [14]	2015	They also introduced a central traditional clustering scheme to avoid the Sybil nodes assisting in cluster selection, the node could create multiple virtual nodes using the fake identities.	They designed a Sybil. attack finding framework which required just the two nodes accessible to the associate	Developed a system for detecting the fake identities caused by Sybil attack
Y. Sompolinsky et al. [12]	2015	They present the Sybil attack resistive method constructed on the Prove of work (PoW) which is helpful for privacy-preserving machine learning systems.	These proposed models offer an important rise in the potential rate, that did not allow for boundless scalability and need complex techniques.	Provide a Sybil attack resistive mechanism.

R. Amuthavalli et al. [16]	2014	They present that the RPC algorithm generates a routing table gathering details about the nodes that are being deployed. One source and destination identify the in-between nodes in a path. The data of the internode is then matched with the RPC database by contact between nodes, which builds on the evaluation results and determines whether the Sybil node or the normal node.	They stored the information in a database which needs time during the information retrieval for every node.	Proposed algorithm RPC based to prevent the Sybil attack.

This paper plans to research and study different Sybil prevention algorithms and available frameworks for this attack and to propose a generalized approach that will cover all the parameters to make blockchain more secure and prevent this attack. We identify the common reason behind this attack and proposed new prevention methods based on these parameters which will make blockchain more secure. After studying different approaches, we find the common parameters and features which use to avoid this Sybil attack in a blockchain transaction. We make these features compulsory to add all blockchain networks which helps in the prevention of Sybil's attack. Our proposed system assigns a node id, timestamp, and password to a normal node during the node formation process. This information is stored in the RPC protocol and compared before the transaction is processed. The transaction is only carried out when the information matches between two nodes. It also identifies the Sybil node and avoids avoid the data being shared with wrong identities. This method is efficient and makes the blockchain network secure and avoids Sybil attacks.

3 Proposed Methodology:

In this paper, we proposed the Sybil attack prevention system that prevents attacks in the blockchain network shown in Figure 1. This addresses the various traffic stages and protection issues during data transmission in the blockchain network. In the blockchain, the transaction is carried out between many nodes, as a Sybil attack generates nodes with fake identities which is called the Sybil node. In our proposed algorithm, during the node formation process, we generate a node's id, timestamp of generation, and a password and encryption code. The code is produced with the RSA (RivestShamir- Adleman) Mechanism the main aim is to allow Mutual user authentication with the blockchain framework. The code size ranges from typical 1024 to 4096 bits. This method is used to encrypt and decrypt modern computer Messages. It is an asymmetric algorithm in cryptography. Asymmetric means two distinct keys exist. It also happens that public-key cryptography is called although one of the keys could be done to everybody. The other thing needs to be kept secret. So only honest nodes can care about this code with each other.

We store this information in the routing table (table-RPC) that stores the data of every node such as id, password, and time, the middle nodes in the communication route are recognized between the source and the destination. Remote Procedure Call (RPC) is an effective technique for developing client-server-based, decentralized applications such as blockchain. This is based on expanding the traditional local calling protocol so that the so-called method does not need to reside within a similar address range as the calling protocol. This middle node data is then matched with the data available in the RPC database. If the given information matches up, then the node is regular and the normal node else node is the Sybil node.

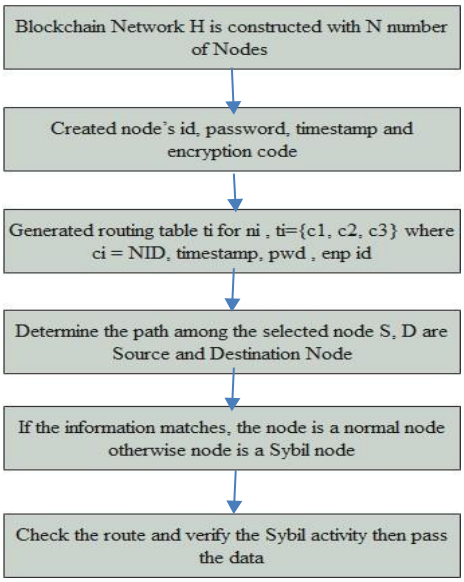

Figure 1: Proposed System Architecture

Every communication operation is cryptographically developed by both participating organizations which are utilizing the secure authorization method. This confirms the contribution of every consumer that involved in a contract is indisputable. Large amounts of nodes are placed in the network arbitrarily below the administrator's control. They are well-arranged, promising, and power-efficient nodes in the network. This technique requires that the RPC system assigns random values to each node. These nodes test if the nodes are regular nodes. In this algorithm, a Sybil node is identified originally through the data broadcast process, with no information loss, which results in time and energy loss with node saves. It also gives rise to enhance network performance.

4 Conclusion:

To tackle the security issues in the Blockchain network we proposed an algorithm to Identify the Sybil attack and find the parameter which is used in Sybil attack prevention algorithms to prevent this attack. Every node has a node id, password, and timestamp that indicates the node formation time and birth time in that network, and this information is stored in the RPC routing table. The two-way authentication is carried out before the actual data transmission which will make the blockchain network more secure. The honest node contains all the information and this algorithm compares it before the transaction. This algorithm identifies the Sybil nodes in the early stage, this permits the blockchain network to take on their further communication with no fear of Sybil attack.

5 References:

[1] Y. Lu, "The blockchain: State-of-the-art and research challenges," Journal of Industrial Information Integration, vol. 15. Elsevier B.V., pp. 80–90, 01-Sep-2019, doi: 10.1016/j.jii.2019.04.002.

[2] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," IEEE Wirel. Commun., vol. 25, no. 6, pp. 12–18, Dec. 2018, doi: 10.1109/MWC.2017.1800116.

[3] S. Zhang and J. H. Lee, "Double-Spending with a Sybil Attack in the Bitcoin Decentralized Network," IEEE Trans. Ind. Informatics, vol. 15, no. 10, pp. 5715–5722, Oct. 2019, doi: 10.1109/TII.2019.2921566.

[4] "Blockchain Attacks, Analysis and a Model to Solve Double Spending Attack | Request PDF." [Online]. Available: https://www.researchgate.net/publication/335228042_Blockchain_Attacks_Analysis_and_a_Model_to_Solve_Double_Spending_Attack. [Accessed: 20-Jul-2020].

[5] D. C. Sánchez, "Zero-Knowledge Proof-of-Identity: Sybil-Resistant, Anonymous Authentication on

Permissionless Blockchains and Incentive Compatible, Strictly Dominant Cryptocurrencies," SSRN Electron. J., May 2019.

[6] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges, and future prospects," J. Netw. Comput. Appl., vol. 163, p. 102635, Aug. 2020, doi: 10.1016/j.jnca.2020.102635.

[7] K.-F. Ssu, W.-T. Wang, and W.-C. Chang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," Comput. Networks, vol. 53, no. 18, pp. 3042–3056, Dec. 2009, doi: 10.1016/j.comnet.2009.07.013.

[8] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," Futur. Gener. Comput. Syst., vol. 107, pp. 770–780, Jun. 2020, doi: 10.1016/j.future.2017.08.048.

[9] Z. Li, J. Hou, H. Wang, C. Wang, C. Kang, and P. Fu, "Ethereum Behavior Analysis with NetFlow Data," in 2019 20th Asia-Pacific Network Operations and Management Symposium: Management in a CyberPhysical World, APNOMS 2019, 2019, doi: 10.23919/APNOMS.2019.8893121.

[10] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey," IEEE Access, vol. 8, pp. 21127–21151, 2020, doi: 10.1109/ACCESS.2020.2969820.

[11] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from a security perspective," J. Bank. Finance. Technol., vol. 3, no. 1, pp. 1–17, Apr. 2019, doi: 10.1007/s42786-018-00002-6.

[12] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2015, vol. 8975, pp. 507–527, doi: 10.1007/978-3-662-47854-7_32.

[13] H. Turesson, M. Laskowski, A. Roatis, and H. M. Kim, "Privacy-Preserving Blockchain Mining: Sybilresistance by Proof-of-Useful-Work," Jul. 2019.

[14] M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A sybil attack detection scheme for a centralized clusteringbased hierarchical network," in Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015, 2015, vol. 1, pp. 318–325, doi: 10.1109/Trustcom.2015.390.

[15] J. Lim, H. Yu, and J. Gil, "Detecting Sybil Attacks in Cloud Computing Environments Based on FailStop Signature," Symmetry (Basel)., vol. 9, no. 3, p. 35, Mar. 2017, doi: 10.3390/sym9030035.

[16] R. Amuthavalli, R. B. of theoretical & applied information, and undefined 2014, "DETECTION AND PREVENTION OF SYBIL ATTACK IN WIRELESS SENSOR NETWORK EMPLOYING RANDOM PASSWORD COMPARISON METHOD."

[17] S. Kumari, S. F.-2020 4th I. C. on, and undefined 2020, "Blockchain-based Data Security for Financial Transaction System," ieeexplore.ieee.org.

[18] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," IEEE Access, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[19] Asadullah, M., Khan, M. A., Abbas, S., Athar, A., Raza, S. S., & Ahmad, G. (2018). Blind channel and data estimation using fuzzy logic-empowered opposite learning-based mutant particle swarm optimization. Computational intelligence and neuroscience, 2018.

[20] Khan, F., Khan, M. A., Abbas, S., Athar, A., Siddiqui, S. Y., Khan, A. H., ... & Hussain, M. (2020). Cloud-based breast cancer prediction empowered with soft computing approaches. Journal of healthcare engineering, 2020.

[21] Rehman, A., Athar, A., Khan, M. A., Abbas, S., Fatima, A., & Saeed, A. (2020). Modeling, simulation, and optimization of diabetes type II prediction using deep extreme learning machine. Journal of Ambient Intelligence and Smart Environments, 12(2), 125-138.

[22] Khan, M. A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M. I., ... & Ali, A. (2020). A machine learning approach for blockchain-based smart home network security. IEEE Network, 35(3), 223-229.

[23] Khan, M. A., Abbas, S., Atta, A., Ditta, A., Alquhayz, H., Khan, M. F., & Naqvi, R. A. "Intelligent cloud-based heart disease prediction system empowered with supervised machine learning," Computers, Materials & Continua, vol. 65, no.1, pp. 139–151, 2020.

[24] Khan, M. A., Umair, M., Saleem, M. A., Ali, M. N., & Abbas, S. (2019). CDE using improved opposite-based swarm optimization for MIMO systems. Journal of Intelligent & Fuzzy Systems, 37(1), 687-692.

[25] Saleem, M., Khan, M. A., Abbas, S., Asif, M., Hassan, M., & Malik, J. A. (2019, July). Intelligent FSO link for communication in natural disasters empowered with fuzzy inference system. In 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE) (pp. 1-6). IEEE.

[26] Ata, A., Khan, M. A., Abbas, S., Khan, M. S., & Ahmad, G. (2021). Adaptive IoT-empowered smart road traffic congestion control system using a supervised machine learning algorithm. The Computer Journal, 64(11), 1672-1679.

[27] Siddiqui, S. Y., Athar, A., Khan, M. A., Abbas, S., Saeed, Y., Khan, M. F., & Hussain, M. (2020). Modeling, simulation, and optimization of diagnosis cardiovascular disease using computational intelligence approaches. Journal of Medical Imaging and Health Informatics, 10(5), 1005-1022.

[28] Fatima, A., Adnan Khan, M., Abbas, S., Waqas, M., Anum, L., & Asif, M. (2019). Evaluation of planet factors of the smart city through multi-layer fuzzy logic (MFL). The ISC International Journal of Information Security, 11(3), 51-58.

[29] Hussain, S., Abbas, S., Sohail, T., Adnan Khan, M., & Athar, A. (2019). Estimating virtual trust of cognitive agents using a multi-layered socio-fuzzy inference system. Journal of Intelligent & Fuzzy Systems, 37(2), 2769-2784.

[30] Asif, M., Khan, M. A., Abbas, S., & Saleem, M. (2019, January). Analysis of space & time complexity with PSO-based synchronous MC-CDMA system. In 2019 2nd international conference on computing, mathematics, and engineering technologies (iCoMET) (pp. 1-5). IEEE.

[31] Ihnaini, B., Khan, M. A., Khan, T. A., Abbas, S., Daoud, M. S., Ahmad, M., & Khan, M. A. (2021). A smart healthcare recommendation system for multidisciplinary diabetes patients with data fusion based on deep ensemble learning. Computational Intelligence and Neuroscience, 2021.

[32] G. Ahmad, S. Alanazi, M. Alruwaili, F. Ahmad, M. A. Khan et al., "Intelligent ammunition detection and classification system using convolutional neural network," Computers, Materials & Continua, vol. 67, no.2, pp. 2585–2600, 2021.

[33] Hanif, M., Naqvi, R. A., Abbas, S., Khan, M. A., & Iqbal, N. (2020). A novel and efficient 3D multiple images encryption scheme based on chaotic systems and swapping operations. IEEE Access, 8, 123536-123555.

[34] Saleem, M., Abbas, S., Ghazal, T. M., Khan, M. A., Sahawneh, N., & Ahmad, M. (2022). Smart cities: Fusion-based intelligent traffic congestion control system for vehicular networks using machine learning techniques. Egyptian Informatics Journal.

[35] Asif, M., Abbas, S., Khan, M.A., Fatima, A., Khan, M.A., and Lee, S.W., 2021. MapReduce-based intelligent model for intrusion detection using machine learning technique. Journal of King Saud University-Computer and Information Sciences.

[36] F. Alhaidari, S. H. Almotiri, M. A. Ghamdi, M. A. Khan, A. Rehman, et al., "Intelligent software-defined network for cognitive routing optimization using deep extreme learning machine approach," Computers, Materials & Continua, vol. 67, no.1, pp. 1269–1285, 2021.

[37] Naz, N. S., Khan, M. A., Abbas, S., Ather, A., & Saqib, S. (2020). Intelligent routing between capsules empowered with deep extreme machine learning technique. SN Applied Sciences, 2(1), 1-10.

[38] A. H. Khan, M. A. Khan, S. Abbas, S. Y. Siddiqui, M. A. Saeed, et al., "Simulation, modeling, and optimization of intelligent kidney disease predication empowered with computational intelligence approach," Computers, Materials & Continua, vol. 67, no.2, pp. 1399–1412, 2021.

[39] Abbas, S., Khan, M. A., Athar, A., Shan, S. A., Saeed, A., & Alyas, T. (2022). Enabling smart city with intelligent congestion control using hops with a hybrid computational approach. The Computer Journal, 65(3), 484-494.

[40] Rizvi, S. S. R., Sagheer, A., Adnan, K., & Muhammad, A. (2019). Optical character recognition system for Nastalique Urdu-like script languages using supervised learning. International Journal of Pattern Recognition and Artificial Intelligence, 33(10), 1953004.

[41] Hussain, S., Naqvi, R. A., Abbas, S., Khan, M. A., Sohail, T., & Hussain, D. (2021). Trait-based trustworthiness assessment in human-agent collaboration using multi-layer fuzzy inference approach. IEEE Access, 9, 73561-73574.

[42] Q. Khan, S. Abbas, M. A. Khan, A. Fatima, S. Alanazi et al., "Modelling intelligent driving behavior using machine learning," Computers, Materials & Continua, vol. 68, no.3, pp. 3061–3077, 2021.

[43] N. Tabassum, A. Ditta, T. Alyas, S. Abbas, H. Alquhayz, et al., "Prediction of cloud ranking in a hyper-converged cloud ecosystem using machine learning," Computers, Materials & Continua, vol. 67, no.3, pp. 3129–3141, 2021.

[44] Ghazal, T.M., Abbas, S., Ahmad, M. and Aftab, S., 2022, February. An IoMT-based Ensemble Classification Framework to Predict Treatment Response in Hepatitis C Patients. In 2022 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-4). IEEE.

[45] Abbas, S., Fatima, A., Asif, M. and Saleem, M., Energy Optimization in Smarts Homes by using Fuzzy Inference System.

[46] Khan, T.A., Khan, M.S., Abbas, S., Janjua, J.I., Muhammad, S.S. and Asif, M., 2021, April. Topology-Aware Load Balancing in Datacenter Networks. In 2021 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob) (pp. 220-225). IEEE.

[47] Alyas, T.A.T., 2018. Data Breaches Security Issues for Cloud Based Internet of Things. International Journal for Electronic Crime Investigation, 2(1), pp.7-7.