Hindawi
Security and Communication Networks
Volume 2021, Article ID 5550153, 14 pages
https://doi.org/10.1155/2021/5550153

Research Article

Blockchain-Enabled 5G Edge Networks and Beyond: An Intelligent Cross-Silo Federated Learning Approach

Sandi Rahmadika,[1] **Muhammad Firdaus**,[1] **Seolah Jang**,[1] **and Kyung-Hyune Rhee**[2]

[1]*Department of Artificial Intelligence Convergence, Pukyong National University, Busan 48513, Republic of Korea*
[2]*Department of IT Convergence and Application Engineering, Pukyong National University, Busan 48513, Republic of Korea*

Correspondence should be addressed to Kyung-Hyune Rhee; khrhee@pknu.ac.kr

Received 22 January 2021; Revised 2 March 2021; Accepted 21 March 2021; Published 28 March 2021

Academic Editor: Jinwei Wang

Edge networks (ENs) in 5G have the capability to protect traffic between edge entry points (edge-to-edge), enabling the design of various flexible and customizable applications. The advantage of edge networks is their pioneering integration of other prominent technologies such as blockchain and federated learning (FL) to produce better services on wireless networks. In this paper, we propose an intelligent system integrating blockchain technologies, 5G ENs, and FL to create an efficient and secure framework for transactions. FL enables user equipment (UE) to train the artificial intelligence model without exposing the UE's valuable data to the public, or to the model providers. Furthermore, the blockchain is an immutable data approach that can be leveraged for FL across 5G ENs and beyond. The recorded transactions cannot be altered maliciously, and they remain unchanged by design. We further propose a dynamic authentication protocol for UE to interact with a diverse base station. We apply blockchain as a reward mechanism in FL to enable computational offloading in wireless networks. Additionally, we implement and investigate blockchain technology for FL in 5G UE.

1. Introduction

Mobile edge computing (MEC) technology, introduced and standardized by the ETSI Industry Specification Group (ISG) in December 2014, aims to enhance user experiences with high bandwidth, low latency, and real-time communications [1]. This technology reduces delay and response time in decision-making computation by leveraging the edge node as local server infrastructure. The concept of edge network (EN) intelligence, combining MEC with artificial intelligence (AI), has emerged to address the challenges arising as a result of accelerating growth in new computing and communication technologies in 5G networks and beyond. In EN intelligence, an AI system manages edge resources to allow powerful computational processing and massive data acquisition on local ENs [2]. Furthermore, in complex environments with heterogeneous resources and numerous devices, AI can achieve efficient self-aggregating communication and intelligent system orchestration, while considering the austere delay constraints as well as other performance requirements of 5G networks and beyond [3].

However, there are concerns about user equipment (UE) privacy issues because EN intelligence transactions still rely on a centralized approach. Hence, federated learning (FL) is offered as a new approach, with the main purpose of protecting UE privacy by building machine learning models without the need to centralize the training data on a central server. This approach empowers a central server to organize the training's orchestration without handling the UE's valuable data. Moreover, a shared AI global model for participating UE is trained using a decentralized approach [4]. In this sense, FL allows all UE involved to train their data locally without revealing the data used to optimize the system model [5], as well as without being able to read the valuable data of other UE. Moreover, the cross-silo FL setting enables the model to be trained on silo data to accommodate flexible and customizable applications. This setting supports UE incentive sharing mechanisms to train the model based on their data,

but the data cannot be shared directly due to confidentiality and legal constraints or differing geographical regions [6]. Several studies have recently proposed this approach in various fields, such as financial risk prediction for reinsurance, pharmaceutical research, electronic health record mining, and medical data segmentation [6].

Additionally, cross-silo FL's incentive mechanism aims to motivate honest UE (as data owners) to provide relevant contributions and encourage long-term participation in system sustainability. Through smart contracts, blockchains can be a solution to accommodate a proper cross-silo FL incentive mechanism. The blockchain enables securely registering and updating transactions in a decentralized manner. Furthermore, the blockchain is secure by design because the data record is irrevocable, tamper-resistant, uses consensus-based decision-making, and inexpensive per transaction overall. Moreover, blockchain technology, as a distributed ledger, facilitates transparent, irreversible, and traceable transactions by leveraging its smart contracts [7]. It is worth noting that smart contracts can be self-executing to improve UE security and transaction efficiency in a secure and immutable manner. Hence, blockchains and smart contracts construct reliable transactions for UE [8], while also improving the system's efficiency.

In this paper, we propose an intelligent system framework by using blockchain technology and smart contracts to provide secure transactions for cross-silo FL as an EN intelligence service in 5G networks and beyond. FL enables UE to train the AI model without exposing its valuable data publicly, while the recorded transactions cannot be altered because the data on blockchains are immutable [9]. The blockchain can be utilized as an incentive mechanism to encourage UE to contribute honestly to improve and maintain the reliability and sustainability of the system. We also consider developing a secure cross-domain transaction system to optimize 5G EN intelligence by applying an adjustable pairing-based cryptography technique, that is, a dynamic authentication protocol. This protocol is employed to support the continuity of cross-silo FL activities by enabling the UE to interact with diverse base stations as well as different provider models in the 5G ENs. In short, the main contribution of this study can be summarized as follows:

- We design the proposed architecture to enable secure and intelligent system orchestration for 5G networks and beyond by leveraging MEC, AI, and blockchain technology.
- We present a dynamic authentication pairing technique to perform an authentication mechanism among different providers with distinct models and remove the intermediaries from the authentication process.
- We formulate an intelligent cross-silo FL prototype and evaluate its performance based on simulation results.
- We design a proportional incentive mechanism based on the data used by leveraging Ethereum smart contracts. This scheme aims to motivate UE to jointly contribute to maintain cross-silo FL activities and ensure the system's security.
- We analyze several essential concerns and remark on our findings related to the gas, or computational cost, required by Ethereum, and flaws of centralized server models within the 5G architecture.

The remainder of this paper is organized as follows. The related work is presented in Section 2. Section 3 provides the background knowledge related to core system components and instrumentation technologies. The proposed architecture of blockchain-enabled 5G edge networks and beyond with cross-silo FL is described in Section 4. We further discuss the simulation results and remark on further directions in Section 5. Section 6 provides concluding statements.

2. Related Work

Implementation of the edge network paradigm usage is significantly expanding owing to 5G technology requirements to provide low latency in reliable communication. MEC plays a crucial role in enabling edge resource sharing by handling content storage and computing at the mobile network edge [10]. Moreover, it supports several tasks, including content caching and resource management, which can be leveraged in cellular and ad hoc networks. In the work by Tran et al. [11], the authors leverage the MEC approach that lies at the cellular network edge to overcome the limitations of the existing radio access network. MEC is proposed to form a context-aware framework in real time that works collaboratively with an underlying communication network. The authors also explained three use cases representing MEC's applicability in 5G networks, including mobile edge orchestration, collaborative video caching and processing, and multilayer interference cancelation. To significantly decrease network latency using MEC, the authors in [12] proposed a two-tier computation offloading framework to minimize the UE's overall energy consumption in heterogeneous networks. Moreover, by leveraging the concept of a software-defined network, the authors in [13] proposed task offloading on the edge of network computing resources to reduce task duration, while considering the UE's battery capacity in software to define an ultradense network.

Despite the above studies focusing on MEC performance and efficiency, some studies used AI to enhance the usefulness of MEC in achieving edge intelligence. For instance, in the study by Zhang et al. [14], the authors designed an optimal offloading scheme using a joint MEC server and a deep Q-learning approach to minimize transmission costs, ensure offloading reliability, and improve system utility. However, current AI learning schemes remain a severe security and privacy vulnerability to mobile devices on the network edge. Hence, the FL approach has been extensively researched in academia and industry, along with the increasing concern for partially resolving the flaws of conventional learning with centralized training systems. Google's Gboard [15] is a successful application as well as a pioneer in FL implementation to its advances in next-word prediction and suggestion. The authors in [15] trained a recurrent neural network language model called the coupled

input and forget gate using FL in a virtual mobile keyboard for smartphones. Comprehensive research continues on FL implementation in various fields. Recently, several studies have been conducted based on the advantages of the FL approach in wireless networks. In the study by Lu et al. [16], the authors used FL as a distributed edge intelligence system to protect user privacy in vehicular cyber physical systems. They proposed a two-phase mitigation scenario, including intelligent data transformation and collaborative data leakage detection. In the study by Chen et al. [17], the authors proposed a joint FL framework to optimize the UE selection and resource allocation mechanism. This framework also aims to solve the FL loss function issue in the training process and improve system performance. The authors in [18] presented an efficient protocol for managing user selection using the FL algorithm based on their resource conditions. Further, to improve FL's activities using a control algorithm, the authors in [19] formulated an FL model over wireless networks capturing two trade-offs, including computational and communication latencies along with energy consumption.

By contrast, to motivate UE contribution to FL activities and enhance system security, blockchain technology has been widely used as an incentive platform by providing computational benefits to the devices along with requests for computational contributions. In this sense, the blockchain guarantees transaction security in a peer-to-peer (P2P) manner among users in ENs without central intermediaries. In the study by Yao et al. [20], the authors used a blockchain to formulate the resource management and pricing problem between cloud miners and cloud providers using Stackelberg game modeling. In the study by Weng et al. [21], the authors introduced DeepChain as a decentralized framework by forming blockchain-based incentive mechanisms to achieve three goals: confidentiality, auditability, and fairness during collaboration training. DeepChain is proposed to preserve local gradients' privacy and ensure auditability of the training process by leveraging blockchain smart contracts and cryptography primitives. In the study by Firdaus and Rhee [22], the authors proposed a decentralized incentive mechanism based on blockchain and smart contracts to achieve trustworthy security environments. Moreover, the authors in [23] presented a secure P2P data-sharing system for vehicular networks by exploiting smart contracts and applying a vehicle reputation scheme to improve system efficiency. Here, the authors used a three-weight subjective logic model to manage vehicles' reputations. Furthermore, some studies have explored the integration of blockchain and AI in wireless networks. In the study by Dai et al. [24], the authors proposed an architecture for a next-generation wireless network by empowering blockchain and AI to form secure and intelligent resource sharing management and orchestration system. They also introduced four use cases based on their proposed architecture: spectrum sharing, content caching, energy trading, and computation offloading. Similar to [24], the authors in [3] proposed a framework for edge intelligence on 5G networks and beyond using blockchain and AI by leveraging a cross-domain sharing strategy to achieve a secure and efficient edge resource scheduling scheme.

3. Instrumentation Technologies: Core System Components

3.1. Cross-Silo Federated Learning. Federated learning (FL) was recently introduced by the Google AI team as a machine learning approach that allows collaboration among multiple entities (users) to solve a machine learning problem under the coordination of a central server or service provider. This approach aims to minimize the risk of privacy breach and enhance model training. Here, each user only transfers the information necessary to update the learning objective, while the valuable data are distributed among the users' local device storage. Hence, the FL approach makes it difficult for security attacks because no centralized server holds all the data [25]. According to the typical characteristics and application scenarios, FL is broadly classified into cross-device FL and cross-silo FL [6]. The cross-device FL consists of a large number of mobile and IoT devices under computational and communication constraints. Hence, data availability and reliability can be a bottleneck for cross-device FL settings. In contrast, cross-silo FL consists of a small number of users or different organizations (e.g., financial or medical) that might provide better data availability and reliability [6].

Moreover, cross-silo FL has significantly tighter privacy and learning performance requirements compared to cross-device FL. Considering this, the system should impose minimum constraints on the training mode, system architecture, and learning algorithm [26]. Several studies have used additively homomorphic encryption (HE) to protect privacy by masking the user's trained model during the aggregation process on the aggregator server. For instance, in the study by Zhang et al. [26], the authors proposed an efficient HE by encoding a batch of quantized gradients to achieve a secure cross-silo FL, as well as to improve system performance by reducing computational and communication overhead. Furthermore, the notion of differential privacy is broadly discussed to form strict privacy guarantees in cross-silo federated learning. This notion aims to protect against different actors or threat models and limit how much can be compromised in worst-case scenarios [25].

3.2. Blockchain-Assisted Information Distribution. Blockchains have recently received increasing attention as a promising technology for providing distributed and secure solutions [27]. They are open databases that guarantee data security by enabling anonymous and trustworthy transactions on an immutably distributed ledger without the help of a central intermediary [28]. Each transaction is recorded with a timestamp to be validated by the consensus mechanism before it is stored on a blockchain network. Blockchain is secure by design in offering several features, such as decentralization, traceability, transparency, and irrevocable transactions [29]. Moreover, by leveraging their smart contracts, blockchains have been utilized to form fairness incentives by providing a decentralized approach to overcome the risks of any single point of failure on a centralized incentive approach. Therefore, a decentralized incentive might effectively encourage user participation and

contributions, creating a secure framework for users to share their data to improve system reliability and sustainability [30].

In the context of wireless networks, the blockchain can be utilized to provide a distributed and secure network for next-generation wireless networks by reducing the administrative expense of the dynamic access. Blockchains can also establish secure and trusted data sharing and resource allocation frameworks in wireless networks [24, 31]. Moreover, by leveraging the MEC framework, blockchains are expected to be deployed to end users' mobile devices. In this system, UE has the capability to conduct mining tasks and participate in the consensus mechanism of the blockchain network. However, because of UE resource constraints, these tasks can be offloaded to nearby ENs to achieve better computation and reduce energy consumption. In short, blockchain and MEC enable computational offloading to ENs, while respecting user privacy and protecting transaction security in a distributed manner.

3.3. 5G Ultradense Network. An ultradense cellular network (UDN), consisting of a large number of small cells, has emerged to satisfy seamless coverage by providing massive multiple-input multiple-output (MIMO) and millimeter wave technology [32]. Here, small cells are used to increase network throughput and minimize energy consumption. In 5G cellular networks, massive MIMO technology leverages hundreds of antennas to be integrated into base stations (BSs). Thus, these MIMO antennas enhance the spectrum efficiency and provide a high-speed transmission rate for wireless traffic. Moreover, millimeter wave technology has been proposed to provide high bandwidth with terahertz communication for wireless transmission [32]. Thus, millimeter wave bands enable higher carrier frequency and very high coverage throughput and support the implementation of massive MIMO technology [33]. Therefore, both technologies are complementary to form UDNs for 5G networks.

Furthermore, several studies have been conducted to explore ultradense wireless networks. In the study by Yunas et al. [34], the authors studied different deployment strategies of ultradense wireless networks, such as densification of classic macrocell BSs, ultradense indoor femtocell BSs, and outdoor distributed antenna systems, to observe the spectrum and energy efficiency in different scenarios. Additionally, to provide a secure authentication scheme, the authors in [35] proposed fast authentication of UE using blockchain technology and a practical byzantine fault tolerant (PBFT) approach by grouping trusted BSs to improve the access efficiency. In the study by Luo et al. [36], the authors proposed an efficient task-VM (virtual machine) matching algorithm for computation offloading in 5G UDN by leveraging blockchain and MEC technology.

4. Blockchain-Enabled 5G UDN for Cross-Silo FL

4.1. State of the Art. The 5G architecture principally consists of an access network, a core network [37], and user equipment, in order to preserve network connectivity and various application services [38]. A cooperative, distributed, and self-managed system is required because the accelerating massive growth of wireless network applications can cause traffic and other issues. In terms of cross-silo federated learning, several variations are needed to ensure FL activity sustainability, such as network traffic characterization [39], computing power options, commensurate incentive schemes, and tamper-proof historical data records. Benefiting from blockchain capabilities, 5G ENs combined with decentralized approaches can be gradually designed to provide a secure, distributed, and efficient operational environment for numerous services. The advantages of these combinations deliver low-cost transactions and address many shortcomings in centralized systems. Therefore, in this section, we explicate an intelligent cross-silo federated learning approach empowered by blockchain technology and collaborative mobile edge computing in 5G networks and beyond.

The blockchain-enabled 5G UDN architecture envisioned for cross-silo FL consists of three planes (we refer to [24], as shown in Figure 1): a user plane, an edge plane, and a cloud plane. The cloud plane holds the set of servers with super computation, caching, and processing capabilities. This layer is effective in executing operations involving massive amounts of data for various applications. However, the central authority is still difficult to avoid, even though it is expected to be equipped with tamper-resistant hardware. The central authority in this concept also helps set security parameters for several entities such as macro base stations (MBS), small base stations (SBS), roadside units (RSU), and UE.

Network functions' virtualization and software-defined networks can make the edge plane more programmable and flexible in conducting cross-silo FL activities. Mobile edge computing servers with powerful computation resources, caching, and AI functions can provide shared intelligent wireless computing for UE. Meanwhile, through Ethereum smart contracts, blockchain technology can record all transactions created in the wireless network and establish a distributed ledger to increase security in the wireless environment [40]. An edge plane with network functions' virtualization (abstract physical resources) can neglect vendor and protocol diversity. It can also achieve rapid function deployment by designing, transferring, and terminating virtual machines among scattered edge entities. Eventually, the user plane's main entities consist of a certain number of UE devices connected with several edge plane entities.

4.2. Cross-Silo FL Activities and Blockchain-Based Incentive. By design, UE can gradually improve a global model by aggregating gradient values from local training results from various devices. The term cross-silo is appended to FL because we utilize a combination of a small number of devices for simulation purposes. The users in cross-silo FL are signified by the number of devices $UE_1, UE_2, \ldots, UE_n \in UE_{(i,j)}$ within the same environment. Each UE increases the global model's performance by sending executed gradient values using their respective private datasets.

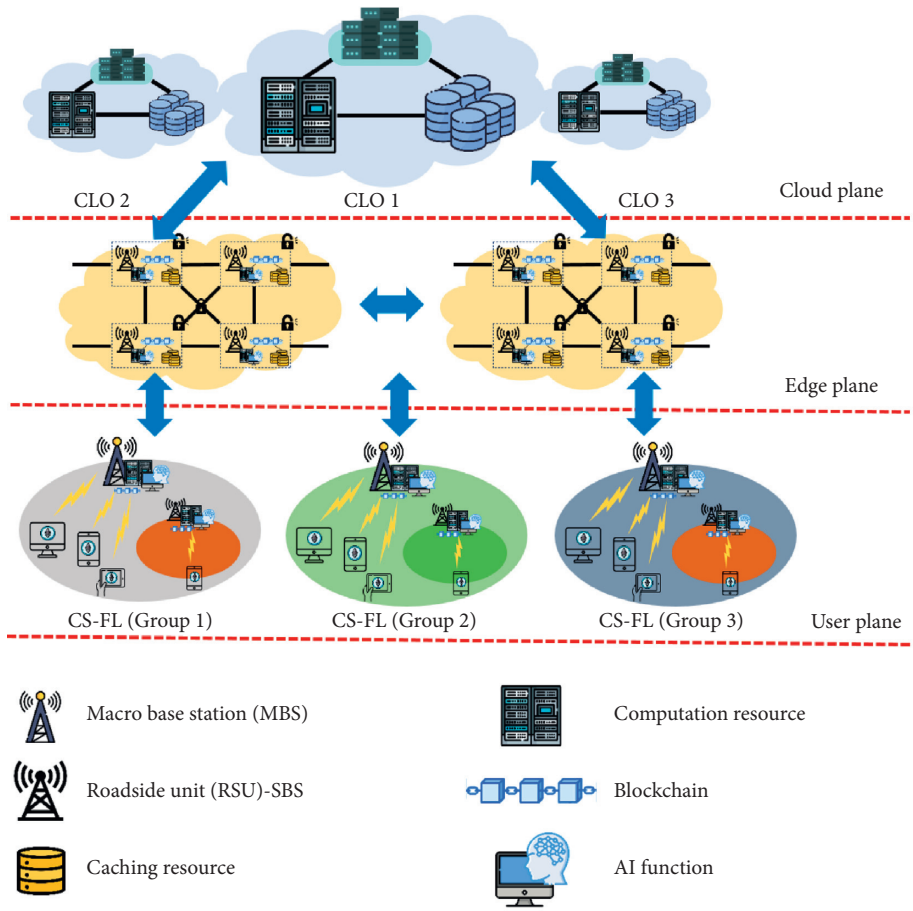

Figure 1: State-of-the-art blockchain-enabled 5G UDN for cross-silo FL.

The initial global model is marked with GM_{clox}^{v0} (in case CLO is a provider), and every new version update is signified with $GM_{clox}^{v(n+1)}$. Cross-silo FL can be performed in groups or independently. For a clustered system, the newest gradient values are handled collectively for each device, and then, a leader sends group gradient values to a model provider. Nevertheless, our proposed approach uses independent cross-silo FL to communicate (request, send, and receive gradient values) directly with a provider via a secure channel for ease of presentation.

The global model was constructed using convolutional neural networks, which are fundamental techniques in deep learning environments. The data were automatically labeled (image recognition for the digits 0–9, containing 1000 images each). The size of each image was $28 \times 28 \times 1$ pixels, corresponding to the height, width, and channel size. The convolutional layer consisted of an image input layer, a 2D convolutional layer, a batch normalization layer, and a rectified linear unit-activation function layer. In the first layer of the convolutional neural network (ConvNet), we set the input to be 1, the output was 25, the kernel size was 5, and the stride was 1. We used a fully connected layer and softmax function layer for classification. A fully connected layer consisted of a fixed-sized input image of 4×4 for feature size with 50 channels combined in totals. The batch normalization layer normalizes activations and gradients distributed across the network and increases the network training speed. Eventually, the softmax function layer normalizes the fully connected layer's output consisting of positive numbers (sum to one) as classification probabilities.

When the FL cross-silo activity is finished, the provider propagates the UE incentives based on their resource contributions using Ethereum smart contracts. The incentive mechanism for a cross-silo FL environment requires agile development time [41], dynamic interaction, and security for applications that can be supported by Ethereum smart contracts. In general, a transaction in Ethereum consists of the following information [42].

Receiver of the message

Sender's digital signature

Total number of ether that must be transferred from the CLO to UE

An optional data field

A *start-gas* value, signifying the upper limit of the computational steps for completing the transaction

A *gas-price* value, signifying the fee given by the sender per computational step

The transition function of the Ethereum smart contract is illustrated in Figure 2 and can be described as follows:

Check if the transactions are correct and the signatures are valid (return *ERROR* if the condition is not satisfied)

Calculate the transaction fee as *start-gas***gas-price* (return an *ERROR* message if the amount of balance is not adequate)

Assign-gas = *start-gas* and subtract a specific amount of gas per byte (for the transaction bytes)

Move the transaction amount from the sender's wallet (CLO) to the receiver's wallet (UE)

Finally, each device holds a convolutional model with comparable settings and capabilities to train the CLO global model (CLO is from the cloud layer) with the blockchain as an incentive mechanism to propagate the cryptocurrency. This type of activity illustrates a real-world FL cross-silo application with a diversity of data (type and amount), device models, and network capabilities to train deep learning models. In cross-silo FL, the provider can also add filtering to detect suspicious gradient values from malicious clients.

4.3. Dynamic Authentication. Dynamic authentication is required to support the continuity of cross-silo FL activities, notably for UE systems. The primary authentication mechanism for UE in the 5G network was established by the Third Generation Partnership Project (3GPP) [43]. The 5G standardization arranged by 3GPP focuses on all essential lines such as network slicing security, authentication and key agreement (AKA), UE security, user plane, and authorization mechanism [44]. Intelligent cross-silo FL is expected to enable novel applications of decentralized learning. Because these combinations of technologies are not carried out in a monolithic network, a one-suits-all authentication mechanism is no longer adequate for UE.

To obtain access to the FL services, UE are required to perform authentication, which is governed by the primary authentication mechanism in the 5G system. By doing so, the network services can identify the UE, and afterward, UE is also required to send a permanent subscription identifier (SUPI). Regarding the authentication perspective in 5G ENs, 3GPP standardization cannot be freely customized by users. The security protocols of 5G architecture consist of an authentication server function (AUSF), security anchor function (SEAF), authentication credential repository and processing function (ARPF), and a security policy control function [45], where the primary authentication of an anchor key K_{SEAF} can be utilized for all accesses. These components are useful for subsequent communication between UE, control panels, core access, as well as for access and mobility management functions (AMF). Every cross-silo FL device must execute a primary authentication to access mobile network services, while users can adjust the secondary authentication as per their preference. We limit the scope of this research by designing a dynamic authentication that can be used as a secondary authentication component for cross-silo FL activities on 5G UE.

We propose an adjustable pairing-based cryptography technique as a dynamic authentication for UE to be appropriately authenticated at the user plane layer, edge plane layer, and cloud plane layer in the intelligence cross-silo FL. Pairing-based cryptography defines a fully functional identity-based encryption scheme (IBE) [46], which can be understood as a type of public key encryption where UE can create a public key from a recognized unique identifier. This technique is based on pairing functions. Specifically, it maps a pair of points on an elliptical curve to a finite field. The pairing functions' unique features are suitable for adoption in cross-silo FL in the 5G EN environment.

The pairing protocol generates two cryptographic groups to the next group with a mapping $\widehat{e} \longrightarrow G_1 \times G_2 \longrightarrow G_T$ to construct or analyze cryptographic systems for cross-silo FL entities. Suppose G_1 and G_2 are a pair of additive cyclic groups of the prime order q, and G_T is another cyclic group of the order q inscribed multiplicatively (G_T is also known as the target group or resource group). The pairing is a bilinear map $\widehat{e} \longrightarrow G_1 \times G_2 \longrightarrow G_T$ that should meet the following criteria.

Bilinearity. The map $\widehat{e} \longrightarrow G_1 \times G_2 \longrightarrow G_T$ is bilinear if $\widehat{e}(g^a, g^b) = \widehat{e}(g, g)^{a.b}$ for every a and $b \in G_1$ and a and $b \in Z$. The bilinearity attributes can be defined as follows:

$$\forall a, b \in F_q^*, \forall P \in G_1, Q \in G_2 : \widehat{e}(aP, bQ) = \widehat{e}(P, Q)^{a.b}. \tag{1}$$

Nondegeneracy. Every group performs the computation using a different base point because G_1 and G_2 denote groups of the prime order q, where G_1 is in the base point/generator P. Furthermore, the bilinear map must be $\widehat{e} \neq 1$.

Computable. There exists an adequate algorithm to calculate $\widehat{e} \longrightarrow G_1 \times G_2 \longrightarrow G_T$. The adopted protocol must be computable for all rounds of the bilinear map.

A concrete pairing-based cryptography protocol enables dynamic authentication of cross-silo FL entities. Intelligent FL over 5G ENs requires rapid communication and transaction among entities because the bandwidth and network latency are no longer the primary concern. An entity in cross-silo FL can be defined as several UE devices, an SBS, an MBS, or a cloud plane (see Figure 3). Entities received unique information from Ganache CLI (the latest version of *TestRPC* from *Truffle-Suite*) in the form of a prefix for a hexadecimal numeric constant (in base 16). Every master public key of an entity is derived from a public key generator (PKG). By combining the public parameters and master keys, the PKG can generate secret keys for each entity (Sec_{uex}^{k1}, Sec_{sbsx}^{k1}, Sec_{mbsx}^{k1}, and Sec_{clox}^{k1} for UE, SBS, MBS, and cloud, respectively). The parameters used by PKG consist of a prime number p, a group G with a base point, the master key, $Q = g^a$, and the hash function of the two groups $Hash_{g1}$ and $Hash_{g2}$, where $Hash_{g1}: \{0,1\}^* \longrightarrow G$, $Hash_{g2}$

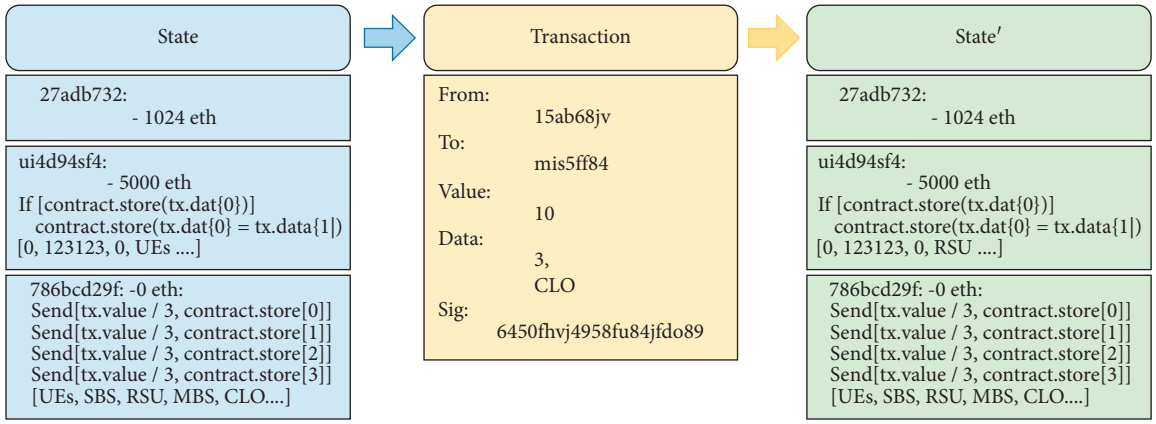

Figure 2: Transition states of the Ethereum smart contract.

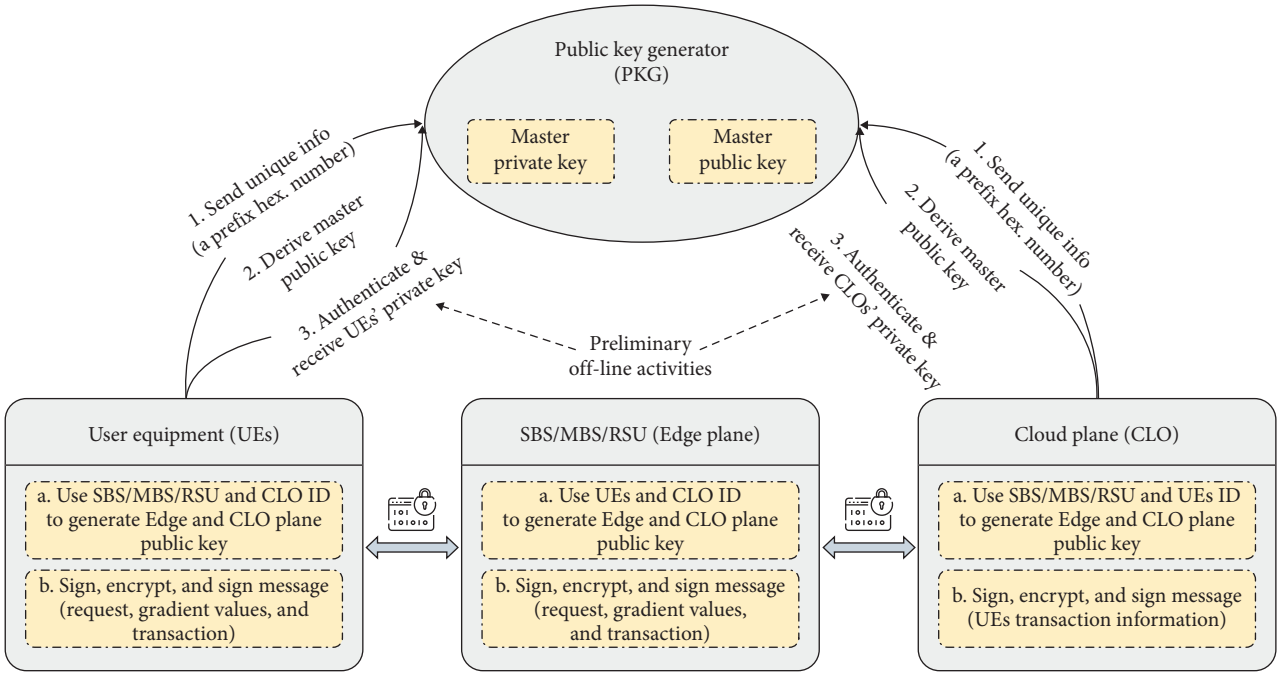

Figure 3: UE ID-based encryption for cross-silo FL.

: $\{0,1\}^l$. In the case of UE encryption, UE sets a cipher text $CTx = [Cx_1, Cx_2]$ from two distinct groups with $Cx_1 = g^r$ and Cx_2 defining a series of values, as shown in equation (2). The decryption process is given in the following equation:

$$txs \oplus Hash_2\left(\widehat{e}\left(Hash_1\left(\text{prefix hex}\right), Q\right)\right),$$
$$txs\text{: UEs'transaction}\left(msg\right), \tag{2}$$

$$txs = Cx_2 \oplus Hash_2\left(\widehat{e}\left(Sec_{uex}^{k1}, \ldots, Sec_{clox}^{k1}\right), Cx_1\right). \tag{3}$$

We define a concrete cross-silo FL with a target group G_T as a multiplicative written group. The bilinear map is set to be an integration of three entities from three different layers, namely, UE from the user plane layer, SBS/MBS from the edge plane layer, and cloud services from the cloud layer. Each party involved $Q(UEs, SBS, MBS, CLO)$ in the transaction delivers a public key to the corresponding parties $Q(Q^{\text{sec}}g_1, Q^{\text{sec}}g_2)$, while keeping the entities' private key confidential. The parties can calculate the same shared secret key using the bilinear map function. For instance, the user of UE_1 computes the bilinear map using MBS's public key Pub_{mbs1}^{k1} and the cloud CLO's public key Pub_{clo1}^{k1} and calculates the transaction using the secret/private key of UE_1 and Sec_{ue1}^{k1}, as shown in equation (4). Similarly, the transaction submitted by MBS and CLO can be executed by correspondence entities' public key combined with the sender's private key, as denoted in equations (5) and (6). Because the protocol applied for the cross-silo FL system consists of two cyclic groups, (G_1 and G_2), we can determine equations (4)–(7) as a solid unit equivalent to $\widehat{e}\left(g_1, g_2\right)^{\forall Sec_{entities}^{k1}}$ or comparable to the target group. Finally, the shared secret key for this case is defined as in equation (7):

$$\text{User equipment 1}\left(UE_1\right) \longrightarrow \widehat{e}\left(Pub_{mbs1}^{k1}, Pub_{clo1}^{k1}\right)^{Sec_{ue1}^{k1}}, \tag{4}$$

$$\text{Micro base station}\left(MBS_1\right) \longrightarrow \widehat{e}\left(Pub_{clo1}^{k1}, Pub_{ue1}^{k1}\right)^{Sec_{mbs1}^{k1}}, \tag{5}$$

$$\text{Cloud services}\left(CLO_1\right) \longrightarrow \widehat{e}\left(Pub_{ue1}^{k1}, Pub_{mbs1}^{k1}\right)^{Sec_{clo1}^{k1}}, \tag{6}$$

$$\text{For} \forall \text{ bilinear map} \longrightarrow \widehat{e}\left(G_1, G_2\right)^{Sec_{ue1}^{k1}, Sec_{mbs1}^{k1}, Sec_{clo1}^{k1}}. \tag{7}$$

Intuitively, adjustable pairing-based cryptography is valuable in intelligent FL activities because it is constructed properly. This can generate considerably large finite fields to obtain solutions to a computationally difficult discrete logarithm problem [47], yet it is small enough to perform computations efficiently. In the symmetrical form, the pairing protocol can be further utilized to reduce a hard problem in one group to a distinct, generally more straightforward problem in another group. Finally, by performing the pairing-based cryptography protocol, the UE can encrypt a transaction without requiring a receiver's public key; for instance, the macro base station's key in the edge plane layer that has been approved in advance.

5. Results and Discussion

5.1. Preparatory Experiments. Blockchain-enabled 5G edge networks and beyond with cross-silo federated learning in practice has three core approaches, namely, a decentralized ledger, distributed learning, and 5G technology. Each approach has its settings, data, and prerequisites that are distinct from one another. We also designed a dynamic authentication for the UE to be able to use alternative services from different providers. The experiments were carried out on a personal computer with a 7th Generation Intel Core i7 Processor i7-7700 having a processor base frequency (PBF) of 3.60 GHz and a maximum turbo frequency (MTF) of 4.20 GHz (bus speed was 8.00 GT/s), supported with 16.00 GB of RAM modules installed.

The dataset used is the image of handwritten digits (28×28 pixels each image) with their respective labels representing 0 to 9 digits. The dataset was derived from Mathwork Digits [48] consisting of 10,000 synthetic grayscale images of handwritten digits. The maximum number of training sets contained 750 images, and the minimum number of training sets contained 75 images. The amount of training data used in the simulation was added by a multiple of 10% (75 images), starting from the minimum amount of data to the maximum until it reached 100% of the data (750 images).

The proposed cross-silo FL was constructed to preserve the value driven by distributed learning in enhancing users' privacy in 5G/6G edge networks. Each UE in the network employed a global model with varying amounts of data. Training was performed in various iterations, including iterations per epoch for each transaction. Meanwhile, the decentralized incentive scheme for the UE was constructed by following blockchain technology approaches. Our decentralized reward approach is based on blockchain technology. We leveraged the smart contract feature in the Ethereum platform by using the Ganache CLI-Truffle-Suite interface, which provides a prefix for a hexadecimal numeric constant for every entity. The reward propagation is conducted in the automining mode, with the muirglacier hard fork mode, which is run on the remote procedure call (RPC) server. Each entity was provided with a virtual ether and a private key to perform the transactions. Finally, the gas price and gas limit were automatically calculated by the system.

5.2. Performances and Analysis

5.2.1. UE Dynamic Authentication. Typically, each entity must be authenticated securely by service providers to verify the requester's identities before using the available services. There are many techniques for achieving this objective. For the intelligent cross-silo FL in 5G ENs, dynamic authentication is essential because there are many entities involved within the same network (5G architecture and mobile devices). Therefore, we proposed a dynamic authentication mechanism that relies on the adjustable pairing-based cryptography techniques presented in Section 4.3.

For ease of presentation, we set UE (user equipment A) as a requester for artificial intelligence models available in the network. The CLO in the cloud layer serves as a model provider and a central aggregation server. The CLO also prepares rewards for UE that have completed training using personal data and have improved global models. The UE has a pair of master public keys derived from the public key generator (PKG) in advance. The UE takes a prefix for the hexadecimal numeric constant of an entity (visible to the public) for each layer plane to deploy a dynamic authentication. In this case, the UE selects the macro base station A (MBS) and cloud services A (CLO) from the edge and cloud planes, respectively. Eventually, by implementing an adjustable pairing-based cryptography protocol, the UE can be authenticated by the system, and the UE transactions can be encrypted using a shared secret key, $UE_s \longrightarrow \widehat{e}\left(Pub_{mbs1}^{k1}, Pub_{clo1}^{k1}\right)^{Sec_{ues}^{k1}}$, as denoted in equation (4). The entity of the model provider allows more than one provider. Therefore, the UE can also take different prefix hexadecimal values depending on the entities involved.

The performance results of the UE dynamic authentication tests are summarized in Figure 4. The experiments were divided into two groups. First, UE only involves the MBS in an adjustable pairing technique, assuming that the MBS is the model provider. This experiment was carried out to determine the time spent generating a shared key with only two entities involved (user equipment A and macro base station A). Second, our primary objective of pairing implementation involves three different entities from three different layers. The CLO functions as a model provider and an aggregation server.

We performed the experiments with 20 repetitions each. The first group consists of UE, and MBS requires 65.64 ms (drawn in the pink line) on average to generate a shared key

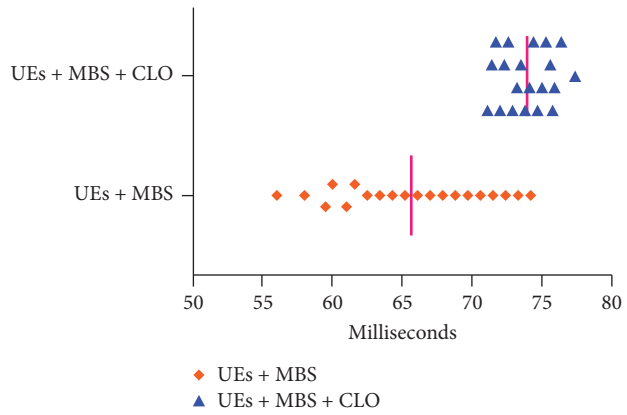

Figure 4: Distribution marks of time spent by the UE in generating a shared key to submit a UE transaction (the data are recorded for 20 repetitions).

between them. The fastest generation time was recorded as 56.00 ms, and the longest time was 74.2 ms. We note that the distribution points of generation time are almost evenly distributed (from the longest to the fastest) for each repetition, as illustrated in Figure 4 (in orange points). By contrast, the distribution points of the generating time were not significantly distinct for each repetition. The average time for the second group was recorded at 73.98 ms. The longest time was 76.4 ms, and the fastest generation time was 71.13 ms. Because the time range for each group was significantly varied, the protocol presented here can be used to support cross-silo FL with many entities incorporated in an intelligent system over 5G ENs.

5.2.2. Cross-Silo Federated Learning. Our learning process for cross-silo FL was conducted serially using a single graphics processing unit (GPU). A GPU is shared in embedded systems such as mobile phones and workstations in overlay networks to accelerate the command-line computing process within a single machine. Cross-silo FL activities are run independently using the same dataset, but every UE is differentiated by the amount of data used in training. Explicitly speaking, every UE device holds a different number of private datasets. The capabilities of the devices in conducting each training were comparable to one another. All the settings that we described were for simulation purposes. In real-world implementations, federated learning consists of a massive number of devices with various geographical locations. We illustrate cross-silo federated learning on a single CPU divided into multiple computing capacity within a single machine due to the hardware limitations. Likewise, personal datasets are distinct from one UE to another and the capabilities of the devices used.

The UE first executes transactions to obtain a global model GM^{v0}_{clox} from the provider. In this case, we anchored the CLO in the cloud layer as the global model GM^{v0}_{clox} provider used by each UE (same version of GM^{v0}_{clox}). UE then carries out training privately in stages and assigns gradient values from the training to obtain the model's latest version $GM^{v(n+1)}_{clox}$. This process is implemented continuously with diverse UE devices and data and is processed until the results satisfy the conditions set by the provider. Nevertheless, we recorded the training activities for one full epoch for each device for ease of presentation. The cross-silo FL performance can be extended to a real-world implementation with different data and device capabilities. The model provider can send the model to the UE after performing the authentication process described in Section 4.3. The model provider and the UE may vary. Therefore, dynamic authentication is required to periodically verify the party's identities without broadcasting a public key.

To ascertain the difference in each UE performance, we differentiated the amount of training data that affected validation accuracy, iterations per epoch, and maximum iterations. Each training was set to five epochs, yet iterations and iterations per epoch varied depending on the amount of data used in training. The amount of data used to train the global model affects the incentives received by the UE. We describe the incentive mechanism in Section 5.2. We used ten devices starting from UE_1 with 75 data points (10% of the total training data), followed by UE_2 holding 20% of the total training data and so on until the learning reached UE_{10} possessing 750 training data or equal to 100% of training data. The learning rate schedule for each training is set constant at 0.001. Moreover, we have elaborated the global model used in this research in Section 4.2.

Figure 5 depicts the performance of UE for different amounts of training data used in cross-silo FL. We recorded $UE_1$with 75 data points or equal to 10% of the maximal training data (least among others). We also showed the performance of UE_{10} with 750 training data points or equal to 100% of the total data. We note that UE_1has 60.39% accuracy with five iterations per epoch. The result is followed by UE_2 with 150 data points having 79.46% accuracy and 11 iterations per epoch. The training accuracy was enhanced when it reached UE_5 with 50% of the total data, with an accuracy of 91.71% (29 iterations per epoch). Finally, UE_{10} with the most training data was recorded to have 97.84% accuracy with 58 iterations per epoch. The accuracy values were enhanced by increasing the training cycle during training. Based on the simulation results, we can infer that the performance of cross-silo FL is identical to that of deep learning in general. The distinction between them is the confidentiality of the data. Further information about the UE performance has been presented in Table 1.

5.2.3. Reward Mechanism. Secure and proportionate incentive mechanisms are required in the FL cross-silo system to motivate UE to build a deep learning model collectively. The amount of incentive received by the UE depends on the number of data used in training (given linearly). In summary, each UE receives different incentives even though they build the same deep learning model in the same system. The model provider propagates a certain amount of cryptocurrency by relying on Ethereum smart contracts. The scheme of this approach is presented in Section 4.2.

UE incentives are provided by the provider considering the FL cross-silo performance (gradient values for each device) and are based on the UE information stated through smart contracts. The provider has the ability to check the

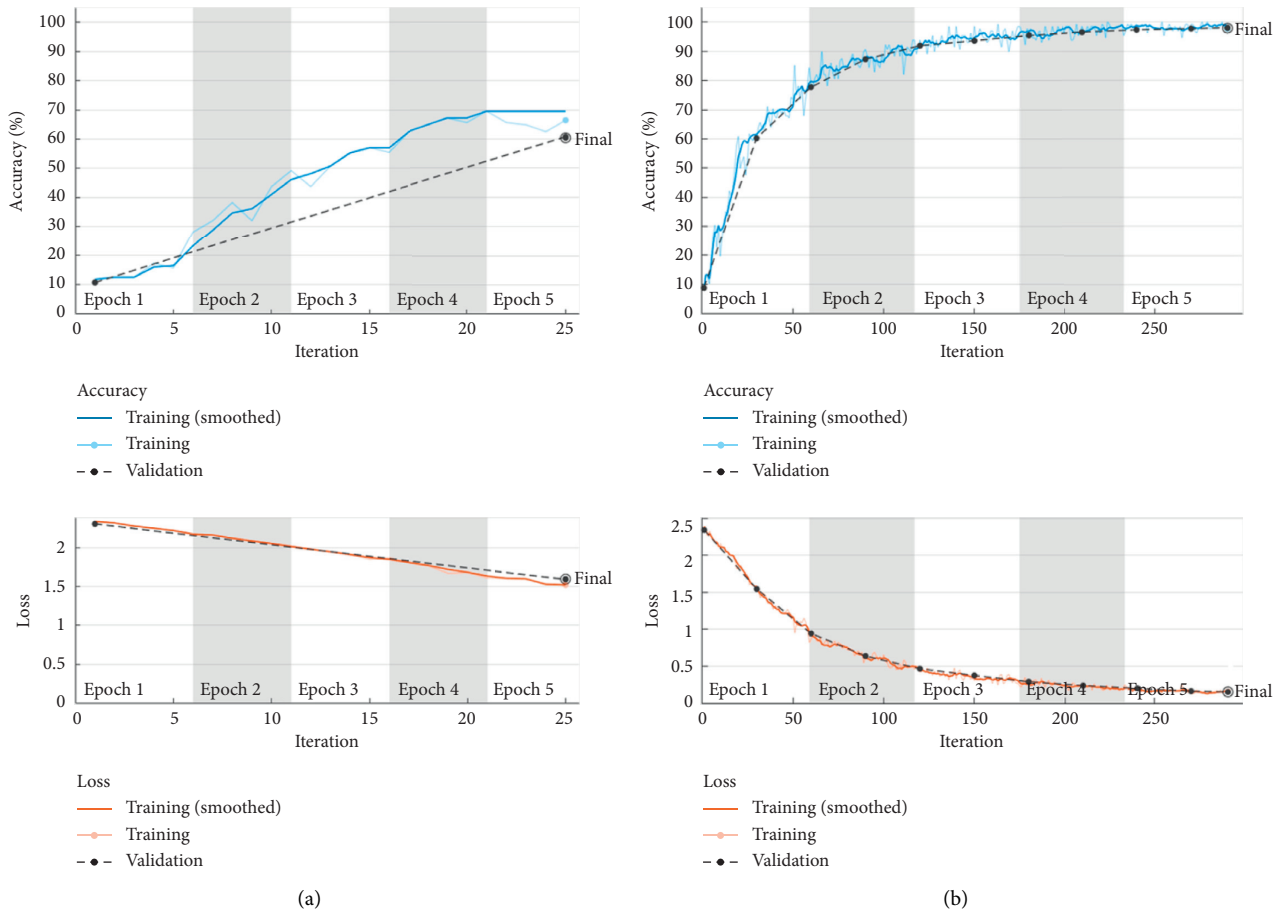

Figure 5: Performances of UE on different amounts of training data. (a) UE with the least amount of data (75 data or 10% of the maximal set). (b) UE with the maximum number of data (750 data or 100% of the maximal set).

Table 1: Performance of cross-silo FL for UE_1–UE_{10} along with information on the Ethereum transaction.

Tx-n	TD (%)	Number of TD	Accuracy (%)	Iteration	Iteration per epoch	Gas used (units)		ETH received
						UE	CLO	
1	10	75	60.39	25 of 25	5	102246	81732	1.25×10^{-3}
2	20	150	79.46	55 of 55	11	103267	81637	2.50×10^{-3}
3	30	225	87.34	85 of 85	17	101453	81349	3.75×10^{-3}
4	40	300	87.54	115 of 115	23	102391	81901	5.00×10^{-3}
5	50	375	91.71	145 of 145	29	99948	81730	6.25×10^{-3}
6	60	450	94.78	175 of 175	35	100621	81632	7.50×10^{-3}
7	70	525	96.69	205 of 205	41	101998	81536	8.75×10^{-3}
8	80	600	96.51	230 of 230	46	101904	81442	1.00×10^{-2}
9	90	675	96.86	260 of 260	52	103363	81922	1.13×10^{-2}
10	100	750	97.84	290 of 290	58	103387	81725	1.25×10^{-2}

Tx-n: transaction numbers; TD: training data; ETH: ether received by the UE.

gradient values received from various devices. Then, the provider confirms and validates the contract precisely before the incentive is distributed and recorded on the distributed ledger. We differentiated the number of incentives (ether) received by UE with varying amounts of data (10% up to 100% of the data with a deviation of 10% for each device sequentially). UE with 10% of the maximum training data received 0.00125 ETH, and at 20% of the training data, UE received 0.00375 ETH. Each 10% difference in data was set to obtain an extra 0.00125 ETH. Eventually, the UE with 100% training data earned 0.0125 ETH (see Table 1). The nominal amount of ETH received by the UE can be freely set by the model provider.

Figure 6 presents UE and CLO's transaction performance in terms of gas consumed on the Ethereum platform. UE transactions are in the form of statements that are

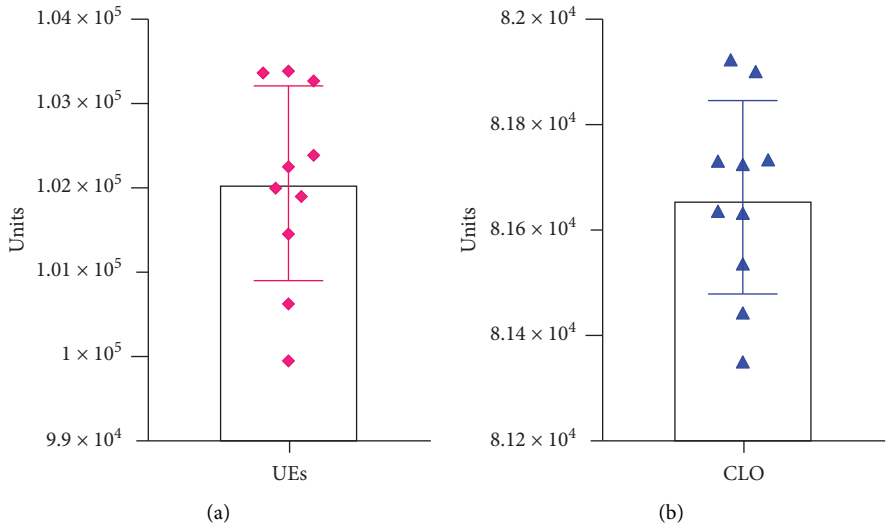

Figure 6: Amount of gas used to conduct a transaction. (a) UE with respective data input (transactions to claim revenue). (b) CLO as a model provider with the gas used is comparable for every transaction.

recorded in smart contracts. UE describes information related to the global model used, gradient values (the result of local training), and knowledge of the dataset, to name a few. Meanwhile, CLO (as the model provider) can verify the transactions executed by the UE. The first three rows of transactions (UE_1, UE_2, and UE_3) required 102,246, 103,267, and 101,453 units of gas, respectively, to process transactions. The most gas usage occurred in the 10th transaction, which was 103,387 units because UE_{10} had a longer arbitrary input than the others. Meanwhile, the 5th transaction by UE_5 had the least input transactions with 99948 units of gas required to conduct the transaction. The average gas usage for UE in conducting the transactions is approximately 102,057 units.

On the CLO side, providers' use of gas does not differ from one transaction to another because there is no significant change in arbitrary input. This point can be seen from the maximum gas usage of 81992 units and minimum usage of 8139 units, with an average of 8166 units. As of today, the total gas usage from the Ethereum network continues to increase every year. This can be seen in Table 2 [49], which illustrates a significant difference between 2015 and 2021. Therefore, it is necessary to consider the arbitrary input in cross-silo FL transactions in future research.

5.3. Concerns and Remarks. An intelligent cross-silo FL system that integrates the blockchain in 5G edge networks has been discussed in the previous sections. Comprehensively, our approach is encouraging for application in real-world settings, as evidenced by the simulation results. However, to be applied effectively, we highlight several points and concerns and provide some remarks as follows.

Ethereum Gas Used. To confirm the validity of the training that has been carried out, UE make transactions through the Ethereum smart contract by inputting some of the required information. The amount of gas used to make a transaction depends on the number of arbitrary UE values. The larger the input of an arbitrary value, the higher the amount of gas used. The amount of gas used is also adjusted to the amount used in conducting transactions, affecting the gas price, confirmation time, and block rewards. This concern is illustrated in Figure 7 [50]. The gas price (gwei) and average confirmation time (s) constantly change over the course of each day. On January 14, 2021, the lowest gas price was recorded at 53 gwei, and the highest gas price was recorded at 75 gwei, with an average of 73 gwei.

Table 2: Ethereum daily gas usage information as an illustration of the historical total daily gas usage of the Ethereum network.

No.	Date (UTC)	Unix TimeStamp	Total value
1	8/1/2015	1438387200	0
2	8/7/2015	1438905600	49353826
3	1/1/2016	1451606400	292262422
4	1/1/2017	1483228800	1122085141
5	1/1/2018	1514764800	39876127062
6	1/1/2019	1546300800	32962591808
7	1/1/2020	1577836800	37203395960
8	1/1/2021	1609459200	80034402241

Figure 7 also depicts the Ethereum daily block rewards. It is a combination of total ether supplied to the Ethereum network with several references to the Ethereum block count. The highest daily block reward was recorded on July 30, 2015, where 39,316.09375 ether was propagated on the Ethereum network. The lowest daily block rewards of 10,304.625 ether were distributed on January 1, 2020. The significant change in gas used affects the amount of incentive received by the UE, which is also directly related to the amount of private data used in training. The UE's privileged network position enables it to see estimated incentive values before others, allowing users to place their transaction before prices change.

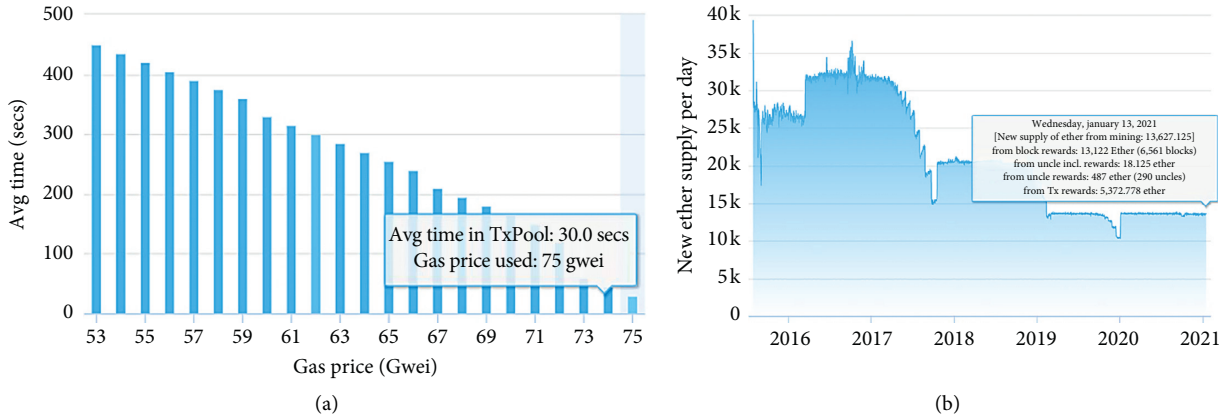

Figure 7: (a) Confirmation time × gas price (last 1000 blocks). (b) Ethereum daily block rewards' chart.

Centralized Aggregation Server. The aggregation server plays an important role in FL cross-silo activities. The servers generously process updated gradient values without any intervention from outsiders. As algorithms for analyzing the secret in gradient values evolved, it became possible for the server to reveal confidential data from the UE devices via their respective gradient values. Furthermore, bottleneck issues cannot be completely avoided in cross-silo FL. The bottlenecks are inherent in a centralized system, even though the aggregation server (cloud) is equipped with powerful and capable computing power.

The Initial Global Model Is Not Evenly Distributed. In a real-world implementation, the cross-silo FL may face an obstacle in distributing the UE global model. This is caused by several factors such as device or network failures, the UE devices in the idle mode, charging time, and client failures.

6. Conclusions

In this paper, we proposed a new machine learning paradigm empowered by blockchain technology on 5G edge networks and beyond. Our approach focuses on state-of-the-art blockchain-enabled 5G UDNs for cross-silo FL with proper dynamic network authentication of UE. UE can perform a secure authentication process strengthened by various parties at three different layers (user plane, edge plane, and cloud plane) without continuously sending the public key to the corresponding parties. We showed the performance of UE in generating a shared key with different settings to support an intelligent cross-silo FL in 5G ENs with a simulation of the proposed model. Furthermore, blockchain-based incentive techniques are utilized in this research as reward propagation mechanisms. Using the Ethereum platform with smart contract features, we have shown that rewards are propagated by the system adequately in a secure manner. The model provider can independently adjust the amount of rewards allocated to end users. Ultimately, all the objectives of this research were satisfied, as evidenced by the simulation results. We also outlined research challenges related to centralized server utilization within 5G architecture and the possibility of information leakage from UE gradient values during training activities.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT) (no. NRF-2018R1D1A1B07048944) and partially supported by the Republic of Korea's MSIT (Ministry of Science and ICT), under the High-Potential Individuals Global Training Program) (2020-0-01596) supervised by the IITP (Institute of Information and Communications Technology Planning and Evaluation).

References

[1] X. Chen, H. Zhang, C. Wu, S. Mao, Y. Ji, and M. Bennis, "Mobile edge computing—a key technology towards 5G. ETSI white paper," *IEEE Internet of Things Journal*, vol. 11, no. 11, 2015.

[2] S. Bazrafkan and P. M. Corcoran, "Pushing the AI envelope: merging deep networks to accelerate edge artificial intelligence in consumer electronics devices and systems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, p. 55, 2018.

[3] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5G beyond for the industrial internet of things," *IEEE Network*, vol. 33, no. 5, p. 12, 2019.

[4] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, *Federated Learning: Strategies for Improving Communication Efficiency*, pp. 1–10, The University of Edinburgh, Edinburgh, Scotland, 2016.

[5] S. Lugan, P. Desbordes, E. Brion, L. X. Ramos Tormo, A. Legay, and B. Macq, "Secure architectures implementing trusted coalitions for blockchained distributed learning (TCLearn)," *IEEE Access*, vol. 7, pp. 181789–181799, 2019.

[6] P. Kairouz, "Advances and open problems in federated learning," *Machine Learning*, vol. 4, pp. 1–105, 2019.

[7] A. Singh, R. M. Parizi, Q. Zhang, K.-K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: approaches and challenges to address vulnerabilities," *Computers & Security*, vol. 88, p. 101654, 2020.

[8] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, May 2016.

[9] S. Rahmadika and K.-H. Rhee, "Toward privacy-preserving shared storage in untrusted blockchain P2P networks," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 6219868, 13 pages, 2019.

[10] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, p. 4298, 2020.

[11] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, "Collaborative mobile edge computing in 5G networks: new paradigms, scenarios, and challenges," *IEEE Communications Magazine*, vol. 55, no. 4, p. 54, 2017.

[12] Y. Dai, D. Xu, S. Maharjan, and Y. Zhang, "Joint computation offloading and user association in multi-task mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, p. 12313, 2018.

[13] M. Chen and Y. Hao, "Task offloading for mobile edge computing in software defined ultra-dense network," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, p. 587, 2018.

[14] K. Zhang, Y. Zhu, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Deep learning empowered task offloading for mobile edge computing in urban informatics," *IEEE Internet of Things Journal*, vol. 6, no. 5, p. 7635, 2019.

[15] A. Hard et al., "Federated learning for mobile keyboard prediction," 2018, http://arxiv.org/abs/1811.03604.

[16] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Federated learning for data privacy preservation in vehicular cyber-physical systems," *IEEE Network*, vol. 34, no. 3, p. 50, 2020.

[17] M. Chen, Z. Yang, W. Saad, C. Yin, H. Vincent Poor, and S. Cui, "A joint learning and communications framework for federated learning over wireless networks," *IEEE Transactions on Wireless Communications*, vol. 20, 2019.

[18] T. Nishio and R. Yonetani, "Client selection for federated learning with heterogeneous resources in mobile edge," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Shanghai, China, May 2019.

[19] N. H. Tran, W. Bao, A. Zomaya, M. N. H. Nguyen, and C. S. Hong, "Federated learning over wireless networks: optimization model design and analysis," in *Proceedings of the IEEE Conference on Computer Communications*, Paris, France, May 2019.

[20] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, p. 3602, 2019.

[21] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 8, p. 1, 2019.

[22] M. Firdaus and K.-H. Rhee, "On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks," *Applied Sciences*, vol. 11, no. 1, p. 414, 2021.

[23] J. Kang, R. Yu, X. Huang et al., "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2019.

[24] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Network*, vol. 33, no. 3, p. 10, 2019.

[25] M. Heikkilä, A. Koskela, K. Shimizu, S. Kaski, and A. Honkela, *Differentially Private Cross-Silo Federated Learning*, ResearchGate, Berlin, Germany, 2020.

[26] C. Zhang, S. Li, J. Xia et al., "Efficient homomorphic encryption for cross-silo federated learning," in *Proceedings of the 2020 USENIX Annual Technical Conference (ATC'20)*, Boston, MA, USA, July 2020.

[27] S. Zhang, Y. Cao, Z. Ning, F. Xue, D. Cao, and Y. Yang, "A heterogeneous IOT node authentication scheme based on hybrid blockchain and trust value," *KSII Transactions on Internet and Information Systems*, vol. 14, 2020.

[28] M. Firdaus and K. H. Rhee, "Empowering blockchain for secure data storing in industrial IoT," in *Proceedings Of the Korea Information Processing Society Conference*, pp. 231–234, October 2020, https://www.koreascience.or.kr/article/CFKO202024664104787.page.

[29] J. Xue, C. Xu, and Y. Zhang, "Private blockchain-based secure access control for smart home systems," *KSII Transactions on Internet and Information Systems*, vol. 12, 2018.

[30] S. Rahmadika and K.-H. Rhee, "Reliable collaborative learning with commensurate incentive schemes," in *Proceedings of the 2020 IEEE International Conference on Blockchain*, Rhodes, Greece, November 2020.

[31] K. Veeramani and S. Jaganathan, "Land registration: use-case of e-Governance using blockchain technology," *KSII Transactions on Internet and Information Systems*, vol. 14, 2020.

[32] X. Ge, S. Tu, G. Mao, C.-X. Wang, and T. Han, "5G ultra-dense cellular networks," *IEEE Wireless Communications*, vol. 23, no. 1, p. 72, 2016.

[33] N. Bhushan, J. Li, D. Malladi et al., "Network densification: the dominant theme for wireless evolution into 5G," *IEEE Communications Magazine*, vol. 52, no. 2, p. 82, 2014.

[34] S. Yunas, M. Valkama, and J. Niemelä, "Spectral and energy efficiency of ultra-dense networks under different deployment strategies," *IEEE Communications Magazine*, vol. 53, no. 1, p. 90, 2015.

[35] Z. Chen, S. Chen, H. Xu, and B. Hu, "A security authentication scheme of 5G ultra-dense network based on block chain," *IEEE Access*, vol. 6, p. 55372, 2018.

[36] S. Seng, C. Luo, X. Li, H. Zhang, and H. Ji, "User matching on blockchain for computation offloading in ultra-dense wireless networks," *IEEE Transactions on Network Science and Engineering*, vol. 2020, p. 1, 2020.

[37] D. A. Chekired, M. A. Togou, L. Khoukhi, and A. Ksentini, "5G-Slicing-Enabled scalable SDN core network: toward an ultra-low latency of autonomous driving service," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 8, p. 1769, 2019.

[38] S. Rahmadika, K. Lee, and K. H. Rhee, "Blockchain-Enabled 5G autonomous vehicular networks," in *Proceedings of the International Conference on Sustainable Engineering and Creative Computing*, pp. 275–280, Bandung, Indonesia, August 2019.

[39] U. Majeed, L. U. Khan, and C. S. Hong, "Cross-silo horizontal federated learning for flow-based time-related-features oriented traffic classification," in *Proceedings of the 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Daegu, South Korea, September 2020.

[40] A. E. Azzaoui, S. K. Singh, Y. Pan, and J. H. Park, "Block5-GIntell: blockchain for AI-enabled 5G networks," *IEEE Access*, vol. 8, p. 145918, 2020.

[41] S. Rahmadika and K.-H. Rhee, "Rethinking blockchain and decentralized learning: position paper," in *Advances In Computer Science And Ubiquitous Computing*, pp. 127–133, Springer, Berlin, Germany, 2021.

[42] M. Singh, A. Singh, and S. Kim, "Blockchain: a game changer for securing IoT data," in *Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, February 2018.

[43] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5G evolution: A view on 5G cellular technology beyond 3GPP release 15," *IEEE Access*, vol. 7, 2019.

[44] X. Zhang, A. Kunz, and S. Schroder, "Overview of 5G security in 3GPP," in *Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, Helsinki, Finland, September 2017.

[45] J. Kim, D. Kim, and S. Choi, "3GPP SA2 architecture and functions for 5G mobile communication system," *ICT Express*, vol. 3, 2017.

[46] M. de Ree, G. Mantas, J. Gao, J. Rodriguez, and I. E. Otung, "Public key cryptography without certificates for beyond 5G mobile small cells," in *Proceedings of the 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, Porto, Portugal, July 2020.

[47] Z. Shang, M. Ma, and X. Li, "A secure group-oriented device-to-device authentication protocol for 5G wireless networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 11, p. 7021, 2020.

[48] Mathworks, "H and written digits-datasets," 2020, https://www.mathworks.com/help/deeplearning/ug/data-sets-for-deep-learning.html.

[49] Etherscan, "Ethereum daily gas used (January 2021)," 2021, https://etherscan.io/chart/gasused.

[50] Etherscan, "Ethereum gas: chart display and information," 2021, https://etherscan.io/chart/.