Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5730196, 8 pages
https://doi.org/10.1155/2022/5730196

Research Article

HeteroFL Blockchain Approach-Based Security for Cognitive Internet of Things

Shivani Wadhwa,[1] Shalli Rani,[1] Gagandeep Kaur,[2] Deepika Koundal,[3] Atef Zaguia,[4] and Wegayehu Enbeyle[5]

[1]*Chitkara University Institute of Engineering and Technology, Rajpura 140401, India*
[2]*Department of Computer Science, Punjabi University, Patiala 147001, India*
[3]*Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India*
[4]*Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. BOX 11099, Taif 21944, Saudi Arabia*
[5]*Department of Statistics, Mizan-Tepi University, Tepi, Ethiopia*

Correspondence should be addressed to Wegayehu Enbeyle; wegu0202@gmail.com

Received 21 October 2021; Revised 22 December 2021; Accepted 12 January 2022; Published 7 March 2022

Academic Editor: Celimuge Wu

Cognitive learning is progressively prospering in the field of Internet of Things (IoT). With the advancement in IoT, data generation rate has also increased, whereas issues like performance, attacks on the data, security of the data, and inadequate data resources are yet to be resolved. Recent studies are mostly focusing on the security of the data which can be handled by blockchain. Blockchain technology records the learned data into the block which is generated after completing proper consensus mechanism. In this paper, Hetero Federated Learning approach is used to apply cognitive learning on data produced by Internet of Thing devices. Security on cognitiveIoT data is provided by blockchain using Proof of Work consensus mechanism. By applying blockchain over heteroFL approach, we have conducted various simulations to check the performance of our proposed framework. Parameters taken into consideration during performance evaluation are effect of number of blocks on memory utilization and impact of data sample size on accuracy according to different learning rates.

1. Introduction

Previous Google chief director, Eric Schmidt made this striking IoT forecast: "The Internet will vanish. There will be numerous IP addresses, such countless gadgets, sensors, things that you are wearing, things that you are cooperating with, that you will not detect it. It will be important for your essence constantly." In-numerable efforts have been done from academia community, network providers, service providers, and various standard developing organizations, to provoke the growth of IoT devices [1]. It is expected that greater than 64 B devices based on IoT will exist worldwide by 2025. Most focused areas of research include networking, security, computations, communication, and energy harvesting but without cognitive ability, i.e., without brain, IoT seems awkward [2]. Entitling high level intelligence into the IoT gives rise to Cognitive Internet of Things [3].

Cognitive Internet of Things (CIoT) is a new paradigm, where physical or virtual things are connected with least human interruption. The communication with the things occurs by utilizing the approach of understanding. Understanding can be done from the actual climate, sensed data, and social communities. They store the gained connotation and additional data gathered in form of data sets and adjust to changes by means of computation and resource efficient algorithms for decision making. CIoT assists in bringing together physical world with the social world in an intelligent manner. It includes smart learning, smart resource allocation, spectrum sensing, capturing high precision data, smart service provisioning, and information

processing. Figure 1 illustrates the smart features that can be incorporated in the CIoT.

Smart data being produced by smart devices may suffer from security attacks like denial of service (DoS), physical attacks, malware, and malicious data injection [19]. Traditional machine learning approaches may not provide prevention from such attacks. Federated learning is a recent approach which learns from the dispersed data by incorporating collaborative models that are embedded in the local nodes. This approach learns iteratively till it reaches the threshold value set by the global model. Hetero Federated learning (HeteroFL) models are designed for devices that need different computation requirements and communication abilities.

With the rapid development of new technologies, the data generation rate has also increased. As the number of devices is increasing, the data production rate will also increase. It is of utmost importance to provide security to the users who are relying on the data produced by IoT devices. Lot of work is done in the field of research of IoT security [4]. However, few areas of research in IoT security are still unexplored. Meanwhile, as an arising innovation, blockchain innovation steadily stirs consideration of the scholarly community and industry. Blockchain innovation depends on a decentralized shared organization, based on cryptography, time-managed information of all events, well-defined consensus mechanisms, and with proper traceability and check of information to be stored.

Cognitive computing is assisting a lot in making IoT become smarter by providing human intelligence to the systems. However, privacy leakage of heterogeneous clients of IoT is not addressed by most of the technologies developed so far. In our proposed framework, cognitive computing is done by using heterogeneous federated learning to serve the needs of heterogeneous IoT clients. However, poisonous attacks can also be done on federated learning which will degrade the performance of the system [5]. Hence, integration of blockchain is done to protect the system from attacks and make the system more secure.

The structure of this paper is organized as follows. In section 2, related work is discussed. Then, the proposed cognitive learning through hetero federated learning and privacy through blockchain is presented in section 3. Section 4 discusses the performance evaluation parameters. Conclusion and future work are mentioned in section 5.

2. Related Work

In last few years, cognitive computing in Internet of Things has gained momentum in different ways. Various technologies collaborated with this are federated learning and blockchain. To guarantee the intelligent sensing of data, the Quality of Information Coverage (QIC) fulfillment metric is utilized to decide how gathered information tests can fulfill CIoT necessities. Experiments conducted in this model proved the accuracy of the QIC algorithm [7]. Hierarchical architecture is proposed for the heterogeneous IoT system based on blockchain [8]. Content caching

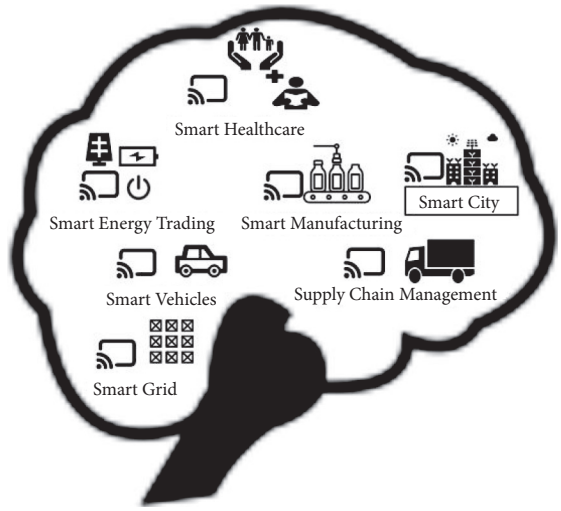

Figure 1: Cognitive internet of things.

architecture is proposed for the interaction between different vehicles and Road Side Units. Blockchain technology is also adopted to provide trust among the users which are connected to each other [9]. Edge networks are used to facilitate blockchain in vehicular decentralized environments. The selected edge nodes perform the task of maintaining blockchain. Selection of edge nodes is done by considering the velocity, distribution, and link of the vehicles. The proposed method provides improved performance in block dissemination for the implementation of blockchain in vehicular decentralized environments [10]. Authors highlighted that future research area will be to improve protocols of vehicular IoT which can support blockchain and also to frame efficient blockchain which can satisfy the essential requirements for the vehicular IoT [11]. Multichannel blockchain architecture is proposed for Internet of Vehicles where optimization of all channels is done by using vehicle density as well as based on requirements of applications. The proposed method improves the latency, transaction success ratio, and through put for varying number of vehicles [12]. The decentralized model for huge data based on cognitive processing, federated learning, and blockchain together is fostered. Blockchain empowered federated learning assists fast assembly with high-level verifications and selection of members [13]. To maximize the throughput, transmission scheduling for CIoT based on Q-learning approach is proposed. A Markov choice interaction-based model is detailed to portray the state transformation of the framework [14]. Cognitive computing technologies with IoT provide solutions to many existing challenges like big sensory data, efficient computation at CIoT edge, and various data sources [15]. Energy and spectrum efficiency are considered as very important parameters in CIoT. Metric is identified which provides the characteristics of network design space [18]. To increase the network utilization and throughput, the hybrid model is proposed for energy constraint devices and data aggregation of IoT devices. Deep Reinforcement Learning is applied with the

Double Q-learning algorithm to provide optimization using multiobjective ant colony optimization (MOACO) and greedy method techniques [19]. Internet of Multimedia Things based services are provided by the proposed algorithm, i.e., cognitive-based middleware for private data mashup (CMPM). Privacy issues are taken into consideration to provide proper environmental monitoring of data [20]. Table 1 presents the work done by different researchers in the field of cognitive IoT.

Although many studies are focusing on the integration of blockchain in IoT, blockchain in cognitive learning, and cognitive learning in IoT, there arises a need to solve the problem of heterogeneous IoT clients by incorporating cognitive learning and blockchain which can provide improvement in accuracy, learning rate, and latency.

Due to limited research carried out for security of IoT data produced by heterogeneous clients using HeteroFL, the research in this area is in its infancy. Therefore, this paper focusses on providing security to heteroFL-based cognitive learned data using blockchain.

3. Blockchain-Based Privacy on Cognitive Learned Data

Different applications of IoT involve variety of clients because of connectivity of heterogeneous devices. As different clients possess varying computation and capabilities of communicating with each other, they are assigned different complexity levels. First, the learning takes place on their respective local model and then the aggregation of all parameters of local models gives rise to parameter of the single global model. In our proposed framework, the cognitive model uses heterogeneous federated learning for training of the IoT data and then the trained data are secured by using blockchain.

3.1. Cognitive Learning Based on HeteroFL. Mobile devices, Gaming, and IoT devices generate huge amount of data. Based on cognitive computing, models can be made to store the data and then train the models locally. Federated learning (FL) is an approach of machine learning where parameters of local models are trained and their aggregation produces the global model which is independent of raw data. Generally, local models and global model share the same architecture. However, there can be various scenarios where miscellaneous types of local models will exist with the wide range of computing complexities. To meet the requirements of heterogeneous clients of IoT devices, another unified learning system named HeteroFL is used to outfit the entirely different computations and their communication abilities [6].

The process of training global model is done from local data $\{x1, \ldots, xn\}$ available at heterogeneous IoT devices. Local model parameters are expressed as $\{w1, \ldots, wn\}$. The model averaging of the local parameters is done to find the global parameter wg. This process is done in various iterations, and wg calculated at ith iteration is passed on to the local parameters of $(i+1)th$ iteration.

For effective cognitive learning to take place, size of network can be modulated by changing width of the network. This can help in decreasing the local parameters, whereas architecture of local and global parameters remains in the same model class. This also improves the stability of aggregation in the global model. In heteroFL, selection of global parameters is done based on the size of input channel (ig), output channel (og), and computation complexity level (c). Figure 2 shows the federated learning approach with various complexity levels of computations on the data produced by heterogeneous IoT devices. Calculation of shrinkage ratio plays very important role for hidden layers. Equations of shrinkage ratio of output channel are expressed as mentioned in the following equation:

$$s1 = \left(\frac{o_l^{c+1}}{og}\right)^{1/c}. \tag{1}$$

Formula for shrinkage ratio of input channel is shown in the following equation:

$$s2 = \left(\frac{i_l^{c+1}}{ig}\right)^{1/c}. \tag{2}$$

For simplification, let $s1 = s2 = s$.

Shrinkage ratio of local model parameter is mentioned in the following equation:

$$SR = w_l^c = wg * s^{2(c-1)}. \tag{3}$$

According to the calculated potential of the local model parameter, global model parameters can be constructed based on allocated subsets. The concept of set difference is mostly used in the calculations of the global parameter. Figure 3 shows different regions according to set differences. According to Figure 3, total clients $m = 6$ are shown. Here, 3 clients are of complexity level 3 (represented by m_3 in red region), 2 clients are of complexity level 2 (represented by m_2 in yellow region), and 1 client is of complexity level 1 (represented by m_1 in blue region).

Aggregation of smallest local model parameter (red region) is done as follows:

$$w_l^3 = \frac{\left(w_1^3 + w_2^3 + w_3^3\right)}{3}. \tag{4}$$

Calculation of subset of yellow region is done as follows:

$$w_1^2 - w_1^3 = \frac{1}{(m - m_3)} * \sum_{m=1}^{m-m_3} w_1^2 - w_1^3. \tag{5}$$

Calculation of subset of blue region is done as follows:

$$w_1^1 - w_1^2 = \frac{1}{(m - m_2 - m_3)} * \sum_{m=1}^{(m-m_2-m_3)} w_1^1 - w_1^2. \tag{6}$$

Calculation of subset of global model parameter is done as follows:

Table 1: Related work in CognitiveIot and Blockchain.

Ref. no	Parameters	Technology used	Application	Proposed model	Future scope
[7]	Information density, price, collection of data samples	Non-cooperative game	Intelligent sensing intelligence system	Quality of information coverage algorithm	Considering privacy for the growth of internet of things
[16]	Smart contract	Cognitive engine for machine translation, blockchain, intrusion detection	Shopping center	Cognitive recommender system	Applicability of proposed framework for web of things
[9]	Cache hit rate and robustness	Caching strategy, deep learning and machine learning algorithms	Internet of vehicles	Blockchain and cognitive-engine-enabled content caching strategy	—
[17]	Average delay, processing time	Convolutional neural networks (CNN), smart contract, machine learning algorithms	Sharing economy services in mega smart cities	MEC-based sharing service economy system, which includes the blockchain	Testing different sharing economy cases at a bigger level
[18]	System utility, no. of average packet loss	Markov decision process	Wireless data	Q-learning algorithm and stacked autoencoders deep learning model	Process to create more relays
[18]	Energy and spectrum efficiency	Dynamics of spectrum sharing and energy harvesting	Solar energy harvesting	Cloud enabled CIoT platform	—
[19]	Energy and throughput	Deep reinforcement learning and double Q-learning algorithm	—	Multiobjective ant colony optimization (MOACO)	Considering security parameters

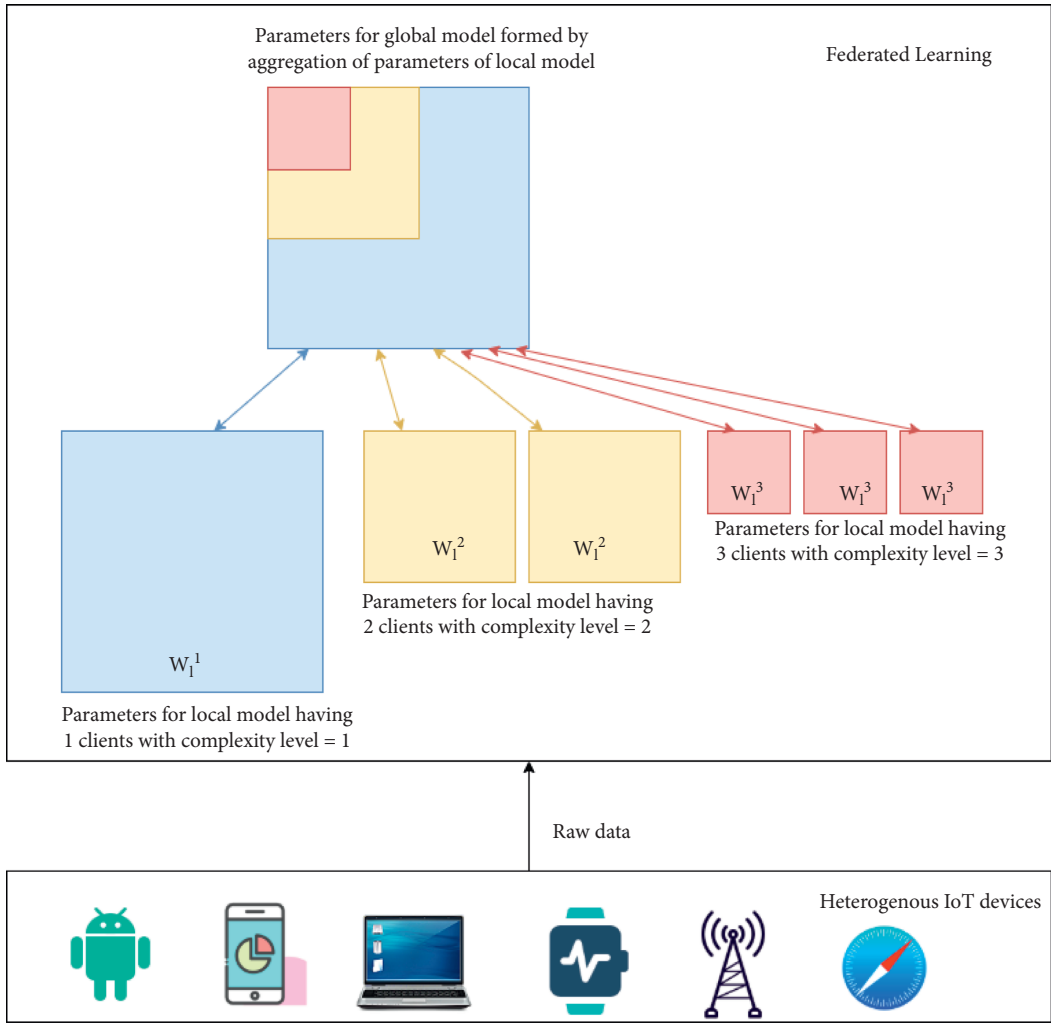

Figure 2: Federated learning from data produced by IoT devices.

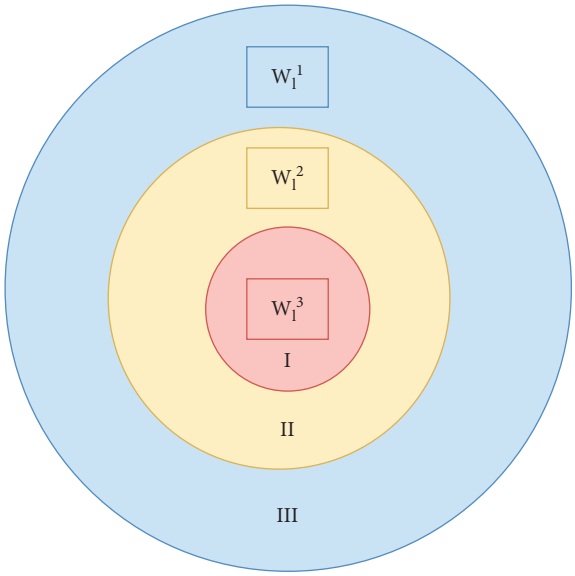

Figure 3: Venn diagram of different complexity levels.

$$w_g = w_1^3 \cup \left(w_1^2 - w_1^3\right) \cup \left(w_1^1 - w_1^2\right). \tag{7}$$

Aggregation of all those clients is done whose parameter is the part of the parameter matrix. Hence, model having intermediate complexities contains the parameters completely aggregated with the bigger models whereas moderately with the smaller models. Also, aggregation is more in case of smaller local models which can benefit global model. The data stored at the global model become the learning part of the cognitive learning. Algorithm 1 and Algorithm 2 are mainly designed for applying cognitive learning using heteroFL and sending client updates.

3.2. Blockchain on Cognitive Learned Data. Blockchain assumes a significant part to protect the performance of cognitive learned data. As these data will be used for making further decisions, it is very important to provide privacy to these data. Important characteristics of blockchain-like immutability, tamper-resistant, decentralized, pseudonymous identity, and so on are the contributing factors of security and privacy.

This subsection explains the role of blockchain to the data stored in a global model. Here, blockchain guarantees the security of the global model parameters by storing the learned data into the blocks [21]. Here, blockchain guarantees the security of the global model parameters by storing the learned data into the blocks. The framework of the blockchain of our proposed model is the same as that of the basic blockchain. Figure 4 explains the task of process of computing block. All blocks consist of previous hash, a hash of the current block, timestamp, nonce, and data field which contains cognitive learned data. The first block is the genesis block whose previous hash field contains all zeroes. All blocks are cryptographically linked to each other through the hash of the previous block. A very minute change in any one of the fields of the block can change the hash of the entire block. Applicability of the consensus algorithm on the block completes the process of verification and validation of the block and then appends the block to the distributed blockchain. The Proof of Work (PoW) consensus algorithm is used in our approach. The miners keep on trying to create the random nonce until they reach the constraints of the target nonce [22]. Once a miner gets the desired nonce, miner obtains the authority of broadcasting the block as a new block to the distributed blockchain. All miners will append the new block to their blockchain, which makes the blockchain consistent. Algorithm 3 explains the procedure followed by miners to compute block by completing the task of nonce calculation.

4. Implementation and Performance Evaluation

Amazon AWS platform has been used which includes different types of 1000 nodes. Some of these nodes are SPV nodes and few are full nodes. Nodes are configured with a Linux Virtual Machine. The privacy of the learned data is tested on the testing environment. Testing was done in 4 sets by changing the number of clients according to different complexity levels. Accuracy, latency, and block generation rate are evaluated to check its performance. The SHA-256 algorithm is used to compute the ID of IoT devices added in this framework. Computed ID is 16 bytes long. All IoT devices are assigned public key and private key for interaction with the other devices and providing secure signatures.

The IoT devices connected to the framework are known by 16 bytes ID. HeteroFL approach is applied for successful cognitive learning to take place. HeteroFL technique minimizes the computation as well as communication complexity of complete process. Training of local models is done in lesser number when compared with the global model. Private Ethereum platform is used for performing blockchain computations. Core i7-8565U CPU 1.80 GHz, 1992 Mhz, 4 Core(s), and 8 Logical Processor(s) are used for implementation. The performance of our proposed scheme has been evaluated for different parameters such as accuracy and memory utilization [23].

Memory utilization of different sizes of blocks is considered, i.e., 10 transactions per block, 20 transactions per block, and 30 transactions per block. Memory utilization mainly depends on the size of basic information of block excluding transactions data and size of the transactions. The data produced by the global models are stored in the blocks. However, to evaluate the appropriate number of transactions to be stored in the block, evaluation of this parameter is done. Figure 5 presents the reduction in memory utilization with the increase in the transactions per block. Experiment proves that less number of transactions per block will consume less memory.

The performance is also evaluated at different learning rates, i.e., 0.005, 0.05, and 0.5. Good accuracy is observed at large data sample sizes also as shown in Figure 6. It is clear from the graph that initially learning is done linearly in all three cases and then it becomes constant, but the best

(i) **Variables**: $w1, wg, s, p, m$
(ii) **Procedure input**: data generated by heterogeneous IoT devices, X_i, and local clients with the data, x_i
(iii) Begin: Initialization of global model parameter, wg, and local clients with the data, x_i
(iv) **for** each round of data production $t = 0, 1, 2, \ldots$ **do**
(v) S ← random set of active clients
(vi) **for** all clients, $k \in S$
(vii) Compute complexity level 'c' based on local information
(viii) Compute output channel shrinkage ratio ($s1$), input channel shrinkage
(ix) ratio ($s2$) and hidden shrinkage ratio (SR)
(x) **End**
(xi) **for** all complexity levels, c **do**
(xii) Compute global model parameter using aggregation of local model parameter
(xiii) **end**
(xiv) **end**
(xv) End

Algorithm 1: Algorithm for cognitive learning using HeteroFL.

(i) Variables: T, l, η
(ii) Procedure input: wk, Xk
(iii) Begin: $B_k \leftarrow$ splitting of local data X_k into various batches of size, T
(iv) After regular interval of time, t do
(v) for batch $bk \in T$ do
(vi) for all clients, $k \in S$
(vii) $l_k \leftarrow \eta \Delta l(Wk, bk)$
(viii) $Wk \leftarrow Wk - lk$
(ix) ratio ($s2$) and hidden shrinkage ratio (SR)
(x) End
(xi) End

Algorithm 2: Blockchain protected cognitive learned data.

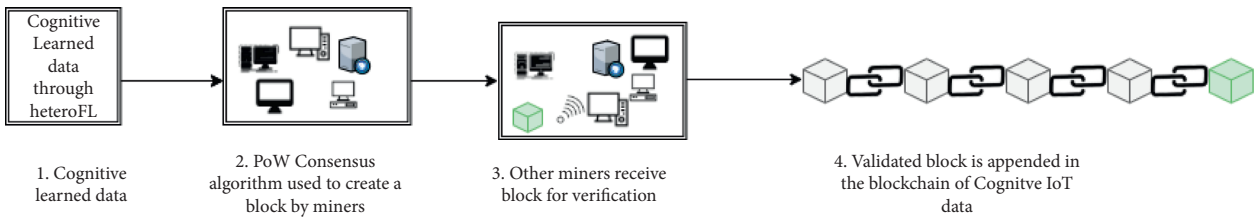

Figure 4: Blockchain protected cognitive data.

(i) Variables: b_i
(ii) Procedure input: cognitive learned data, Y_i, and Miners, M_i
(iii) Begin: Fetch cognitive learned data, Y_i
(iv) while Y_i do
(v) Upload Y_i of fixed size to Miners M_i
(vi) If M_i finds the nonce
(vii) Block b_i of that data is created
(viii) b_i is appended to all local ledgers
(ix) Computation done by other miners is dropped
(x) end
(xi) Winning miner M_i gets the incentive
(xii) Compute global model parameter using aggregation of local model parameter
(xiii) end
(xiv) End

Algorithm 3: Blockchain protected cognitive learned data.

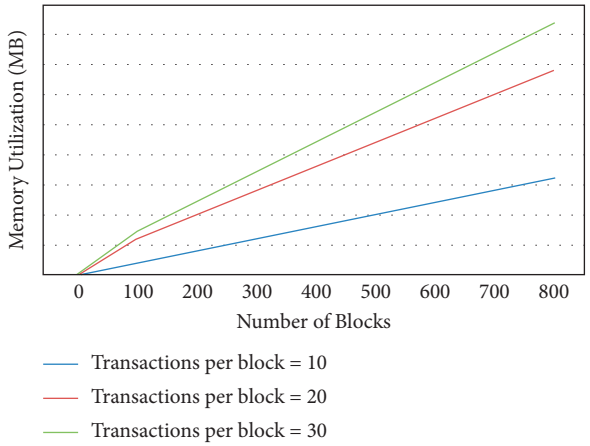

Figure 5: Effect of number of blocks on memory utilization.

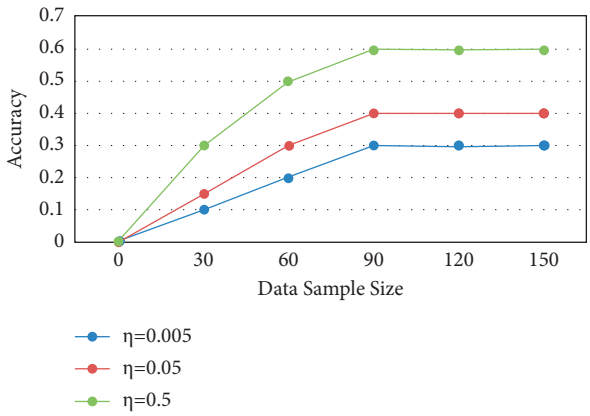

Figure 6: Impact of data sample size on accuracy according to different learning rates.

accuracy is observed in case of high learning rate. Similar graph is expected in case of larger data sample sizes (in thousands). This also guarantees high scalability.

Figure 7 presents execution time taken for the creation of blocks with 10, 20, and 30 transactions per block using one thread. Figure 8 presents execution time taken for the creation of blocks with 10, 20, and 30 transactions per block using two threads. Figure 9 presents execution time taken for the creation of blocks with 10, 20, and 30 transactions per block using four threads. Figure 10 presents execution time taken for the creation of blocks with 10, 20, and 30 transactions per block using eight threads. As the count of blocks rises with rise in number of transactions per block, the execution time also increases whereas the increase in number of threads reduces the execution time. Figure 9 shows very less execution time as the number of threads is four and the number of cores of our system is also four. Evaluation of this parameter proves that there is a dependency on the system's configuration for the execution time of a block. Less execution time will ultimately improve the performance of the network by updating the blocks in a blockchain very quickly, which will make the system consistent with the more recent learned data in its ledger.

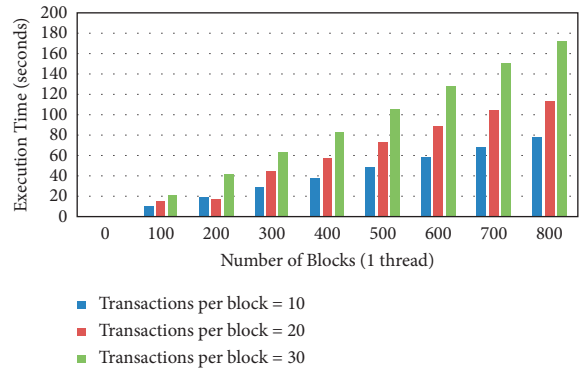

Figure 7: Execution time with 1-thread.

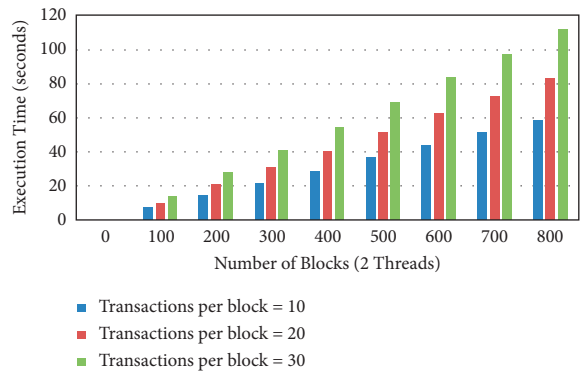

Figure 8: Execution time with 2-threads.

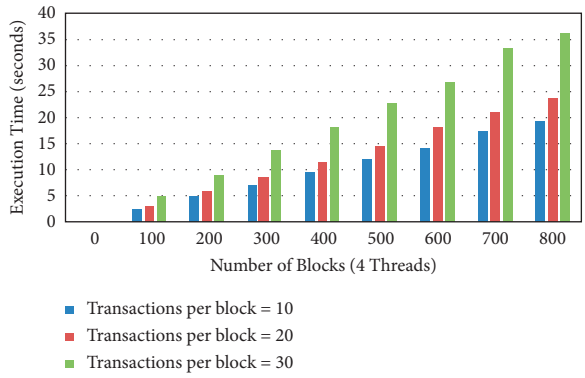

Figure 9: Execution time with 4-threads.

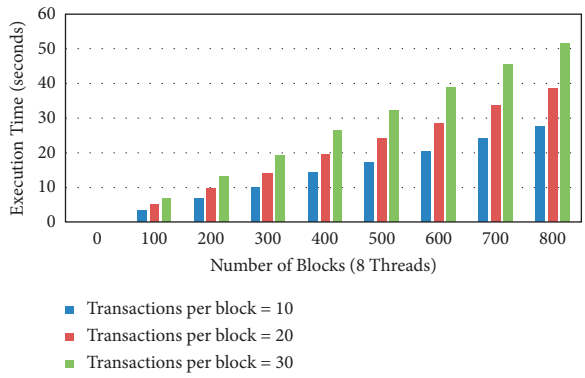

Figure 10: Execution time with 8-threads.

5. Conclusion

We propose heteroFL for cognitive learning to take place from the raw data produced by IoT devices. In this approach, local models are trained by exploiting their full capabilities, and then their aggregation is done to infer an individual global model. HeteroFL takes less number of iterations to produce best results. Blockchain is employed to provide the privacy to the learned data. The PoW consensus algorithm is used to verify and validate a block. From the experiments, accuracy at different learning rates and memory utilization at different number of transactions per block are computed. This approach achieves good results for heterogeneous clients of IoT devices. In future, multimodal learning can be used for addressing heterogeneous learning.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by Taif University Researchers Supporting Project Number (TURSP-2020/114), Taif University, Taif, Saudi Arabia.

References

[1] P. Datta and B. Sharma, "A survey on IoT architectures, protocols, security and smart city based applications," in *Proceedings of the 2017 8th in- Ternational Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–5, Delhi, India, 2017 July.

[2] R. Chhabra, S. Verma, and C. R. Krishna, "A survey on driver behavior detection techniques for intelligent transportation systems," in *Proceedings of the 2017 7th International Conference on Cloud Computing, Data Science Engineering-Confluence*, pp. 36–41, Noida, India, 2017 January.

[3] F. Li, K. Y. Lam, X. Li, Z. Sheng, J. Hua, and L. Wang, "Advances and emerging challenges in cognitive internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5489–5496, 2019.

[4] Y. Qian, Y. Jiang, J. Chen et al., "Towards decentralized IoT security enhancement: a blockchain approach," *Computers & Electrical Engineering*, vol. 72, pp. 266–273, 2018.

[5] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: analysis and design challenges," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4734–4746, 2020.

[6] E. Diao, J. Ding, and V. Tarokh, "HeteroFL: computation and communication efficient federated learning for heterogeneous clients," arXiv preprint arXiv:2010.01264, 2020.

[7] Y. Liu, A. Liu, T. Wang, X. Liu, and N. N. Xiong, "An intelligent incentive mechanism for coverage of data collection in cognitive Internet of Things," *Future Generation Computer Systems*, vol. 100, pp. 701–714, 2019.

[8] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, "Blockchain for managing heterogeneous internet of things: a perspective architecture," *IEEE network*, vol. 34, no. 1, pp. 16–23, 2020.

[9] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, "Blockchain-based privacy-aware content caching in cognitive internet of vehicles," *IEEE Network*, vol. 34, no. 2, pp. 46–51, 2020.

[10] S. Buda, C. Wu, W. Bao et al., "Empowering blockchain in vehicular environments with decentralized edges," *IEEE Access*, vol. 8, pp. 202032–202041, 2020.

[11] C. Peng, C. Wu, L. Gao, J. Zhang, K.-L. Alvin Yau, and Y. Ji, "Blockchain for vehicular internet of things: recent advances and open issues," *Sensors*, vol. 20, no. 18, Article ID 5079, 2020.

[12] L. Gao, C. Wu, T. Yoshinaga, X. Chen, and Y. Ji, "Multi-channel blockchain scheme for internet of vehicles," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 192–203, 2021.

[13] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A blockchained federated learning framework for cognitive computing in industry 4.0 networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2964–2973, 2020.

[14] J. Zhu, Y. Song, D. Jiang, and H. Song, "A new deep-Q-learning- based transmission scheduling mechanism for the cognitive Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2375–2385, 2017.

[15] Y. Zhang, X. Ma, J. Zhang, M. S. Hossain, G. Muhammad, and S. U. Amin, "Edge intelligence in the cognitive internet of things: improving sensitivity and interactivity," *IEEE Network*, vol. 33, no. 3, pp. 58–64, 2019.

[16] A. M. Saghiri, M. Vahdati, K. Gholizadeh, M. R. Meybodi, M. Dehghan, and H. Rashidi, "A framework for cognitive Internet of Things based on blockchain," in *Proceedings of the 2018 4th International Conference on Web Research (ICWR)*, pp. 138–143, Tehran, Iran, 2018 April.

[17] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[18] A. Afzal, S. A. R. Zaidi, M. Z. Shakir et al., "The cognitive internet of things: a unified perspective," *Mobile Networks and Applications*, vol. 20, no. 1, pp. 72–85, 2015.

[19] S. Vimal, M. Khari, R. G. Crespo, L. Kalaivani, N. Dey, and M. Kaliappan, "Energy enhancement using Multiobjective Ant colony optimization with Double Q learning algorithm for IoT based cognitive radio networks," *Computer Communications*, vol. 154, pp. 481–490, 2020.

[20] A. M. Elmisery, M. Sertovic, and B. B. Gupta, "Cognitive privacy middleware for deep learning mashup in environmental IoT," *IEEE Access*, vol. 6, pp. 8029–8041, 2017.

[21] J. Ren, J. Li, H. Liu, and T. Qin, "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT," *Tsinghua Science and Technology*, vol. 27, no. 4, pp. 760–776, 2021.

[22] L. Li, P. Shi, X. Fu, P. Chen, T. Zhong, and J. Kong, "Three dimensional Tradeoffs for consensus algorithms: A review," *IEEE Transactions on Network and Service Management*, 2021.

[23] S. A. Kumar and J. Vassileva, "User acceptance of usable blockchain-based research data sharing system: an extended TAM-based study," in *Proceedings of the 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, IEEE, Los Angeles, CA, USA, 2019.