VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2021, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 9, Number 4, October-December 2021 *pp:51-61*

Data privacy issue in Federated Learning Resolution using Block Chain

Mansoor Ahmad Rasheed*, Shahan Uddin, Hafiz Abdullah Tanweer, Mannan Ahmad Rasheed, Mishaal Ahmed & Hudabia Murtaza

University of *Management and Technology, Lahore Pakistan*
*Corresponding author email address: S2020114015@umt.edu.pk, mansoorahmadrasheed@gmail.com

ABSTRACT
Reliable and timely traffic patterns have become an increasingly critical aspect of intelligent transport networks for traffic control. However, current predictive models of traffic flow focused on centralized machine learning need to capture raw data for model education that entails significant privacy risks. Federated learning (FL) that exchanges model changes without raw data sharing have recently been launched as an innovative way to resolve these concerns to the security of personal data. The current federal learning system is based on a central coordinator model dealing with serious security problems, including a single failure point. The Literature review is presented in this study will focus on the integration of blockchain in federated learning. Federated learning (FL) based on blockchain is thus suggested in the paper to support decentralized, efficient, and stable federated learning. The model includes three primary components; customers, blockchain technology, and machine learning engineers. In addition, different methods are communicated to protect model privacy on the blockchain further, and the advantages of the new learning system federated built on the blockchain are discussed.

KEYWORDS
Integration of blockchain in federated learning., communicated to protect model privacy on the blockchain, big data Opportunity & challenges, Data Privacy Issue In Federated Learning using Block Chain, Federated learning (FL) based on blockchain.

JOURNAL INFO
HISTORY: Received: October 11, 2021 Accepted: December 15, 2021 Published: December 31, 2021

1. INTRODUCTION

Nowadays, one of the main concerns is data privacy [1], particularly for solving the problem of data privacy in deep learning. A new mechanism termed Federated Learning (FL) was introduced by Google to provide updates in local machine learning models. It has been deployed in edge devices to make similar updates in their global models of deep learning, which are centralized being hosted on various cloud platforms [2][3]. It preserves privacy as the models are trained without needing the data on the actual server itself; thus, federated learning effectively protects data privacy[4].

FL works because the edge devices perform on-board the execution of their models locally and continuously update their execution environments. Thus, the edge devices work in tandem, making it a collaborative learning scheme. If a notable change is detected in any edge device at any point, the new information gets pushed to the centralized models. The process is done after confirming that the necessary measures for privacy and security have been taken. The global models use this new information for training, and their updates are then pushed towards any relevant edge devices. FL helps lower potential, optimize bandwidth, preserve privacy, and establish secure data channels[5]. Melis *et al.*, has highlighted that the scams of the updated gradient approach and have affirmed that it can reveal necessary information by using this approach about the training data of the customers [21]. Moreover, recovered data from the updated gradients uploaded by the attackers [22]. Above and beyond, the FL approach is susceptible to poisoning attacks when used to train the machine learning model [23].

A distributed training model is used in FL, having two roles, centralized server and edge devices. The devices at the nodes will not upload their private and locally update and upload only those information, i.e., updated pitches. The centralized server then collects all local updates, integrating them to set up an updated model. This benefit of privacy preservation has helped FL attract attention from a growing number of researchers in recent years. In this approach, the manufacturers upload an initial model with a few parameters initialized, accessible for customers to download on their devices on the blockchain. The device collects data periodically, and the model uses the extracted features from the collected data. Blockchain technology supports the model manufacturer to review and assess the malicious updates uploaded by the customers [25].

As mentioned above, a server in an FL setting does the vital job of aggregating updates, selecting clients, and maintaining the global model. The server needs a high network bandwidth to collect updates from various clients, then broadcasting the latest model to clients requires excessive network bandwidth. Moreover, if the server is being hosted on a cloud, the cloud provider's stability can affect it [6]. Client bias also occurs in specific scenarios, skewing the global model. The server may maliciously use this method to collect sensitive data from clients' updates. Using third-party centralized servers such as edge computing (MEC) servers can result in information leakage [24].

Conventional federated learning cannot tell if an update is coming from a compromised node in an internal attack by malicious nodes. These updates are taken and aggregated as

regular updates, causing the global model to be unable to link up. If an external attack occurs, then the termination of the entire federated learning process occurs. Thus, the conventional system lacks essential security features and is not very robust [7].

One approach is removing the server instead of executing its tasks on the nodes only. The blockchain, used as decentralized storage, can be employed to maintain FL. Several protocols can then be designed for doing the execution tasks on the customer site. BAFFLE [8] expresses using blockchain for sharing and storing the global model. Thus, when the central server gets wholly taken out of the picture, the abovementioned problems are no longer relevant. But another problem that arises is from the network transmission and computation operations being transferred to the nodes. Because the nodes now have to do the consensus tasks, computation costs per round become higher[22].

I have suggested a framework of joined knowledge which is decentralized blockchain-based technology. The off-chain storage is implemented in our proposed framework using the IPFS that stores the clutter of data locations on the blockchain rather than storing the actual files. The cluster is familiarized to discover a particular file over the system. The network speed is controlled using the consensus algorithm IBFT2 that controls the number of validators. The proposed approach uses three intelligent contracts, i.e., ERC20 token smart contract, store or fetches machine learning models, and models Manager smart contract. Our approach offers scalability for large tasks offered by the decentralized, federated learning models.

OBJECTIVES

1) To analyze the data privacy in hospitals during Covid-19
2) To examine the data security by using FL combined with blockchain system
3) By using FL framework based on blockchain for the data of patient's

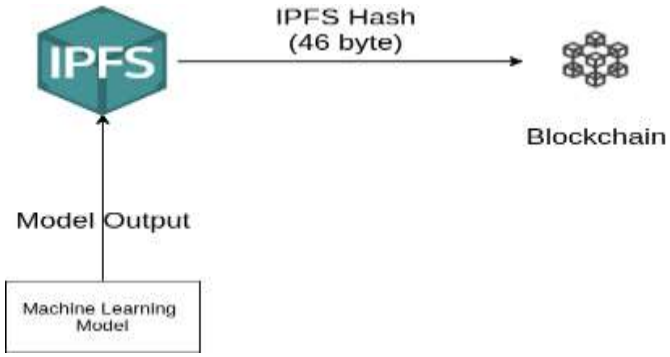


Figure 1: IPFS interacting with blockchain

2. LITERATURE REVIEW

Researchers have recently proposed some early implementations of FL based on blockchain. Hu *et al.*, proposed a method for model segmentation and a decentralized FL algorithm which is segmentation based along with gossip protocol for improving performance at convergence and maximizing the substitution between the two [9].Li *et al.*, came up with a decentralized FL framework based on blockchain to reduce internal attacks' influence, from malicious nodes, on federating learning [10]. Roy *et al.*, proposed another decentralized FL framework that is peer-to-peer to be used in medical scenarios, showing peer-to-peer environment dynamics, which is of elevated degree [11].

Zhou *et al.*, have proposed blockchain for maintaining the global model to reach a consensus within the edge nodes' community. It updates and transmits the model between several communities, using the all reduce protocol. The different communities all promote and continuously update the global model [12].

Chen *et al.*, have further proposed leveraging blockchain to record all the updates from various nodes for

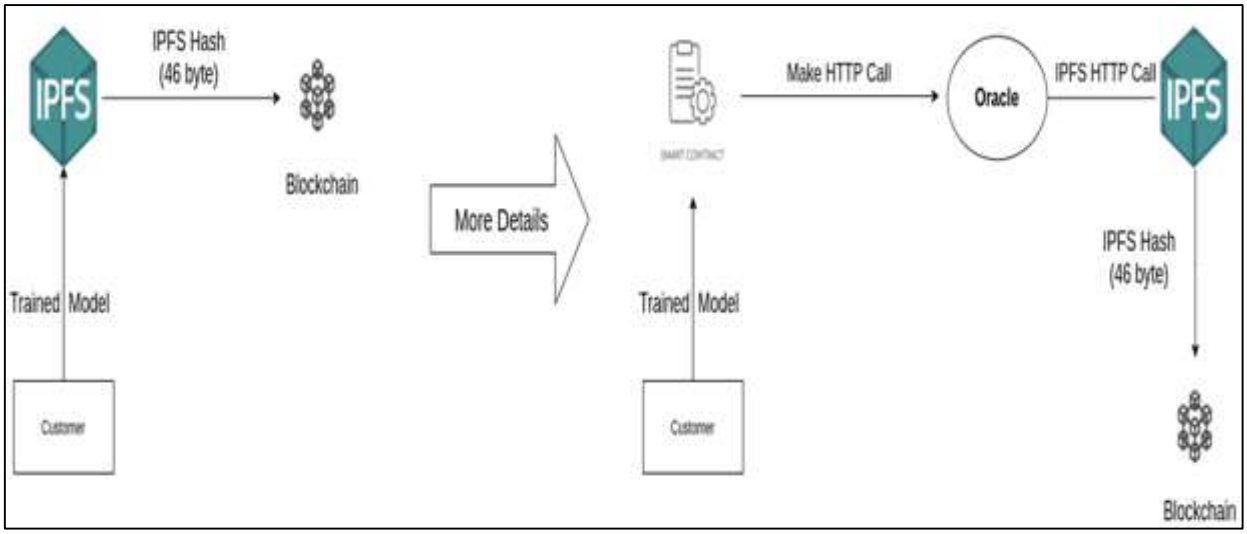


Figure 2 IPFS Section

evaluating those updates later[13]. As a precaution, underrated nodes can be removed from the community altogether to protect against malicious nodes. But, simultaneously maintaining multiple blockchain networks makes model sharing much more difficult. Different nodes from differing communities can rarely receive the updated history record or models of other communities. Moreover, suppose an entire community is somehow compromised and is malicious. In that case, the other communities might not detect and therefore resist that community, thus requiring a global detection mechanism [21].

Blockchain works as a distributed ledger to keep all reported operations and becomes unwilling to tamper. Blockchain uses the centralized server from collaborative machine learning models to be removed, increasing security. Podgorelec et al., proposed a method based on machine learning that improves the signing of transactions and has a method of identification for malicious transactions. Some blockchain-based applications can also employ deep strengthening learning; these include mobile edge calculating, industrial IOTs, the internet of vehicles, and cognitive radio networks[14].

Federated learning is an application of blockchain that has increased researchers' focus in recent years. The possibility of FL clients being cruel is always present. Thus, all clients should record their local updates under a blockchain-based federated learning setting.

Vistro *et al.*, talked about the speed of convergence of FL and its stability. The challenges can reduce To overcome these challenges, a method based on blockchain is proposed [15]. Umer *et al.*, Also, propose another architecture based on blockchain that aims to carry out aligned learning with several global models [16]. Furthermore, Bao *et al.*, came up with another federated learning architecture, blockchain-based, which utilizes past performance and various node data to develop a trusty consensus [33,34].

Many other projects consolidate federated learning into various blockchain technologies. A recent study supports the implementation of the federated learning framework in mining the blockchain [15]. However, this cannot be easy to realize as it requires extensive adjustments to the consensus protocols. Another decentralized framework of AI that uses blockchain is proposed and implemented [19]. But the problem here is that all the training data needs to be made available on the blockchain for implementing it. It completely removes the benefits of privacy that are meant to be the primary goal of federated learning. The authors noted this as well, as they state that a similar decentralized framework that also provides data privacy is an essential part of their upcoming work[18][53-67]. A BFLC algorithm which is a decentralized blockchain-based, algorithm of federated learning that lowers effects of nodes that are malicious which are internal that cast gradient attacks at selecting few nodes which are trusted to build an assembly to authenticate gradients [17]. Vistro *et al.*, suggested an approach that is completely decentralized peer-to-peer (P2P) to multi-party ML blockchain-based termed as Biscotti. This approach can defend against known attacks and possess comparatively better achievement on adaptable and fault-tolerant systems [20].

Li. *et al.*, proposed a BFLC algorithm, a decentralized blockchain-based, a federated learning algorithm that lowers the effects of internal malicious nodes that cast gradient attacks when selecting a few nodes trusted to build an assembly to authenticate gradients [10]. Vistro *et al.*, suggested an entirely decentralized peer-to-peer (P2P) approach to multi-party ML blockchain-based termed as Biscotti. This approach can defend against known attacks and possess comparatively better adaptability and fault-tolerant systems. Decentralized blockchain-based, merged learning has undoubtedly made much progress in past years, yet some problems still need solving [18]. Our presented study has tried to fulfill the gap in the existing literature.

3. METHODOLOGY

One of the critical primary features of blockchain is decentralization. Managing multiple nodes to achieve a common task is not simple. A procedure is required using which all Blockchain network peers should reach a standard agreement regarding the current situation of the distributed ledger known as a consensus algorithm.

While there are several consensus protocols, we will use Proof-Of-Authority (POA). It is faster, costs less computing power than the POW, and offers trusted validated nodes to manage [26, 27,28].

We have three smart contracts:

1. **ERC20 token smart contract**
   - 1.1 Import OpenZepplin.
   - 1.2. Customize token (token name, symbol, mint...etc)
2. **Store/Fetch machine learning models**
   - 2.1 IPFS
   - 2.2 Oracle to make IPFS calls
3. **Models Manager smart contract**
   - 3.1 Manage model status: initial, filling, and done
   - 3.2 Condition to parse from one state to another.

A consensus method called POA gives the ability towards authenticated transactions or else interactions alongside network along and to upgrade the presents less or else more registry which is distributed to a small and designated quantity of blockchain. It is similar to Proof of Stack, but it gives node validator privilege based on identities, not cryptocurrency holding. POA has a lot of consensuses algorithms. One of the most famous mechanisms is Clique and another new consensus algorithm, IBFT2. A clique consensus algorithm could work with only one node for testing or three for production [29,30].

We need to select between two different consensus protocols. Comparing the two algorithms with each other: In Clique networks, getting to consensus and happening blocks is quicker. The probability of a fork grows as the quantity of validators increases for Clique [Comparing POA Reference]. We will use IBFT2 as we can control the network speed by the number of validators. We can offer scalability for large tasks

offered by Federated learning models [31,32].

3.1 IPFS SECTION

The model sizes may be quite large, thus we need a storage system to save data. Such third-party storages are quite expensive. Saving data on the blockchain may be a good idea but it will not be scalable for a large amount of data because of the block size limit. This is why we propose a decentralized storage system. [Fig. 1]

A protocol alongside a network that is peer-to-peer is used to save and allocate data in a file system which is distributed termed as InterPlanetary File System (IPFS). Content-addressing is being used in IPFS to uniquely detect each file in a global namespace joining all computing devices. By the use of IPFS, off-chain collection can be used than a collect cluster of data locations inside blockchain blocks as we already know the IPFS hash size of 46 bytes.

3.2. SMART CONTRACTS

A self-executing contract called smart contract between seller and buyer besides agreement's term being straightly written within code's lines. The agreements and code carried therein subsists over a decentralized network of blockchain which is distributed. It is where the blockchain store the business logic.

3.3 ORACLE

Solidity smart contracts can't make HTTP calls so we use an oracle to make HTTP calls. We need HTTP calls to manage IPFS from the inside of the smart contracts. The detailed design of IPFS interacting with blockchain will be something like in [Fig. 2].

3.4. TOKENS ERC20

Peers training models on their devices got some tokens as a reward. ERC20 is a common standard on Ethereum Blockchain. We are going to use it for token implementation to distribute rewards. All ERC20 token implementations could be imported from the OpenZeppelin library [35,36,37].

3.5. BLOCKCHAIN SYSTEM DESIGN

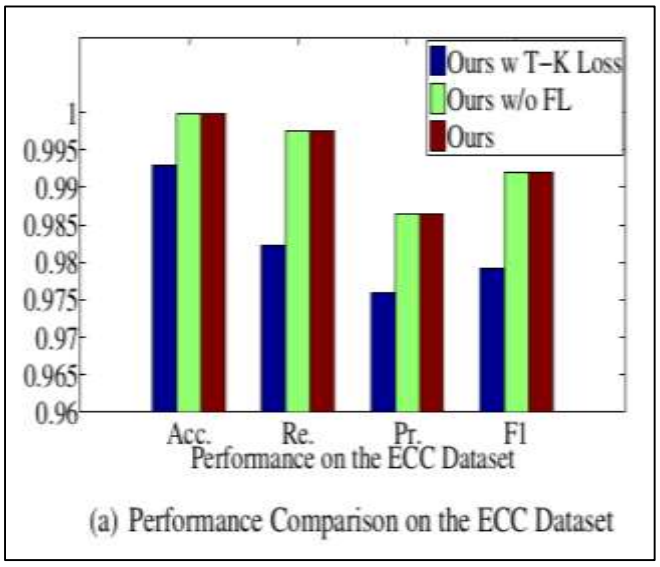
For the Blockchain Network, We need at least four validator nodes. One of them should be a boot node if we work on the testing environment. For actual production, we will use eight nodes. Two of them are boot nodes. To make the network Gas-Free, we are going to set the gas limit to 0x1fffffffffffff, and the contract size limited to 2147483647. While launching the blockchain network, ensure that the min gas option is set to 0. [38,39,40].

Initial state -> Filing state by machine learning engineer request. Filing state -> done state by time/storage/request. Example: after six months, after ten gigabytes of storage, or after the user requested to parse status.

- Gathering data requirements to check if the user is appropriate to gather data from.
- Reward distributions.
- Save all users' data to be traceable.

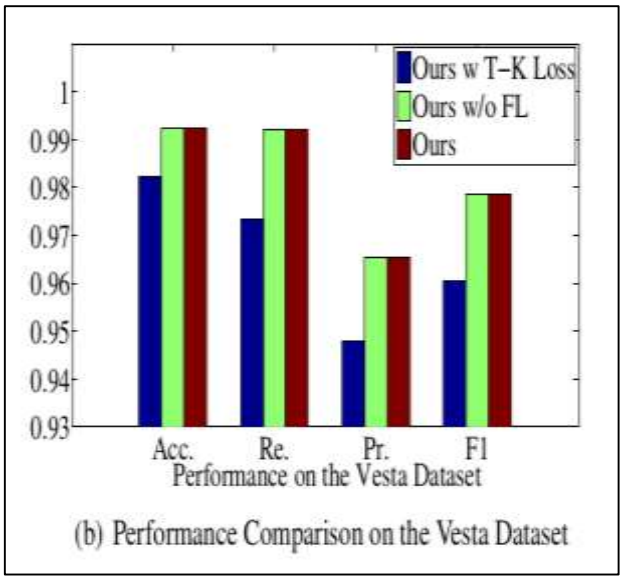
a) THE STATE-OF-THE-ART STUDY ASSOCIATED WITH COVID-19 PATIENTS' DIAGNOSIS COMPARISON

For the credit cards fraud detection model, Eight banks had participated in this experiment with four different types of datasets in different hospitals during Covid-19 outspread .(ECC,RA,SD,VESTA) (Appendix 1).



(a) Performance Comparison on the ECC Dataset

Figure 3: Comparison of performance base 1



(b) Performance Comparison on the Vesta Dataset

Figure 4: Comparison of performance bas 1

3.6. DATASETS DESCRIPTIONS

ECC (European credit cards) dataset provided by the ULB ML Group. Mohammed *et al.*, carries credit card

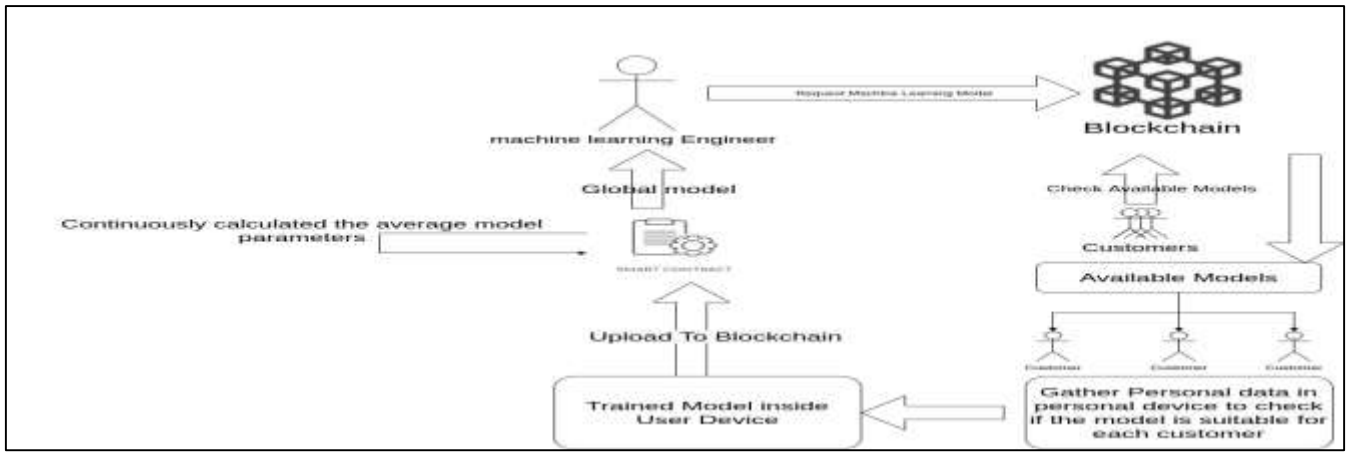


Figure 5: The proposed model for federat 1

transactions of about ten million with an unbalanced ratio of 1: 16, which comprises fraudulent transactions of about 5.96%. SD data sets were sourced from Kaggle to evaluate the performance of fraud detection methods [5]. VESTA, sourced from Kaggle, holds real-world transactions of e-commerce and consists of a massive range of features from device type to product features [40,41,42].The performance comparison based on ECC and Vesta datasets is mentioned in [Fig. 3] and [Fig. 4].

3.7. SYSTEM OVERVIEW

Figure 1 shows the proposed model for federated learning (FL) based on blockchain technology. It contains three primary components, i.e., customers, blockchain technology, and machine learning engineers [43,44,45]. The working of the proposed system model is entailed as follows.

1. The machine learning engineer requests a machine learning model to build and upload an initial model with a condition to stop and user requirements. The smart contracts should upload all data to the IPFS then save the hash inside the blockchain. Because of the large size of the model, The IPFS is used as a distributed storage solution [41].

2. Customers who want to participate in the FL process can download a primary model submitted via a machine learning engineer from blockchain technology.

3. Customers fetch the model requirements, and the customer's device starts to gather the data to ensure that the customer meets the requirements. If the customer meets the requirements, his device starts collecting the data periodically to apply the FL task on his local device.

4. The customer's device extracts the features from the collected data. The partitioned deep model training approach is used in our proposed model because some of the customer's devices cannot extract the features or train the machine learning model[42].

5. The MEC server is given by some third party with a fair probability of information. Leakage. Thus, the training procedure is then divided into 2 phases, i.e., the training of the customer's device and the training of the MEC server.

6. Customers train the ultimately linked layers within a server of MEC. The device transfers privacy-protective features alongside the actual labels toward the server of MEC. The server trains fully connected layers in the deep learning model.

7. Because putting the original data into the model might degrade its accuracy, the layers of the convolution neural network are employed as a feature extractor to extract the attributes from the original data gathered into the customer's device.

8. After the feature extraction phase, the differential privacy (DP) noise is added alongside conventional privacy guarantee to fluster the attributes earlier, unloading them to ultimately linked sheets in the server of MEC. The proposed model implements off-chain storage using IPFS. The hashes of the data locations are stored on the blockchain rather than the actual files themselves.

9. The loss produced in the training phase is reimbursed to the device to update the front layers in the training model. In traditional batch normalization, bounds within a batch size are improved by removing the constraints of mean and variance, N (The normalization is done using the formula).

10. After training, the customers upload the models to blockchain technology. Validator nodes ensure the signature is proper and the transaction is valid. Once the machine learning engineer downloads the global model, all customers who successfully participated in the federated learning task get some tokens as a reward while the malicious customers are punished. [Fig. 5] [46,47,48].

4. RESULTS

The result compares the two proposed models and the state-of-the-art in deep learning. The first proposed model for COVID-19 patients can help detect COVID-19 by the lung screening from CT scans as hospitals share their private data to train a global and better model. The proposed model used three hospitals in the experiment to achieve these outputs. The classification accuracy, loss, and time of datasets against the number of iterations are presented in [Fig. 6,7, 8].

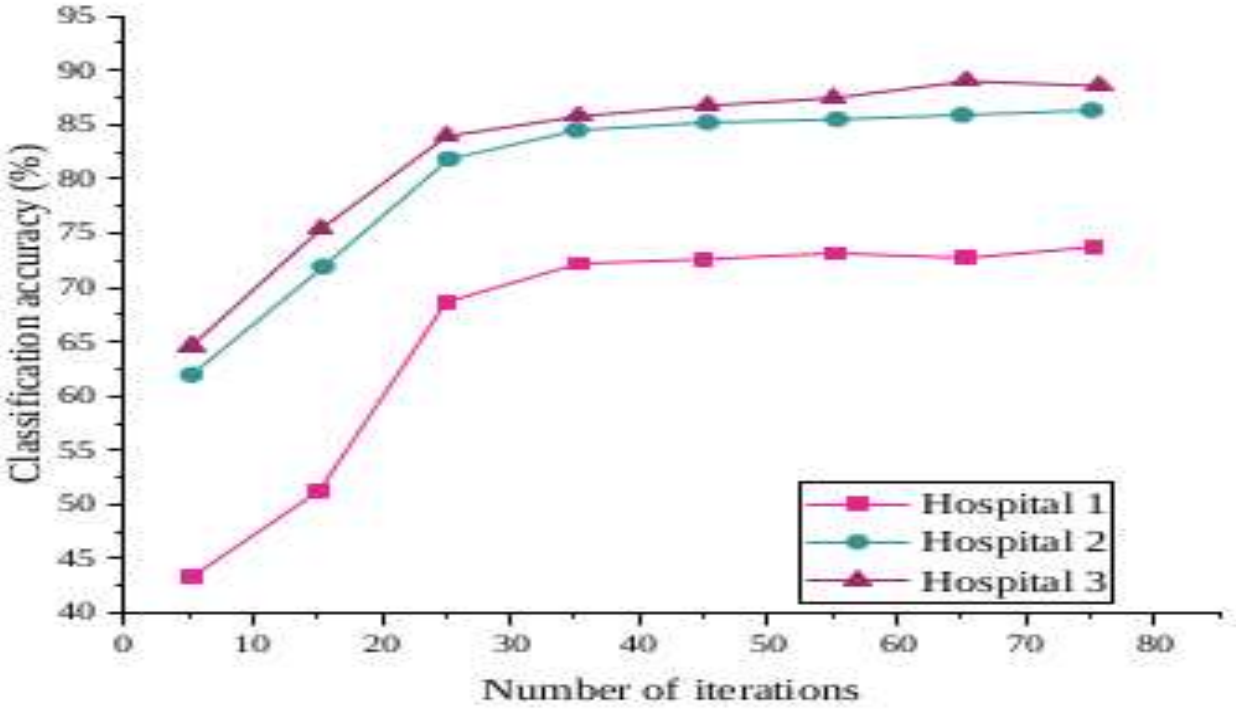


Figure 6: Classification accuracy agains 1

In figure 6 they show us a graph between classification accuracy and number of iterations.

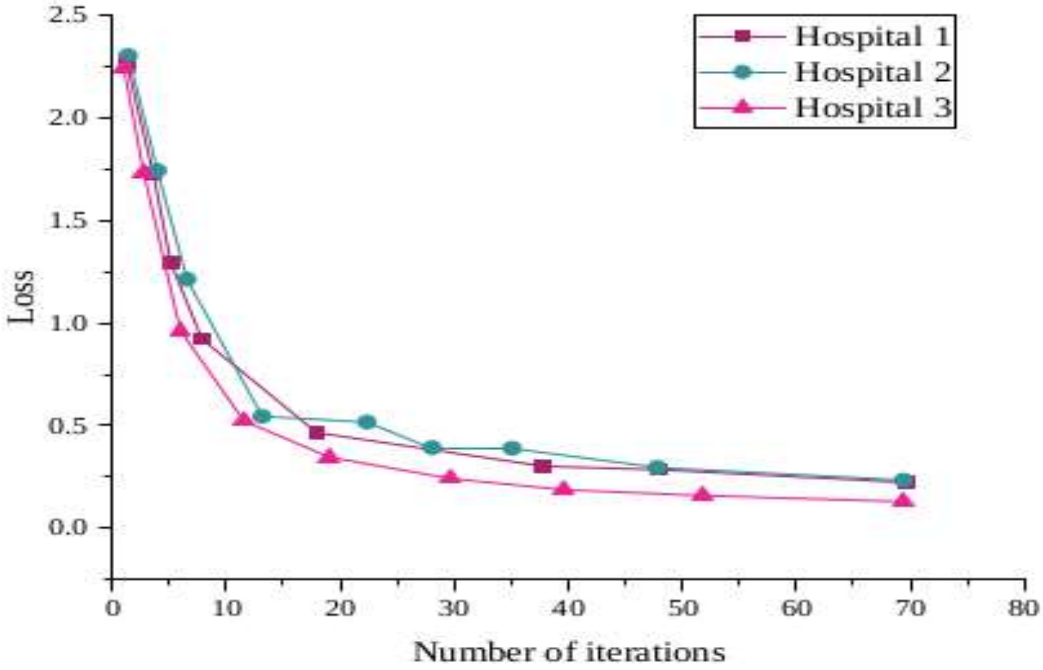


Figure 7: The Loss of dataset COVID-19 f 1

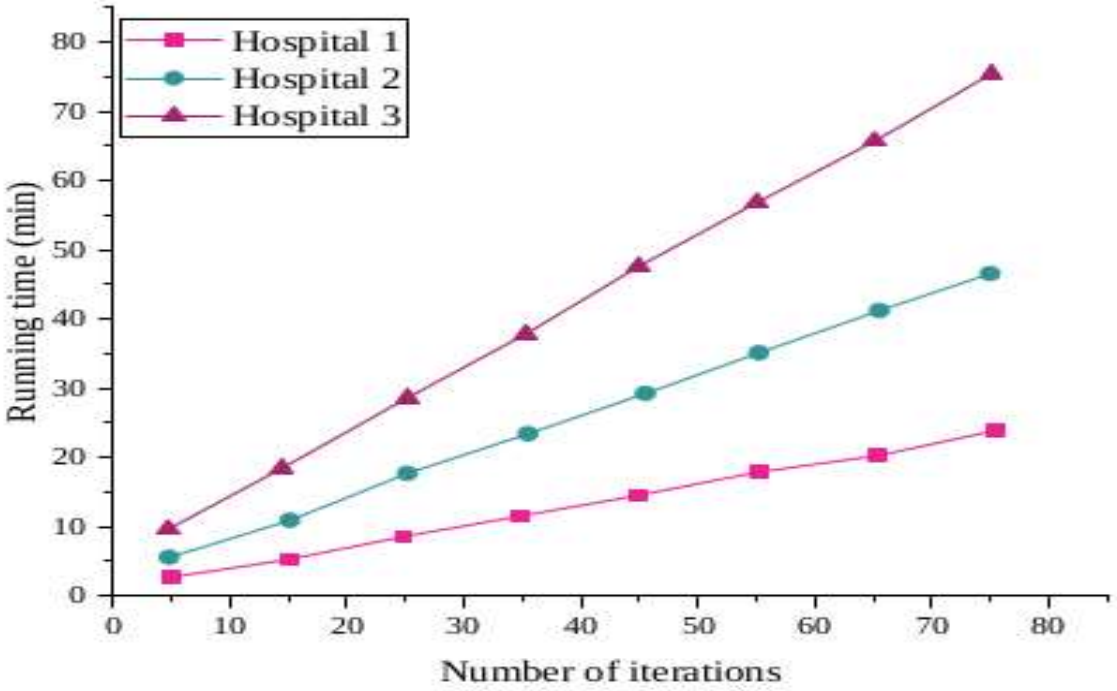


Figure 8: The time of dataset COVID-19 f 1

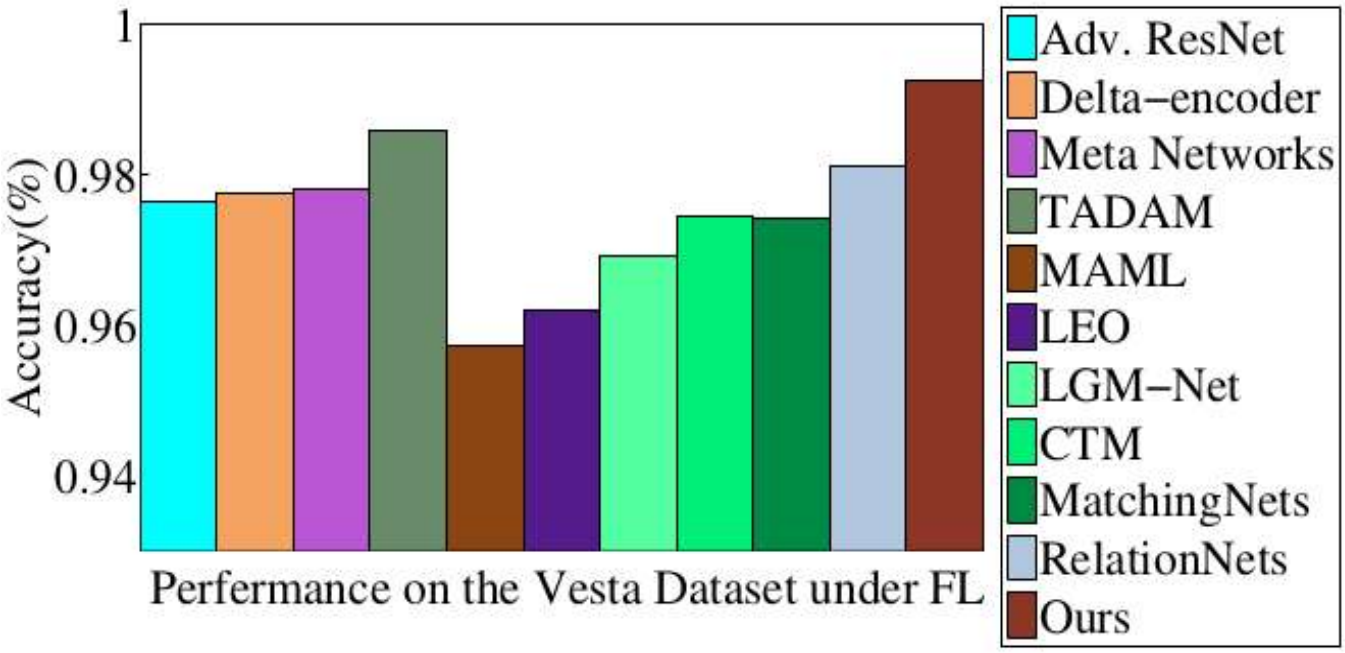


Figure 9: Accuracy of the Models 1

Figure 7 depicts the loss of the dataset COVID-19 for several providers. The graph depicts the relationship between Loss and the number of iterations.

Figure 8 shows the time for dataset COVID-19 for several providers. The graph depicts the relationship between running time and the number of iterations.

a. ACCURACY OF THE PROPOSED MODEL

Figure 9 shows the accuracy graph of the proposed model.The proposed model is better than all other federated meta-learning model approaches, with better accuracy and performance. For both hospitals and banks, federated learning proposed a way to share data more effectively than the traditional machine learning models. In contrast, they are protecting the privacy of each institution. During training, institutions can provide the dataset, and details about their dataset are disclosed by analyzing the distributed model with blockchain to protect the decentralized network from possible information leakage [Fig. 9]. [49,50].

CONCLUSION

We proposed a spread-out framework learning system in this paper that depends on the blockchain, a merged learning structure based on blockchains with a committee agreement (BFLC). We provide the research for the IPFS, Smart Contracts, Oracle, Tokens ERC20, and Blockchain System Design model. The results for the above analysis show that without a uniform structure. A strategy for model splitting and a reorganized FL calculation based on the splitting and commotion convention improve execution by mixing and improving substitution between the two. A method with which all the blockchain network participants agree in the current situation with the distributed data set of COVID patient in hospital. The network's speed is controlled by the IBFT2 covenant algorithm, which controls the number of validators.

During validation, the nodes should calculate the average of the model's parameter values to obtain the global model.

DIFFERENT APPROACHES

This section will demonstrate two use cases solved by the federated learning/meta-learning using the blockchain. The two cases have complex challenges to be solved by traditional machine learning models regarding data privacy, and the state-of-the-art will compare their results in deep learning. Few challenges are demonstarated that are now resolved by using this model with its system.

The first challenge related to COVID-19, How to share data about the patients while keeping their privacy? It's hard to identify the positive cases. So the system gathers data from hospitals' CT scans for COVID-19 patients then trains the model. Once the model is ready then share it with the blockchain. All hospitals keeps their data private and share the weight and the gradients only. The blockchain will be responsible for sharing the data securely between hospitals to create the global model using federated learning [51,52].

CREDIT AUTHOR STATEMENT

Mansoor Ahmed Rasheed: Conceptualization, Methodology,blockchain system design,Figures. **Shahan Uddin:** Writing-Original draft preparation, datasets descriptions,**Hafiz Abdullah Tanweer:** System Overview.Results, Smart Contracts,Tables. **Mannan Ahmad Rasheed:** related work help, accuracy of the proposed model,**Hudabia Murtaza:** Objectives, Literature Review, **Mishaal Ahmed**: IPFS Section, datasets descriptions ,editing

COMPLIANCE WITH ETHICAL STANDARDS

It is declare that all authors don't have any conflict of interest.Furthermore, informed consent was obtained from all individual participants included in the study.

REFERENCES

[1] H. Ström, S. Sasic, K. Jareteg, and C. Demazière, "Behaviour and stability of the two-fluid model for fine-scale simulations of bubbly flow in nuclear reactors," International Journal of Chemical Reactor Engineering, vol. 13, no. 4, pp. 449-459, 2015.

[2] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Artificial Intelligence and Statistics, 2017: PMLR, pp. 1273- 1282.

[3] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," arXiv preprint arXiv:1610.05492, 2016.

[4] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential Privacy-Based Blockchain for Industrial Internet-of- Things," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4156-4165, 2019.

[5] H. ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Towards blockchain-based reputation-aware federated learning," in IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020: IEEE, pp. 183-188.

[6] J. Konecný, H. B. McMahan, F. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency. CoRR abs/1610.05492 (2016)," arXiv preprint arxiv:1610.05492, 2016.

[7] Y. Hu, W. Xia, J. Xiao, and C. Wu, "GFL: A Decentralized Federated Learning Framework Based On Blockchain," arXiv preprint arXiv:2010.10996, 2020.

[8] P. Ramanan, K. Nakayama, and R. Sharma, "BAFFLE: Blockchain based aggregator free federated learning," arXiv preprint arXiv:1909.07452, 2019.

[9] C. Hu, J. Jiang, and Z. Wang, "Decentralized federated learning: A segmented gossip approach," arXiv preprint arXiv:1908.07782, 2019.

[10] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, "A Blockchain- based Decentralized Federated Learning Framework with Committee Consensus," arXiv preprint arXiv:2004.00773, 2020.

[11] A. G. Roy, S. Siddiqui, S. Pölsterl, N. Navab, and C. Wachinger, "Braintorrent: A peer-to-peer environment for decentralized federated learning," arXiv

preprint arXiv:1905.06731, 2019.

[12] S. Zhou, H. Huang, W. Chen, P. Zhou, Z. Zheng, and S. Guo, "Pirate: A blockchain-based secure framework of distributed machine learning in 5g networks," IEEE Network, 2020.

[13] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When machine learning meets blockchain: A decentralized, privacy- preserving and secure design," in 2018 IEEE International Conference on Big Data (Big Data), 2018: IEEE, pp. 1178-1187.

[14] B. Podgorelec, M. Turkanović, and S. Karakatič, "A Machine Learning- Based Method for Automated Blockchain Transaction Signing Including Personalized Anomaly Detection," Sensors, vol. 20, no. 1, p. 147, 2020.

[15] Vistro, D. M., Farooq, M. S., Rehman, A. U., & Sultan, H. (2021, September). Applications and Challenges of Blockchain with IoT in Food Supply Chain Management System: A Review. In *3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)* (pp. 596-605). Atlantis Press

[16] U. Majeed and C. S. Hong, "FLchain: Federated learning via MEC-enabled blockchain network," in 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2019: IEEE, pp. 1-4.

[17] Vistro, D. M., Farooq, M. S., Rehman, A. U., & Khan, M. A. (2021, September). Fraud Prevention in Taxation System of Pakistan Using Blockchain Technology. In *3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)* (pp. 582-586). Atlantis Press.

[18] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained on-device federated learning," IEEE Communications Letters, vol. 24, no. 6, pp. 1279-1283, 2019.

[19] J. D. Harris and B. Waggoner, "Decentralized and collaborative ai on blockchain," in 2019 IEEE International Conference on Blockchain (Blockchain), 2019: IEEE, pp. 368-375.

[20] Vistro, D. M., Farooq, M. S., Rehman, A. U., & Bilal, M. (2021, September). A Framework for the Promotion of Tourism Industry Using Blockchain Technology. In *3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)* (pp. 568-572). Atlantis Press.

[21] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in IEEE Symposium on Security and Privacy (S&P), 2019.

[22] B. Hitaj, G. Ateniese, and F. Perez-Cruz, "Deep models under the GAN: information leakage from collaborative deep learning," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 603–618.

[23] C. Fung, C. J. Yoon, and I. Beschastnikh, "Mitigating sybils in federated learning poisoning," arXiv preprint arXiv:1808.04866, 2018

[24] Y. Zhang, T. Gu, and X. Zhang, "Mdldroid: a chainsgd-reduce approach to mobile deep learning for personal mobile sensing," in 2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN). IEEE, 2020, pp. 73–84

[25] Farooq, Muhammad Shoaib, Misbah Khan, and Adnan Abid. "A framework to make charity collection transparent and auditable using blockchain technology." *Computers & Electrical Engineering* 83 (2020): 106588.

[26] Safarkhanlou, A., Souri, A., Norouzi, M., Sardroud, S.E.H.: Formalizing and verification of an antivirus protection service using model checking. Proc. Comput. Sci. 57, 1324–1331 (2015).

[27] Lv, Z., Chen, D., Lou, R., Song, H.: Industrial security solution for virtual reality. IEEE Internet Things J. 8(8), 6273–6281 (2020)

[28] Lv, Z., Lou, R., Li, J., Singh, A.K., Song, H.: Big data analytics for 6G-enabled massive internet of things. IEEE Internet Things J. 8(7), 5350–5359 (2021)

[29] Chai, H., Leng, S., Chen, Y., Zhang, K.: A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. IEEE Trans. Intell. Transp. Syst. (2020)

[30] Wang, P., Liu, Y.: SEMA: Secure and efficient message authentication protocol for VANETs. IEEE Syst. J. 15(1), 846–855 (2021)

[31] Lv, S., Liu, Y.: PLVA: privacy-preserving and lightweight V2I authentication protocol. IEEE Trans. Intell. Transp. Syst. (2021)

[32] Sheng, H., Near-online tracking with co-occurrence constraints in blockchain-based edge computing. IEEE Internet Things J. 8(4), 2193–2207 (2020).

[33] Qu, Y., et al.: Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J. 7(6), 5171–5183 (2020)

[34] Bao, X., Su, C., Xiong, Y., Huang, W., Hu, Y.: Flchain: a blockchain for auditable federated learning with trust and incentive. In: 2019 5th International Conference on Big Data Computing and Communications (BIGCOM), pp. 151–159 (2019)

[35] Toyoda, K., Zhao, J., Zhang, A.N.S., Mathiopoulos, P.T.: Blockchain-enabled federated learning with mechanism design. IEEE Access 8, 219744–219756 (2020).

[36] Fan, S., Zhang, H., Zeng, Y., Cai, W.: Hybrid blockchain-based resource trading system for federated learning in edge computing. IEEE Internet Things J. (2020)

[37] Cui, L., et al.: CREAT: blockchain-assisted compression algorithm of federated learning for content caching in edge computing. IEEE Internet Things J. (2020)

[38] Sharma, P.K., Park, J.H., Cho, K.: Blockchain and federated learning-based distributed computing defence framework for sustainable society. Sustain. Cities Soc. 59, 102220 (2020)

[39] Wu, X., Wang, Z., Zhao, J., Zhang, Y., Wu, Y.: FedBC: blockchain-based decentralized federated learning. In: 2020 IEEE International Conference on Artificial

Intelligence and Computer Applications (ICAICA), pp. 217–221 (2020).
[40] Pokhrel, S.R., Choi, J.: Federated learning with blockchain for autonomous vehicles: analysis and design challenges. IEEE Trans. Commun. 68(8), 4734–4746 (2020)
[41] Feng, L., Yang, Z., Guo, S., Qiu, X., Li, W., Yu, P.: Two-layered blockchain architecture for federated learning over mobile edge network. IEEE Netw. (2021)
[42] Zhang, K., Huang, H., Guo, S., Zhou, X.: Blockchain-based participant selection for federated learning. In: International Conference on Blockchain and Trustworthy Systems, pp. 112–125 (2020)
[43] Short, A.R., Leligou, H.C., Papoutsidakis, M., Theocharis, E.: Using blockchain technologies to improve security in Federated Learning Systems. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1183–1188 (2020).
[44] Qi, Y., Hossain, M.S., Nie, J., Li, X.: Privacy-preserving blockchain-based federated learning for traffic flow prediction. Futur.Gener. Comput. Syst. 117, 328–337 (2021).
[45] Zhao, Y., et al.: Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet Things J. (2020)
[46] Zhang, Z., Yang, T., Liu, Y.: SABlockFL: a blockchain-based smart agent system architecture and its application in federated learning. Int. J. Crowd Sci. (2020)
[47] Lu, Y., Huang, X., Zhang, K., Maharjan, S., Zhang, Y.: Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. IEEE Internet Things J. (2020)
[48] Toyoda, K., Zhang, A.N.: Mechanism design for an incentiveaware blockchain-enabled federated learning platform. In: 2019 IEEE International Conference on Big Data (Big Data), pp. 395–403 (2019)
[49] Rehman, M.H., Salah, K., Damiani, E., Svetinovic, D.: Towards blockchain-based reputation-aware federated learning. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 183–188 (2020)
[50] Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., Ilie-Zudor, E.: Chained anomaly detection models for federated learning: an intrusion detection case study. Appl. Sci. 8(12), 2663 (2018)
[51] Martinez, I., Francis, S., Hafid, A.S.: Record and reward federated learning contributions with blockchain. In: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 50–57 (2019)
[52] Rahman, M.A., Hossain, M.S., Islam, M.S., Alrajeh, N.A., Muhammad, G.: Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. IEEE Access. 8, 205071–205087 (2020). https://doi.org/10.1109/ACCESS.2020.3037474
[53] Vistro, D. M., Farooq, M. S., Rehman, A. U., & Khan, M. A. (2021, September). Fraud Prevention in Taxation System of Pakistan Using Blockchain Technology. In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021) (pp. 582-586). Atlantis Press.
[54] Vistro, D. M., Farooq, M. S., Rehman, A. U., & Bilal, M. (2021, September). A Framework for the Promotion of Tourism Industry Using Blockchain Technology. In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021) (pp. 568-572). Atlantis Press.
[55] Vistro, D. M., Farooq, M. S., Rehman, A. U., & Sultan, H. (2021, September). Applications and Challenges of Blockchain with IoT in Food Supply Chain Management System: A Review. In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021) (pp. 596-605). Atlantis Press.
[56] Vistro, D. M., Farooq, M. S., Rehman, A. U., & Malik, S. (2021, September). Smart Application Based Blockchain Consensus Protocols: A Systematic Mapping Study. In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021) (pp. 573-581). Atlantis Press.
[57] Khelifi, A., Aziz, O., Farooq, M. S., Abid, A., & Bukhari, F. (2021). Social and Economic Contribution of 5G and Blockchain With Green Computing: Taxonomy, Challenges, and Opportunities. IEEE Access, 9, 69082-69099.
[58] Farooq, M. S., Khan, M., & Abid, A. (2020). A framework to make charity collection transparent and auditable using blockchain technology. Computers & Electrical Engineering, 83, 106588.
[59] Vistro, D. M., Rehman, A. U., Abid, A., Farooq, M. S., & Idrees, M. (2020). Analysis of cloud computing based blockchain issues and challenges. Journal of Critical Reviews, 7(10), 1482-1492.
[60] Vistro, D. M., Rehman, A. U., Farooq, M. S., Abid, A., & Idrees, M. (2020). A SURVEY ON CLOUD COMPUTING SECURITY WITH CROSS PLATFORM. Journal of Critical Reviews, 7(10), 1439-1445.
[61] Vistro, D. M., Rehman, A. U., Abid, A., Farooq, M. S., & Idrees, M. (2020). CLOUD BASED ARCHITECTURE FOR SMART EDUCATIONAL SYSTEM USING MODERN TECHNOLOGY. Journal of Critical Reviews, 7(10), 1493-1503.
[62] Vistro, D. M., Rehman, A. U., Farooq, M. S., Abid, A., & Idrees, M. (2020). A survey ON the role OF security and integrity issues IN cloud. Journal of Critical Reviews, 7(10), 1456-1469.
[63] Vistro, D. M., Rehman, A. U., Farooq, M. S., Abid, A., & Idrees, M. (2020). A survey ON the role OF security and integrity issues IN cloud. Journal of Critical Reviews, 7(10), 1456-1469.
[64] Naeem, A., Farooq, M. S., Khelifi, A., & Abid, A. (2020). Malignant melanoma classification using deep learning:

datasets, performance measurements, challenges and opportunities. IEEE Access, 8, 110575-110597.

[65] Farooq, M. S., Khan, M., & Abid, A. (2020). A framework to make charity collection transparent and auditable using blockchain technology. Computers & Electrical Engineering, 83, 106588.

[66] Vistro, D. M., Rehman, A. U., Abid, A., Farooq, M. S., & Idrees, M. (2020). A ROLE OF NETWORKING TECHNOLOGIES BASED IOT WITH RESEARCH sCHALLENGES. Journal of Critical Reviews, 7(9), 1673-1679.

[67] Tehseen, R., Farooq, M. S., & Abid, A. (2020). Earthquake prediction using expert systems: a systematic mapping study. Sustainability, 12(6), 2420.