International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

Leveraging Edge Computing for Real-Time Data Security in Multi-cloud Infrastructures

Sai Sandeep Ogety,

Independent Researcher

Raleigh, United States, ogetysaisandeep04@gmail.com

Abstract:

In the recent era, prosumer growth plays a significant role and makes a lot of advantages and flexibility to create interest in other activities in order to manage the energy to be consumed or produced. As in that kind of system, a lot of data is involved as it needs privacy among the users. In federated learning, the problem of dependent and identical data distribution problem occurs and those data contain user information. As that information should be more effective to make a decision-making process by ensuring privacy among the user information. In this paper, a novel federated-based data clustering technique is proposed as it improves the degree of data sampling based on multiple iterations. Using this model degree, weight of each client is measure by considering the client distribution of independent and identical problem. Based on the proposed model, communication rounds get reduced and number of iteration as compared to FedAvg algorithm. Then the data accuracy also gets improved using clustering and weighted clients based on the distribution of non-independent and identical data.

Keywords: Federated learning, data distribution, energy consumption, clustering, prosumers.

I. INTRODUCTION

With the widespread adoption of smart metres, enormous volumes of precise data on electricity consumption may be gathered [1]. The power industry is in the process of being dereglementated in nations all over the world, notably in terms of power consumption and distribution. As a result, retail electricity markets are becoming competitive. As a result, fine-grained smart met data can be utilised to advance the companies of various retail market participants [2]. Clustering-based power consumption pattern extraction is one method for revealing the values of smart metre data in the big data era, hence assisting retailers and distribution network operators (DNOs) in improving their understanding of consumer behaviours. This enables the provision of a variety of services and the adoption of different business models.

Personalized price design [3], demand response targeting, and load forecasting are a few examples of these services and methodologies. Various clustering algorithms, including hierarchical clustering, k-means, fuzzy k-means, and modified follow-the-leader, along with various dimension reduction techniques, including Sammon map, principal component analysis (PCA), and curvilinear component analysis (CCA), were utilised for the classification of power consumers. Used an adaptive k-means algorithm and hierarchical clustering to extract typical consumption patterns from over 66 million daily load profiles. The integrated approach can effectively handle a considerable number of datasets. A multi-resolution clustering (MRC) method was suggested to classify each customer's daily profiles using Gaussian mixture models after discrete wavelet transform (DWT) was used to extract the spectral properties of the load profiles (GMMs) [4].

The suggested MRC technique can model the volatility and uncertainty of smart metre data in a flexible manner. Modelling of peak demand and significant drivers of fluctuation in load profiles was merged with an FMM-based clustering technique. Two subspace projection approaches, subspace clustering and projected clustering, were used to capture the subspaces (i.e., local shape variability) of the load profiles, as opposed to treating the daily load profile as a whole. [5] Used a sparse representation technique to extract partial consumption patterns from power demand, which depict the behaviours of distinct sorts of customers. [6] Studied how the temporal resolution of input data affects the quality of the clustering process and the consistency of cluster membership. Although a variety of load pattern extraction algorithms have been created in the past, all of the ones we've described so far have been implemented centrally and are predicated on access to all smart mete data.

However, it is likely that the data from different merchants or even individual consumers themselves, who may be participants in a competitive retail market, own the smart meters [7]. Traditional centralized clustering algorithms are not appropriate in this context because they risk the privacy of the retailers or the customers. Indeed, governments and organisations around the world are becoming more devoted to data privacy protection. The General Data Protection Regulation (GDPR), for instance, began to be implemented in the European Union [8]. There are numerous literary works addressing protecting the privacy of smart met data. By separating customer data from load profiles, anonymization is a straightforward method for protecting privacy.

Only the attribute information of consumers is concealed. Keep in mind that load profiles themselves contain private data, which should also be secured since it can be used to operate the grid and establish retail prices, among other things [9]. Thus, numerous recent efforts have been done to change load profiles through strategic scheduling of flexible resources such as energy storage and thermal loads. The load profiles were reshaped using an electrical battery to strike a balance between privacy and energy cost. In order to balance the advantages of data utilisation and safeguarding consumer privacy in deregulated smart grids, a game theoretic model was developed. The privacy of smart meter data throughout the transmission process has also been investigated [10].

The Paillier algorithm was used to safeguard smart meter privacy during the transmission process. This served as the foundation for the implementation of convolutional neural networks (CNNs)-based energy theft detection [11]. Each resolution was encrypted with an individual key underneath a hierarchical keying method. While smart meter data privacy protection technologies are varied, few are suited for electricity usage pattern extraction. As far as we are aware, only one work has addressed privacy-preserving electrical load profile clustering. In this study, proposed algorithm was created. It is a key tool for converting k-means, fuzzy c-means, and Gaussian mixture model clustering approaches into their distributed variants. While the networked method mentioned potentially accomplish the same clustering results as the comparable centralized method, it must be built community, necessitating a massive wide range of network links between consumers or sellers.

This research uses the unique privacy-preserving machine learning framework known as federated learning to address this issue because it requires less communication effort. Federated learning has been widely explored. Recent changes to federated learning, such as new algorithms and applications, can be found in [12]. Federated learning can be divided into horizontal federated learning; vertical federated learning, and federated transfer learning, depending on how the datasets are organized. In supervised learning, when the loss function is known and only global variables, like the human brain weights W, need to be optimizer, the majority of federated learning algorithm studies have been developed. There are two approaches that can be used to jointly train the global model [13]. The initial tactic is model averaging. Using this strategy, each client trains the model using its own data at each step.

The objective of this paper is organized as,

- The straightforward and useful Federated Learning based Cluster Chaining (FL-CC) algorithm is chosen. Based on this algorithm, several improvements are performed, and a new algorithm, FL-CC algorithm is created that is more suited for the direction of our research.
- In order to achieve the effect of the model average and weaken the degree of parameter deviation, we utilize the degree of model parameter differentiation from the average characteristic to determine the weight for every client's updates of the model parameters.
- Multiple local model trainings and the establishment of three-layer architecture can significantly minimise the number of communication rounds.

The rest of this paper is organized as follows,

II. LITERATURE SURVEY

In recent years, artificial intelligence has advanced rapidly, and a wide range of machine learning-based applications such as computer vision, natural language processing, recommendation systems, speech recognition, and so on have all achieved remarkable success. The success of these technologies is dependent on a significant volume of data [14]. However, in many fields, data cannot be gathered indiscriminately. Data privacy and security concerns, as well as data island difficulties, are the two greatest obstacles impeding the advancement of artificial intelligence [15] and [16].

Federated learning [17] is one of the methods that can effectively address the issues highlighted above. It can train machine learning models without concentrating all the data on a single storage location. Comparable to distributed learning, transfer learning adds the concern of privacy protection on top of distributed learning. The main idea behind federated learning is to organise the nodes that have data sources. Each node is trained locally, and then the model parameters are shared (instead of private data) to create a global model. This global model's performance is comparable to what would be achieved by training all of the data at once [18]. The algorithm described in this study can be

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

implemented as follows: the private data of each client cannot be shared, each client sample is encrypted and aligned, a model is trained locally, and then the model parameters are updated by gradient sharing to achieve the joint training model goal [19-24].

Federated learning may create a unified training model for numerous sources of data while sacrificing security or privacy. Consequently, it will have a broad range of application situations in a variety of fields. Consider the multi-cloud infrastructures system as an illustration. With the rapid development of my country's consumer goods market, a user-oriented multi-cloud infrastructures system, such as the peer-to-peer approach, coordinated scheduling-based scheme, and centralized control technique, is urgently needed [25]. These tactics lack smart tools as represented in figure 1.

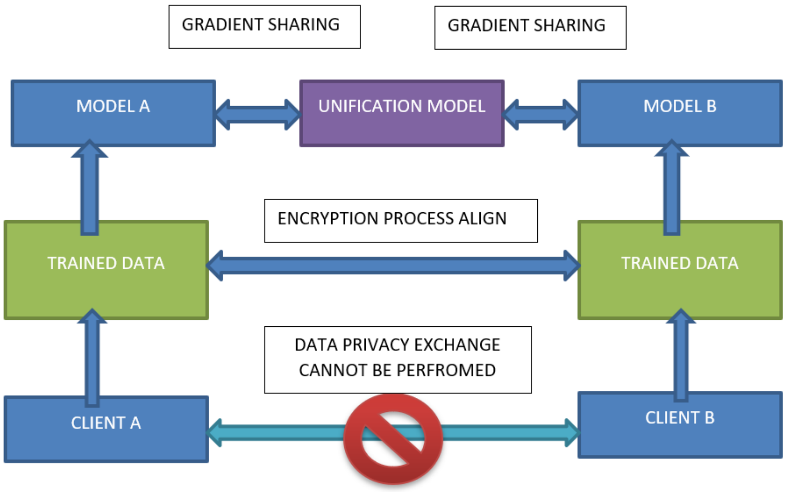


Figure 1. Federated learning Framework

Compatible with existing multi-cloud infrastructures systems and fail to segment users to increase product consumers' durability [26]. Right now, developing a set of user data training model based on federated learning to take part in the assistance decision-making of the multi-cloud infrastructures system is a good solution to overcome the aforementioned issues. It is anticipated that in the not-too-distant future, federated learning will remove barriers that currently exist between different businesses and build a new model for the preservation and dissemination access information and informational data [27]. After acquiring improved parameters, to iterate in parallel and synchronize with the server, which can significantly cut down on communications and speed up convergence [28-30].

Proposed FL-CChain mechanism can alleviate the issue of data Non-IID in federated learning. However, the accuracy of the proposed algorithm is diminished when the imbalance of data feature distribution between customers is considerable. In this instance, the degree of parameter variance between each client and the service terminal relative to the average parameters might be used to indicate the influence. When a customer's numerical variance is big, we make the parameter less important so that the algorithm can process data more accurately Non-IID. At the same time, we observe that the data Non-IID issue with each client does not directly reflect the updating of model parameters.

III. RESEARCH METHODOLOGY

Most successful federated learning management systems rely heavily on SGD's improved optimization, and the federated averaging method (FedAvg) is also based on SGD to develop a federated optimization algorithm. McMahan et al. [14] first introduced the FL-CC method. It allows each client to iterate simultaneously and synchronises with the server after getting better parameters, which can significantly cut down on communications and hasten convergence of the model.

FL-CC algorithm can alleviate the issue of data Non-IID in federated learning. However, the accuracy of the FL-CC algorithm is diminished when the imbalance of data feature distribution between customers is considerable. In this instance, the degree of parameter variance from each client to the service terminal compared to the overall characteristics might be used to describe the influence. We decrease the value of the a variable when a client's parameter deviation is

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

substantial, allowing the algorithm to handle Non-IID data with more precision. At the same time, we observe that the data Non-IID issue with each client does not directly reflect the updating of model parameters.

We suggest splitting clients with large distribution disparities in the sample into smaller clients using sample clustering, and extracting the training set by stratified sampling for multi-level iteration, so as to lower the degree of non-independent and homogeneity of variance data. Then, utilising weighted method, stochastic adjust may keep updating the variables of a single client more precisely.

A. Federated Learning Environment:

Actually, federated learning is gaining popularity in the power and energy sectors as a means of fully utilising smart me data spread across several consumers or merchants. The goal of identifying consumer attributes was presented as a federated learning issue in [34], and three weighted model averaging approaches were contrasted.

The reliability of household load forecasting was increased by using edge computing and federated learning, as described in reference number. Bayesian neural networks (BNNs) were trained in a federated fashion to decompose home solar PV generation from behind the metre (BTM) in. A federated forecasting model was developed in [ ] to estimate the charging demand of electric car networks. A federated reinforcement learning model was used in [ ] for home multi-cloud infrastructures in order to fully utilize the operational data from numerous smart homes. These projects are essentially federated supervised learning, like regression or classification models. The literature on federated unsupervised learning, particularly for clustering, is currently relatively limited.

Federated learning may create a unified training model for numerous sources of data while sacrificing security or privacy. Consequently, it will have a broad range of application situations in a variety of fields. Consider the multi-cloud infrastructures system as an illustration. With the rapid development of my country's consumer goods market, a user-oriented multi-cloud infrastructures system, such as the peer-to-peer approach, coordinated scheduling-based scheme, and centralised control technique, is urgently needed. These tactics lack smart tools compatible with existing multi-cloud infrastructures systems and fail to segment users to increase product consumers' durability. Right now, developing a set of user data training model based on federated learning to take part in the assistance decision-making of the multi-cloud infrastructures system is a good solution to overcome the aforementioned issues. It is anticipated that in the not-too-distant future, federated learning will remove barriers that currently exist between different businesses and build a new model for the preservation and exchange of information and data.

B. Simulation Environment:

- **CloudSim:**

CloudSim [16] is a popular multi-multi-cloud computing simulation platform that is a function library built on the discrete event simulation package SimJava. CloudSim encourages multi-multi-cloud computing creation and research as well as the modelling and simulation of various multi-multi-cloud computing infrastructures. Because of this, CloudSim has inspired a number of spinoff projects, such as iFogSim [17], CloudSimSDN [18], and Container CloudSim [19], which aim to improve upon the original.

- **ifogSim:**

ifogSim [17] is a toolkit designed to simulate a fog compute cluster, which is conceptually related to edge computing. iFogSim employs both a central server and an edge server that is located closer to the user. It can be used to construct an integrated edges and clouds modeling scenario for assessing multi-multi-cloud - based resources management practices. The control of computer resources, such as CPU, memory, and storage, is the main focus of iFogSim. On the contrary, in addition to these functions, our simulation platform may implement more complicated network functions.

An edge-based collaborative learning framework called CLONE [20] is used primarily to address the tension between edge intelligence and privacy protection as well as the constraint of insufficient bandwidth. CLONE training and CLONE inference are its two application scenarios for collaborative model training and inference on edge devices. The main concept is that a group of dispersed edge nodes working under the direction of an edge server may complete training and inference activities. The edge server is in charge of aggregating or carrying out any other required operations on the uploaded parameters before sending the modified parameters back to the edge node. Each edge node trains the neural network simulation individually based upon the private tutoring material and pushes the associated variables to the endpoint during training/inference.

- **Kubernetes based Multi-multi-cloud Platform:**

With Kubernetes' widespread use as a containerized programmed that administers numerous hosts on the multi-multi-cloud platform, it is now easy and effective to deploy containerized apps. Kubernetes is, however, created for multi-multi-cloud data center's. The first Kubernetes-based open-edge computing platform in the world, KubeEdge [21], offers cloud-side collaborative features. For cloud-edge

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

cooperation, resource heterogeneity, and lightweight functionality, it depends on Kubernetes' scheduling and container orchestration features. K3S [22] is made for R&D operation and maintenance staff who manage Kubernetes in a resource-constrained setting. The goal is to run tiny Kubernetes clusters on edge nodes with x86, ARM64, and ARMv7D architectures.

The cloud-edge collaboration is not involved because K3S's entirety—including the server and agent—runs on the edge. Although these connected systems show how their frameworks can be used, creating one of these systems takes a lot of resources and time to set up the environment and run the corresponding model. In order to execute large-scale, cost-effective simulation and evaluation for particular offloading decision or resource scheduling algorithms, it is still important to develop a toolkit that is both efficient and lightweight. This requirement is met by creating a quick simulation tool for analysing work offloading choices and tactics in edge-multi-multi-cloud scenarios.

C. Problem Statement:

In this recent scenario, there are various learning mechanism are established as it is associated with federated learning and it performs data training process using various data source repository. Main challenges faced by the learning mechanism are not to compromise the security and privacy while transmitting the data between the client and server. This learning mechanism is being used by various real time applications. While deploying the multi-cloud infrastructures system, users have to apply approach based on peer to peer, scheduling co-ordinately and centralized scheduling method. As the above strategies are deployed, there are various challenges faced such as, tool compatibility and failure in the segmentation of user as it helps to improve the consumer product profit. Based on the integration of learning mechanism and federated learning, training the data is performed as it helps to make improved decision making in the multi-cloud infrastructures system. The new management system has to ensure security and privacy among the data's being transferred in the application.

D. Proposed Federated Learning based Clustering Chain (FL-CC) Algorithm:

According to FL-CC approach, Cluster Chain (C-Chain) Algorithm is deployed gets classified into two terminal such as, client and server. Then, exchange is initiated between the client and server.

1. Data cluster gets initiated based on the personal information based on attributed present in the data value.
2. Then classified sampling is performed to extract the trained datasets on the client.
3. In order to train the data model, M_0 → Model Parameter using cluster sampling as it downloads those model parameters from the terminal server.
4. By performing multiple repetitions on the above process, model parameter M gets updated in 'P' client's personal information.
5. Then the updated model parameters are periodically sent to the terminal server.
6. The updated 'M' will be returned to the terminal service as it reaches with 'P' clients and then it generates the summary report.
7. The latest model parameter gets updated and it is denoted as M_0'.

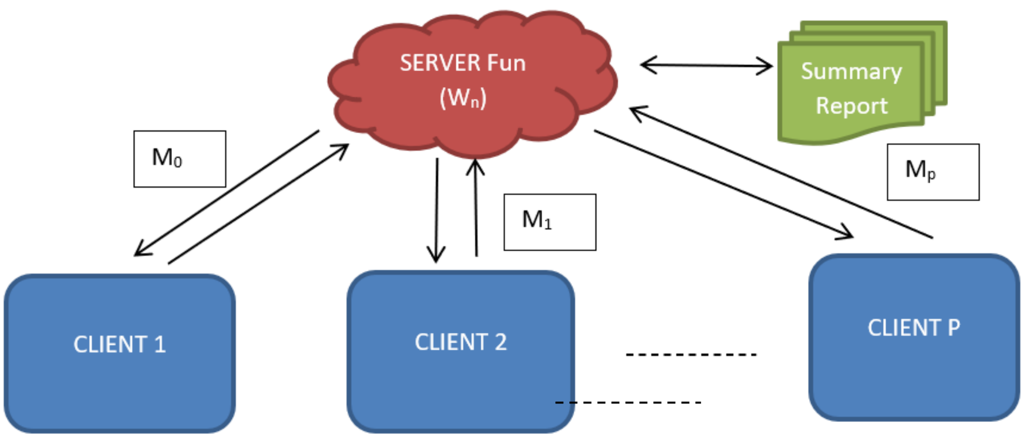


Figure 2. Clustering Chain Process

$$min_{m \in R^d} f(M) \tag{1}$$

$$f(M) = \frac{1}{n} \sum_{i=1}^{n} f_i(M) \tag{2}$$

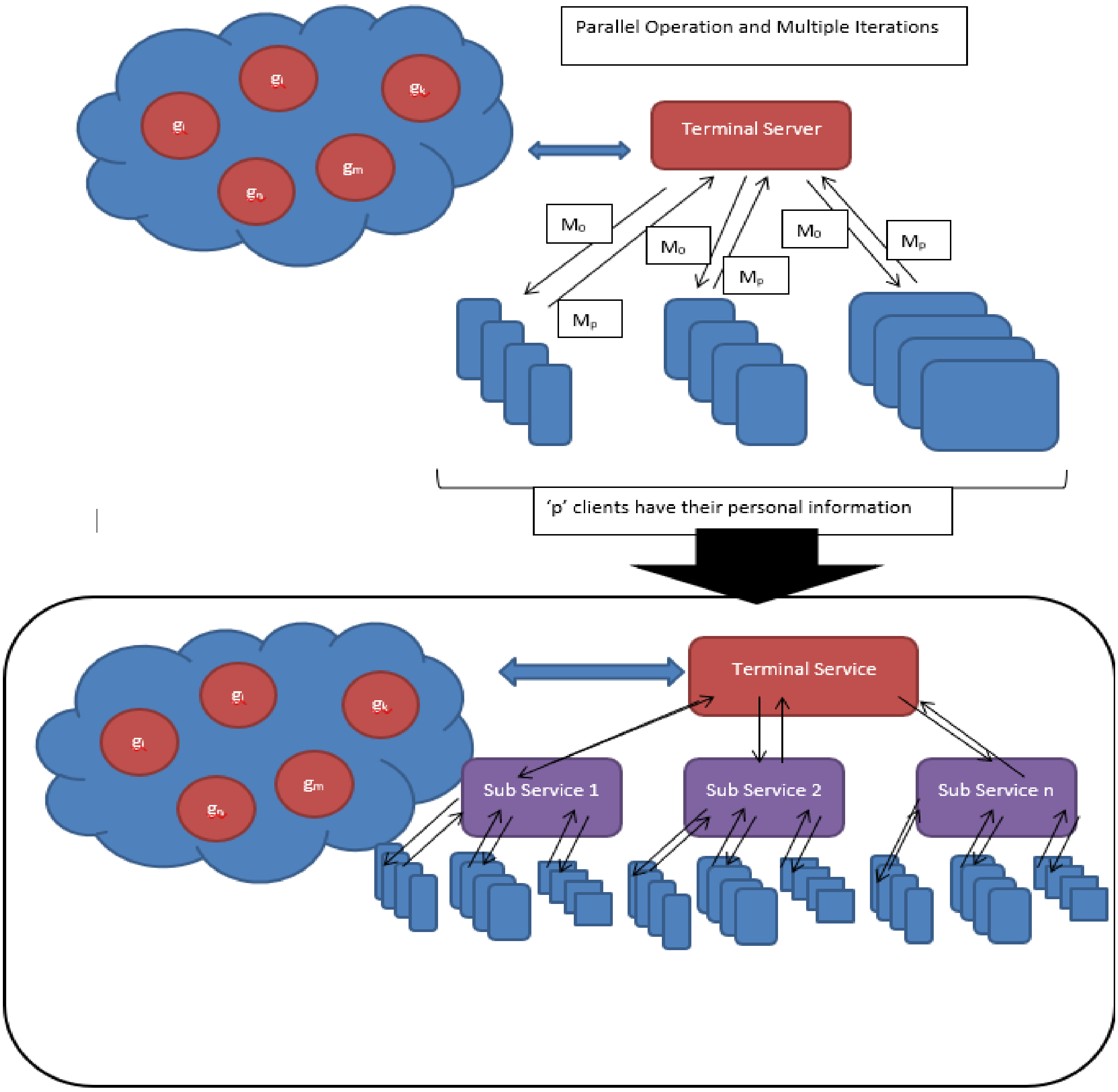
$$f_i(M) = l\ (X_i, Y_i;\ M_i) \tag{3}$$

In federated learning, there are ‘p’ clients as all participate in training process. Where D_p denotes the local data of all ‘p’ clients with size of ‘n_p’.

$$F(w) = \sum_{p=1}^{p} \frac{n_p}{n} F_p\ (M) \tag{4}$$

$$F_p(M) = \frac{i}{n_p} \sum_{i \in D_p} f_i\ (M) \tag{5}$$

$$f_i\ (M) = l(x_i, y_i;\ w_i) \tag{6}$$



3. Proposed FL-CChain Mechanism

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

Algorithm 1: FL-CChain Algorithm

Input: Cluster Center → Y

n^{th} Sample for P^{th} client → D_{pi}

Cluster Set for P^{th} client → I_p

Output: Client 'P' distributed Information.

Based on the cluster set 'Y'

Assume threshold → Θ

If (0 < Θ < 1)

{

Y_1 → Y_1 // Only if ($Y_1 € D_p$)

Y_2 → Y_2 // Only if ($|Y_2 - Y_1|$) >= $|Y_i - Y_1|$, $Z_i € D_p \setminus Y_1$)

}

For ($Z_i € Z$)

For ($D_{pi} € D_p \setminus Y_1$)

$D_{ij} = \| D_{pi} - Z_j \| = \sqrt{(D_{pi} - Z_j)^2}$

// Determine the distance between all the samples for all cluster center 'p'

For i = 0,1,2,….. p

If ($D_s > Θ_{D12}$)

Apply min max method on D_p,

$D_{12} = \| Z_1 - Z_2 \| = \sqrt{(Z_1 - Z_2)^2}$

Based on the algorithm 1, the clients and their personal information are distributed into small federated architecture.

Algorithm 2: Client Side FL-CChain

Input: Small clients are distributed using algorithm 1.

Output: Gradient Gra for each personal clients 'P'

1. Assume recent model parameter as 'M_p' for each clients 'P'
2. If('P' Small Clients =1)
3. {
4. Assign Sample D_{Pj} and consider model parameter for all 'P' Clients as M_p,
5. Determine the gradient 'Gra' of the sample Clients 'P' set.
6. Transfer the 'Gra' to the clients 'P'.
7. }
8. // Client 'P'
9. Attain 'Gra' for all the clients as Gra_{P1}, Gra_{P2}, ….. $Gra_{Pn\,Pj}$,
10. Determine the average weight,
11. $\overline{Gra} = \sum_{m=1}^{n_{pj}} \eta Gra_{pm}$
12. Where,
13. $\eta = \frac{\|\widetilde{Gra} - Gra_{pm}\|}{\sum_{m=1}^{n_{pj}} \|\widetilde{Gra} - Gra_{pm}\|}$
14. $\widetilde{Gra} = \sum_{m=1}^{n_{pj}} \frac{n_{pj}}{n_p} Gra_{pm}$

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

15. {
16. Assign Sample D_{Pj} and consider model parameter for all 'P' Clients as M_p,
17. Determine the gradient 'Gra' of the sample Clients 'P' set.
18. Transfer the 'Gra' to the clients 'P'.
19. }

Based on the algorithm 2 and 3, accuracy of the model gets improved as the proposed mechanism uses the determined weight of the client and the updated model parameter. Then above parameter makes to calculate the parameter degree based on deviation.

Algorithm 3: Terminal Service

Input: Model Parameter 'M'

Output: Average weight M_{p+1}

1. Attain $M_{(t+1)1}$, $M_{(t+1)2}$, ….. $M_{(t+1)p}$ for all client personal information.
2. Determine the local parameter of the weighted value as,
3. $$M_{p+1} = \sum_{m=1}^{K} \eta M_{(p+1)m}$$
4. $$\eta = \frac{\|\widetilde{M} - M_{(p+1)m}\|}{\sum_{m=1}^{p} \|\widetilde{M} - M_{(p+1)m}\|}$$
5. $$\widetilde{M} = \sum_{m=1}^{p} \frac{n_p}{n} M_{(p+1)m}$$
6. Send the parameter updated M_{p+1} for all 'P' clients and it gets updated for the next process.

IV. PERFORMANCE ANALYSIS

In this analysis, two existing algorithms are analysed such as, FedClusAvg and FebAvg as they are analysed based on the federated learning dataset. The parameters such as, accuracy, precision, recall and F1Score are determined by using certain formulae as mentioned below,

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{2}{F1} = \frac{1}{P} + \frac{1}{R}$$

$$F\ Measure = \frac{2TP}{2TP + FP + FN}$$

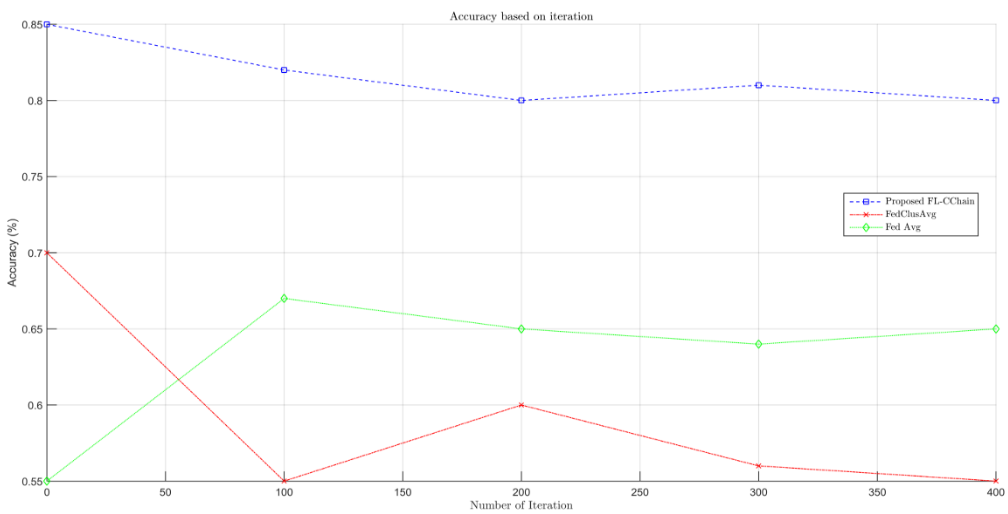


Figure 4. Number of Iteration Vs. Accuracy

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

In Figure 4, the accuracy of data is determined based on the iteration variation from 0 to 400. The proposed FL-CChain mechanism get improved accuracy as it gradually increases from 0.80 to 0.85. The proposed mechanism performs better as compared to the FedClusAvg and FedAvg existing algorithms.

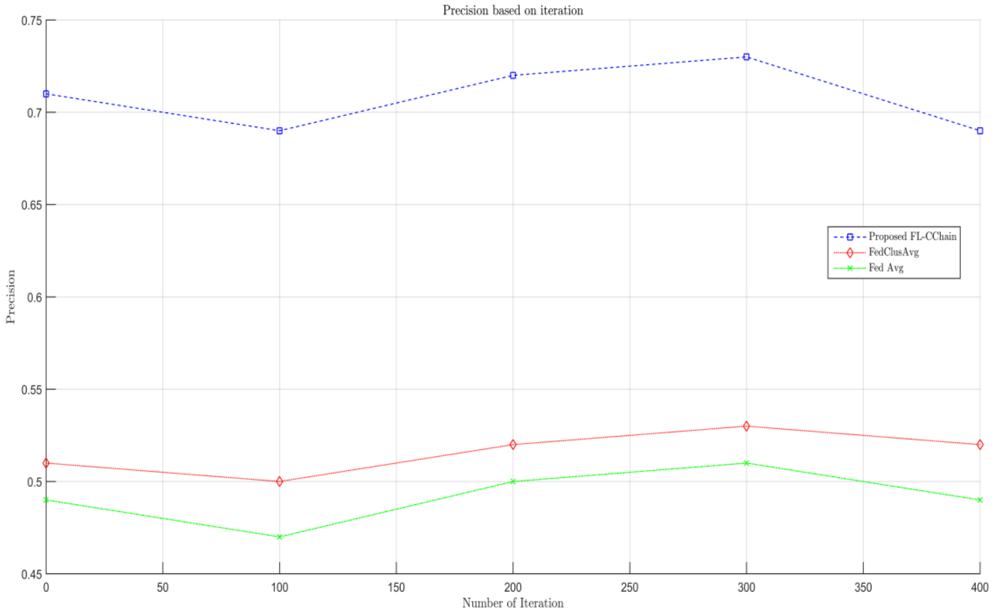


Figure 5. Number of Iteration Vs. Precision

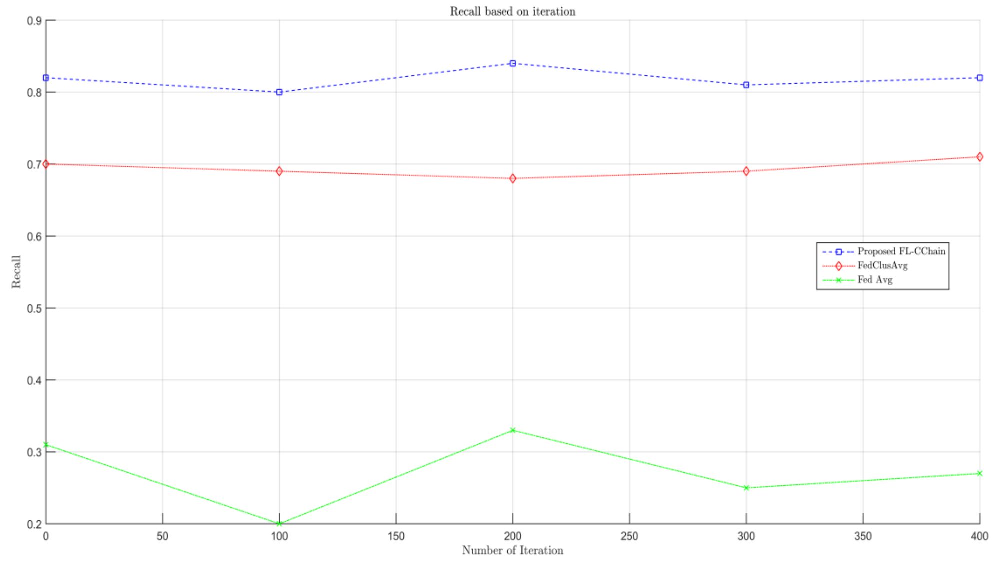


Figure 6. Number of Iteration Vs. Recall

In Figure 5, the data precision value is calculated based on the variation in iteration from 0 to 400. The proposed FL-CChain mechanism gets improved as the existing ones performs 0.3 and 0.7 values for FedAvg and FedClusAvg. Also, the proposed mechanism performs better interm of data recall with value ranges from 0.80 to 0.85 as represented in figure 6. The proposed mechanism outperforms better compared to the two existing ones such as, FedClusAvg and FedAvg.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

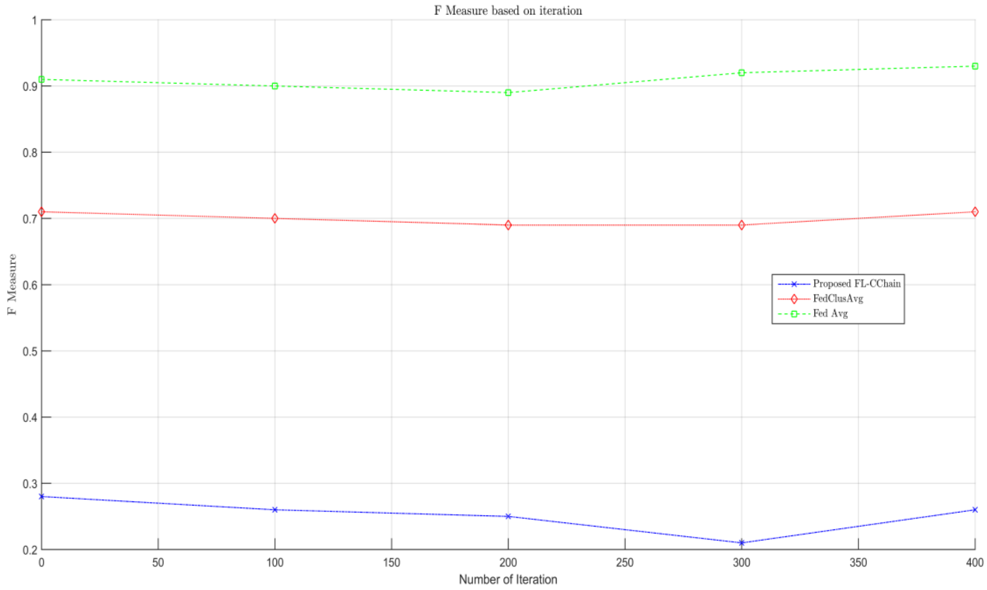


Figure 7. Number of Iteration Vs. F-Measure

In Figure 7, F-Measure is calculated and it gets improved with value between 0.90 to 0.95 for the proposed mechanism and it performs better as compared to other two existing ones such as, FedClusAvg and FedAvg.

V. CONCLUSION

The FedclusAvg and FedAvg method is the basic foundation of this research, which uses it to address the issue of Non-IID of data in federated learning. The algorithm outputs are more accurate and the model can have fewer communications by enhancing and optimizing's it. To counteract the effect of the generic gradient descent algorithm's accuracy loss when the client data distribution is wide, the FL-CChain mechanism is proposed and introduces the degree of departure from the average parameter. Concurrently, the client split approach is employed to equalize data distribution within the client. When there is a significant amount of non-IID data, the model is significantly impacted and the algorithm produces superior results.

References:

[1]. Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," IEEE Trans. Smart Grid, vol. 10, no. 3, pp. 3125–3148, May 2019.

[2]. G. Chicco and A. Mazza, "Chapter 13—Load profiling revisited: Prosumer profiling for local energy markets," in Local Electricity Markets, T. Pinto, Z. Vale, and S. Widergren, Eds. Amsterdam, The Netherlands: Academic, 2021, pp. 215–242.

[3]. C. Feng, Y. Wang, K. Zheng, and Q. Chen, "Smart meter data-driven customizing price design for retailers," IEEE Trans. Smart Grid, vol. 11, no. 3, pp. 2043–2054, May 2020.

[4]. P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2886–2927, 3rd Quart., 2019.

[5]. F. Farokhi, "Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling," IET Smart Grid, vol. 3, no. 5, pp. 605–613, 2020.

[6]. J. Yang, J. Zhao, F. Wen, and Z. Dong, "A model of customizing electricity retail prices based on load profile clustering analysis," IEEE Trans. Smart Grid, vol. 10, no. 3, pp. 3374–3386, May 2019.

[7]. R. R. Avula, J.-X. Chin, T. J Oechtering, G. Hug, and D. Månsson, "Design framework for privacy-aware demand-side management with realistic energy storage model," IEEE Trans. Smart Grid, vol. 12, no. 4, pp. 3503–3513, Jul. 2021.

[8]. J.-X. Chin, K. Baker, and G. Hug, "Consumer privacy protection using flexible thermal loads: Theoretical limits and practical considerations," Appl. Energy, vol. 281, Jan. 2021, Art. no. 116075.

[9]. G. Giaconi, D. Gündüz, and H. V. Poor, "Privacy-cost trade-offs in smart electricity metering systems," IET Smart Grid, vol. 3, no. 5, pp. 596–604, 2020.

[10]. D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, "Energy theft detection with energy privacy preservation in the smart grid," IEEE Internet Things J., vol. 6, no. 5, pp. 7659–7669, Oct. 2019.
[11]. M. Jia, Y. Wang, C. Shen, and G. Hug, "Privacy-preserving distributed clustering for electrical load profiling," IEEE Trans. Smart Grid, vol. 12, no. 2, pp. 1429–1444, Mar. 2021.
[12]. T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, May 2020.
[13]. Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," ACM Trans. Intell. Syst. Technol., vol. 10, no. 2, pp. 1–19, 2019.
[14]. A. Benaissa, B. Retiat, B. Cebere, and A. E. Belfedhal, "TenSEAL: A library for encrypted tensor operations using homomorphic encryption," 2021, arXiv:2104.03152.
[15]. S. Lee and D.-H. Choi, "Federated reinforcement learning for multi-cloud infrastructures of multiple smart homes with distributed energy resources," IEEE Trans. Ind. Informat., vol. 18, no. 1, pp. 488–497, Jan. 2022.
[16]. Y. M. Saputra, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz, M. D. Mueck, and S. Srikanteswara, "Energy demand prediction with federated learning for electric vehicle networks," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1–6.
[17]. J. Lin, J. Ma, and J. Zhu, "A privacy-preserving federated learning method for probabilistic community-level behind-the-meter solar generation disaggregation," IEEE Trans. Smart Grid, vol. 13, no. 1, pp. 268–279, Jan. 2022.
[18]. D. Xu, Q. Wu, B. Zhou, C. Li, L. Bai, and S. Huang, ``Distributed multi-energy operation of coupled electricity, heating, and natural gas networks," IEEE Trans. Sustain. Energy, vol. 11, no. 4, pp. 2457-2469, Oct. 2020.
[19]. H. Ming, B. Xia, K.-Y. Lee, A. Adepoju, S. Shakkottai, and L. Xie, ``Prediction and assessment of demand response potential with coupon incentives in highly renewable power systems," Protection Control Mod. Power Syst., vol. 5, no. 1, pp. 1-14, Dec. 2020.
[20]. S. K. Injeti and V. K. Thunuguntla, ``Optimal integration of DGs into radial distribution network in the presence of plug-in electric vehicles to minimize daily active power losses and to improve the voltage prole of the system using bio-inspired optimization algorithms," Protection Control Mod. Power Syst., vol. 5, no. 1, pp. 1-15, Dec. 2020.
[21]. H. Zhu, R. S. M. Goh, and W.-K. Ng, ``Privacy-preserving weighted federated learning within the secret sharing framework," IEEE Access, vol. 8, pp. 198275-198284, 2020.
[22]. T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, ``Federated learning: Challenges, methods, and future directions," IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50-60, May 2020.
[23]. Y. Yan, S. Liu, Y. Jin, Z. Qian, S. Zhang, and S. Lu, ``Risk minimization against transmission failures of federated learning in mobile edge net- works," IEEE Access, vol. 8, pp. 98205-98217, 2020.
[24]. S. Kim, ``Incentive design and differential privacy based federated learning: A mechanism design perspective," IEEE Access, vol. 8, pp. 187317-187325, 2020.
[25]. B. Han and H. Jiang, ``An improved pam algorithm for numerical data under non-independent and identical distribution," (in Chinese), J. Qilu Univ. Technol., vol. 33, no. 2, pp. 56-61, 2019.
[26]. B. Pan, H. Qiu, and J. Zhang, ``Research on federated machine learning technology with different data distribution," (in Chinese), in Proc. 5G Netw. Innov. Seminar, 2019, p. 6.
[27]. Q. Yang, Y. Liu, T. Chen, and Y. Tong, ``Federated machine learning: Concept and applications," ACMTrans. Intell. Syst. Technol., vol. 10, no. 2, pp. 1-19, 2019.
[28]. M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, ``Federated learning: A survey on enabling technologies, protocols, and applications," IEEE Access, vol. 8, pp. 140699-140725, 2020.
[29]. [26] Z. Huang, B. Fang, and J. Deng, ``Multi-objective optimization strategy for distribution network considering V2G-enabled electric vehicles in building integrated energy system," Protection Control Mod. Power Syst., vol. 5, no. 1, p. 27, Dec. 2020.
[30]. H.Wang, Y. Liu, B. Zhou, C. Li, G. Cao, N. Voropai, and E. Barakhtenko, ``Taxonomy research of articial intelligence for deterministic solar power forecasting," Energy Convers. Manage., vol. 214, Jun. 2020, Art. no. 112909.