A novel and innovative blockchain-empowered federated learning approach for secure data sharing in smart city applications.

HAI, T., WANG, D., SEETHARAMAN, T., AMELESH, M, SREEJITH, P.M., SHARMA, V., IBEKE, E. and LIU, H.

2023

A Novel & Innovative Blockchain-Empowered Federated Learning Approach for Secure Data Sharing in Smart City Applications

Tao Hai[1,2,3], Dan Wang[4,5,*], Tamizharasi Seetharaman[6], Amelesh M[6], Sreejith PM[6], Vandana Sharma[7], Ebuka Ibeke[8,*], Hong Liu[3]

[1] School of Computer and Information, Qiannan Normal University for Nationalities, Duyun, Guizhou, 558000, China

[2] Key Laboratory of Advanced Manufacturing Technology of the Ministry of Education, Guizhou University, Guizhou, 550025, China

[3] School of Information and Artificial Intelligence, Nanchang Institute of Science and Technology, Nanchang, China

[4] School of Mathematics and Statistics, Qiannan Normal University for Nationalities, Duyun, Guizhou 558000, P. R. China

[5] Key Laboratory of Complex Systems and Intelligent Optimization of Guizhou Province, Duyun, Guizhou 558000, P. R. China

[6] Department of AI & ML, Acharya Institute of Technology, India

[7] Amity Institute of Information Technology, Amity University, Noida, India

[8] School of Creative and Cultural Business, Robert Gordon University, AB10 7AQ, United Kingdom

Corresponding author: tamizharasi2539@acharya.ac.in, wangdansci@aliyun.com, e.ibeke@rgu.ac.uk

Abstract: The very existence of smart cities forms the stepping stone in the evolution of many technological advancements in the future era. While smart cities have already grown in their way, the tremendous amount of data generated from them paves the way for new perspectives of development. This is because security and privacy remain to be the major constraint across smart city applications. Further, smart city applications such as smart homes, smart transportation, and smart healthcare are generating a huge amount of data every day and it is often complex to collect and manage all the data together at a single location. To address these constraints, this paper presents a novel and innovative blockchain-assisted federated learning approach for secure data sharing in IoT Smart Cities. Here, we implement a federated learning approach, where the process of learning is made in a distributed fashion. The use of blockchain in turn adds more security and resilience to smart city applications. The security analysis proves that the proposed approach offers comparatively better performance and remains more resistant to various security threats and vulnerabilities.

Keywords: Smart City; Federated Learning; IOT; Secure data Sharing; Blockchain.

1. Introduction

In the last few decades, smart cities have grown significantly, and it has been expanded across different parts of the world with numerous advantages. The prime objective of smart cities is to provide optimized city functions and encourage economic growth while improving the quality of life through smart technologies and data analysis [1,2]. It is often crucial for smart cities to manage various domains such as having access to clean energy, sufficient water access, smart buildings that meet the occupant's requirement, and the potential of travelling efficiently while maintaining the city greener. The growth of smart cities is closely associated with the fact that "how efficiently the technology is being used rather

than how much of technological advancement is available." Building smart city infrastructure is often related to efficient data management. It is most vital to collect data from various smart applications, transfer it to information, extract insights, state actions, and develop strategies. It is the 'data' collected from various applications that make the smart city powerful. The effective integration of data from various smart city applications imposes a tangible benefit in improving people's quality of life and assisting in collectively building innovative solutions that assist in sustainable development [3,4].

Since a billion 'things' are connected across the smart city infrastructure. The widespread adoption of IoT technologies across smart cities increases the risk of security vulnerabilities exploited by malicious actors and cybercriminals. Any compromise in the security of the smart city applications will not only impact the productivity and efficiency of the city infrastructure but also greatly affect the residents and authorities [5]. Smart city applications are subject to several security vulnerabilities, some of the potential threats include privacy, data & identity theft, permanent denial of service attacks, device hijacking, Man in the middle attack, and application-level distributed denial of service attacks. These issues can be resolved through the effective implementation of security countermeasures such as authentication, access control, encryption, security monitoring and analysis, and security life cycle management. Security concerns are constantly raising as smart city applications continuously seek to modernize their services by connecting through the internet, easily creating an attack surface for cyber attackers. Hence, there is a crucial need for connected smart city devices to be protected by comprehensive IoT security solutions [6].

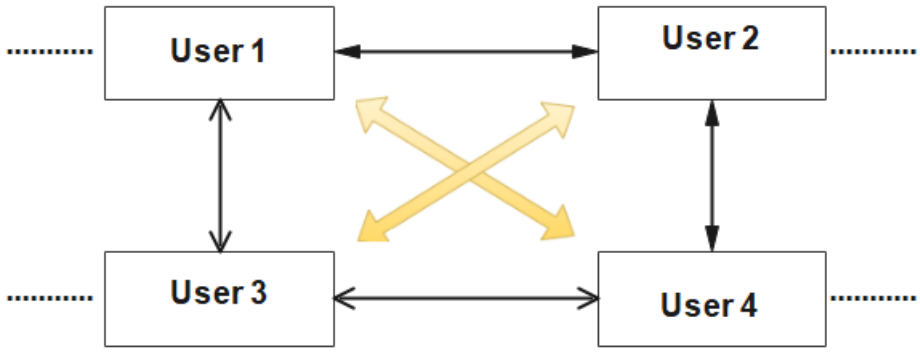

Figure 1. Proposed Model of Decentralized Architecture

Further, the ultimate goal of smart cities is to apply cutting-edge technologies and intelligence to a wide range of services to enable them to operate independently with real-time response and operations [7,8]. This can attract people towards smart cities and at the same time attaining this objective requires a complex system of architecture that has to be constantly monitored from the technology and security standpoint. One of the major concerns associated with the existing smart city application is that most of them are dependent on a central server and third-party cloud system to store and access the data. In general, all smart city applications aim to provide smart, safe, and efficient services to their end users through the exploitation of modern technologies. It is predicted that the smart city application may approximately produce more than 4,000 GB of data soon. Effective utilization and mining of the data will greatly assist in the automation of various services such as smart healthcare, smart transportation, smart homes, and many more. Despite technological advancements, the present-day smart city infrastructures are still traditional and require greater improvement in terms of security and privacy. Many of the security problems remain open and extensive efforts are required to address them efficiently. For example, let us consider a smart transportation application, real-time traffic status assessment is vital to prevent road accidents, manage traffic, and road closure, which saves people time. Similarly, the process of collecting and mining real-time travel data from a wide range of smart devices will significantly improve the quality of services relating to smart city applications. At the same time, such a process will result in numerous security concerns [9,10].

1. Most of the existing smart city applications are centralized in nature and they are subject to 'single point of failure' and congestion.
2. Automation of smart city applications requires users' real-time data, which may sometime result in the compromise of user data privacy.
3. Smart city users do not have any control over how their data is being used. If compromised, the smart city applications will not only behave maliciously but also affect user privacy and result in serious security concerns.

To overcome these issues efficiently, this paper presents a promising solution with blockchain and federated learning technologies. The proposed approach makes use of blockchain and federated learning to devise a real-time smart city information collection system called FedChain that is both secure against the vulnerable threat on the system and protects the user's private information. The major contribution of the proposed approach is twofold. First, we define a blockchain and federated learning-based decentralised architecture for secure data sharing in smart city applications. Next, we define a security scheme called FedChain to increase security and resilience in smart city infrastructure. Moving towards the growth plan of developing and developed countries, it is envisaged that smart cities will encounter numerous advancements. Which in turn creates the need for security and privacy requirements. In this regard, the proposed FedChain model is practical and efficient enough to share the data across the smart city environment in a secure manner. It enables safer training of the user data and sharing it securely among users through blockchain. Since, both the blockchain and federated learning follow the decentralized architecture, its application in real-time is highly feasible and efficient.

The rest of the paper is organized as follows: Section 2 provides a brief literature review of the proposed system. Section 3 defines the proposed architecture in detail. Section 4 depicts the security analysis of the proposed scheme and section 5 concludes the paper.

2. Related Works

Securing smart city applications is an emerging area of research. In this section, we precisely explore some of the related technologies and frameworks that are closely associated with the proposed system.

Haque et al. [11] provide a brief conceptualization of smart city applications. The prime objective of this paper is to provide seamless access to smart city services with intelligent decision-making and optimized resource management functionalities. Various security and privacy threats that emerge from smart city applications are briefly illustrated regarding future work.

In [12] the authors briefly discuss the problem of secure computation outsourcing of IoT data across cloud computing platforms. The author emphasises the need for a global common approach to secure IoT data. Further, the impact of cloud computing and IoT technologies on the deployment of smart applications are also discussed in detail. The author focuses on both the technologies of cloud and IoT. They also explore the list of security issues that occurs with the integration of these technologies with appropriate countermeasures.

The authors Yang, Qiang, et al. in [15] have briefly explored the concept and application of federated learning. They have introduced a secure federated learning approach safely share data across IoT applications without compromising user privacy.

In [13] the author proposes a blockchain-enabled federated learning approach for securing critical IoT infrastructures. The prime focus of this work is to establish trustworthiness among the users. In general, network trustworthy solutions are highly challenging, especially for critical infrastructures as IoT devices can be easily compromised for security vulnerabilities. This approach integrates blockchain and federated learning approaches to establish the factor of network trustworthiness and security. The improved accuracy and detection rate of security vulnerabilities.

The authors Cui, Lei, et al. in [14] present an efficient approach for anomaly detection in IoT infrastructures. The objective here is to focus on robustness, security, and efficiency-related challenges. To address these issues the authors have proposed a blockchain-powered asynchronous federated learning framework. The results are evaluated with real-time datasets, and it attains comparatively better results.

In [16], the authors have attempted to effectively utilize blockchain technology for securing smart city applications. This work has effectively addressed some of the imperative research challenges in the IoT environment. However, this approach was unable to address all the security concerns associated with IoT systems as they vary dynamically from one context to another.

In [17], the authors have presented a deep block scheme for securing smart city applications. They have attempted to integrate deep learning and blockchain technologies for securing smart city applications. The key objective of this approach is to preserve security and privacy factors.

Moving forward, a quantum-inspired cybersecurity-based blockchain protocol is given by Abd El-Latif, Ahmed A., et al. [18]. They have proposed an authentication protocol based on Quantum Inspired Quantum Walk (QIQW). This approach can be extensively used for securing IoT devices. Rather than using the conventional hash functions to manage the blockchain paradigm, this approach makes use of quantum hash functions.

In [19] a blockchain-based efficient authentication and authorization protocol is presented for smart city applications. This work offers a novel solution for the decentralized management of user identity and authorization policies by leveraging blockchain technology. The experimental results indicate that this approach provides comparatively better results than the existing algorithms.

In [20] blockchain-based hybrid network architecture is proposed for smart city systems. This approach receives the benefits of both the centralized and decentralized architecture. The proof-of-work deployed in this scheme ensures better security and privacy measures.

Summary of Literature: Although much of the existing literature [21,22,23,24,25] focuses on the analysis of various cyberattacks and tries to implement blockchain and federated learning-based solutions, many of them face the challenge of higher computational complexity and privacy concerns (leakage of sensitive user information). Further, with the decentralized system models, most of the existing approaches were using linear models. Secure federated learning for smart city applications with heterogeneous models remains to be an open issue that requires more in-depth research. An effective strategy to address these constraints will be discussed throughout the remaining section.

3. Blockchain-Empowered Secure Federated Learning

This section provides a detailed description of the proposed system. It provides the proposed system architecture, system entities and the working of the proposed approach in a detailed manner.

3.1 System Architecture

To attain the design goals and to effectively address the security challenges defined in the threat model, we design an efficient architecture, which is clearly illustrated in figure 2. The proposed architecture is mainly composed of three major components. First is the data collection module which is closely related to the users involved with the system. Next, is the feature extraction module that extracts meaningful features from the data collected from IoT devices. Next is the Fedchain-based privacy preserving aggregation module that optimize the interaction between the users of s mart city applications and the cloud [26]. This module also ensures the data integrity and confidentiality measures between the users/IoT devices and the cloud systems.

Given the proposed system architecture, each entity could be an IoT device or a personal device such as a desktop or smartphone. Initially, every user will have a local model and that model is trained on a private dataset. Since the proposed approach implements a heterogenous model, information such as the type of model, parameters associated with the model, learned classes, and model information is stored across the blockchain. The user can search for the calibration of the data sample and can test the model on the blockchain only during their allocated time slot [27, 28]. If a valid sample is obtained, the user can broadcast it over the blockchain and they can also update the models on the chain. This procedure is also called Fed-off-chain data mining. The users or miners associated with the system acquire the calibration sample which is broadcasted by the learning users and validated based on the design protocol. If a sample is validated by the user who possesses the authority to write the next block, then they can update the model on the blockchain and this is called the calibration process. Depending upon various pre-defined model update protocols, the user can construct a legal block header, update model information, and create a new block. All these processes including calibration, block construction, and sample validation are called "Fed-on-chain mining." Since the updated information of the model is stored across blocks and can be viewed by every participant across the system, all the users including both fed-on-chain and fed-off-chain can get the privilege to build a new block.

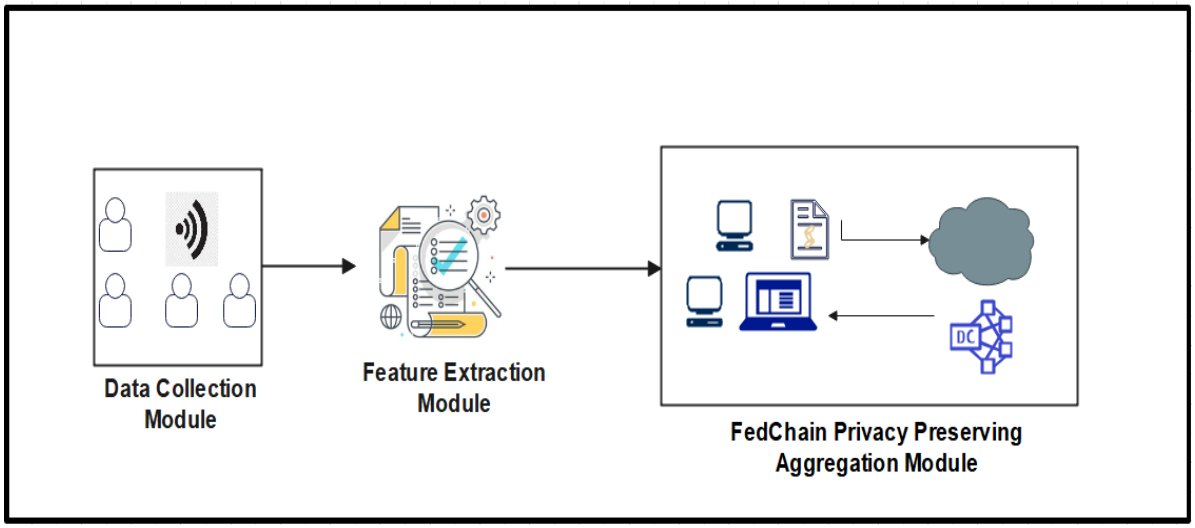

Figure 2. System Architecture of the Proposed Scheme

There are mainly three different kinds of users associated with the system. Original users (OU) start the blockchain and they collaboratively work with one another to acquire better local models without sharing the identity of the local data. Regular Users (RU) make use of the system after initialization. Each RU possesses a local model and that model is trained based on their local dataset. This enables the system to learn more robust local models and assist in the efficient classification of data even from unknown classes. Miner builds the blockchain based on consensus protocol. They are usually IoT devices with an adequate computing device or an edge device.

3.2 System Definition:

Let us consider a decentralized learning system with N users. Such that every user a$\in [1, N]$ posses a local data $F_i = (u_i, v_i) = \{((u_a^1, v_a^1), \dots, (u_a^{na}, v_a^{na})\}$ with n_a samples of data including their labels. For any user $a \in [1, N], F_i \subseteq F$. Thus F={u,v} remains to be the global dataset and $v = \{i, \dots, e\}$ represent the set of total e classes. In consideration of the learning system, every user has to possess a local model d_a that is already trained F_a. Just because the classifier is trained with a partial set of F, there is a probability it may misclassify unknown data samples into the wrong class $V' \in V_a$ and also from its unknown space $V \not\subset V_a$. For every user a, its classifier$d_a: u_a \rightarrow v_a$ can be attained through training of a local model w_a with model parameter θ_i, which significantly varies from other users. For a particular data sample a, the output d_a is defined as

$$d_a(u) = arg^{max}_{v \in v_a} j_a(\theta_a, u, v)$$

Here, $j_a(\theta_a, u, v)$ can be represented as a score function associated with the local model d_a. This, in turn, return the predicted possibility of u. It is also well known that the traditional federated learning system is dependent on a central server to initiate the process of learning and calibrate local models. There is no doubt that it turned out to be a single point of failure. Thus, to solve this issue proposed approach makes use of a decentralized federated learning system that does not have any central server.

For a given set of models $D = \{d_1, \dots, d_N\}$ the value of max-model predictor is obtained as

$$d_D(u) = arg^{max}_{v \in V, a \in [1,N]}\ j_a(u, v)$$

The value of multi-party multi-class margin for a data sample is computed as,

$$\rho(u, v, v^-) = j_i(u, v) - j_m(u, v^-)$$

Where v^- is an incorrect class label for u, and $i = arg_a max_{j_a}(u, v), v \in v_a,\ \ m, v^- = arg_{a,v'} max_{j_i(u,v'),} v' \in v_a | \{v\}$.

Such that each user knows about all the other users in the learning model. At every iteration, each user will make use of their local data to acquire a valid calibration sample (u, v, v^-). Such that $\rho \leq 0$ and transfer the sample to both the parties *i* and *m* based on the equation defined above. Further, with the help of various model update methods, user I can amplify the significance of (u,v) by raising $j_m(u, v^-)$. Once the iterations of model calibration are completed, all the users can update their local model and at least they make use of the max-model predictor to make a classification.

3.3 Threat Model

The most challenging cyberattack associated with a decentralized system is a byzantine attack. In this regard, the attacker follows the system protocols but introduces malicious information to system users. This will significantly degrade the system's performance. Type I and Type II byzantine attacks are the most common among the existing models.

3.4 Secure Blockchain-based Federated Learning (Fedchain)

The proposed scheme consists of three important steps namely system initialization, Fed-off-chain data mining and Fed-on-chain mining. During the phase of system initialization, OU enrols their identities and model information to the blockchain. Next, the RU registers their credentials to the blockchain. Then it is followed by Fed-of-chain and Fed-on-chain mining. The Fed-off-chain is used to appropriate data samples for model calibration, while Fed-on-chain mining is used to calibrate the exact local model depending on the samples and records found on the new block.

System Initialization

Let us consider there are a total of W(W<N) OU, with each having a local model, such that $a \in [1, w], V_i \subset V$. Here, jV_a denotes the trained model over the data from the class V_a. Such that, every OUbroadcast their model information with the corresponding ID. The model information of the first block is computed as,

$$[\{j_{v_i}^{Q^p}, j_{w_a}^{Q^p}, v_1, AF_QP_1\} \dots . \{j_{w_b}^{Q^p}, V_w, A\ F_QP_b\}]$$

Once the above condition is satisfied, OU will prove the initialization model $j_{w_b}^{Q^P}$ for RUh on the blockchain. As a result, the message $< j_{v_l}^{TP}, IF_{TP_h}, Sign\ OU_a >$ is broadcasted. This is also included as a

new block in the chain. Otherwise, the model is found to be unfit for classification, and this process cannot be registered into the system.

Fed-off-Chain Mining

In this phase, every user associated with the system is stimulated to make use of the local model on the blockchain using their dataset, with the intent to find a data sample that helps to calibrate a few of the models. The proposed approach makes use of more secure methods such that it is resistant to byzantine attacks.

$$\rho(u, v, v^{-}) = j_i * (u, v) - i_m * (u, v^{-}), v^{-} \epsilon \mathrm{V} \backslash \{\mathrm{v}\}$$

$$j, (u, v) = \frac{1}{S} \sum_{S_{d \to j}} j_d(u, v)$$

$$j_{m^*}(u, v^{-}) = \frac{1}{S} \sum_{S_{d \to m}} j_d(u, v^{-})$$

$$i = arg^{min}_{h \in m(v')} \sum_{S_{d \to h}} |j_d(u, v) - j_h(u, v)|$$

$$V^{-} = arg^{max}_{v' \in v | \{v\}} j_a(u, v')$$

$$a = arg^{min}_{h \in m(v')} \sum_{S_{d \to h}} |j_d(u, v') - j_h(u, v')|$$

Here, $d \overset{s}{\to} h$ represent S closest value to $j_h(.,.)$, m(v) and m(v^{-}) denotes the set of users who possess the data that belong to class V and also in class v^{-} correspondingly. A($0<\alpha\leq 1$) represents the control parameter.

Fed-on-chain-mining

For every broadcasted sample (u,v,v^{-}) desires to be validated by the miner before it is utilised for model calibration. For a calibration sample (u,v,v^{-}), the miner check is validated as,

$$\rho(u, v, v^{-}) \leq 0$$

$$j_{i^*}(u.v) \geq \delta$$

$$MAX_{d \overset{s}{\to} i} |j_d(u, v) - j_{i^*}(u, v)| \sigma$$

Where δ and σ represent the predefined thresholds. And the above equation confirms that (u,v,v^{-}) is eligible for calibration. Once, all the conditions mentioned above are satisfied, the miner can adapt the sample for model calibration.

4. Security Analysis

The security analysis of the proposed Fedchain model is examined in this section. In general, there exist two types of byzantine attacks, when it comes to the implementation of decentralized multiparty federated learning. In the case of the type1 byzantine attacks, RU's are validated by taking advantage of OUs. The control parameter M specifies the requirement on the model of RU_n demanding the users to join the system. To be more specific, R$U_{n's}$ model, i.e, Y_a^{RU}, needs to act based on the appropriate OU's local models that includeY_n across their learning space. Further, with the proposed model Fedchain assisted system, the process of model update is performed publicly and is later validated for every

model update process, irrespective of the fact that the newly registered RU's models can be slightly malicious at the commencement.

TypeII byzantine attacks are the additional major security threat across the proposed system. In such cases, the bogus calibration sample will seriously interrupt the process of updating a model. We prove that the proposed fed chain algorithm is resistant against type II byzantine attacks and has bounded performance through the following proof:

Let us consider the set of constant models (p)=$\{q_1, \dots, q_{|S(P)|}\}$. The objective here is to classify the data across class P. Let $|S(P)|=N^{S(P)}+M^{S(P)}$ denotes the number of honest models and malicious models. Let us assume $M^{S(P)}< f < N^{S(P)}$. Also, for a given data sample (a,b), let $q_{min}(a,b)$ and $q_{max}(a,b)$ represent the minimum and maximum output of the honest models, respectively. Then the value of $q_x * (a,b)$ in the worst case is computed by

$$q_{min}(a,b) - \frac{m^{S(b)}}{f}(q_{max}(a,b) - q_{min}(a,b)) < q_x * (a,b) < \frac{q_{max}(a,b)+M^{S(P)}/f}{q_{max}(a,b) - q_{min}(a,b)}$$

$$< q_{max}(a,b) + \frac{M^{S(P)}}{f} / q_{max}(a,b)$$

In the same way, let us assume the set of models $S(b^-)$ that can categorize the data in class b^-. For a data sample (a,b^-), $q_y^*(a, b)$, the worst-case scenario is bounded by,

$$q_{min}(p, q^-) - \frac{M^{(b^{-1})}}{f}$$

$$(q_{max}|a, b^-) - q_{min}(a, b^-))$$

To analyze the bounds in the scenario, such that we assume the byzantine models are included in the aggregation. Such that,

$$q_{x^*=\frac{1}{f}(\sum_{f-m}^{m} q_l^B + \sum q_n^o)}$$

Further, the ground truth is defined as $\frac{1}{N}\sum_{i=1}^{N} q_i + [q_{min}, q_{max}]$, consequently the additional term in q_{x^*} is defined as $\sum^{f-m} q_h^o \in [f-m]q_{min}, (f-m)q_{max}]$.

Here, the major objective is to direct the aggregated value q_{x^*} as possible as smaller or larger. Henceforth, we will deliberate the attack in two worst cases.

Case 1: In this case, the threat models intend to steer q_{x^*} smaller, where $q_m < q_{min} \leq q_x$.

$$|q_1^\beta - h_x| + \cdots . + |q_m^\beta - q_x + \cdots |q_{f-m}^0 - q_x| < |q_{m+1}^0 - q_a| + \cdots + |q_f^0 - q_x| + |q_1^0 - q_x| + \cdots + |q_{f-m}^0 - q_x|$$

Due to $q_m^\beta < q_x < q_{f-m+1}^0$, the inequality associated here is rewritten as

$$M_{q_x} - \sum_{t=1}^{m} q_j^\beta < \sum_{t=f-m+1}^{f} q_1^b - m^{q_a}$$

$$\sum_{t=1}^{f} q_1^\beta > 2mq_x - \sum_{l=f-m+1}^{t=f} q_1^0 > 2fm\, q_{min} - mq_{max}$$

$$\sum_{l=1}^{m} q_1^{\beta} + \sum_{l=1}^{f-m} q_1^0 > 2m\, q_{min} - mq_{max} + (f-m)q_{min}$$

$$= (\text{f+m})\, q_{min} - f_m q_{max}$$

$$= q_x^* > q_{min} - \frac{m}{f}(q_{max} - q_{min})$$

Case II: All the threat models intend to steer q_x^*, greater, where $q_1^{\beta} > q_{max} \geq q_a$. Likewise, we obtain

$$|\left|q_1^{\beta} - q_a\right| + \cdots + |q_m^{\beta} - q_a| + |q_{n-f}^0 \text{+m+1} - q_x| + \ldots + |q_{n-f+m}^0 - q_{a1} + \left|q_{n-f}^0 + m + 1 - q_x\right| + \cdots + |q_n^0 - q_x|$$

Due to the reason, $q_1^{\beta} > q_x > q_{n^{n-f}}^0 + m$, we have

$$\sum_{l=1}^{n-f+m} q_l^{\beta} < 2m^h x - \sum_{l=N-f+1}^{l=N-f+m} q_1^0 < 2mq_{mx} - m_{min}^q + (f-m)q_{max} - mq_{min}$$

$$q_x^* < q_{max} + \frac{m}{f}(q_{max} - q_{min})$$

5. Results and Discussions

The simulation of the proposed model is made with the help of the MNIST dataset. The dataset contains 60,000 training samples and 10,000 testing samples. Every image has a fixed pixel size of 28x28. To perform the simulation with multiple parties, we have separated the dataset with various data distributions and four cases are developed for simulation. In the proposed model of a decentralized system, every party posse a LeNET-5 that is the same as the centralized model. The major difference is that in the proposed method we adopt both fully connected neural networks and convolutional neural networks. The setup of the calibration model is based on the user updates on the corresponding local models. A comparison is made with the baseline models in terms of prediction accuracy and attack resilience measures.

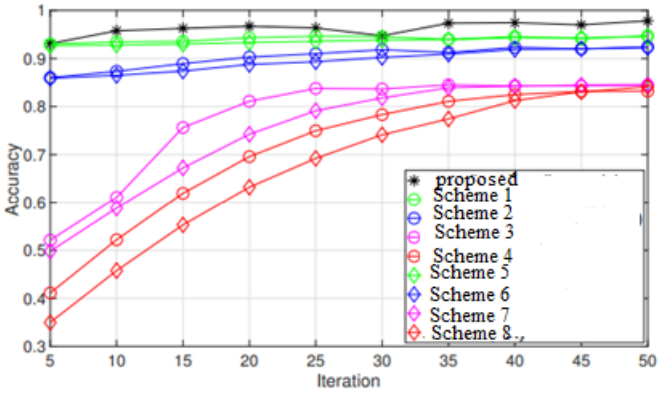

Figure 3 Comparison of prediction accuracy with the proposed Scheme

The results of the comparison of the prediction accuracy measure are clearly illustrated in Figure 3. The performance of the proposed decentralized model is observed to be comparatively better than the conventional baseline methods. The competitive security measure value of every security scheme is analyzed in detail, and it's found to be relatively greater than the existing schemes. In the case of observation between every 5 to 10 parties, the prediction speed measure is also found to be better than traditional methods. From this, we can conclude that the proposed decentralized scheme can act as a genuine alternative to the baseline methods. Further, the security resilience measure of the proposed scheme is also observed to be relatively greater than conventional methods.

6. Conclusions

In this article, we proposed a scheme called the secure and privacy-preserving FedChain model for securing smart city applications. This approach attains the data from IoT devices associated with the smart city applications and applies blockchain and federated learning techniques for securing it efficiently. The aggregation model is designed in a decentralized manner that prevents emerging security threats across the smart city environment. The security feasibility of the proposed approach is evaluated in detail with the security analysis model and this approach is found to be more secure against major security threats.

In future, the scope of the proposed approach could be extended towards various applications including autonomous vehicles, wearable devices, etc. It finds an appropriate place in applications where the secure transmission of data sharing has become inevitable. It further, helps efficiently to learn data across organizations, especially across heterogeneous networks.

Further, as discussed earlier the proposed model of FedChain enhances the security and privacy features of the smart city applications, and it paves the way for several new questions that have to be addressed efficiently. One major limitation is that learning over organizations and mobile phones is quite difficult and often a complicated process. This is because the training data is distributed across the edge. The other limitations include statistical heterogeneity, expensive communication, and system heterogeneity.

References

1. Moreno, M. Victoria, et al. "Applicability of big data techniques to smart cities deployments." IEEE Transactions on Industrial Informatics 13.2 (2016): 800-809.
2. Odendaal, Nancy. "Everyday urbanisms and the importance of place: Exploring the elements of the emancipatory smart city." Urban Studies 58.3 (2021): 639-654.
3. Zhang, Kuan, et al. "Security and privacy in smart city applications: Challenges and solutions." IEEE Communications Magazine 55.1 (2017): 122-129.
4. Lacinák, Maroš, and Jozef Ristvej. "Smart city, safety and security." Procedia Engineering 192 (2017): 522-527.
5. Braun, Trevor, et al. "Security and privacy challenges in smart cities." Sustainable cities and society 39 (2018): 499-507.
6. Habibzadeh, Hadi, et al. "Sensing, communication and security planes: A new challenge for a smart city system design." Computer Networks 144 (2018): 163-200.
7. Cui, Lei, et al. "Security and privacy in smart cities: Challenges and opportunities." IEEE Access 6 (2018): 46134-46145.
8. Li, Yibin, et al. "Privacy protection for preventing data over-collection in smart city." IEEE Transactions on Computers 65.5 (2015): 1339-1350.
9. Qi, Lianyong, et al. "Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment." IEEE Transactions on Industrial Informatics 17.6 (2020): 4159-4167.
10. Moreno, M. Victoria, et al. "Applicability of big data techniques to smart cities deployments." IEEE Transactions on Industrial Informatics 13.2 (2016): 800-809.

11. Haque, AKM Bahalul, Bharat Bhushan, and Gaurav Dhiman. "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends." Expert Systems 39.5 (2022): e12753.
12. Singh, Debabrata, et al. "Security issues in IoT and their countermeasures in smart city applications." Advanced Computing and Intelligent Engineering. Springer, Singapore, 2020. 301-313.
13. Otoum, Safa, Ismaeel Al Ridhawi, and Hussein Mouftah. "Securing critical IoT infrastructures with blockchain-supported federated learning." IEEE Internet of Things Journal 9.4 (2021): 2592-2601.
14. Cui, Lei, et al. "Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures." IEEE Transactions on Industrial Informatics 18.5 (2021): 3492-3500.
15. Yang, Qiang, et al. "Federated machine learning: Concept and applications." ACM Transactions on Intelligent Systems and Technology (TIST) 10.2 (2019): 1-19.
16. Hakak, Saqib, et al. "Securing smart cities through blockchain technology: Architecture, requirements, and challenges." IEEE Network 34.1 (2020): 8-14.
17. Singh, Sushil Kumar, et al. "DeepBlockScheme: A deep learning-based blockchain driven scheme for a secure smart city." Hum.-Centric Comput. Inf. Sci 11 (2021): 12.
18. Abd El-Latif, Ahmed A., et al. "Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities." Information Processing & Management 58.4 (2021): 102549.
19. Esposito, Christian, Massimo Ficco, and Brij Bhooshan Gupta. "Blockchain-based authentication and authorization for smart city applications." Information Processing & Management 58.2 (2021): 102468.
20. Sharma, Pradip Kumar, and Jong Hyuk Park. "Blockchain-based hybrid network architecture for the smart city." Future Generation Computer Systems 86 (2018): 650-655.
21. Wang, Zhilin, and Qin Hu. "Blockchain-based federated learning: A comprehensive survey." arXiv preprint arXiv:2110.02182 (2021).
22. Demertzis, Konstantinos. "Blockchained federated learning for threat defense." arXiv preprint arXiv:2102.12746 (2021).
23. Li, Dong, Zai Luo, and Bo Cao. "Blockchain-based federated learning methodologies in smart environments." Cluster Computing 25.4 (2022): 2585-2599.
24. Yu, Feng, et al. "Blockchain-empowered secure federated learning system: Architecture and applications." Computer Communications 196 (2022): 55-65.
25. Issa, Wael, et al. "Blockchain-based Federated Learning for Securing Internet of Things: A Comprehensive Survey." ACM Computing Surveys (CSUR) (2022).
26. Ngabo, D., Dong, W., Ibeke, E., Iwendi, C., & Masabo, E. Tackling pandemics in smart cities using machine learning architecture. *Mathematical biosciences and engineering*, (2021). *18*(6).
27. Mantey, E. A., Zhou, C., Mani, V., Arthur, J. K., & Ibeke, E. Maintaining privacy for a recommender system diagnosis using blockchain and deep learning. *Human-centric computing and information sciences* (2022).
28. Latif, S. A., Wen, F. B. X., Iwendi, C., Li-li, F. W., Mohsin, S. M., Han, Z., & Band, S. S. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber-physical systems. *Computer Communications*, (2022): *181*, 274-283.