Blockchain-Enabled Technique For Privacy Preserved Medical Recommender System

Rajesh Kumar V[1], Vivek S[2], Nirmalkumar C[3], Manisakthi G[4], Rabbin M[5]
[1, 2, 3, 4, 5] Dept of Computer Science and Business Systems
[1, 2, 3, 4, 5] Sethu Institute of Technology, Pulloor, Kariapatti. 626 115, India

Abstract- *By employing blockchain's immutable ledger and decentralized architecture. Sensitive patient data is securely stored and accessed only by authorized entities through smart contracts. It guarantees that the model gradients which are trained by each node are not disclosed all through the universal training and modeling procedure. Considering that the model ensures that users can only obtain their necessary inquiries, neither medical data suppliers nor users can obtain access to raw data. The proposed technique guarantees that the model gradients which are trained by each node are not disclosed all through the universal training and modeling procedure. This makes the raw data inaccessible to either the health data provider or the user. Considering that the model ensures that users can only obtain their necessary inquiries, neither medical data suppliers nor users can obtain access to raw data. Thus, it reduces the issues of safeguarding medical data sets to the issues of securing data processing. Using numerical analysis and experiments the proposed technique is compared with other existing techniques, the result shows that the proposed system is efficient and secures recommender data management training and modeling technique and that it performs previously designed techniques as compared.*

Keywords- Blockchain, Privacy, SPK proof, Secret Key, De-centralized and Authentication

I. INTRODUCTION

A recommender system is a subclass of an artificial intelligent-based (AI-based) system for information filtering and prediction on a list of products for different organizations [1],[2]. Generally, such kinds of systems are common big data applications. On the internet of medical things system, several hospitals extensively utilize the recommender system to obtain excellent recommendations based on the interest and requests of their patients[3]. The recommender system can generate its recommendations through either collaborative filtering or content-based filtering. The former is a method of obtaining the list of predictions by establishing the interrelation between users' history and other users' interests, while the latter involves exploring both the user's profile and their corresponding items. Most hospitals and companies store users' confidential data and make use of collaborative filtering to achieve optimal recommendations.[4],[5],[6], [7],[8],[9],[10],[11],[12],[13],[14]In this kind of recommendation, the profiles of different users are designed from their respective histories coupled with the user's rating. Consequently, there is the possibility of having the issue of data privacy in an AI-based system. Recently, hospitals gathered and save a massive quantity of patient data for future recommendations, however, patients are concerned about the privacy of their confidential data which are stored on different platforms. a blockchain-based recommender and training system which is referred to as Secured Recommender and Training Technique, which locally stores data but uploads data directories and structures to the chain.

II. SYSTEM MODEL

As a result of the incorporation of cryptographic techniques and distributed algorithms, Bitcoin which is an offset of Blockchain technology is fundamentally a distributed system that is difficult to interfere with and upholds reliability without the need for a central control [15].Likewise, contractual algorithms are a vital aspect of blockchain technology and have been attracting cutting-edge research ideas [16], [17],a product of blockchain technology, operates as a distributed system, resistant to interference and without central control. Contractual algorithms drive innovative research in blockchain. Given the vulnerability of blockchain operations, extensive fault tolerance and privacy-enabled algorithms are necessary to protect transmitting nodes.

A.FEDERATED LEARNING AN RECOMMENDER SYSTEM DATA TRAINING AND MODELING

Federated learning (FL) allows machine learning models to learn from diverse datasets located in different places, such as local servers or data centers, without exposing the training data. [18] This approach securely stores confidential data locally, minimizing the risk of data breaches. FL enables multiple entities to collaborate on a universal model without centralizing training data. It addresses data breach challenges by enabling learning on end-user devices while ensuring data privacy. FL involves model modeling, training, and inference. In the process, ML models are trained

on local datasets, with errors corrected automatically. Parameters are periodically exchanged between local data centers without sharing data samples, enhancing data security. A shared global model is created, with features distributed to local data centers to integrate into their machine learning models.FL process topples the challenges of data breaches by permitting recurrent learning on end-user devices while guaranteeing that end-user data does not leave end-user devices [19]. Federated schools comprise model modelling and training and model inference [18]. A fundamental context for FL and centralized training is described in Fig.1.In the framework, conventional ML models are trained on local heterogeneous datasets. For instance, as users make use of an ML application, several errors could be spotted in the application's predictions and these mistakes are automatically modified. A local training dataset is generated in each user's connected device. Then, the parameters of the models are periodically switched over between these local data centers. Several models encrypt these parameters before sharing. However, local data samples are not exchanged. This enhances data security and cyber security. In the end, a shared global model is created, and the features of the global model are distributed to local data centers to incorporate the global model into their machine learning local models.

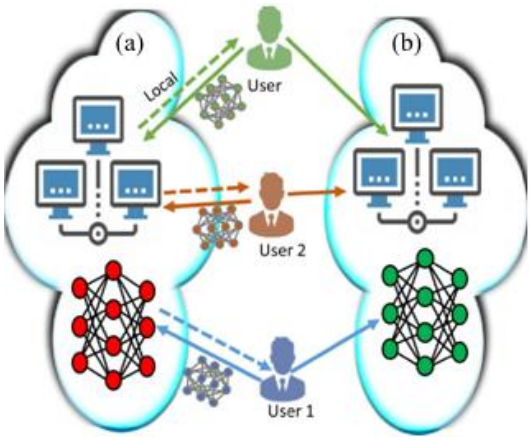

FIGURE 1. A fundamental framework for two different training systems: federated training and centralized training.(a)Federated Training. (b) Centralized Training.

III. SERTT DESIGN AND SECURITY MODEL

This section will address the SERTT framework to realize the core security features that were pointed out earlier. The four stages of the modules' exchanges include contract deployment, requirements matching, execution preparation, and contract execution.

A. CLASSIFIED SHAPLEY PROXY PROOF-OF-STAKE (CSPPoS) MECHANISM

In recommender system modeling and training, active participation of data providers in the data-sharing process is crucial for achieving optimal success. The study proposes a model called Classified Shapley Proxy Proof-of-Stake (CSPPoS), which combines Shapley values and Proxy Proof-of-Stake (PPOs) to ensure the interests of all participants and achieve consensus on the blockchain. In the proposed SERTT system, a classified proxy mechanism is employed, where the primary node's authority is no longer absolute, and its position can be challenged by other nodes through an election process. Each node vying for the primary node position demonstrates its qualifications by transmitting messages to other nodes. Once a consensus is reached among the majority of nodes, the operational node with the dominant log information is elected as the primary node

IV. PERFORMANCE OF SERTT MODEL

A. THE BASIC PROCEDURES OF FEDERATED TRAINING IN THE SERTT SYSTEM

In this section, the three vital security features on which the SERTT system is designed will be extensively discussed. All these features are targeted at safeguarding data against theft from nodes.

1) INITIALIZATION

The coordinators initialize system parameters for the public recommendation model of the blockchain during the installation process. The genesis block contains parameters {H, V, v, r, e, f, N, ζ}. In the second phase, contract deployment occurs, where coordinators can use the Enroll technique to create a long-term account (pl y = R y , cl y = G y) based on system features from the genesis block. At this stage, the Classified Shapley Proxy Proof-of-Stake (CSPPoS) Algorithm 1 is employed.

Input: mutual recommender data for nodes participating in
Declare: and as previous and current blocks, respectively
1. while in the proxy cycle do
2. Each participant casts their vote depending on the irrespective contribution.
3. Categorize the vote results to realize the list referred toas 'sorted_vote_list'.
4. Choose the X highest-voted candidates from the sorted_vote_list.
5. Acquire Y candidates from the sorted_vote_list → Candidates.
6. Shamble candidates → randomly disarrange candidates.
7. for select the stuffing node do

#P B ∗ (C B) → to obtain the slot
8. To get representative index slot → mod Y
9. if present node is index, then.
10. if the present node rank is manager, then.
11. Add the administrator's contribution level of FL to the record.
12. end if
13. Stored all candidate's contributions, authenticate

That it makes use of each.

The transmitted smart contract will be inputted to the blockchain mechanism the moment it is successfully approved by the proof procedure. In the third stage, both private and public keys are generated and shared. First, the public/private keys are generated as. {(δ,ρ),(X x PL ,X x CL),(P PL x ,P x CL),L = (L 1 ,L 2)} (1) for each user x, (x ∈ L,|L| = X), considering (δ,ρ) and L = (L 1 ,L 2)} as the private keys utilized in homomorphic hash and pseudorandom functions, respectively. Thus, the system utilizes (X x PL ,X x CL),(P PL x ,P CL x) to exploit the local gradient (x a) of the user x. Secondly, through a secure channel, the user x broadcasts the public key (X x PL ,X x CL) to the cloud server. Thirdly, broadcasted data from at least i users (which is denoted as L 1 ⊆ L) is received by the server slide. This point i represents the threshold the Shamir's i − out − of – X protocol utilized by the system. Else, stop the operation and restart again. Transmit {y,X y PL ,P PL y ,τ = sum} y ∈ L1 to respective users considering τ = sum the statistical tag to be estimated. For better understanding, a detailed description of all mathematical symbols is presented in Table 1.

TABLE 1. Description of mathematical symbols.

S/N	Symbols	Descriptions
1	(x_a)	Local gradient
2	$\{H, V, v, r, e, f, \square, \zeta\}$	Initially generated blocks
3	$L = (L_1, L_2)\}$	Private key for pseudorandom functions
4	(δ, ρ)	Private key for homomorphic hash
5	(X_x^{PL}, X_x^{CL})	Public key
6	i	threshold the Shamir's protocol
7	$\tau = \text{sum}$	Estimated statistical tag
8	cl_y	Secret key utilized to track record
9	$\frac{L_2}{L_3}$	Server-data broadcasting users
10	$L_4 \subseteq L_2$	User acquired data
11	(m, n)	Directed Edge between different tensor
12	Φ_n	Computational cost of every element
13	$-A(\Phi_{m,n})$	Number of floating-point activity

2) REGISTRATION FOR THE AGGREGATED RECOMMENDER MODEL

The system begins by retrieving basic settings from the blockchain, such as the default administrator (e.g., Alice). It then initiates the registration process for an Administrator by activating the long-term account established during initialization, using the Enroll command. This account is characterized by the public key (Ry) and the corresponding private key (Gy).similaryly,the registration process for a User follows the same steps as that of an Administrator. In this method, ownership of the long-term account is shared among administrators, serving solely for tracking purposes rather than executing transactions or acting as a proxy.As a result, the registration task is a one-time operation, and the generated long-term account \(Ry \) can be employed only once.In the proposed method, the ownership of the long-term account is mutual to the administrators, and it is only used for tracking and not for issuance of transactions or proxy.In the proposed method, the ownership of the long-term account is mutual to the administrators, and it is only used for tracking and not for issuance of transactions or proxy. Consequently, the registered task is only a one-time operation, and the generated long-term account pl_y can only be utilized once.

3) FEDERATED TRAINING GRADIENTS UPDATE

In this stage, the system checks if $L_3 \geqslant i$and $L_3 \subseteq L_2$. Assuming the expression is negative, stop operation and restart. Then, decrypt each;

$$\frac{P_{x,y} \forall y \in L_2}{\{x\}} \qquad (2)$$

as, $x||y||XxCL,y||\beta x,y \leftarrow$ AE.decLA.agree$PCLx,PPLy,$Px,y.

Proceed and transmit nXxCL,y|y ∈LL23o and βx,y| y ∈$L_3$to the cloud server. At this point, $_L^L3^2$ denotes the users who have broadcasted data to the server but withdrew prior to uploading data to the cloud server. Then, acquire data from at least i users which denotes $L_4 \subseteq L_2$. Else, stop operation and restart. Estimate $\beta_x \leftarrow$ C.recon$\beta_{x,yy} \in_L 4$,i and the Proof of accumulated gradients {W,Z,K,R,□) as follows.

$$W = \sum_{x=1}^{Y} W_x; \quad (3)$$

$$Z = \sum_{x=1}^{\chi^{x=|L_3|}} Z_x; \quad (4)$$

$$K = \sum_{x=1}^{\chi^{x=|L_3|}} K_x; \quad (5)$$

$$R = \sum_{x=1}^{\chi^{x=|L_3|}} R_x; \quad (6)$$

$$\delta = \chi_{x=|L^3|} \delta_x; x=1 \quad (7)$$

Then, send result to each of the user $\in L_4$ as;

$$B_{\text{result}} = \{\delta = \chi_{x=|L_3|} \alpha x, W, Z, K, R, \delta \quad (8)$$

4)VERIFICATION OF MODEL

In the verification process, the following generated parameters are check;

$$PA_{L1}(x) = (\gamma_x, v_x) \quad (9)$$

$$PA_{L2}(\tau) = (\gamma, v) \quad (10)$$

The system then calculates;

$$\mu = \chi \quad (\gamma_x \gamma + v_x v)\ x \in L_3 \quad (11)$$

and

$$\phi = a(h,k)^{\mu} \quad (12)$$

therefore, the system verifies;

$$(W,Z) = W, Z$$

$$a(W,k) = a(h,Z); a(K,h) = a(h,R),$$

$$\phi = a(W,k) \cdot a(K,h) \quad (13)$$

Assuming any of the above commands are invalid, the system rejects the result of the aggregation. If not, the obtained result is accepted, and the operation proceeds to the initial round.

5) DATA SORTING AND MANAGEMENT APPROACH USING REDMANA

The proposed SERTT model incorporates a key component called Recommender Data Management Neural Architecture (REDMANA), aimed at significantly reducing human intervention, especially in data management, model design, and modification processes. REDMANA introduces automated, process-driven, and efficient solutions for managing data. onenotable technique employed within REDMANA is neural architecture search, which involves automatically designing neural networks. This approach enables algorithms to construct high-performing network architectures based on sample datasets. These generated architectures often rival or surpass those designed by human professionals in certain tasks. Moreover, they can even identify network structures previously undiscovered by humans, thereby effectively minimizing the costs associated with implementing and utilizing neural networks. However directly applying neural architecture search to data sorting and management can lead to significant time and resource consumption. Therefore, REDMANA is proposed as a solution within the SERTT model to mitigate unnecessary expenditures of time and resources in these processes.on creating data sorting and management model. In a given structural search scenario, REDMANA targets at identifying the optimally performing training hyper-parameters. This study implements the frequently used cell-based architecture search environment.

A cell in this architecture is considered as a $Y-$ node coordinated acyclic graph which is completely connected to (DAG)$\{X_1, X_2, \ldots, X_Y\}$. Each node $X_n$accepts the dependent nodes as input and generates an output through a sum operation as follows.

$$Xm = \sum_{n<m}^{X} o^{(n,m)}(Xn) \quad (14)$$

Each node signifies a different tensor, and each directed edge (m,n) between $X_n$and $X_m$illustrates an operation $o^{(m,n)}$ which is realized from the equivalent operation search space O(m,n).This pruning process continues until the search space is reduced to only one hyperparameter. As a result, a classification sharing associated with the computational cost for every element in \(8n\) is introduced and presented as;

$$b\ \xi_{m,n} = \frac{\exp -A\ 8_{m,n}}{\sum_{n} \exp -A\ 8_{m,n}} \quad (15)$$

Considering the quantity of floating-point operations as a function \(-A \), with dimensions \(8m, n \), the operations produce a set \(J \) with diverse subsets \(

j_{\text{ref}}, j_{\text{pos}} \), and \(j_{\text{neg}} \). These subsets are continuously iterated over in the initial operations \(L \) for 30 times, serving as a training category for the Random Forest (RF). The RF tree comprises a group of \(J \) which also includes auxiliary samples from \(J \).

$$N_y = P_y K P_y - P_{\{pos,y\}} K P_{\{pos,y\}} - P_{\{neg,y\}} K P_{\{neg,y\}} \quad (16)$$

$$K P_y = \frac{P \left(j_{ref,n} - j_{ref,Py2} \right)}{j_{ref} n \in P_y} \quad (17)$$

$$|P_y|$$

2) DATA SORTING AND MANAGEMENT PROOF ANALYSIS

The data and model used in this study are obtained from the previous part through the federated average method. The overall performance of the data sorting and management proof is described in Algorithm 3.Additionally,the study incorporates a Weight of Proof (WOP) mechanism in coding the original autonomous variables into the algorithm. These variables need to be discretized or grouped, and the WOP value for each group \(N \) can be estimated post-discretization. The detailed process is outlined in Algorithm 2.as:

V. SECURITY ANALYSIS

In this system, the entirety of user data is not directly stored on the blockchain. Instead, only data indices are saved on the chain, while the complete model is transmitted instead of the raw data. Furthermore, an unknown secret key associated with the transmitter's secret address provides a Secure Private Key (SPK) proof, which is leveraged within the SERTT mechanism to facilitate secure communications.The proposed SERTT system offers several security features and mechanisms to ensure privacy protection and optimal data security within the blockchain Distributed Secure Mechanism (DSM) application

1. Privacy Mechanism: Unlike previous approaches that primarily utilized blockchain for data transmission, the SERTT system ensures optimal data security by not storing the entire user data directly on the blockchain.

2. SPK Proof and Secret Key: SERTT mechanism to chain communications securely, adding an additional layer of security to the communication process.

3. Credential Confirmation and Identity Validation:. This validation process maps a long-term address to the participants' actual identity, enhancing trust and security within the system. In case of malicious operations, the administrator can use trace and find operations via smart contract's secret code to recover the long address and corresponding credentials.

4. Trust Devolution: CSPPoS (Cooperative Subjective Proof of Stake) proxy mechanism within the federated learning process to appoint a provisional trusted manager for cooperation. This approach helps in reducing the content and mitigating risks associated with data leakage.

Overall, the SERTT system employs a combination of privacy mechanisms, SPK proofs, credential confirmation, and trust devolution to enhance security and privacy within the blockchain DSM application, thereby ensuring optimal data security and privacy protection.

SERTT Framework

Input: B A = φ;B 2A = φ;B 3A = φ
Set: η(n) and λ(n) as initial data escalation factors
Declare: B l as DSM network trained periods Train
w,z DSM models
Declare: DSM training functions from w period
for the sum of z − w periods k = φ;R = φ
Declare: k to represent the network history group
and Q as the hyper-parameters group while |Q A | & lt;
lowest
N in it do
Trim and filter redundant hyper-parameters
Remove the threesome loss parameters of
the
DSM valuation focus Q i
Add Q i to Q
DSM = Random architecture()
DSM.accuray = Train (DSM, 0, A)
Add DSM model to B A and k end
while
for n = 1 → X do
for n = 1 → X0 do
Randomly display DSM model from
BA;B2A;B3A
offspring model = Random mutate of DSM model
off spring.accuray = Train (offspring model, 0, A)
Add offspring model to B A and k end

for
for DSM model = top 1 to X 2 DSM model in B A do
DSM model.accuracy = Train(DSM model, 2A,3A)
Transfer DSM model B 2A → B 3A end
for
Remove dead DSM model from B A ;B 2A ;B 3A
end for
return optimal M DSM models in k, M = 1 in the system model

The secret code which is generated by the data vendor, thus making it difficult for an attacker to either ‘‘poison’’ or obtain access to the model by modifying the directory, likewise, the data owner cannot disagree about the data considering that it is sealed with its own secret key.

VI. PERFORMANCE ANALYSIS

The proposed SERTT system is evaluated and the result of its design is demonstrated in this section.

A. DATASET AND EXPERIMENTAL BACKGROUND

This study utilized two datasets as provided from certified pharmaceutical web sites known as Druglib.com and Drug.com. The datasets contain patient recommendations

Algorithm 3 Data Sorting and Management Proof Technique
Input: DSM records which are shared using federated training model

1. Estimate the user’s probability of default d 1 = ,d = $\overline{\quad}$ $\overline{\quad}_z$. $\overline{\quad\quad}$ $1-d$ $1+a$
2. Compute the weight of proof WOP_n= In$^{m\ n}_{x}\,n/^{m}_{x}i^{i}$
3. Compute the DSM groups by the data record record= $M-N$ log(odd c)
4. group(c) = ($c \geqslant record_o$) + ($c \geqslant record_1$) + ... + $c \geqslant cy-1$
5. Transform all individual gate circuit to anR1CS constraint. Create these constraints. using Lagrange interpolation, and then utilized the no-knowledge evidence technique to construct proofs.
6. Utilize Lagrange interpolation algorithm to convert the R1CS constraints to Polynomial function
7. **return** data sorting and management proof outcomes

B. ANALYSIS AND COMPARISON OF SYSTEM PERFORMANCE

In Table 2, the percentage of the values of contribution which are generated from the federated learning of the contributors is presented. The first three rows shows the no-attacked case of the local dataset, while the last row indicates a case where even though there are four data providers, but the dataset of the last data provider Z is attacked.

TABLE 2. Contribution portion comparison for varying federated learning.

Types of Federated Learning	Contribution (%)			
	W	X	Y	Z
Two-party	42.66	49.50	_	_
Three-party	29.54	31.32	33.44	_
Four-party	22.65	25.32	20.20	23.12
Sum	62.45	60.50	60.21	-85.82

The performance of the recommender data management proof and DSM proof algorithm were analyzed using six 64-bit Ubuntu18 servers which are powered with 8GB of RAM each and 8-core CPUs. In a setting with a total of 30 nodes, each machine propelled The description in Fig.2 shows that the trained model is basically the same as if the models were federated provided that each party reliably supplies their respective local data for federated learning.Furthermore, the performance of the recommender data management proof and DSM proof algorithm were analyzed using six 64-bit Ubuntu18 servers which are powered with 8GB of RAM each and 8-core CPUs. In a setting with a total of 30 nodes, each machine propelled

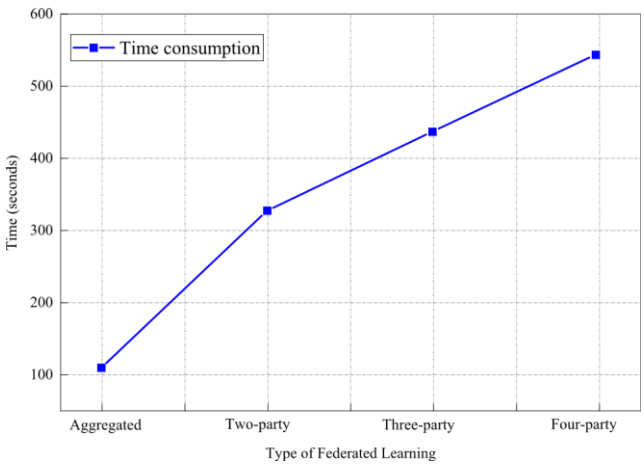

FIGURE 2. Comparison of consumption time for different types of federated learning.

The experimental results which illustrate the performance comparison result of the proposed CSPPoS are shown in

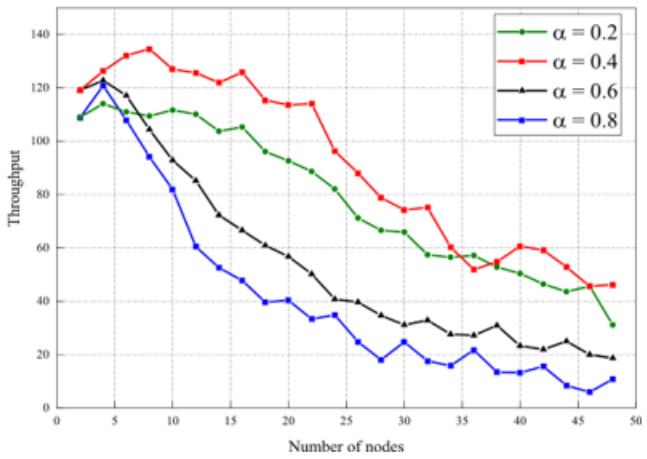

FIGURE 3. Performance comparison of throughput CSPPoS algorithm using different values of α.

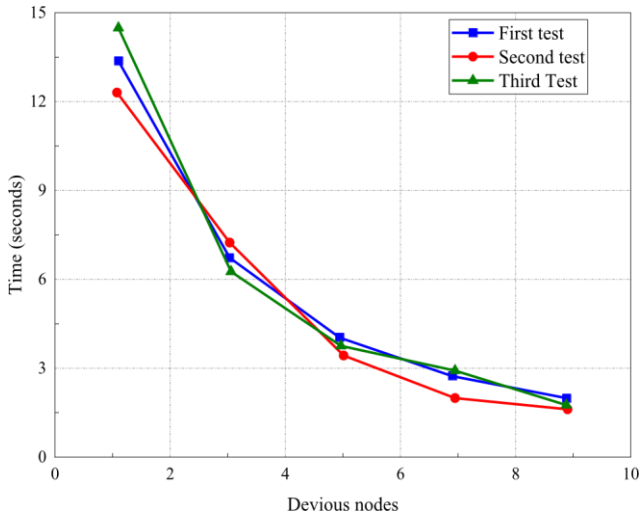

FIGURE 4. The effect of devious nodes on the computational time consumption in CSPPosS.

Fig. 3 and 4. In Fig. 3, the number of concurrency is set at 800, while the data throughput is measured against varying nodes qualities. The experiment shows that in a cluster of different nodes, the overall throughput of the CSPPoS algorithm drops while the latency rises with every rise in the number of nodes. The metric utilized in testing the throughput of the algorithm is comparatively higher when α = 0.4. On the other hand, the latency of the proposed algorithm is lower at α = 0.6 and α = 0.8. Similarly, the illustration in Fig.4 indicates that when the number of preliminary devious nodes in the cluster rises, the computational time necessary for the alteration of a primary node to a devious node reduces

C. COMPARISON WITH OTHER METHODS

The experiment in Fig.5 compares the performance of the proposed SERTT technique with other recently proposed methods such as, KiRKi [1], ANCILE [2], TCUGA [3] and Private-Rec [4]. As observed in the Figure, the overall time grows correspondingly in proportion to the quantity of the

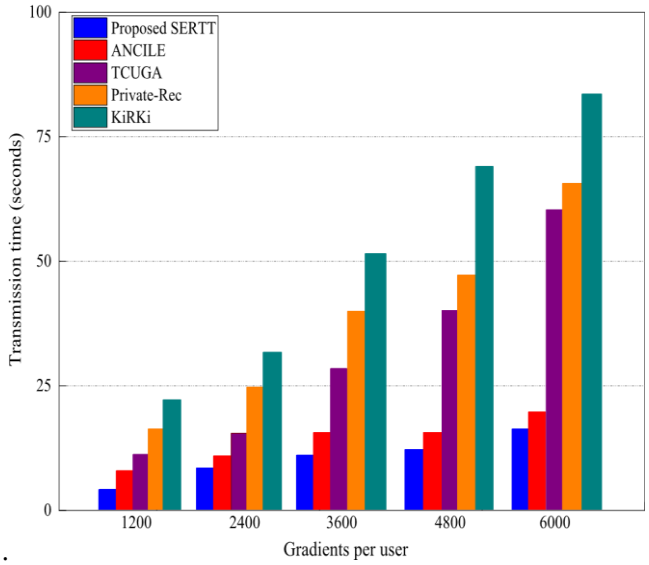

FIGURE 5. Comparison of gradients per user effect on transmission time.

utilized datasets. As soon as there is a modification in SERTT technique, it takes approximately 10 seconds to attain a proxy operation.Inconclusion, the experiment indicates that in comparison to other existing methods, the proposed SERTT training mechanism outperforms them with respect to transmission and computational time. Likewise, with the same metric for gradients per user and dropout metrics, the compared existing methods show greater amount of training success for the proposed SERTT.

VII. CONCLUSION

With the recent rapid evolution of artificial intelligence technology, secure medical data recommender training and modelling techniques are more and more important. Preserving user data from unauthorized access has occurred to be a pressing concern. Therefore, this chapter of the thesis was focused on providing a new solution for handling the issue of analyzing user medical data for training while sustaining user privacy. This section proposed a SERTT technique, which is an incorporation of a federated learning and blockchain for data training and modelling. For proficient data model designing, the study proposed a REMANA approach which is based on neural structural search, and which provides an efficient data sorting management (DSM) model design. For a secured training of federated learning, the study utilized the blockchain no-knowledge proof system. Results of the experiment show that SERTT technique is secure with optimal performance. Nonetheless, there are still

some latitudes for improving performance and security in the proposed technique. In order to achieve this in further research, the study will further optimize the efficiency of the distributed learning system of federation learning and will also reduce federated learning's training time using a proficient gradient distribution algorithm. Additionally, the study will further require optimizing the proficiency of data management model search and design to further improve the accuracy performance of the system's DSM model. Moreover, the no-knowledge proof process in this study was deployed in an ethereum smart contract, which is a less efficient verification approach at the core layer, thus, further attention can be given to integrating no-knowledge proof algorithms in the blockchain source code layer, to optimize the proficiency and performance of the proposed SERTT system.

REFERENCES

[1] s.B. Patel, P. Bhattacharya, S. Tanwar, and N. Kumar, ''KiRTi:A blockchain-based credit recommender system for financial institutions,'' *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1044–1054, Apr. 2021, doi: 10.1109/TNSE.2020.3005678.

[2] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, ''Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,'' *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.

[3] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K.-R. Choo, ''A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems,'' *IEEE Access*, vol. 6, pp. 28203–28212, 2018.

[4] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen, ''A blockchain-based trusted data management scheme in edge computing,'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2013–2021, Mar. 2020.

[5] L. Xu, T. Bao, and L. Zhu, ''Blockchain empowered differentially private and auditable data publishing in industrial IoT,'' *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7659–7668, Nov. 2021.

[6] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, ''Federated learning in mobile edge networks: A comprehensive survey,'' *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2031–2063, 3rd Quart., 2020.

[7] L. U. Khan, S. R. Pandey, N. H. Tran, W. Saad, Z. Han, M. N. H. Nguyen, and C. S. Hong, ''Federated learning for edge networks: Resource optimization and incentive mechanism,'' *IEEE Commun. Mag.*, vol. 58, no. 10, pp. 88–93, Oct. 2020.

[8] H. Kim, J. Park, M. Bennis, and S.-L. Kim, ''Blockchained on-device federated learning,'' *IEEE Commun. Lett.*, vol. 24, no. 6, pp. 1279–1283, Jun. 2020.

[9] N. Rieke, J. Hancox, W. Li, F. Milletarì, H. R. Roth, S. Albarqouni, Bakas, M. N. Galtier, B. A. Landman, K. Maier-Hein, S. Ourselin,M. Sheller, R. M. Summers, A. Trask, D. Xu, M. Baust, and M. J. Cardoso, ''The future of digital health with federated learning,'' *NPJ Digit. Med.*, vol. 3, no. 1, pp. 1–7, Sep. 2020.

[10] C. Iwendi, S. Khan, J. H. Anajemba, A. K. Bashir, and F. Noor, ''Realizing an efficient IoMT-assisted patient diet recommendation system through machine learning model,'' *IEEE Access*, vol. 8, pp. 28462–28474, 2020, doi: 10.1109/ACCESS.2020.2968537.

[11] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov,C. Kiddon, J. Konečný, S. Mazzocchi, H. B. McMahan, T. Van Overveldt, D. Petrou, D. Ramage, and J. Roselander, ''Towards federated learning at scale: System design,'' 2019, *arXiv:1902.01046*.

[12] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, ''A survey on federated learning,'' *Knowl.-Based Syst.*, vol. 216, Mar. 2021, Art. no. 106775.

[13] C. Iwendi, J. H. Anajemba, C. Biamba, and D. Ngabo, ''Security of things intrusion detection system for smart healthcare,'' *Electronics*, vol. 10, no. 12, p. 1375, Jun. 2021.

[14] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, ''A survey on security and privacy of federated learning,'' *Future Gener. Comput. Syst.*, vol. 115, pp. 619–640, Feb. 2021.

[15] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, ''Federated learning for Internet of Things: Recent advances, taxonomy, and open challenges,'' *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1759–1799, 3rd Quart., 2021.

[16] Y. Li, Y. Zhou, A. Jolfaei, D. Yu, G. Xu, and X. Zheng, ''Privacy-preserving federated learning framework based on chained secure multipartycomputing,'' *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6178–6186, Apr. 2021.

[17] D. Ngabo, D. Wang, C. Iwendi, J. H. Anajemba, L. A. Ajao, and C. Biamba, ''Blockchain-based security mechanism for the medical data at fog computing architecture of Internet of Things,'' *Electronics*, vol. 10, no. 17, p. 2110, Aug. 2021.

[18] E. A. Mantey, C. Zhou, J. H. Anajemba, I. M. Okpalaoguchi, and O. D.-M. Chiadika, ''Blockchain-secured recommender system for special need patients using deep learning,'' *Frontiers Public Health*, vol. 9, Sep. 2021, Art. no. 737269.

[19] E. A. Mantey, C. Zhou, V. Mani, J. K. Arthur, and E. Ibeke, ''Maintaining privacy for a recommender system

diagnosis using blockchain and deep learning,'' *Hum.-Centric Comput. Inf. Sci.*, to be published.

[20] Y. Qu, M. P. Uddin, C. Gan, Y. Xiang, L. Gao, and J. Yearwood,''Blockchain-enabled federated learning: A survey,'' *ACM Comput. Surv.*, vol. 55, no. 4, pp. 1–35, Apr. 2023.