Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.039487

ARTICLE

A Blockchain-Assisted Distributed Edge Intelligence for Privacy-Preserving Vehicular Networks

Muhammad Firdaus[1], Harashta Tatimma Larasati[2] and Kyung-Hyune Rhee[3,*]

[1]Department of Artificial Intelligence Convergence, Pukyong National University, Busan, 48513, Korea

[2]School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, 40132, Indonesia

[3]College of Information Technology and Convergence, Division of Computer Engineering and AI, Pukyong National University, Busan, 48513, Korea

*Corresponding Author: Kyung-Hyune Rhee. Email: khrhee@pknu.ac.kr

Received: 01 February 2023 Accepted: 20 April 2023 Published: 08 October 2023

ABSTRACT

The enormous volume of heterogeneous data from various smart device-based applications has growingly increased a deeply interlaced cyber-physical system. In order to deliver smart cloud services that require low latency with strong computational processing capabilities, the Edge Intelligence System (EIS) idea is now being employed, which takes advantage of Artificial Intelligence (AI) and Edge Computing Technology (ECT). Thus, EIS presents a potential approach to enforcing future Intelligent Transportation Systems (ITS), particularly within a context of a Vehicular Network (VNets). However, the current EIS framework meets some issues and is conceivably vulnerable to multiple adversarial attacks because the central aggregator server handles the entire system orchestration. Hence, this paper introduces the concept of distributed edge intelligence, combining the advantages of Federated Learning (FL), Differential Privacy (DP), and blockchain to address the issues raised earlier. By performing decentralized data management and storing transactions in immutable distributed ledger networks, the blockchain-assisted FL method improves user privacy and boosts traffic prediction accuracy. Additionally, DP is utilized in defending the user's private data from various threats and is given the authority to bolster the confidentiality of data-sharing transactions. Our model has been deployed in two strategies: First, DP-based FL to strengthen user privacy by masking the intermediate data during model uploading. Second, blockchain-based FL to effectively construct secure and decentralized traffic management in vehicular networks. The simulation results demonstrated that our framework yields several benefits for VNets privacy protection by forming a distributed EIS with privacy budget (ε) of 4.03, 1.18, and 0.522, achieving model accuracy of 95.8%, 93.78%, and 89.31%, respectively.

KEYWORDS

Edge intelligence; federated learning; differential privacy; blockchain; vehicular networks

1 Introduction

In recent years, a vast amount of heterogeneous data created from numerous devices has growingly increased a deeply interlaced cyber-physical system in supporting various internet-connected applications, such as smart industry [1], smart healthcare [2], smart grids [3], and Intelligent Transportation

systems (ITS) [4]. In order to provide smart cloud services that inquire strong computational processing capabilities with low latency, the study of Edge Intelligence System (EIS) [5], which takes advantage of Artificial Intelligence (AI) and Edge Computing Technology (ECT), has been emerging. In the ITS context, EIS offers a promising approach to enforcing future Vehicular Networks (VNets). AI reduces decision-making delays and provides smart cloud services with high performance [6]. Meanwhile, ECT offers reliable storage and computation, where local resources are at the edge of a network that performs computational processing and data storage rather than relying on a central server or data center. Thus, by leveraging its intelligent edge resources, EIS improves real-time services and low-latency communication, offers powerful computational processing, and enables self-aggregating communication systems in VNets [7].

However, the current AI approach suffers from several privacy risks, including massive overhead in gathering and updating the training data, the possibility of private data leakage, and the occurrence of a Single Point of Failure (SPoF) because it trains the model and aggregates the user's data on a central aggregator centrally [8]. Further, there is a rising need for privacy-preserving AI due to the recent establishment of data privacy preservation rules [9], including the General Data Protection Regulation (GDPR) [10] and the Health Insurance Portability and Accountability Act (HIPAA) [11]. Thus, Federated Learning (FL) arose as a favorable method to address these issues. FL keeps the local data stored on the user's devices and allows a collaborative model training approach among distributed mobile devices without exposing the training data [12]. Further, FL demonstrates its effectiveness and preserves user privacy through local collaborative training and shared machine learning model updates without exposing individual datasets. In the context of VNets, FL has presented a potential solution to improve VNets' performance and address several challenges, including the limited availability of data due to privacy concerns and the high mobility of vehicles, which can cause data to be unreliable or untrustworthy. Some works have been widely considering the merits of FL for VNets. In [13], the authors introduced the Federated Vehicular Network (FVN), a resilient distributed VNets that can provide data/computation-intensive applications by utilizing both millimeter wave (mmWave) communication and dedicated short-range communications (DSRC) to reach stable and scalable performance. The authors in [14] offered a selective model aggregation approach, which reduces communication overhead and computational complexity while maintaining the accuracy of the trained model. They also introduce the two-dimension contract theory with selection criteria to facilitate the interactions between users and aggregator server as well as determine the most suitable models for aggregation. Moreover, to address the challenge of heterogeneous model distribution and varying communication quality, the work in [15] suggested a two-layer FL approach with heterogeneous model aggregation for VNets supported by 6G networks. The first layer involves local FL among the vehicles in the same cluster, while the second layer aggregates the models from different clusters using a weighted model aggregation scheme.

Although FL has great potential to support EIS in improving VNets performance, it is not immune to adversary attacks, including poisoning [16] and membership inference attacks [17]. Poisoning attacks, in which an adversary seeks to corrupt the global model by transmitting malicious updates during the collaborative training phase. On the other hand, in membership inference attacks, an adversary attempts to reverse engineer the users' confidential data by examining the trained model updates. Hence, those attacks represent significant threats to the security and integrity of FL systems. Moreover, the central aggregator that coordinates the FL process is vulnerable to SPoF issues, which can compromise user data confidentiality and disrupt the system's functioning. Thus, these vulnera-

bilities may discourage users from participating in developing FL-based edge intelligence systems for VNets. For these reasons, to discourse on the issues mentioned above, we require a robust framework that not only prioritizes VNets performance but also provides privacy and security guarantees to motivate users to supply appropriate contributions with long-term participation. Therefore, this paper aims to bridge the gap by introducing a distributed EIS framework that leverages the advantages of FL, blockchain technology, and Differential Privacy (DP) to address the existing FL-based EIS challenges in the context of VNets application. By incorporating blockchain into the FL process, we aim to improve users' privacy and security by using immutable distributed ledger networks and enhance the accuracy of decentralized traffic prediction. Blockchain can be utilized to establish a decentralized network of EIS, where all involved node maintains a copy of the same data, thereby making it more resilient to data loss or tampering. Additionally, blockchain can be a rewarding scheme to encourage users to collaborate in improving the global model based on the local model training process. We also utilize DP to ensure the secrecy of the trained local model and protect user data from adversarial attacks during data-sharing transactions in VNets. Moreover, since FL involves multiple users contributing data to the training process, DP allows each user to maintain ownership of their data while contributing to the overall training process. Through the combination of FL, blockchain, and DP, we seek to enhance the security and privacy of edge intelligence systems.

The remainder of this paper is organized as follows. We provide a comprehensive overview of the background knowledge relevant to the components of EIS technology in Section 2 before examining previous studies in the field in Section 3. Section 4 introduces our proposed model for secure edge intelligence in VNets. In Section 5, numerical findings are discussed. Lastly, Section 6 concludes the paper.

2 Preliminaries

2.1 Federated Learning

Traditionally, Machine Learning (ML) techniques involve training models on centralized servers by aggregating data from multiple users, which may contain sensitive information. In this sense, in the user-server architecture of classical ML, the training process is always possessed on the server. Users solely perform as data providers, whereas the server accomplishes data training and aggregation. Hence, these approaches can pose significant privacy risks, including the possibility of data leakage and the threat of SPoF, as well as incurring overhead in data collection and storage [18]. In order to tackle these challenges, Google presented FL [19] as a novel, communication-efficient optimization algorithm for distributed machine learning. FL is a technique that enables distributed mobile devices to work together to train models without the need to centralize the training data and keep the data held locally on the devices [20]. Moreover, it can enable a wide range of applications, including personalization on mobile devices [21], predictive maintenance in the IoT industry [22], personalized medicine in healthcare [23], improved fraud detection in finance [24], and improved traffic prediction and personalization of autonomous vehicles in VNets [25].

At its core, Federated Learning (FL) seeks to facilitate the collective training of models across multiple entities without the necessity of sharing private data. In this way, sensitive information remains confined to individual devices and is never disseminated [21]. FL endeavors to optimize

the global loss function $F(\omega)$ by using FL optimization objectives that can be aggregated through empirical risk minimization (ERM) techniques, as described in Eq. (1).

$$\min_{w} F(\omega) = \sum_{m=1}^{k} p_m F_m(\omega) \tag{1}$$

where the notation employed encompasses the model parameters denoted as ω, the number of participating devices represented by k, p_m represents the proportion of data points originating from device m in relation to the overall data points, and $F_m(\omega)$ is notation for the loss function evaluated on device m.

Fig. 1 depicts the general federated learning procedure [19]. The central server, serving as the model provider, disseminates the global model to the participating users. Each user downloads the global model and generates a model update by training it on their local data, which is then uploaded to the central server acting as the aggregator. The aggregator server then averages all the updated models from the users to produce a new global model for the subsequent round. Thus, through this process, federated learning effectively enhances user privacy by blocking various attacks that could potentially compromise access to the local training data.

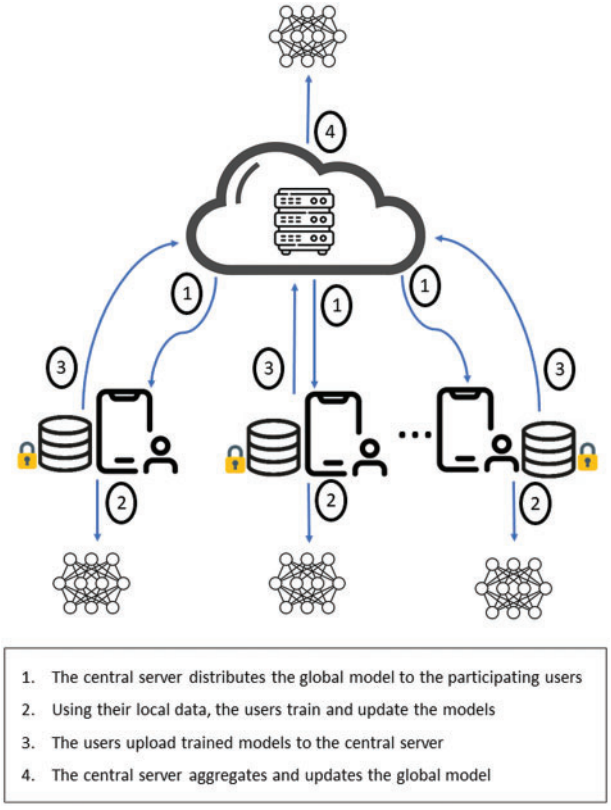


Figure 1: Illustration of FL procedures

2.2 Edge Computing Technology

ECT is a distributed computing paradigm that brings computation and data storage closer to the location needed to improve response times and save bandwidth [26]. It expands upon the idea of cloud

computing by bringing its capabilities to the edge of the network. The objectives of ECT are similar to those of cloudlets or fog computing in other literature. Furthermore, ECT provides data storage and performs computational processing locally at the edge of the infrastructure, closer to the data provider or user. Consequently, ECT delivers low-latency communication, real-time services, and location awareness. Additionally, it also reduces delay and conserves bandwidth by eliminating the need for transferring data to remote nodes in the VNets systems [27]. In ECT, devices such as smartphones, IoT sensors, and other connected devices perform computation and store data locally rather than transmitting it to a centralized server or cloud for processing. This can be advantageous in situations where internet connectivity is limited or unreliable or where the data being processed is sensitive and must remain on-premises for security purposes. ECT can be beneficial in applications where low latency is of the utmost importance, such as in autonomous vehicles or virtual and augmented reality systems. Ultimately, edge computing aims to improve computation speed and efficiency by bringing it closer to the edge of the network, closer to the devices and users that require it.

Moreover, ECT is also helpful when large amounts of data are generated in real-time and require immediate processing. For instance, in the context of robotic and facility control systems [28], ECT with AI integration can enable real-time data processing and decision-making capabilities at the edge of the network where the robots and facilities are located. Hence, the system can better adapt to changing environmental conditions and resource availability, enabling efficient resource synchronization and sharing among robots and facilities in a distributed system. Therefore, it can improve the overall efficiency and responsiveness of the system and reduce reliance on centralized cloud servers.

2.3 Blockchain

Blockchain technology, first introduced in 2009 by the mysterious figure known as Satoshi Nakamoto through the creation of the first decentralized digital currency, Bitcoin has recently garnered significant attention from both industry professionals and academics for its potential to revolutionize a wide range of applications through the creation of decentralized and secure systems [29]. By eliminating the need for centralized servers, blockchain technology can be utilized to address inefficiencies and improve data security through anonymous and trustworthy transactions [30]. Transactions recorded on a blockchain are added to a decentralized ledger with timestamps, preventing any single authority from endorsing events in secrecy. The decentralized nature of blockchain technology allows it to operate without the need for a central authority, instead relying on consensus among the participating nodes. This consensus-driven approach helps to ensure the integrity and security of the blockchain, as any attempt to alter the records would need to be coordinated across a majority of the network in order to succeed.

A blockchain comprises a series of interconnected blocks, each of which contains a record of multiple transactions and a unique cryptographic hash. These hashes are generated using complex mathematical algorithms, which are used to identify and verify the authenticity of each block. The structure of a blockchain is illustrated in Fig. 2, with each block comprising a header containing information such as the block number, the previous block's hash, a timestamp, and other metadata, and a body containing the transactions recorded on the network.

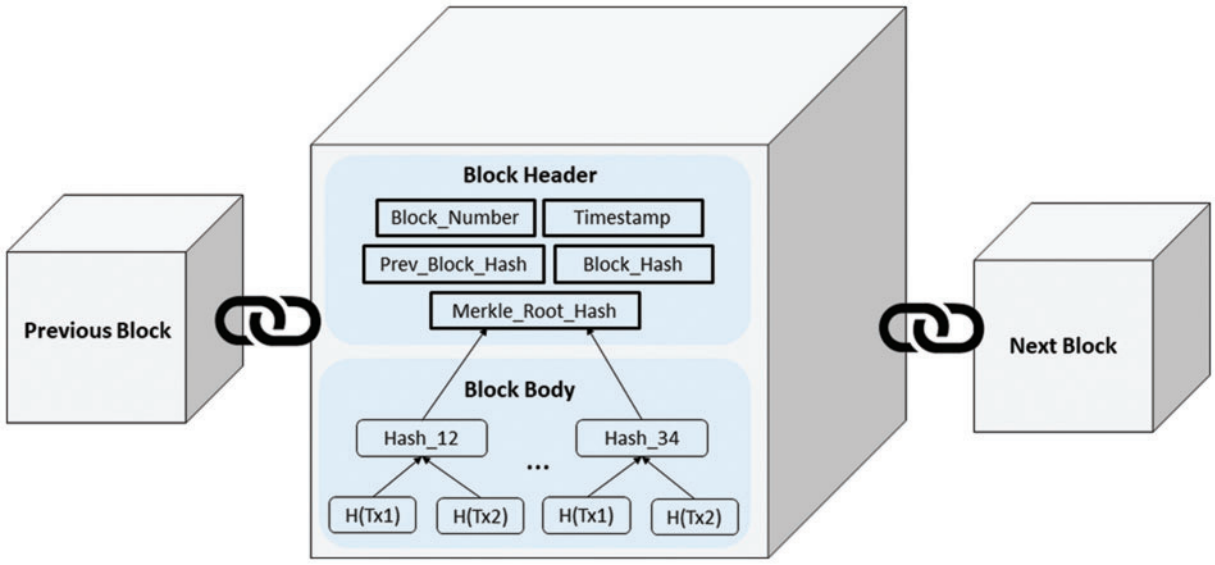


Figure 2: Illustration of blockchain structure

2.4 Differential Privacy

Differential privacy (DP) [31] is a mathematical concept that aims to provide strong privacy guarantees for data collection and analysis. It has been widely recognized as a strong and effective privacy protection mechanism and endorsed by organizations such as the US Census Bureau [32] and the Australian Bureau of Statistics [33]. In a few years, it has also obtained an extensive engagement in AI and machine learning. DP works by adding carefully calibrated noise to a dataset, which helps to obscure sensitive information and prevent the identification of individual records. This noise, such as Gaussian or Laplacian noise distribution, is added in such a way as to maximize the utility of the data while still providing strong privacy protections. In order to implement differential privacy, a privacy budget (ε) must be chosen, which represents the maximum amount of privacy loss that is acceptable in order to gain the benefits of the data [34]. This budget is then used to determine the appropriate noise level to add to the dataset. The standard definition of differential privacy is explained as follows [31].

Definition 1 (Differential Privacy): *A randomized mechanism M provides (ε, δ)-differential privacy if for any two neighboring database D_1 and D_2 that differ in only a single entry, $\forall S \subseteq Range(M)$*

$$\Pr\left(M\left(D_1\right) \in S\right) \leq e^{\varepsilon} \Pr\left(M\left(D_2\right) \in S\right) + \delta. \tag{2}$$

If $\delta = 0$, M is stated to attain a state of ε-differential privacy. Here, δ represents slight odds of failure. Furthermore, as Eq. (2) shows, a larger value of ε leads to a lower degree of privacy, whereas a smaller value of ε leads to a higher degree of privacy (i.e., more extra noise).

3 Related Work

Edge Intelligence System (EIS) is a subfield of the Internet of Things (IoT) and ECT that focuses on enabling intelligent decision-making at the edge of the network rather than relying on a centralized cloud infrastructure. It is built upon two key technologies: ECT and ML. ECT refers to processing data close to the source rather than sending all data to a central location for processing [35,36]. It enables

low-latency, high-bandwidth, and real-time data processing, which is critical for many IoT applications such as industrial control, autonomous vehicles, and augmented reality. Conversely, ML is a subset of AI that enables computers to learn from data and make predictions or decisions without explicit programming. ML models require large amounts of data to be trained and often require significant computational resources [37]. By combining the benefits of these two technologies, EIS enables the deployment of sophisticated ML models on edge devices such as IoT gateways, edge servers, and edge nodes, thereby allowing for real-time data analysis and the ability to execute complex models on devices with limited computational resources [38].

Currently, several works utilize FL, an ML subfield, to enhance EIS's usability. FL enables multiple devices to collaborate and improve a shared model without needing a centralized dataset. This can be done in a decentralized way without the need for a central authority to control the data or the model. FL is beneficial for edge intelligence applications, as it allows for the training of models using data that is distributed across multiple devices while preserving data privacy. In [39], the authors survey various FL techniques and protocols that have been proposed for mobile edge networks and highlight the challenges, opportunities, and future research directions. They also provide a taxonomy for categorizing the existing literature in the EIS field. Moreover, in order to enhance the performance of FL-assisted EIS, Wang et al. [40] introduced a novel approach, referred to as In-edge AI protocol which incorporates FL techniques to optimize mobile edge computing, caching, and communication. This protocol aims to optimize resource utilization, reduce transmission overhead, and increase data privacy. The authors in [38] proposed a communication-efficient method to perform FL in wireless EIS for IoT, which addresses the challenges caused by the limited resources and high mobility of wireless edge devices and balances the trade-off between communication efficiency and model accuracy. The work in [41] proposed a joint learning communication system for FL in wireless networks, which aims to optimize communication efficiency and reduce the transmission delay during the FL process by empowering user selection and resource allocation schemes. Also, Lu et al. [42] leveraged FL to establish collaborative edge intelligence to mitigate data leakage and safeguard user privacy information in the context of vehicular cyber-physical systems.

On the other hand, blockchain, as a distributed ledger technology, has been proposed as a solution to tackle the limitations of conventional data governance systems in VNets. In the context of FL-assisted EIS, blockchain can be leveraged to deliver a decentralized system for incentivizing participation, verifying the integrity of updates to model training, and supporting fair aggregation of global models. Recent research has also explored the potential for merging blockchain and FL in order to enhance privacy. For instance, in [43], a privacy-preserving mechanism for data sharing for the Industrial Internet of Things (IIoT) was suggested for a distributed multi-party scenario, combining FL with the consensus scheme of a permissioned blockchain. Another study [44] presented a framework for preventing dishonest users from accessing the FL system through the use of smart contracts to defend against data or model poisoning attacks. Additionally, a protocol named DeepChain [45] that offers an incentive scheme based on blockchain was proposed to deliver an auditable, fair, secure, and distributed deep learning approach, utilizing incentives to motivate participants to act responsibly and mitigating the drawbacks of a centralized approach.

Moreover, in an effort to safeguard the confidential nature of local training models from potentially malicious actors, various studies have centered on implementing DP to protect users' data. In [46], the authors suggested a hybrid method that addresses the multifaceted challenges of FL, including a lack of accuracy and inference attacks, through the utilization of both DP and secure multi-party computation (SMPC). This strategy reduces the need for increasingly larger amounts of noise injection as the number of users increases across various applications and use cases.

Additionally, another work [47] offered the NbAFL protocol as a means of mitigating data leakage by implementing DP techniques prior to aggregating FL models. This study specifically aims to solve the information leakage issue in FL with distributed stochastic gradient descent (SGD) while also formulating academic conjunction bound for the loss function during FL model training.

4 Towards Secure Edge Intelligence

In this paper, we present a joint framework that synergizes the strengths of FL, Local Differential Privacy (LDP), and blockchain technology to establish a robust EIS in VNets. In this context, EIS, composed of FL and ECT, emphasizes enabling intelligent decision-making at the edge of the network along with providing low-latency, high-bandwidth, and real-time data processing, which is critical for VNets. Moreover, ECT-based EIS nodes are employed to reduce communication and computation costs by providing local storage, communication, and computation capabilities, which allows computational processing to be conducted closer to users (i.e., vehicles) as data providers. On the other hand, LDP is leveraged to defend the vehicle's sensitive data from various threats and strengthen the confidentiality of data-sharing transactions. By using LDP, we enhance the secrecy of transactions, particularly in protecting private or sensitive data during the process of uploading trained models locally. Furthermore, since FL relies on the contribution of data from multiple users to enhance the training process, the use of LDP ensures that each vehicle retains ownership of its data while still actively participating in the overall training process. Additionally, blockchain as a distributed ledger technology addresses the limitations of centralized servers and transparently manages the uploaded parameters of updated models. Therefore, blockchain is used to enrich the privacy and security of model parameters in the edge resources of FL by encrypting the data using a specific cryptography method. In order to grasp the proposed model, this section delves into the architectural design and detailed procedures of the distributed edge intelligence framework for VNets.

4.1 Design Architecture Overview

Fig. 3 depicts the proposed joint framework for distributed EIS. In this framework, roadside units (RSUs) and vehicles serve as essential entities which participate as aggregator servers and user participants, exchanging information through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, which are based on dedicated short-range communication (DSRC) standards. In our scenario, vehicles are considered distributed edge users, leveraging their local data to collaboratively update FL parameters for improved real-time traffic prediction in VNets. Moreover, they are equipped by onboard units (OBUs) with simple communication and computational capabilities that contain various sensors (e.g., GPS, LiDAR, video, fuel, pressure, and infrared sensors) to obtain their local dataset regarding traffic and road-related information, including accident information, safety warnings, traffic jams, and weather conditions. RSUs, on the other hand, are positioned as distributed edge servers along the road, supplied with edge computing servers, and connecting vehicles to roadside infrastructure through wireless communication. Moreover, edge computing servers are utilized to reduce communication and computation costs by providing local storage, communication, and computation capabilities, allowing for computational processing to be conducted closer to vehicles as data providers. It is worth noting that all vehicles must be authorized by a trusted party (TP), such as the Department of Transportation, before accessing the network service to verify the legitimacy of their identity (e.g., driver's licenses or vehicle ID). Additionally, RSUs serve as intelligent edge servers, gathering and consolidating models from dispersed edge users in VNets, storing them in a decentralized ledger blockchain, and managing EIS traffic efficiently.

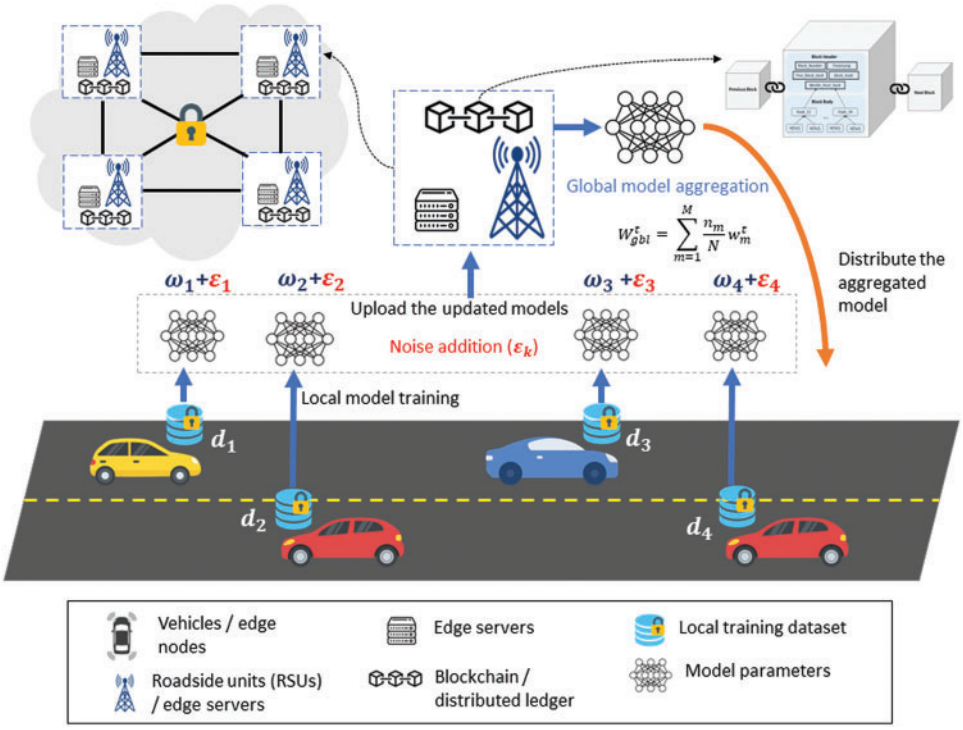


Figure 3: Overview of the joint framework for distributed EIS

Moreover, the proposed model utilizes a consortium blockchain to ensure that the participating EIS nodes (i.e., RSUs) are preselected based on their trustworthiness, thereby enhancing the security and reliability of the overall system. Consortium blockchain guarantees the authenticity of the transactions and mitigates the risk of malicious vehicles compromising the EIS network. As such, the consortium blockchain-based FL method represents a promising solution for secure and efficient data sharing along with boosting traffic prediction accuracy in VNets. Blockchain offers a decentralized platform that is suitable for managing large-scale data sharing in VNets. It can facilitate transparent data sharing by leveraging blockchain's immutability and tamper-proof nature. Furthermore, integrating FL with blockchain can assist in tackling the challenges associated with privacy and data ownership by allowing each vehicle to maintain control over its data while contributing to improving the global model updates.

4.2 Procedures of Proposed Framework

Our design architecture includes local model training among users, protecting and validating model parameters through blockchain-based LDP, and aggregating global models in a distributed EIS. Fig. 4 shows the workflow of proposed architecture. The procedure starts with creating a task contract and initiating the learning model procedure. During initialization, the initial global model parameters ω^0 are uploaded to the blockchain-powered RSUs, which can be integrated with off-chain storage, e.g., the InterPlanetary File System (IPFS). Here, TP has created a task contract that includes ω^0, performance evaluation, and reward mechanism. Public-private key pairs are generated for edge nodes (EN^{pk}, EN^{sk}) to be used in the data-sharing process, and vehicles are also required to generate their own public-private key pairs (m^{pk}, m^{sk}). Subsequently, at iteration t, edge users, in this case,

legitimated vehicles (donated by $m_i = m_1, m_2, \ldots, m_n$) that pass the registration and authentication process, retrieve the global model ω^t from blockchain and perform the training of local model to produce trained models ω_m^t utilizing their local dataset d_m according to Eq. (3).

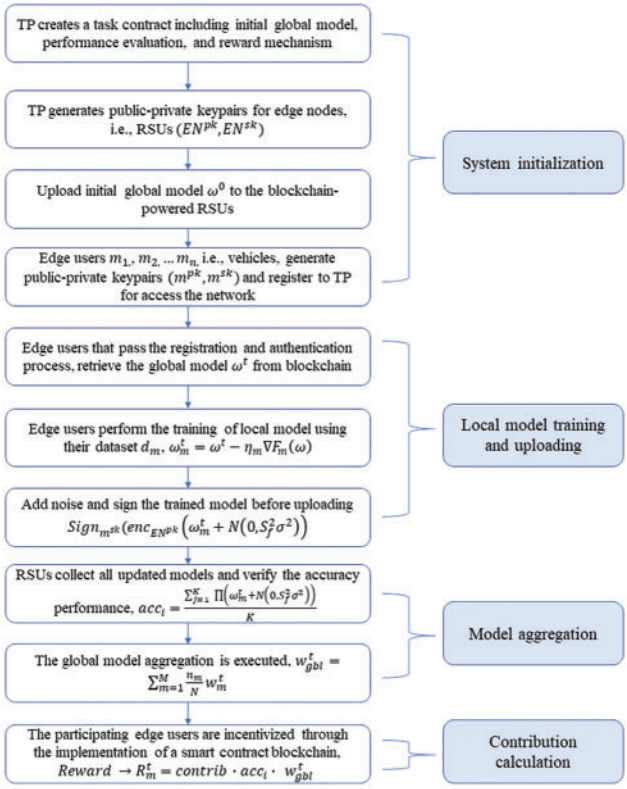


Figure 4: Workflow of the proposed architecture

Algorithm 1:: Distributed Edge Intelligence in VNets. M number of users; EN is edge node; D_m is local datasets of users; T number of iterations; E number of epochs; and η is learning rate, inspired by [47].

Data: T, ω^0, ε, and δ

1. Initialization: $t = 1$ and $\omega_i^0 = \omega^0, \forall i$
2. Public-private keypairs generation $\left(EN^{pk}, EN^{sk}\right), \left(m^{pk}, m^{sk}\right)$
3. Upload ω^0 to distributed ledger blockchain
4. **while** $t \leq T$ **do**
5. **Local model training procedure:**
6. **while** $m_i \in \{m_1, m_2, \ldots, m_n\}$ **do**
7. Download ω^t from blockchain-powered EN
8. Update the local parameters ω_m^t using its D_m as
9. $\omega_m^t = \omega^t - \eta_m \nabla F_m(\omega)$, where $F_m(\omega) = \frac{1}{n_m} \sum_{x_i \in D_m} f_i(\omega)$

(Continued)

Algorithm 1 (continued)

Add random noise ε using Gaussian mechanism $f(D) + N\left(0, S_f^2\sigma^2\right)$ to ω_m^t
Sign and upload the trained local model $Sign_{m^{sk}}\left(enc_{EN^{pk}}\left(\omega_m^t + \varepsilon\right)\right)$ to distributed ledger
Model aggregation procedure:
Collect all ω_m^t from users
Verify the accuracy performance as
$$acc_i = \frac{\sum_{j=1}^{K} \prod \left(\omega_m^t + N\left(0, S_f^2\sigma^2\right)\right)}{K}$$
Aggregate the global model ω_{gbl}^t as
$$\omega_{gbl}^t = \sum_{m=1}^{M} \frac{n_m}{N} \omega_m^t$$
Upload w_{gbl}^t to distributed ledger for next iteration $(t+1)$
Contribution calculation procedure:
Collect the list of participating users $m_1, m_2, \ldots, m_n$
Confirm transaction $H(\omega_{m1}^t, \omega_{m2}^t, \ldots, \omega_{mn}^t)$
Calculate the user contribution as
$$Reward \rightarrow R_m^t = contrib \cdot acc_i \cdot w_{gbl}^t$$
Rewards are given to $m_1, m_2, \ldots, m_n$
end procedure

$$\omega_m^t = \omega^t - \eta_m \nabla F_m(\omega) \tag{3}$$

$$F_m(\omega) = \frac{1}{n_m} \sum_{x_i \in Dm} f_i(\omega) \tag{4}$$

where η_m is learning rate, $\nabla F_m(\omega)$ is the average gradients, f_i is a loss function for i-th data point of m $\left(x_p^{(i)}, y_p^{(i)}\right)$, and n_m donated as the number of samples generated by m from N total number of data points (samples), $N = \sum_{m=1}^{M} n_m$.

Moreover, the LDP mechanism is employed to reinforce privacy during the uploading of these local models by incorporating random noise ε, thereby mitigating the risk of linkability attacks such as membership and model inference attacks. In this step, the addition of noise ε is carried out by m to attain ε-differential privacy through Eq. (2) and the Gaussian mechanism, specified as follows.

$$f(D) + N\left(0, S_f^2\sigma^2\right) \tag{5}$$

where $S_f\sigma$ is standard deviation and $N\left(0, S_f^2\sigma^2\right)$ is the normal distribution with mean 0 [34]. Later, m_i encrypt the LDP-protected model ω_m^t with edge node public key and sign it before uploading.

$$Sign_{m^{sk}}(enc_{EN^{pk}}\left(\omega_m^t + N\left(0, S_f^2\sigma^2\right)\right) \tag{6}$$

After the vehicles collaboratively upload their ω_m^t with LDP protection to distributed edge server RSUs, the blockchain evaluates all updated models from vehicles according to the task contract, where accuracy is the parameter for performance verification that can be calculated through the following formula [48]:

$$acc_i = \frac{\sum_{j=1}^{K} \prod \left(\omega_m^t + N\left(0, S_f^2\sigma^2\right)\right)}{K} \tag{7}$$

$$\prod \left(\omega_m^t + N\left(0, S_f^2\sigma^2\right)\right) = \begin{cases} 0\,\omega_m^t = false \\ 1\,\omega_m^t = true \end{cases} \tag{8}$$

where acc_i represents the accuracy performance and K indicates the total number of test sets. Then, the evaluated results of ω_m^t are recorded with a hash function $H(\omega_{m1}^t, \omega_{m2}^t, \ldots, \omega_{mn}^t)$ to be used in contribution assessment, where:

$$H\omega_m^t \rightarrow \begin{pmatrix} H\left\{m_1^{pk}, \omega_{m_1}^t + N\left(0, S_f^2\sigma^2\right)\right\}, H\left\{m_2^{pk}, \omega_{m_2}^t + N\left(0, S_f^2\sigma^2\right)\right\}, \ldots, \\ H\left\{m_n^{pk}, \omega_{m_n}^t + N\left(0, S_f^2\sigma^2\right)\right\} \end{pmatrix} \tag{9}$$

Later, the global model aggregation is executed as follows:

$$w_{gbl}^t = \sum_{m=1}^{M} \frac{n_m}{N} w_m^t \tag{10}$$

$$Reward \rightarrow R_m^t = contrib \cdot acc_i \cdot w_{gbl}^t \tag{11}$$

where w_{gbl}^t is a new global model that is obtained for the next iteration $(t+1)$. In this step, w_{gbl}^t is stored in blockchain that maintained by RSUs where all legitimated participants in the system can download it. As a result, the model is repeatedly updated until either precise accuracy is achieved or the maximum number of iterations is reached. Finally, users are incentivized through the implementation of a smart contract blockchain, where they are rewarded for fulfilling the transaction requirements of the EIS framework. In summary, Algorithm 1 describes the procedures of the distributed edge intelligence framework for VNets.

5 Numerical Results and Discussion

In this section, we implement our proposed model to form a distributed edge intelligence framework by combining the advantages of DP, blockchain, and FL. The proposed framework has been applied to two conditions: blockchain-based FL for the efficient establishment of decentralized traffic management in VNets and LDP-based FL for providing randomized privacy protection with the aid of the International Business Machines (IBM) Library for DP. In this study, the computational results were obtained on a desktop computer with Ubuntu operating system version 18.04, which was installed on a virtual machine, Oracle VM VirtualBox. The specification computer has an Intel(R) Core (TM) i7-1165G7 11th Gen Central Processing Unit (CPU) operating at a speed of 2.80 GHz, and it was supported by 16.00 GB of Random Access Memory (RAM).

A prototype of VNets was devised with an optimized link-state routing protocol using a discrete event simulator to examine system performance, as depicted in our prior works [49]. Fig. 5 shows the Medium Access Control and Physical Layer (MAC/PHY) overhead in relation to the Packet Delivery Ratio (PDR) during an experiment duration of 100 s to evaluate the performance of VNets. As depicted, after 17 s of simulation, the overhead remains consistently within the range of 0.2 to 0.25 and slowly recedes. In this sense, the more down the overhead, the higher the system's performance, and vice versa. Based on the results mentioned above, our proposed protocol is relatively efficient as it does not incur considerable overhead.

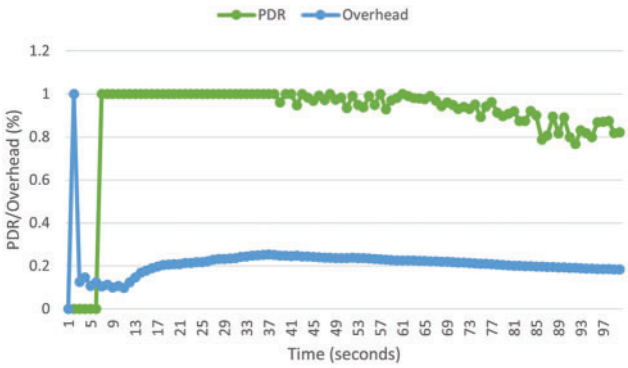
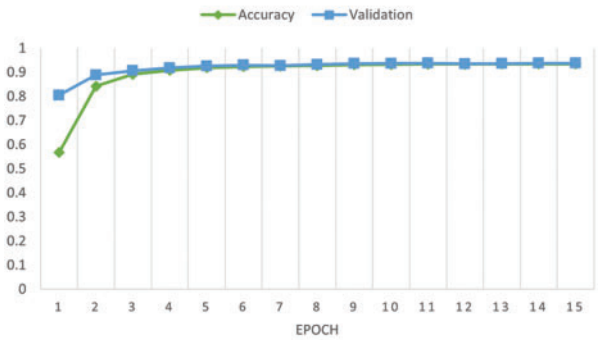


Figure 5: Comparison of PDR ando overhead

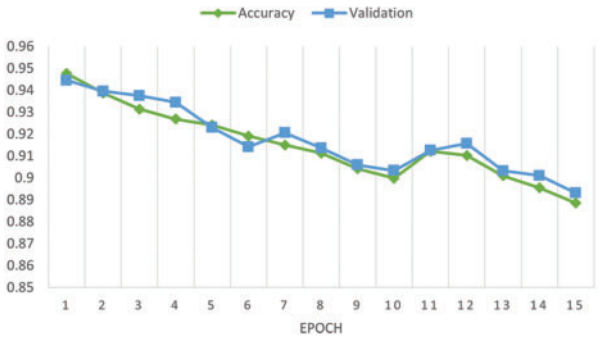
We adopted a consortium setting that employs blockchain to construct a decentralized FL framework. Moreover, we utilize the Ethereum platform to transparently assess participants' contributions toward the global model, establish a decentralized incentivization system, and carry out decentralized FL transactions. In our simulation, we utilized the Modified National Institute of Standards and Technology (MNIST) [50] datasets as a benchmark for image classification, with 60,000 images as training and 10,000 as test examples, where the apiece example consists of a 28×28 gray-level image. Here, MNIST datasets represent the traffic and road-related information that is suitable for FL applications. Moreover, we use the Convolutional Neural Network (CNN) model consisting of two 5×5 convolution layers to represent the FL model in our scenario. We elaborate on the CNN model that is well-suited for image recognition tasks, which are prevalent in the MNIST dataset. Furthermore, to execute the FL with the DP model, we utilized an open-source library based on python developed by IBM, which provides a simple and efficient method for the simulation and implementation of differential privacy over various applications [51]. This library also offers mechanisms for generating the random noise required (e.g., Laplacian and Gaussian mechanisms) to achieve differential privacy, thus making it suitable for our scenario.

Fig. 6 presents the experiment utilizing DP in FL with varying degrees of privacy level, i.e., $\varepsilon = 0.522$, $\varepsilon = 1.18$, and $\varepsilon = 4.03$, over a period of 15 epochs. This scenario examines the impact of privacy levels (ε) on system accuracy by adding varying degrees of noise sampled to local models during training. Moreover, the Gaussian mechanism is used to accomplish this objective. The simulation results demonstrate that Fig. 6a, with a privacy budget of $\varepsilon = 4.03$, attains a model accuracy of 95.8%. Conversely, Figs. 6b and 6c, with privacy budgets of $\varepsilon = 1.18$ and $\varepsilon = 0.522$, respectively, demonstrate a model accuracy of 93.78% and 89.31% (the detailed result can be found in Table 1). Therefore, as the value of ε decreases (i.e., the level of added noise increases), the system's privacy (according to the interval between validation and accuracy) increases; however, the accuracy decreases, and vice versa.

(a) ε = 4.03, δ = 1e − 05



(b) ε = 1.18, δ = 1e − 05



(c) ε = 0.522, δ = 1e − 05

Figure 6: Accuracy comparison of various privacy budget

Fig. 7 shows the value of the loss function with various numbers of vehicles (users), i.e., $m = 10, 20, 30, 40$, and 50. In this experiment, we set 50 epochs training with a learning rate of 0.01. As a result, increasing the number of vehicles leads to better convergence performance because more users will provide larger global datasets for training. On the other hand, Fig. 8 depicts smart contracts' initial migration and deployment based on the platform of Ethereum. The graph illustrates the gas units needed for initial migration (164391, 0.00328782 Ether (ETH)), federated smart contract (263330, 0.0052666 ETH), and participant contribution deployment (1018839, 0.02037678 ETH). With deployed smart contracts, we can adjust the number of participants in local model training and fairly calculate their contributions through blockchain technology.

Table 1: Impact of privacy levels (ε) on system accuracy

Epoch	$\varepsilon = 4.03$			$\varepsilon = 1.18$			$\varepsilon = 0.522$		
	T/S	Acc.	Val.	T/S	Acc.	Val.	T/S	Acc.	Val.
1	60 s 1 ms	0.9403	0.9445	59 s 977 us	0.5681	0.8055	59 s 979 us	0.9477	0.9445
2	59 s 991 us	0.9433	0.9476	58 s 975 us	0.8426	0.8891	59 s 981 us	0.9387	0.9396
3	59 s 990 us	0.9447	0.9506	58 s 970 us	0.8919	0.907	58 s 974 us	0.9314	0.9375
4	59 s 987 us	0.9472	0.9515	58 s 975 us	0.9085	0.9186	59 s 977 us	0.9269	0.9345
5	59 s 984 us	0.9483	0.9523	59 s 975 us	0.9191	0.9262	59 s 976 us	0.9242	0.923
6	59 s 989 us	0.9485	0.9554	59 s 976 us	0.9240	0.9302	58 s 973 us	0.9191	0.9142
7	59 s 982 us	0.9492	0.9533	58 s 972 us	0.9264	0.9278	58 s 974 us	0.9150	0.9206
8	60 s 1 ms	0.9510	0.9560	58 s 968 us	0.9277	0.9326	59 s 977 us	0.9113	0.9137
9	59 s 990 us	0.9526	0.9555	58 s 971 us	0.9316	0.9359	59 s 976 us	0.9042	0.9059
10	59 s 978 us	0.9531	0.9555	58 s 974 us	0.9325	0.9365	58 s 974 us	0.8999	0.9034
11	59 s 982 us	0.9531	0.9565	58 s 974 us	0.9334	0.9375	59 s 976 us	0.9121	0.9126
12	59 s 980 us	0.9545	0.9574	58 s 975 us	0.9338	0.9356	59 s 979 us	0.9103	0.9157
13	59 s 977 us	0.9536	0.9572	59 s 976 us	0.9344	0.936	59 s 976 us	0.9010	0.9033
14	58 s 972 us	0.9548	0.9572	59 s 975 us	0.9343	0.9377	59 s 987 us	0.8955	0.9011
15	58 s 972 us	0.9551	0.9580	58 s 974 us	0.9349	0.9378	59 s 976 us	0.8885	0.8931

Note: *T/S = time/sample, *Acc. = accuracy, Val. = validation, *s = second, ms = millisecond, us = microsecond.

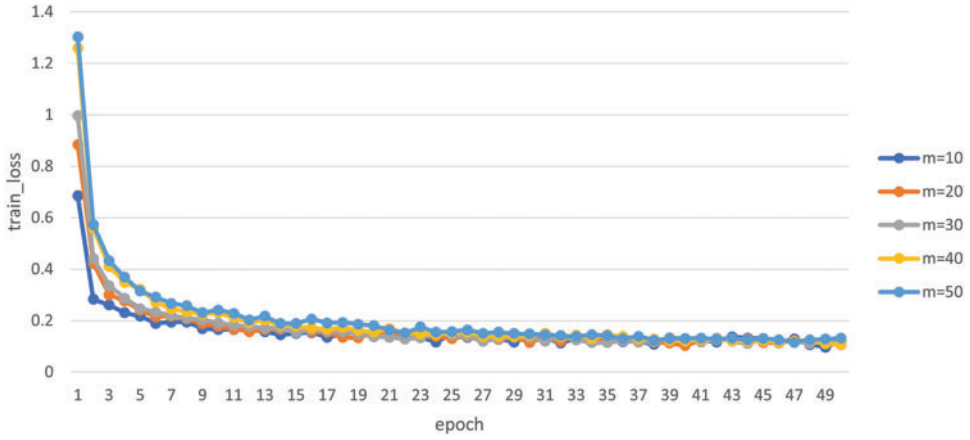


Figure 7: Loss function value for various numbers of vehicles

The distribution of edge servers' contributions towards generating the global model FL based on the Ethereum platform is depicted in Fig. 9. We have designed three separate collaborative edge servers (i.e., RSUs) to work collaboratively to serve as intelligent EIS, gathering and consolidating models from dispersed edge users in VNets, and storing them in a decentralized ledger blockchain. Later, the incentive or reward is distributed to the participating vehicles upon creating a new global model based on their recorded contributions in the blockchain's distributed ledger. Additionally, Fig. 10 shows that, on average, our proposed protocol achieves better performance accuracy than existing works [51,52] and is comparable to the FL baseline [19]. It is worth noting that FedAvg is regarded as the FL's general standard, and the other methods compared are a DP-based FL approach [51] as well as a blockchain-based FL system [52], the detailed comparison can be seen in Table 2. In summary, this scenario seeks

to motivate users to actively participate in preserving the EIS framework and improving the system's performance.

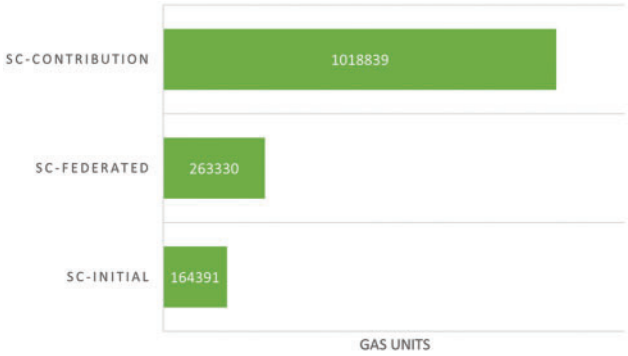


Figure 8: Smart contracts' initial migration and deployment

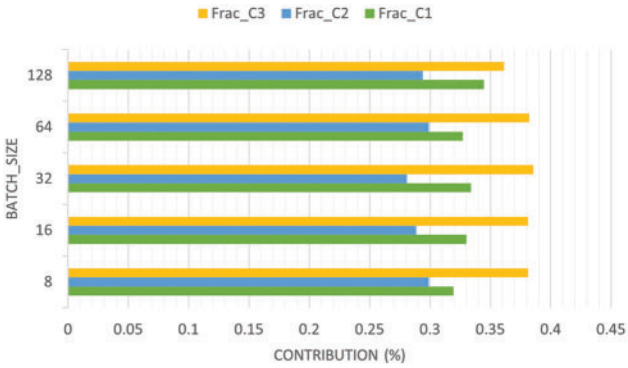


Figure 9: Distribution of edge servers' contributions

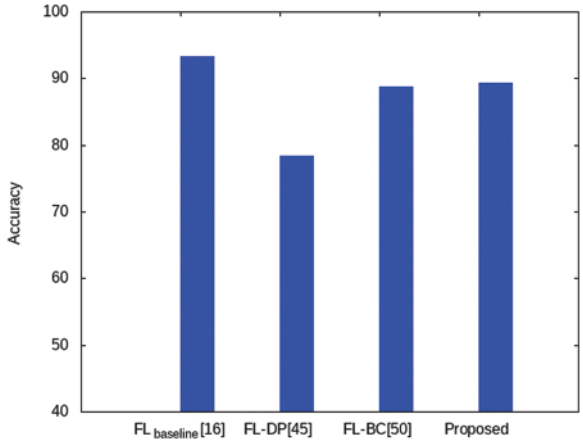


Figure 10: Performance accuracy comparison

Table 2: Comparison of the proposed system with related works

Key parameters	McMahan et al. [19]	Holohan et al. [51]	Cai et al. [52]	This work
Computation and communication cost	Low	Low	High	Low
Against the adversary attacks	No	Yes	No	Yes
Protect the trained model during uploading	No	Yes	No	Yes
Decentralized global model aggregation	No	No	No	Yes
Contribution calculation	No	No	Yes	Yes
Traceability transaction	No	No	Yes	Yes
Contribution calculation	No	No	Yes	Yes

6 Conclusion and Future Work

In this paper, we introduced the concept of distributed edge intelligence, combining the advantages of FL, DP, and blockchain. We consider utilizing blockchain to protect user privacy and security by recording all transactions in immutable distributed ledger networks. Moreover, by incorporating blockchain into the FL process, we aim to enhance the accuracy of decentralized traffic prediction and provide a decentralized rewarding scheme to encourage users to improve the global model collaboratively. FL-based EIS enables intelligent decision-making at the network's edge and provides low-latency, high-bandwidth, and real-time data processing, which is critical for VNets. Moreover, integrating FL with blockchain can assist in tackling the challenges associated with privacy and data ownership by allowing each vehicle to maintain control over its data while contributing to improving the global model updates. Additionally, DP is utilized to ensure the secrecy of the trained local model and protect user data from adversarial attacks during data-sharing transactions in VNets. Numerical results show that our proposed protocol is relatively efficient as it does not incur the considerable overhead of VNets performance. We have designed a distributed EIS framework that gathers and consolidates models from dispersed edge users and stores them in a decentralized ledger based on the Ethereum platform. Furthermore, based on our simulation, it is worth noting that the impact of privacy budget ε on the accuracy is when a smaller ε (more noise added) results in higher privacy but decreased accuracy. Lastly, even though the EIS approach shows great potential compared to the conventional centralized model training framework, there are still significant challenges and potential risks to user privacy and security that need to be addressed. Further research is needed to investigate potential attacks and defenses to create a more robust EIS framework that can be implemented in real-world scenarios. Additionally, it is necessary to consider other critical factors in VNets, such as the user selection mechanism for model training and the impact of system and statistical heterogeneity. Neglecting these factors could lead to inaccurate models and poor convergence, which could significantly hinder the practical implementation of VNets. Therefore, future studies must take a holistic approach to consider all these factors for designing and implementing VNets that can achieve optimal performance and scalability with reliable privacy protection.

Acknowledgement: All authors would like to thank the anonymous reviewers for their constructive suggestions, which improve the quality of this work.

Funding Statement: This research was supported by the Republic of Korea's MSIT (Ministry of Science and ICT), under the ICT Convergence Industry Innovation Technology Development Project (2022-0-00614) supervised by the IITP and partially supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2021R1I1A3046590).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: M.F., K.H.R.; data collection: M.F.; analysis and interpretation of results: M.F., H.T.L.; draft manuscript preparation: M.F., H.T.L., K.H.R. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The MNIST dataset used in this paper refers to [50], which can be accessed at https://yann.lecun.com/exdb/mnist/.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Boyes, B. Hallaq, J. Cunningham and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, no. 8, pp. 1–12, 2018.

[2] S. Tian, W. Yang, J. M. Le Grange, P. Wang, W. Huang *et al.,* "Smart healthcare: Making medical care more intelligent," *Global Health Journal*, vol. 3, no. 3, pp. 62–65, 2019.

[3] F. Al-Turjman and M. Abujubbeh, "IoT-enabled smart grid via SM: An overview," *Future Generation Computer Systems*, vol. 96, no. 6, pp. 579–590, 2019.

[4] L. Zhu, F. R. Yu, Y. Wang, B. Ning and T. Tang, "Big data analytics in intelligent transportation systems: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 1, pp. 383–398, 2019.

[5] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo *et al.,* "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738–1762, 2019.

[6] Y. Dai, D. Xu, S. Maharjan, G. Qiao and Y. Zhang, "Artificial intelligence empowered edge computing and caching for internet of vehicles," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 12–18, 2019.

[7] X. Zhu, H. Li and Y. Yu, "Blockchain-based privacy preserving deep learning," in *Information Security and Cryptology: 14th Int. Conf., Inscrypt 2018*, Fuzhou, China, Springer International Publishing, vol. 11449, pp. 370–383, 2019.

[8] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang *et al.,* "Reliable federated learning for mobile networks," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 72–80, 2020.

[9] Y. Cheng, Y. Liu, T. Chen and Q. Yang, "Federated learning for privacy-preserving AI," *Communications of the ACM*, vol. 63, no. 12, pp. 33–36, 2020.

[10] P. Voigt and A. von dem Bussche, "The EU general data protection regulation (GDPR)," in *A Practical Guide*, 1st ed., Cham: Springer International Publishing, pp. 10-55552017, 2017.

[11] I. G. Cohen and M. M. Mello, "HIPAA and protecting health information in the 21st century," *JAMA*, vol. 320, no. 3, pp. 231, 2018.

[12] M. Firdaus, H. T. Larasati and K. H. Rhee, "A secure federated learning framework using blockchain and differential privacy," in *2022 IEEE 9th Int. Conf. on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th Int. Conf. on Edge Computing and Scalable Cloud (EdgeCom)*, Xi'an, China, pp. 18–23, 2022.

[13] J. Posner, L. Tseng, M. Aloqaily and Y. Jararweh, "Federated learning in vehicular networks: Opportunities and solutions," *IEEE Network*, vol. 35, no. 2, pp. 152–159, 2021.

[14] D. Ye, R. Yu, M. Pan and Z. Han, "Federated learning in vehicular edge computing: A selective model aggregation approach," *IEEE Access*, vol. 8, pp. 23920–23935, 2020.
[15] X. Zhou, W. Liang, J. She, Z. Yan, I. Kevin *et al.,* "Two-layer federated learning with heterogeneous model aggregation for 6G supported internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5308–5317, 2021.
[16] V. Tolpegin, S. Truex, M. E. Gursoy and L. Liu, "Data poisoning attacks against federated learning systems," in *Computer Security-ESORICS 2020: 25th European Symp. on Research in Computer Security, ESORICS 2020*, Guildford, UK, Springer International Publishing, vol. 12308, pp. 480–501, 2020.
[17] R. Shokri, M. Stronati, C. Song and V. Shmatikov, "Membership inference attacks against machine learning models," in *2017 IEEE Symp. on Security and Privacy (SP)*, San Jose, California, USA, pp. 3–18, 2017.
[18] Q. Yang, Y. Liu, T. Chen and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.
[19] H. B. McMahan, E. Moore, D. Ramage, S. Hampson and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. of 20th Int. Conf. Artificial Intelligence and Statistics AISTATS 2017*, Fort Lauderdale, FL, USA, vol. 54, pp. 1273–1282, 2017.
[20] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh *et al.,* "Federated learning: Strategies for improving communication efficiency," pp. 1–10, 2016. [Online]. Available: http://arxiv.org/abs/1610.05492
[21] A. Hard, K. Rao, R. Mathews, S. Ramaswamy, F. Beaufays *et al.,* "Federated learning for mobile keyboard prediction," 2018. [Online]. Available: http://arxiv.org/abs/1811.03604
[22] M. Hao, H. Li, X. Luo, G. Xu, H. Yang *et al.,* "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6532–6542, 2020.
[23] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian *et al.,* "Federated learning for healthcare informatics," *Journal of Healthcare Informatics Research*, vol. 5, no. 1, pp. 1–19, 2021.
[24] W. Yang, Y. Zhang, K. Ye, L. Li and C. Z. Xu, "FFD: A federated learning based method for credit card fraud detection," in *Big Data-BigData*, San Diego, CA, USA, Springer International Publishing, vol. 11514, pp. 18–32, 2019.
[25] Y. Liu, J. J. Q. Yu, J. Kang, D. Niyato and S. Zhang, "Privacy-preserving traffic flow prediction: A federated learning approach," *IEEE Internet Things Journal*, vol. 7, no. 8, pp. 7751–7763, 2020.
[26] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.
[27] 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, pp. 414, 2021.
[28] K. L. Keung, Y. Y. Chan, K. K. Ng, S. L. Mak, C. H. Li *et al.,* "Edge intelligence and agnostic robotic paradigm in resource synchronisation and sharing in flexible robotic and facility control system," *Advance Engineering Informatics*, vol. 52, no. 1, pp. 101530, 2022.
[29] J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS One*, vol. 11, no. 10, pp. e0163477, 2016.
[30] X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.
[31] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation*. Xi'an, China, Berlin Heidelberg: Springer, vol. 4978, pp. 1–19, 2008.
[32] J. M. Abowd, "The U.S. census bureau adopts differential privacy," in *Proc. of the 24th ACM SIGKDD Int. Conf. on Knowledge Discovery & Data Mining*, New York, NY, USA, pp. 2867–2867, 2018.
[33] S. M. Tam and F. Clarke, "Big data, official statistics and some initiatives by the Australian Bureau of statistics," *International statistical Review*, vol. 83, no. 3, pp. 436–448, 2015.
[34] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, nos. 3–4, pp. 211–407, 2013.
[35] S. Deng, H. Zhao, W. Fang, J. Yin, S. Dustdar *et al.,* "Edge intelligence: The confluence of edge computing and artificial intelligence," *IEEE Internet Things Journal*, vol. 7, no. 8, pp. 7457–7469, 2020.

[36] L. Ting, M. Khan, A. Sharma and M. D.Ansari, "A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing," *Journal of Intelligent Systems*, vol. 31, no. 1, pp. 221–236, 2022.
[37] J. Chen and X. Ran, "Deep learning with edge computing: A review," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1655–1674, 2019.
[38] J. Mills, J. Hu and G. Min, "Communication-efficient federated learning for wireless edge intelligence in IoT," *IEEE Internet Things Journal*, vol. 7, no. 7, pp. 5986–5994, 2020.
[39] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y. C. Liang *et al.,* "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.
[40] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen *et al.,* "In-edge AI: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Networks*, vol. 33, no. 5, pp. 156–165, 2019.
[41] M. Chen, Z. Yang, W. Saad, C. Yin, H. Vincent Poor *et al.,* "A joint learning and communications framework for federated learning over wireless networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 269–283, 2020.
[42] Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Federated learning for data privacy preservation in vehicular cyber-physical systems," *IEEE Networks*, vol. 34, no. 3, pp. 50–56, 2020.
[43] Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.
[44] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato *et al.,* "A secure federated learning framework for 5G networks," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 24–31, 2020.
[45] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang *et al.,* "DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2438–2455, 2019.
[46] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig *et al.,* "A hybrid approach to privacy-preserving federated learning," in *Proc. of the 12th ACM Workshop on Artificial Intelligence and Security*, London, UK, pp. 1–11, 2019.
[47] K. Wei, J. Li, M. Ding, C. Ma, H. Yang *et al.,* "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3454–3469, 2020.
[48] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma *et al.,* "A blockchain-based machine learning framework for edge services in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1918–1929, 2021.
[49] M. Firdaus and K. H. Rhee, "A joint framework to privacy-preserving edge intelligence in vehicular networks," in *Information Security Applications*, Jeju Island, South Korea, Cham, Springer Nature Switzerland, pp. 156–167, 2023.
[50] Y. Lecun, L. Bottou, Y. Bengio and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.
[51] N. Holohan, S. Braghin, P. M. Aonghusa and K. Levacher, "Diffprivlib: The IBM differential privacy library," 2019. [Online]. Available: https://arxiv.org/abs/1907.02444
[52] H. Cai, D. Rueckert and J. Passerat-Palmbach, "2CP: Decentralized protocols to transparently evaluate contributivity in blockchain federated learning environments," 2020. [Online]. Available: https://arxiv.org/abs/2011.07516