



Blockchain enabled secure federated learning framework

Hemalatha B M ^{1,*} and Sharath M N ² and Lohith D K ²

¹ Department of Computer Science and Engineering, Rajeev Institute of Technology, Hassan.

² Department of Computer Science and Engineering (AI and ML), Rajeev Institute of Technology, Hassan.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(03), 1640-1648

Publication history: Received on 08 March 2025; revised on 05 June 2025; accepted on 07 June 2025

Article DOI: <https://doi.org/10.30574/wjaets.2025.15.3.0335>

Abstract

Federate machine learning (FML) is a novel concept that trains the model to leverage data from many users rather than store the data. Federated learning (FL) allows participants to be involved without disclosing sensitive data to train the model. The server will initialize the global model with all connected participants. After the initialization, the initial global model gets trained locally with the participant's local data set. The level of security directly affects or impacts the overall performance of the FML. Also, many security frameworks in FML are designed to handle specific types of attacks in the training phase, communication phase, or aggregation phase. Integrating Blockchain into FML system would greatly help to enhance the security further. Therefore, this work propose a Convolution Neural Network (CNN) based novel Blockchain enabled secure federated learning method to leverage security benefits for image processing applications and benchmark the performance in terms of running time for key generation in authentication, global model generation in the server, the model accuracy and loss. The proposed scheme is suitable for generic image processing applications in Healthcare, Agriculture, Face detection etc.

Keywords: FML; CNN; FL

1. Introduction

Blockchain is a decentralized, distributed ledger technology as shown in Figure 1 that enables secure and transparent record keeping of transactions across much a participant (or node) maintains a copy of the entire ledger. Transactions are grouped into blocks, which are then cryptographically linked to form a chain, ensuring data integrity and immutability. One of the key features of Blockchain is its ability to provide trust without the need for intermediaries. This is achieved through consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), which validate and confirm transactions. The decentralized nature of blockchain enhances security, as altering a single block would require consensus from the majority of the network, making it highly resistant to fraud and tampering.

Blockchains are regarded as a significant advancement in secure computing that operates without the need for central authority. Essentially, a blockchain is a decentralized database that organizes ongoing transactions into blocks, creating a chain-like structure among these blocks. From a security perspective, blockchains function on a peer-to-peer (P2P) overlay network and employ consensus mechanisms along with cryptographic algorithms to maintain their Security. The rising popularity of digital cryptocurrencies like Bitcoin has garnered significant attention from governments, regulators, financial institutions, and technology companies [4]. Blockchains are viewed as a promising solution for secure data storage, sharing, and analysis, as well as for trusted network control and resource management. Consequently, blockchains have become integral to daily life and work, impacting areas such as cryptocurrency, digital finance, supply chains, smart cities, and the Internet of Things (IoT).

* Corresponding author: Hemalatha B M

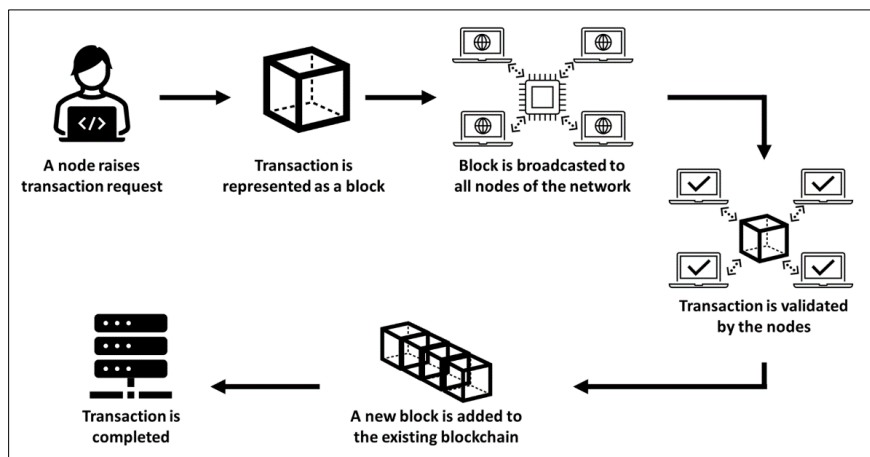


Figure 1 Blockchain transaction

1.1. Types of Blockchain

- The blockchain can be implemented in Public **Consortium**
- Private modes as shown in Figure 2. In this project, private blockchain is used only within the federated learning system.

1.1.1. Public Blockchain

It also known as permission less blockchains, public blockchains operate without a central authority. The associated data lacks specific read and write access controls, allowing any node in the network to join at any time.

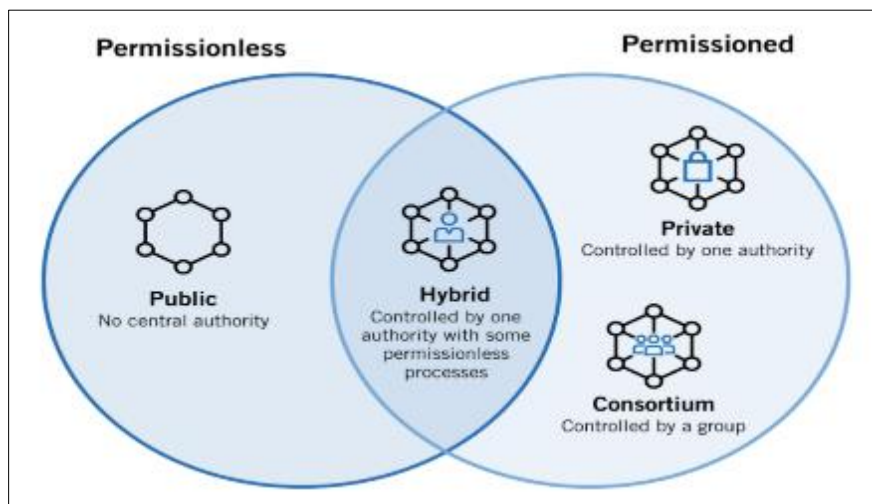


Figure 2 Blockchain types

1.1.2. Consortium Blockchain

It also referred to as permissioned blockchains, consortium blockchains occupy a middle ground between public and private blockchains. They utilize a "partial decentralization" approach and are jointly managed by multiple enterprises or institutions [6].

Participants must register and authenticate in advance, and adding a new node requires approval from other consortium members. Compared to public blockchains, consortium blockchains involve fewer participating nodes. The data is recorded and maintained by authenticated participants who have the right to access it.

1.1.3. Private Blockchain

Private blockchains are controlled by a single organization or individual, with write permissions restricted to the controller. These blockchains have stringent standards for node access, resulting in faster transactions and enhanced privacy. While they offer higher security compared to public blockchains, their level of decentralization is significantly reduced.

In the era of big data, data is considered a valuable asset. Consequently, data privacy protection and security have become paramount concerns. It is evident that the emphasis on data privacy and security has become a global trend, and the introduction of various laws and regulations has made data acquisition more challenging (Refer Figure 3).

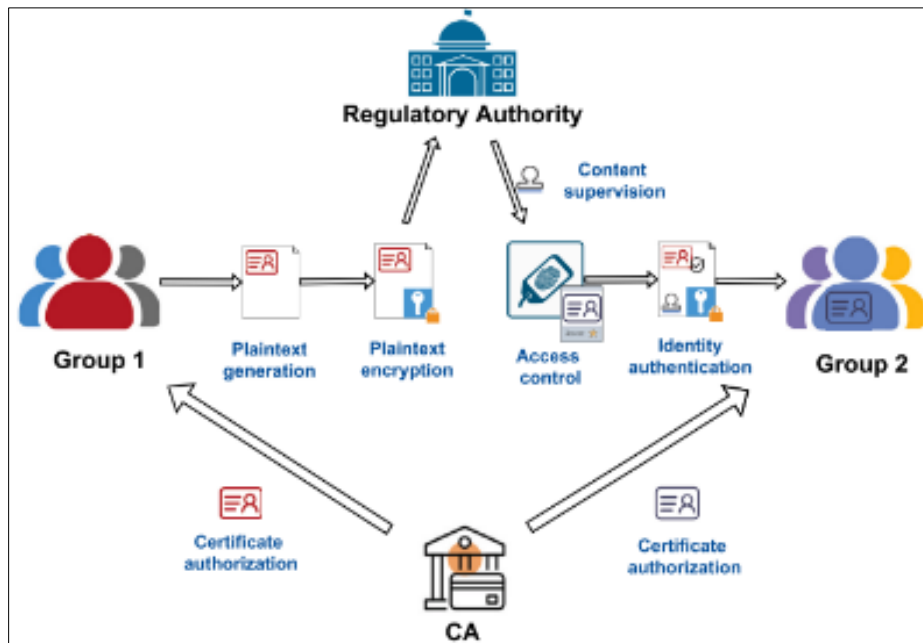


Figure 3 The general configuration of blockchain-based data exchange [7]

1.2. Types of Federated Learning

1.2.1. Horizontal Federated Learning:

In this, datasets are divided horizontally (according to the user dimension) and the portion of the data that has similar user attributes but differs in users is considered for training (Refer Figure 4). It is comparable to when data is divided horizontally within a tabular format. Actually, "horizontal" is derived from the term "horizontal\partition," which is frequently used in relation to a database's conventional\tabular-view.

1.2.2. Vertical Federated Learning

In this, datasets are divided vertically (based on the user feature dimension) and the portion of the data that has similar users but differing user attributes is considered for training. A machine learning technique called Vertical Federated-Learning (VFL) enables several parties to work together on model training without/exchanging raw-data or model parameters.

1.3. Problem Statement

- The federated learning systems tried to protect the privacy of local data on each device. However, there is a high-chance that the system may leak sensitive information to a third-party during communication.
- The model aggregator is totally unaware of the local training process in federated learning.
- The system is vulnerable to various attacks such as model and data poisoning, flipping labels etc.
- The promising privacy-preserving solutions such as differential privacy, homomorphic encryption, secure multi-party computations also face byzantine attack, security breaches, latency, efficiency, and performance deterioration issues.

2. Literature review

This section broadly covers existing works in FL systems, pros and cons of existing systems, introduction to proposed system, tools, technologies and libraries used in the project. Following are the some of the literatures collected on the study.

Zubaydi et al. [5] investigated and analysis of research focused on the integration of blockchain technology with the Internet of Things (IoT). Their study primarily addresses the security and privacy/challenges that arise from this combination. Initially, they provide an overview of the fundamental concepts, principles, and architectures of both blockchain and IoT. Following this, they compared the relevant literature based on application scenarios and technological choices. Finally, discussed the potential for leveraging blockchain to enhance security and privacy in IoT applications.

Mohanta et al. [6] examined the practical deployment of blockchain technology across various sectors from an academic standpoint. The study also evaluates advancements in blockchain application by various entities and elaborates on the security' and privacy challenges associated with blockchain technology.

Guo et al. [7] introduced a decentralized and equitable marginal transaction system leveraging blockchain and differential privacy. The system utilizes blockchain technology to thwart tampering by malicious nodes in transactions and contracts, while introducing an indexing mechanism to safeguard the authenticity and confidentiality of transactions.

3. System design and development

System Design Introduction This section covers the overall system design and development steps required to execute the project.

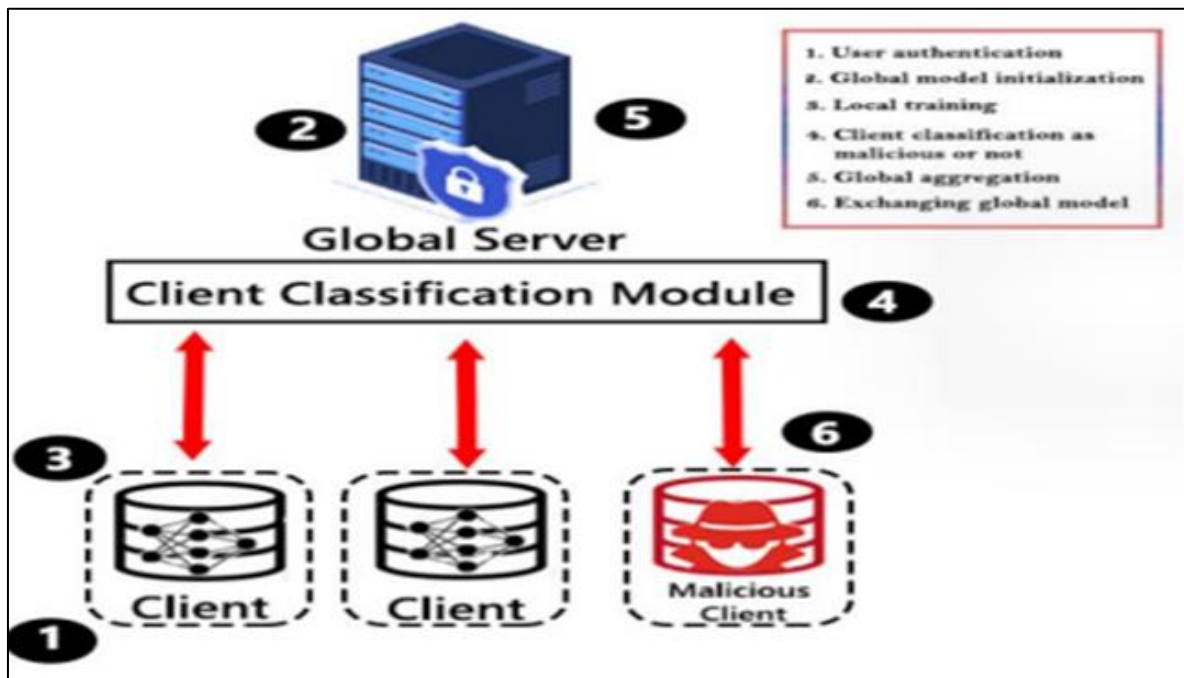


Figure 4 the proposed FL/FML Framework

- Peer-to-peer (P2P) environment: A Blockchain based distributed peer-to-peer environment is created where each node is a block in the Blockchain.
- FL setup: The server initiates the process by sending the initial model parameters to all the participating clients as shown in Figure 4. Using received parameters, each client will execute the local deep learning model on the local data. In each round, aggregated global parameters are exchanged between the beginning clients.

- Privacy Mechanism: The proposed blockchain based secure federated machine learning uses differential privacy as the underlying privacy mechanism to preserve client privacy.
- Authentication: Each client should authenticate to the server before running the machine learning process using ECDSA. The detailed authentication mechanism incorporated in the proposed project is explained in the next section.
- Key Management: The project adopts a fine-grained key-management mechanism to manage authentication keys in the system.

4. Blockchain Integration Mechanism

The Blockchain can be effectively integrated with FL process to store FL transactions such as gradient values as shown in Figure 5.

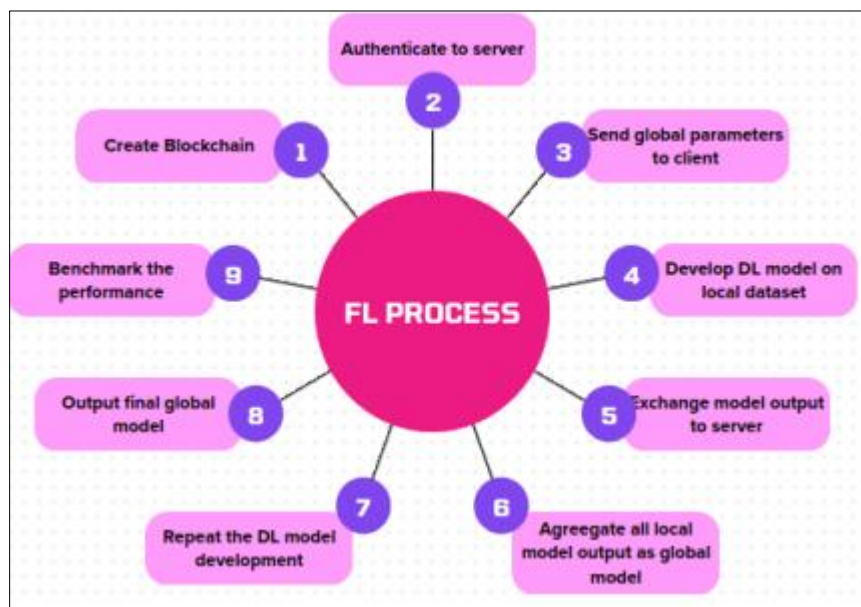


Figure 5 Blockchain integration with FL process

5. Implementation

- Methods and Functionalities Here, Blockchain enabled federated machine' learning framework has been developed in python using VS Code as the development platform. This project mainly contains following files and their brief overview:
- Block.py: This file defines a class called Block with genesis (), adjust Difficulty (), mine Block () functionalities to create a block based on mining output.
- Blockchain.py: This file defines a class called Blockchain with add Block (), is chain valid (), replace chain () functionalities.
- Device.py: This file defines a device class to connect to a fog-server with register device (), authenticate Device (), establish communicaton () functionalities.
- Fogserver.py: This file defines a fog server class add Device (), search database (), authentication request (), search blockchain (), generate keypair () functionalities.
- Clientkey.py: This file defines a generate keys (), print key lengths () functionalities on the client side.
- Serverkey.py: This file defines generate keys (), print key lengths () functionalities on the server side.

5.1. Blockchain node creation

Each client defines a Blockchain class to add a new block and check the validity of the block as shown in Figure 6. The Blockchain is primarily introduced to provide enhanced security, immutability, tamper resistance functionalities.


```

class Blockchain:
    def __init__(self):
        self.chain = list()
        initial_block = block.Block.__genesis__()
        self.chain.append(initial_block)

    def addBlock(self, idfs, idA, idB, prkA, prkB, pukA, pukB, prfs, pbfs, skfs):
        newBlock = block.Block.__mineBlock__(
            prevBlock=self.chain[len(self.chain)-1], idfs=idfs, idA=idA,
            idB=idB, prkA=prkA, prkB=prkB, pukA=pukA, pukB=pukB, prfs=prfs,
            pbfs=pbfs, skfs=skfs
        )
        self.chain.append(newBlock)

    @staticmethod
    def __is_chain_valid__(self, chain):
        first_block = chain[0]
        if (first_block != block.Block.__genesis__()):
            return False

```

Figure 6 The Blackchin class

5.2. Authentication module

In this project, server generates a pair of 256 bits or 512 bits (public, private) keys as shown in Figure 7 a) and sends the public key to each participating client. Similarly, each participating client also generates pair of 256 bits or 512 bits (public, private) keys as shown in Figure 7 b) and sends the public key to the federated learning server.

5.2.1. FML Evaluation

The FML concept is introduced during the evaluation stage by connecting two clients. This strategy includes t numbers of rounds. Server initiates the process by initializing the global settings with the connected users as shown in Figure 7

```

PS C:\Users\Radha\Desktop\Project_Hasan\FML-3> python .\server4.py
2024-08-06 14:59:49.537248: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly different numerical results
due to floating-point round-off errors from different computation orders. To turn them off, set the environment variable 'TF_ENABLE_ONEDNN_OPTS=0'
.
2024-08-06 15:00:14.820627: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly different numerical results
due to floating-point round-off errors from different computation orders. To turn them off, set the environment variable 'TF_ENABLE_ONEDNN_OPTS=0'
.
C:\Users\Radha\AppData\Local\Packages\PythonSoftwareFoundation.Python.3.12_qbz5n2kfra8p0\LocalCache\local-packages\Python312\site-packages\keras\s
rc\layers\convolutional\base_conv.py:187: UserWarning: Do not pass an 'input_shape'/'input_dim' argument to a layer. When using Sequential models,
prefer using an 'Input(shape)' object as the first layer in the model instead.
  super().__init__(activity_regularizer=activity_regularizer, **kwargs)
2024-08-06 15:01:01.241443: I tensorflow/core/platform/cpu_feature_guard.cc:210] This TensorFlow binary is optimized to use available CPU instruct
ions in performance-critical operations.
To enable the following instructions: AVX2 FMA, in other operations, rebuild TensorFlow with the appropriate compiler flags.
INFO : Starting Flower server, config: num_rounds=2, no round_timeout
INFO : Flower ECE: gRPC server running (2 rounds), SSL is disabled
INFO : [INIT]
INFO : Requesting initial parameters from one random client

```

Figure 7 FML Process on Server

6. Results and observations

6.1. Blockchain Block Creation

All the participating client mines the block and creates a new block as shown in Figure 8 and generates a session key between client and server for further use in Blockchain.



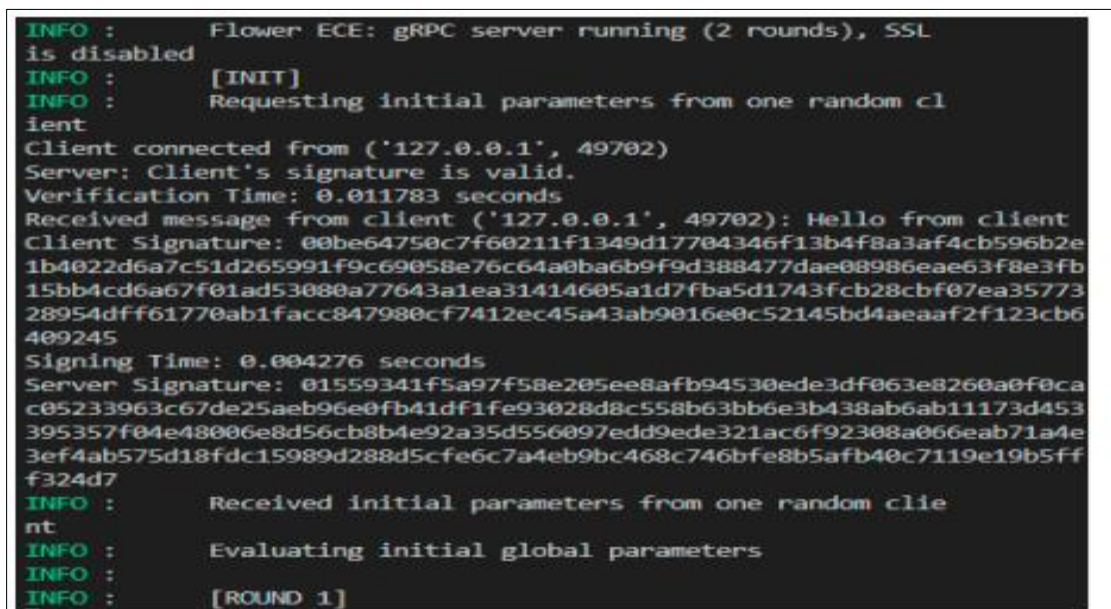
```
PS C:\Users\Radha\Desktop\Project_Hasan\fm1-3> python .\device.py

New block mined!
Key sharing is success
Session Key is: 2f62f576cae5dd077f2b13f0beba5d53c62105b13a45832d1947abf7b1498123139c284babe774888843b9db3cc45327ecb87321cdf005f1100644f390801fa1
Key sharing is success
Session Key is: 669fcb794347c94625dad4b3c5587150ea8c4e31b5855e52f650f9af4d793857aa97a74b0da3835a94affcb770f202012cac6905b4bf33907f0e74562dd22660
```

Figure 8 Block Creation in Blockchain

6.2. Verification of Signature

Each client should be authenticated to the server as shown in Figure 9 before starting the deep learning model. The unauthenticated clients will be removed from the server and not allowed to participate in the federated learning process.



```
INFO : Flower ECE: gRPC server running (2 rounds), SSL
is disabled
INFO : [INIT]
INFO : Requesting initial parameters from one random client
Client connected from ('127.0.0.1', 49702)
Server: Client's signature is valid.
Verification Time: 0.011783 seconds
Received message from client ('127.0.0.1', 49702): Hello from client
Client Signature: 00be64750c7f60211f1349d17704346f13b4f8a3af4cb596b2e
1b4022d6a7c51d265991f9c69058e76c64a0ba6b9f9d388477dae08986eae63f8e3fb
15bb4cd6a67f01ad53080a77643a1ea31414605a1d7fba5d1743fcb28cbf07ea35773
28954dff61770ab1facc847980cf7412ec45a43ab9016e0c52145bd4aeaaf2f123cb6
409245
Signing Time: 0.004276 seconds
Server Signature: 01559341f5a97f58e205ee8afb94530ede3df063e8260a0f0ca
c05233963c67de25aeb96e0fb41df1fe93028d8c558b63bb6e3b438ab6ab11173d453
395357f04e48006e8d56cb8b4e92a35d556097edd9ede321ac6f92308a066eab71a4e
3ef4ab575d18fdc15989d288d5cfe6c7a4eb9bc468c746bfe8b5afb40c7119e19b5ff
f324d7
INFO : Received initial parameters from one random client
INFO : Evaluating initial global parameters
INFO : [ROUND 1]
```

Figure 9 The Signature verification

6.3. Performance Evaluation

The proposed work involves different ECC curves for authentication such as BrainpoolP256R1, BrainpoolP384R1, SECP256K1, SECP256R1, SECP384R1, SECP521R1. Among all these, SECP256K1 curve is taking least time (in seconds) to generate the authentication keys on the server as shown in Figure 10 a). Similarly, SECP256K1 curve is taking least time (in seconds) to generate the authentication keys on the client as shown in Figure 10 b).

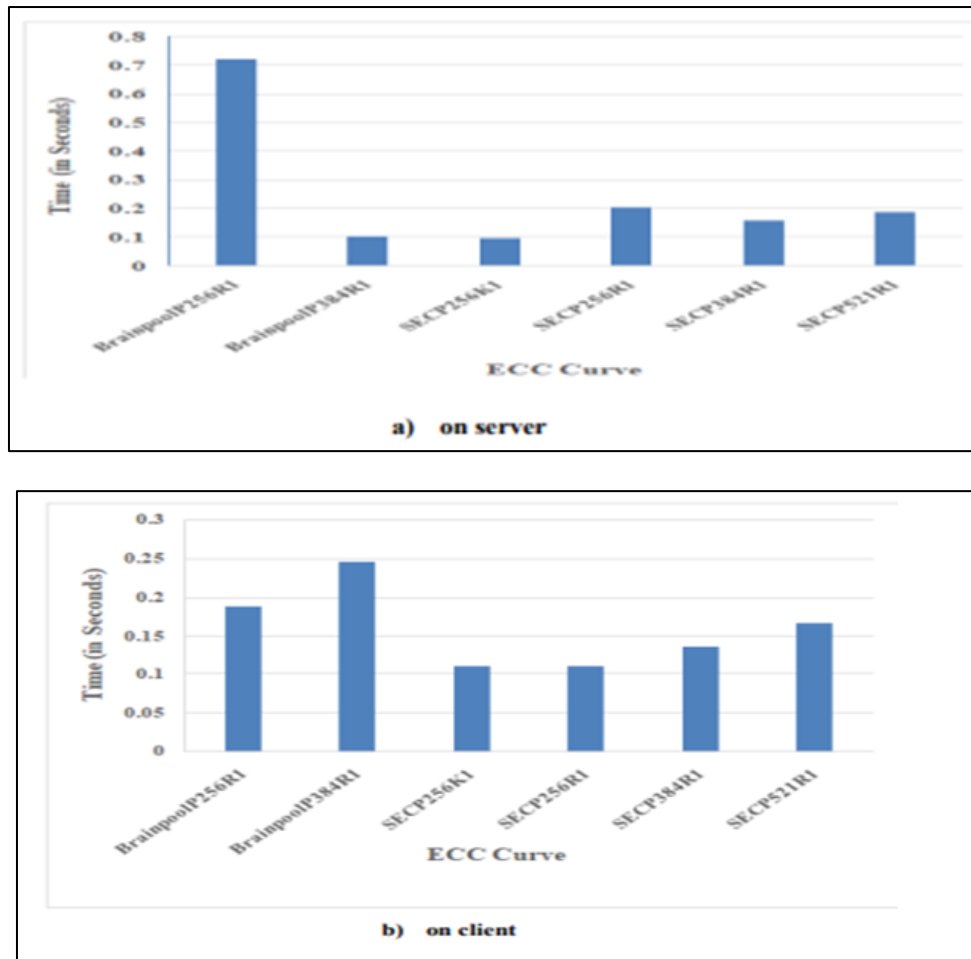


Figure 10 ECC cure v/s generation time

7. Conclusion

The proposed project covers the development of a Blockchain enabled secure federated machine learning framework that has the potential to protect data breach and enhance security while enabling collaborative model training without sharing local data. The Blockchain enabled decentralized FL system will implement an authentication technique to identify valid clients who do not provide faulty model updates and restricts unauthorized access. It also enforces distributed key management strategy for a heterogeneous FML client environment. The proposed work can be demonstrated further in the applications of healthcare, character recognition, agriculture etc. The proposed project is beneficial for organizations that collaboratively address complex problems through cross-organizational insights where data-sharing is restricted and also supports more efficient use of resources by leveraging local computation capabilities. Blockchain enabled federated learning frameworks brings a balance between individual node privacy protection and collaborative model training. This study can be explored in various applications of technologies like Artificial Intelligence, Autonomous Vehicles, Smart Cities, Internet of Things, Natural Language Processing

References

- [1] Omer Faruk Görçün, Dragan Pamucar, Sanjib Biswas, "The blockchain technology selection in the logistics industry using a novel mcdm framework based on fermatean fuzzy sets and Dombi aggregation", *Inf. Sci.* 635 (2023), pp. 345–374.
- [2] Huaqun Guo, Xingjie Yu, "A survey on blockchain technology and its security", *Blockchain Res. Appl.* 3 (2) (2022) 100067.
- [3] LengJidong, LvXueqiang, Jiang Yang, Li Guolin, "Consensus mechanisms of consortium blockchain: a survey", *Data Anal. Knowl. Discov.* 5 (1) (2021), pp. 56–65.

- [4] AmirmohammadPasdar, Young Choon Lee, Zhongli Dong, "Connect api with blockchain a survey on blockchain oracle implementation", *ACM Comput. Surv.* 55 (10) (2023), pp. 1-39.
- [5] HaiderDhiaZubaydi, Pal Varga, Sandor Molnar, "Leveraging blockchain technology for ensuring security and privacy aspects in Internet of things: a systematic literature review", *Sensors* 23 (2) (2023).
- [6] Bhabendu Kumar Mohanta, Debasish Jena, Soumyashree S. Panda and Srichandan Sobhanayak, "Blockchain technology: A survey on applications and security privacy Challenges", *Internet of Things*, Vol. 8, (2023) 100107.
- [7] Jianxiong Guo, Xingjian Ding, Tian Wang, Weijia Jia, "Combinatorial resources auction in decentralized edge-thing systems using blockchain and differential privacy" *Information Sciences*, Vol. 607, (2022) pp. 211-229.
- [8] Liu X, Li H, Xu G, Chen Z, Huang X, Lu R. Privacy-enhanced federated learning against poisoning adversaries. *IEEE Transactions on Information Forensics and Security*. 2021;16:4574-88. doi:10.1109/TIFS.2021.3108434.
- [9] Li Y, Zhou Y, Jolfaei A, Yu D, Xu G, Zheng X. Privacy-preserving federated learning framework based on chained secure multiparty computing. *IEEE Internet of Things Journal*. 2020;8(8):6178-86. doi:10.1109/JIOT.2020.3022911.