Enhancing Security and Privacy in Federated Learning for Connected Autonomous Vehicles with Lightweight Blockchain and Binius Zero-Knowledge Proofs

Ny Hasina ANDRIAMBELO
Cognitive Sciences and Applications
University of Antananarivo
Madagascar
nyhasinas@gmail.com

Naghmeh MORADPOOR
School of Computing, Engineering and the Built Environment
Edinburgh Napier University
Edinburgh, UK
n.moradpoor@napier.ac.uk

***Abstract*— This The rise of autonomous vehicles (AVs) brings with it the need for secure and privacy-preserving machine learning models. Federated learning (FL) allows AVs to collaboratively train models while keeping raw data localized. However, traditional FL systems are vulnerable to security threats, including adversarial attacks, data breaches, and dependency on a central aggregator, which can be a single point of failure. To address these concerns, this paper introduces a peer-to-peer decentralized federated learning system that integrates lightweight blockchain technology and Binius Zero-Knowledge Proofs (ZKPs) to enhance security and privacy. In this system, Binius ZKPs ensure that model updates are cryptographically verified without exposing sensitive information, guaranteeing data confidentiality and integrity during the learning process. The lightweight blockchain framework secures the network by creating an immutable, decentralized record of all model updates, thus preventing tampering, fraud, or unauthorized modifications. This decentralized approach eliminates the need for a central aggregator, significantly enhancing system resilience to attacks and making it suitable for dynamic environments like AV networks. Additionally, the system's design includes Byzantine resilience, providing protection against adversarial nodes and ensuring that the global model aggregation process remains robust even in the presence of malicious actors. Extensive performance evaluations demonstrate that the system achieves low-latency, scalability, and efficient resource usage while maintaining strong security and privacy guarantees, making it an ideal solution for real-time federated learning in autonomous vehicle networks. The proposed framework not only ensures privacy but also fosters trust among participants in a fully decentralized environment.**

Keywords— ZKPs, data integrity, peer-to-peer, cryptography, model poisoning

I. INTRODUCTION

The rise of autonomous vehicles (AVs) has introduced revolutionary changes in the transportation sector, presenting significant opportunities to improve safety, efficiency, and convenience in daily commutes. Autonomous vehicles rely heavily on real-time decision-making, using data from numerous onboard sensors, cameras, and external data sources to navigate dynamic environments and interact with other vehicles on the road. However, the massive amounts of data required for such operations have prompted concerns about privacy, security, and data integrity. To address these challenges, federated learning (FL) has emerged as a promising decentralized approach that enables vehicles to collaboratively train machine learning models without sharing raw data, thereby preserving privacy [5]. Despite its potential, federated learning introduces several critical challenges, including malicious participants, privacy leakage, and the need for trust in model aggregation. This paper introduces an innovative solution that integrates lightweight blockchain technology and Binius Zero-Knowledge Proofs (ZKPs) to enhance both privacy and security in federated learning [9]. The system addresses key issues such as protecting local data privacy, defending against Byzantine attacks, and ensuring verifiable updates to the global model without compromising efficiency, particularly in real-time environments like AV networks. Through this introduction, we aim to outline the significance of privacy-preserving and secure federated learning, the current state of research in this domain, and how our proposed solution contributes to the growing field of secure autonomous vehicle communication and learning [8].

A. The Role of Federated Learning in Autonomous Vehicles

Federated learning has gained traction in recent years as a method to train machine learning models in decentralized environments. In traditional machine learning systems, data from multiple clients is collected and stored centrally to train models, which presents significant privacy risks, especially in sectors like healthcare, finance, and, most recently, autonomous vehicles. The centralized collection of data not only makes it vulnerable to breaches but also raises concerns regarding compliance with privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). In the context of autonomous vehicles, federated learning allows each vehicle to locally train its models using data generated by onboard sensors, without sharing the actual data with a central server. Instead, vehicles share only model updates (gradients or parameters) with a central aggregator, which then combines these updates to generate a global model. The global model is then sent back to the vehicles for further local training. This paradigm ensures that sensitive data never leaves the device, offering significant privacy advantages. However, even

though raw data is kept local, there are still several vulnerabilities, such as model inversion attacks, in which attackers can infer private data from shared model updates. Moreover, federated learning systems are susceptible to Byzantine failures, where adversarial nodes attempt to corrupt the global model by sending malicious updates.

B. Security and Privacy Challenges in Federated Learning

Despite its promising potential, federated learning introduces several security and privacy challenges, particularly in untrusted and dynamic environments such as autonomous vehicle networks. First, federated learning assumes that all participants act honestly, which may not hold true in practice. In a real-world scenario, adversarial nodes may deliberately manipulate their local models to poison the global model, leading to degraded performance or incorrect decisions. This problem is exacerbated in autonomous vehicles, where real-time decisions, such as braking or lane changes, could lead to catastrophic consequences if based on faulty models. Second, while federated learning protects the privacy of raw data by keeping it local, the model updates shared during training still pose privacy risks. Model inversion attacks and membership inference attacks can allow adversaries to reconstruct private data from the updates, making it crucial to enhance the privacy guarantees of federated learning systems. Techniques such as differential privacy and secure multi-party computation (SMPC) have been proposed to mitigate these risks, but they often come at the cost of model accuracy or computational overhead. Additionally, federated learning requires trust in the central aggregator, which is responsible for combining the model updates from all participants. A compromised aggregator could manipulate the global model, leading to reduced accuracy or even dangerous behaviors in autonomous vehicles. This necessitates the development of a decentralized and trustless system that ensures the integrity and correctness of the global model without relying on a central entity.

C. The Role of Blockchain in Federated Learning

To address the issues of trust and security in federated learning, recent research has explored the integration of blockchain technology. Blockchain provides a decentralized and immutable ledger that can record model updates, ensuring that all participants can verify the correctness and provenance of the updates. This eliminates the need for a trusted central aggregator, as all updates are recorded on the blockchain and can be verified by any participant. Additionally, blockchain can be used to incentivize honest behavior and penalize malicious nodes, further enhancing the robustness of the system. Several studies have explored blockchain-based federated learning for autonomous vehicles. For example, Sultana et al. propose a blockchain-enabled federated learning system that logs encrypted model updates on a blockchain, ensuring that no single entity can tamper with the updates [1]. However, while blockchain enhances the security and transparency of the system, it introduces significant computational overhead due to the resource-intensive nature of blockchain consensus mechanisms. This makes traditional blockchain systems unsuitable for real-time applications like autonomous vehicles, where low latency and fast decision-making are critical.

D. The Power of Zero-Knowledge Proofs in Privacy-Preserving FL

Zero-Knowledge Proofs (ZKPs) are cryptographic techniques that allow one party to prove to another that they know a value or that a computation is correct, without revealing the actual value or details of the computation. This makes ZKPs particularly well-suited for privacy-preserving federated learning, as they enable participants to verify that model updates are valid without revealing any sensitive information about the data used to generate them. Recent works, such as RoFL (Robust Federated Learning) and RiseFL, have explored the use of ZKPs to enhance privacy and security in federated learning. zkFL, proposed by Wang et al. [2], uses ZKPs to enable secure gradient aggregation in federated learning systems, offering privacy guarantees for participants while preventing malicious updates. Similarly, RiseFL employs ZKPs to verify that model updates were correctly aggregated without revealing sensitive data used in training. However, these approaches assume that the aggregator behaves semi-honestly, leaving room for potential vulnerabilities if the aggregator is compromised. The proposed system goes beyond these approaches by integrating Binius ZKPs, which provide strong privacy guarantees without relying on a trusted aggregator. In this system, Binius ZKPs are used to verify the correctness of model updates in a fully decentralized manner, ensuring that even if the aggregator is compromised, no sensitive information can be inferred from the model updates. This makes the system resilient to Byzantine attacks and other adversarial behaviors, providing a higher level of security than traditional federated learning systems.

E. Enhancing Federated Learning with Lightweight Blockchain and Binius ZKPs

The proposed system combines lightweight blockchain technology with Binius ZKPs to address the challenges of privacy, security, and trust in federated learning for autonomous vehicles. By using a lightweight blockchain, the system reduces the computational overhead associated with traditional blockchain systems, making it suitable for real-time decision-making in AV networks. The blockchain ensures that all model updates are recorded and verifiable, eliminating the need for a central aggregator and providing a decentralized and transparent system. In addition, the integration of Binius ZKPs ensures that all model updates are cryptographically verified before aggregation, preventing malicious participants from tampering with the global model. This enhances the system's Byzantine resilience, making it robust against adversarial behaviors such as model poisoning. Furthermore, Binius ZKPs allow the system to achieve privacy-preserving verification, ensuring that no sensitive information is revealed during the training process.

The proposed system is evaluated through comprehensive simulations, which demonstrate its ability to maintain high model accuracy while providing strong privacy and security guarantees. The system is also shown to be scalable, with low computational and communication overhead, making it

suitable for large-scale autonomous vehicle networks. Autonomous vehicles present unique challenges for federated learning systems, particularly with respect to privacy, security, and real-time decision-making. The proposed system addresses these challenges by integrating lightweight blockchain technology and Binius Zero-Knowledge Proofs (ZKPs), providing a decentralized and privacy-preserving solution for federated learning in AV networks. This system not only enhances privacy and security but also reduces the computational overhead, making it suitable for real-time applications in autonomous vehicles. Through comprehensive evaluations, the system demonstrates its potential to support the next generation of secure and decentralized AV systems, ensuring that model updates can be verified without compromising privacy or performance.

II. Related work

Federated Learning (FL) has gained significant traction in recent years as a decentralized framework that allows multiple devices to collaboratively train machine learning models without centralizing sensitive data. In the domain of autonomous vehicles (AVs), FL has emerged as a promising approach to facilitate large-scale data processing while maintaining privacy. However, traditional FL frameworks are susceptible to various security and privacy risks, especially when dealing with malicious aggregators or adversarial participants. To address these issues, several research efforts have explored the integration of blockchain and zero-knowledge proofs (ZKPs), providing additional layers of security and privacy in federated learning systems.

A. Federated Learning and Privacy Concerns

In vehicular networks, federated learning introduces unique privacy challenges as data must be exchanged and aggregated in a distributed environment. One major concern is the privacy of local data stored on each vehicle. In traditional FL settings, a central server or aggregator receives local model updates from participants to build a global model, but this process is vulnerable to attacks if the aggregator is compromised. Sultana et al. propose a blockchain-enabled FL system that mitigates this risk by using blockchain to log encrypted model updates from participants, ensuring that no single entity has direct access to raw data [1]. Blockchain serves as a distributed ledger that records model updates, providing transparency and reducing the risk of data tampering. While this approach enhances trust among participants, it relies heavily on the consensus mechanism of blockchain to ensure security. This dependence introduces several inefficiencies, especially in real-time environments like autonomous vehicles. Additionally, the absence of ZKPs limits the system's ability to provide verifiable privacy guarantees for model updates. In comparison, the proposed system in this paper goes beyond blockchain's inherent security properties by integrating Binius ZKPs to ensure that each model update is cryptographically verified without revealing any private information about the data used in the training process. This combination addresses both privacy and security in a more robust manner, ensuring that the aggregation process cannot be compromised by either malicious participants or faulty aggregators.

B. Zero-Knowledge Proofs in Federated Learning

ZKPs have recently been integrated into federated learning to strengthen privacy guarantees, especially when the aggregator is untrusted. The RoFL (Robust Federated Learning) protocol, as demonstrated by Lycklama et al. [3], employs ZKPs to ensure that each client's model updates adhere to certain constraints before being aggregated. This approach protects against malicious model updates, ensuring that no client can send poisoned updates to corrupt the global model [4]. Similarly, RiseFL, proposed by Zhu et al., leverages ZKPs to allow each participant to verify that their model update was correctly aggregated without revealing sensitive data used in training. These ZKP-based protocols have proven effective in preventing model poisoning attacks while maintaining a strong privacy-preserving guarantee. However, both of these works make certain assumptions about the behavior of the aggregator, namely that it behaves semi-honestly and only deviates from the protocol in a limited way. This assumption leaves room for potential vulnerabilities if the aggregator behaves maliciously. The proposed system diverges from these approaches by leveraging Binius ZKPs, which do not rely on trust in the aggregator. Instead, they offer stronger privacy guarantees by ensuring that even a compromised aggregator cannot learn any sensitive information from the model updates. Moreover, the use of ZKPs enhances the system's ability to defend against Byzantine failures and adversarial attacks, where nodes deliberately provide false information to disrupt the learning process.

C. Blockchain and Decentralized FL

The combination of blockchain and federated learning has been widely explored to address the issue of trust in decentralized environments. Blockchain provides an immutable, decentralized ledger that can store model updates and track participants' actions in real-time, eliminating the need for a central authority. PZKP-FL, for example, combines blockchain with ZKPs to enable secure and verifiable federated learning [6, 11, 12, 14]. In PZKP-FL, model updates are recorded on-chain, and participants can use ZKPs to verify the correctness of computations without revealing their underlying data. This approach prevents collusion between participants and ensures that no party can provide dishonest updates without being detected. However, despite its advantages, this method introduces significant computational overhead due to the resource-intensive nature of blockchain operations and ZKP generation. The high latency and scalability limitations of traditional blockchain systems make them impractical for real-time applications like autonomous vehicles, where decisions must be made rapidly. In contrast, the proposed system leverages a lightweight blockchain optimized for low-latency environments, reducing the overhead while maintaining the security benefits of blockchain. By incorporating Binius ZKPs, the system ensures privacy-preserving and verifiable model aggregation, making it a more practical solution for AVs.

D. Byzantine Resilience in Federated Learning

A major challenge in federated learning is defending against Byzantine nodes, which are participants that behave

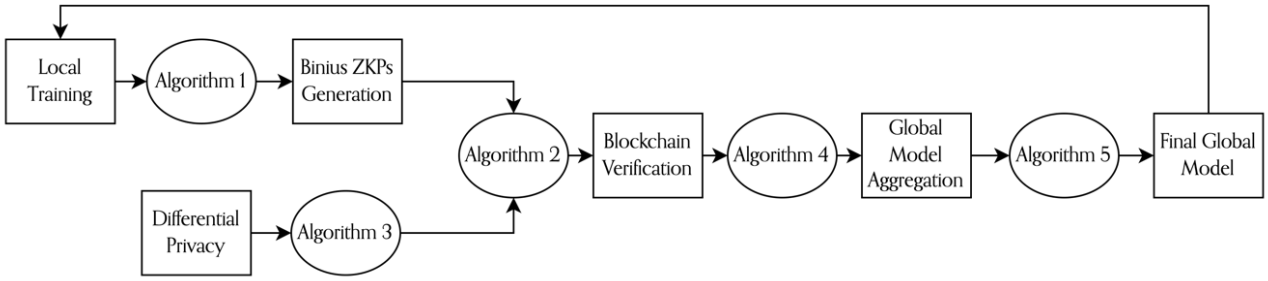

Figure 1. The architecture of our proposed framework

maliciously to corrupt the global model. Byzantine nodes may send incorrect or poisoned model updates, leading to significant degradation in model performance. Existing works, such as stake-based federated learning, introduce mechanisms to handle Byzantine nodes by using staking and voting systems [10, 13]. These methods work by assigning reputation scores to participants based on their past behavior, which allows the system to discount updates from nodes that are deemed unreliable. While this approach offers some level of Byzantine resilience, it is vulnerable to collusion between malicious nodes, where participants coordinate their efforts to circumvent the reputation system. Moreover, stake-based methods do not protect against Byzantine failures at the cryptographic level, leaving the system open to certain types of attacks. The proposed system addresses this limitation by integrating Binius ZKPs, which provide cryptographic guarantees that model updates are valid. By verifying the correctness of each update through ZKPs, the system prevents Byzantine nodes from submitting false or malicious data, thereby enhancing the resilience of the global model against adversarial participants.

E. Applications to Autonomous Vehicles

The application of federated learning to autonomous vehicles introduces several challenges, particularly with respect to latency, real-time decision-making, and privacy concerns. Autonomous vehicles must be able to collaborate in real-time to update their models based on rapidly changing environmental conditions. Blockchain-based FL has been explored as a solution to ensure the integrity of model updates exchanged between vehicles. For example, Kim et al. proposed a system that uses off-chain storage and data integrity mechanisms to ensure that AVs can safely exchange model updates [5, 15]. However, this system suffers from high communication costs and latency due to the blockchain processing overhead.

The proposed system mitigates these issues by using lightweight blockchain protocols specifically optimized for AV networks. This approach significantly reduces the communication burden, allowing vehicles to exchange model updates efficiently. Additionally, the integration of Binius ZKPs ensures that all model updates are privacy-preserving and can be verified without revealing sensitive information about each vehicle's data. This combination makes the proposed system a more suitable solution for real-time federated learning in autonomous vehicles, enabling faster decision-making and stronger privacy guarantees.

III. THE PROPOSED FRAMEWORK

The integration of connected autonomous vehicles (CAVs) into modern intelligent transportation systems has opened new avenues for innovation and efficiency in smart cities. However, the increasing reliance on autonomous systems brings significant challenges in terms of security and privacy, particularly in the exchange and processing of data required to train machine learning models. Federated Learning (FL) addresses some privacy concerns by decentralizing model training, allowing multiple clients (vehicles) to collaboratively train models without exposing their raw data to a central entity. Despite these advantages, traditional FL frameworks remain vulnerable to several security issues, including model poisoning, data leakage, and attacks by malicious participants (also known as Byzantine nodes). In this paper, we propose a comprehensive framework that addresses these challenges by combining Peer-to-Peer Federated Learning (P2P-FL) with Lightweight Blockchain, Binius Zero-Knowledge Proofs (ZKPs), and Differential Privacy (DP). The primary objective of this framework is to enhance the security and privacy of the learning process in a decentralized setting while maintaining the efficiency required for real-time operations in CAVs. The lightweight blockchain ensures immutability and traceability of model updates, Binius ZKPs provide cryptographic guarantees that the updates are valid without revealing sensitive information, and DP protects against data leakage by adding noise to the model updates. In this section, we detail the proposed framework's components, architecture, and algorithms that collectively ensure a secure, private, and efficient federated learning process. The framework is designed to be scalable, Byzantine-resilient, and privacy-preserving, making it ideal for CAV networks where data security and integrity are paramount.

A. Framework Architecture

The architecture of the proposed framework, Figure1, consists of four primary components: the Peer-to-Peer Federated Learning Network, Lightweight Blockchain, Binius Zero-Knowledge Proofs, and Differential Privacy with Adaptive Clipping. These components work in unison to provide a robust and scalable system for secure and private model training and aggregation across a decentralized network of CAVs.

1) Peer-to-Peer Federated Learning Network

Unlike traditional FL systems that rely on a centralized server to coordinate model aggregation and communication,

our framework adopts a Peer-to-Peer (P2P) federated learning approach. In this architecture, each vehicle in the network acts both as a learner and an aggregator, responsible for exchanging model updates with its peers in the network. This decentralized setup eliminates the reliance on a single point of failure (the central server), making the system more robust against attacks and failures. The P2P-FL network is structured as a mesh of autonomous vehicles, where each vehicle is connected to a set of neighboring vehicles. Model updates are exchanged within this network according to a predefined schedule, ensuring that each vehicle receives updates from a diverse set of peers. The communication between peers is encrypted and signed to prevent tampering and eavesdropping.

- Local Training: Each vehicle trains a local model on its private data, such as sensor readings, traffic conditions, and vehicle dynamics.
- Model Exchange: Once training is complete, the vehicle shares its model update with neighboring peers, along with a proof that the update is valid (using ZKPs). These peers aggregate the received updates and integrate them into their models.
- Decentralized Aggregation: Since there is no central server, each vehicle independently aggregates model updates from its peers, using robust aggregation methods to mitigate the influence of any Byzantine nodes.

The following pseudocode illustrates the local training and model exchange process in a peer-to-peer federated learning environment:

Algorithm 1: P2P Federated Learning with Model Exchange

Input: Local data D_i, neighbors N_i, model M_i

Output: Aggregated model M_i

1.For each round $r = 1$ *to* R

1.1 Train local model M_i on data D_i for k epochs

1.2 Clip gradients and add noise to ensure differential privacy

1.3 Generate Zero-Knowledge Proof (ZKP) for the model update

1.4 Send model update and ZKP to neighbors N_i

1.5 For each neighbor j in N_i

- Receive model update and ZKP from j

- Verify ZKP and discard invalid updates

1.6 Aggregate valid updates into model M_i

2. Return: Aggregated model M_i

2) Lightweight Blockchain

The inclusion of a lightweight blockchain ensures the integrity and verifiability of the model updates exchanged in the P2P network. Each model update, along with its corresponding ZKP, is stored on the blockchain, creating an immutable ledger of all updates. This guarantees that model updates cannot be tampered with after they are shared, and it allows for decentralized verification of the learning process. The blockchain operates using a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, which is well-suited for systems with a limited number of participants, such as a network of autonomous vehicles. PBFT ensures that only valid updates (i.e., updates that have passed ZKP validation) are added to the blockchain, and it is resilient against Byzantine nodes. The process of adding model updates to the blockchain is outlined in Algorithm 2.

Algorithm 2: Blockchain-Based Model Aggregation

Input: Model updates U from peers, blockchain B

Output: Updated blockchain B

1. For each model update U_i:

1.1 Verify Zero-Knowledge Proof (ZKP) for U_i

1.2 If ZKP is valid:

- Broadcast U_i to neighboring peers

- Run PBFT consensus mechanism:

- Propose: Peers propose to add U_i to blockchain

- Prepare: Peers validate the proposal and vote

- Commit: If a majority vote is positive, add U_i to blockchain

2. Return: Updated blockchain B

By leveraging a lightweight blockchain, the system ensures that all model updates are stored in a decentralized and tamper-resistant manner. This provides transparency and auditability, which are crucial for maintaining trust in the system, especially in the presence of malicious nodes.

B. Differential Privacy with Adaptive Clipping

Ensuring the privacy of individual vehicles' data is one of the key goals of our framework. To achieve this, we incorporate Differential Privacy (DP), which adds noise to the model updates before they are shared with peers. This prevents adversaries from inferring sensitive information about the data used to train the model. The challenge in applying DP in a federated learning environment is balancing privacy with model accuracy. Adding too much noise can degrade model performance, while too little noise may not provide adequate privacy. To address this, we use an Adaptive Clipping strategy, where the clipping threshold for the gradients is dynamically adjusted based on the norm of the gradients. This ensures that the amount of noise added is proportional to the sensitivity of the data, providing better control over the privacy-accuracy trade-off.

C. Binius Zero-Knowledge Proofs

To ensure the integrity and correctness of model updates, the framework incorporates Binius Zero-Knowledge Proofs (ZKPs). ZKPs enable a vehicle to prove that its model update is valid (e.g., within a certain range) without revealing the actual values of the model parameters. This provides a mechanism for detecting malicious updates without compromising the privacy of the participating vehicles. Each vehicle generates a ZKP for its model update before sharing it with peers. The ZKP proves that the model update satisfies certain conditions, such as being within a predefined range or following the expected gradient distribution. Peers verify the ZKP before accepting the model update. If the proof fails, the

update is discarded, preventing malicious nodes from poisoning the model. Binius ZKPs, as explained by Vitalik Buterin [7], are an advanced form of Zero-Knowledge Proofs designed for decentralized systems like blockchain and federated learning. They focus on reducing computational load while ensuring privacy and verifiability across multiple participants.

Key features include:

- Smaller Proofs: They minimize proof size, enhancing efficiency for systems with limited resources.
- Multi-party Efficiency: Optimized for secure, scalable participation by multiple users without overwhelming the network.
- Adaptive Security: Dynamically adjusts the proof generation based on complexity, balancing speed and security.
- Privacy: Ensures that sensitive data is kept private, verifying conditions without revealing the actual data.

Algorithm 3: Model Update with ZKP Verification

Input: Local model update M_i, noise scale \epsilon, gradient clipping norm, ZKP range

Output: Differentially private and verified model update

1. Clip local gradients to a predefined norm using adaptive clipping
2. Add Gaussian noise to the clipped gradients to ensure differential privacy
3. Encode the model update for ZKP:
• Convert model update to finite field elements
• Generate Binius ZKP for the update
4. Send the model update and ZKP to neighboring peers
5. For each neighbor:
• Verify the ZKP:
• If ZKP fails, reject the model update
• If ZKP succeeds, proceed to the aggregation phase
6. Return: Verified and differentially private model update

The use of Binius ZKPs ensures that malicious nodes cannot introduce faulty or tampered model updates into the system. This is particularly important in a decentralized environment like P2P-FL, where there is no central authority to oversee the model aggregation process.

D. Byzantine Resilience

In any decentralized system, there is a risk of Byzantine nodes—malicious or faulty participants that attempt to disrupt the learning process by submitting incorrect or poisoned model updates. To mitigate the impact of such nodes, our framework includes several Byzantine-resilient aggregation strategies. The choice of aggregation strategy depends on the detected proportion of Byzantine nodes in the network:

- Krum Aggregation: Krum is a robust aggregation method that selects the model update that is closest to the majority of updates, discarding outliers that may have been submitted by Byzantine nodes.
- Trimmed Mean Aggregation: Trimmed Mean removes the highest and lowest k% of the model updates and averages the remaining updates. This strategy is effective when the number of Byzantine nodes is moderate.
- Geometric Median Aggregation: The Geometric Median minimizes the influence of any individual update by computing the median of all updates. This is a more robust method, especially in environments with a high proportion of Byzantine nodes.

Algorithm 4: Byzantine-Resilient Aggregation

Input: Set of model updates U from neighboring peers, Byzantine threshold T

Output: Aggregated global model

1.For each peer:
1.1 Collect model updates from neighbors
1.2 If Byzantine ratio ≤ 0.2:
- Use Krum aggregation
1.3 If Byzantine ratio ≤ 0.3:
- Use Trimmed Mean aggregation
1.4 If Byzantine ratio > 0.3:
- Use Geometric Median aggregation
2.Aggregate the model updates
3. Return: Aggregated global model

By dynamically adjusting the aggregation strategy based on the proportion of Byzantine nodes, the framework ensures that the learning process remains resilient against attacks, even when a significant portion of the network is compromised.

E. Secure Model Exchange Protocol

To prevent eavesdropping and tampering during the exchange of model updates, the framework implements a secure model exchange protocol that combines encryption and digital signatures.

- Encryption: Model updates are encrypted using AES-256 encryption before being transmitted to neighboring peers. This ensures that the updates cannot be intercepted or modified by an attacker during transmission.
- Digital Signatures: Each model update is signed using an RSA digital signature, allowing the receiving peers to verify the authenticity of the update. This prevents malicious nodes from impersonating other peers or modifying the updates.

The secure model exchange process is outlined in Algorithm 5.

Algorithm 5: Secure Model Exchange

Input: Local model update $\boldsymbol{M_i}$, RSA private key, AES encryption key

Output: Encrypted and signed model update

1.Encrypt the model update using AES-256 encryption:
• Generate a random initialization vector (IV)
• Encrypt the model update using the AES encryption key

2. Sign the encrypted model update using RSA private key:

• Compute the SHA-256 hash of the encrypted model update

• Sign the hash using the RSA private key

3. Transmit the encrypted and signed model update to neighboring peers

4. Return: Encrypted and signed model update

This combination of encryption and signatures ensures that the model updates are both confidential and authentic, preventing a wide range of attacks, including man-in-the-middle attacks and impersonation.

In this paper, we presented a comprehensive framework for enhancing security and privacy in peer-to-peer federated learning for autonomous vehicles. By combining lightweight blockchain, Binius ZKPs, and differential privacy, we addressed key challenges such as model poisoning, Byzantine attacks, and data privacy in decentralized learning environments. Our simulations demonstrated the effectiveness of the framework in maintaining model accuracy while providing robust security and privacy guarantees. Future work will focus on further optimizing the system, including adaptive privacy budgets and more sophisticated Byzantine detection mechanisms.

IV. Experiments

In this section, we describe the experiments conducted to evaluate the security, privacy, and performance of our federated learning framework for autonomous vehicles using lightweight blockchain and Binius ZKPs. The experiments focus on assessing the framework's ability to enhance privacy, resist Byzantine nodes, and maintain efficiency and scalability. All experiments were implemented in Python, utilizing PyTorch for model training, NumPy for numerical computations, and Seaborn/Matplotlib for visualization. The dataset used was Gazebo, collected for autonomous navigation tasks in indoor environments. It contains 66,806 samples, with 80% for training and 20% for testing, making it well-suited for evaluating autonomous driving models in decentralized, peer-to-peer federated learning.

A. *Privacy vs. Accuracy Trade-off*

One of the critical aspects of this experiment is to examine the impact of different privacy budgets on model accuracy. We utilized differential privacy with noise addition and gradient clipping, fine-tuning both mechanisms across multiple privacy budgets (epsilon values). Setup: We ran tests with eight different epsilon values ranging from 0.01 to 0.06, incrementing in small steps. Each configuration was executed over five rounds to average the results for more robust conclusions. Results and Discussion: Figure 2 illustrates the privacy-accuracy trade-off. As privacy levels increase through differential privacy, accuracy decreases, but our system maintains high accuracy with robust privacy measures, crucial for autonomous vehicles.

B. *Byzantine Resilience*

The next set of experiments tested the framework's resilience against Byzantine nodes, simulating scenarios with varying ratios of Byzantine participants. Setup: We simulated peer-to-peer training environments with Byzantine node ratios ranging from 0% to 50%, testing their impact on model accuracy. For each Byzantine ratio, multiple participants (10, 50, 100, and 200 nodes) were tested to assess scalability. Results and Discussion: Figures 3 and 4 demonstrate the system's resilience to Byzantine nodes. Using Binius ZKPs, malicious updates are effectively detected and rejected,

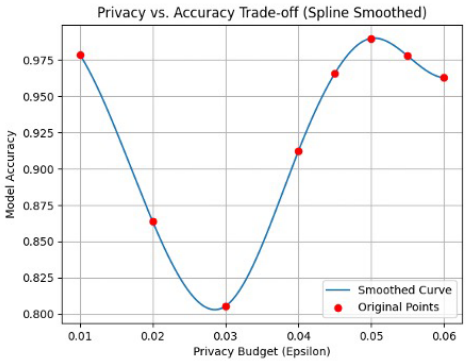

Figure 2. Privacy vs. Accuracy Trade-off

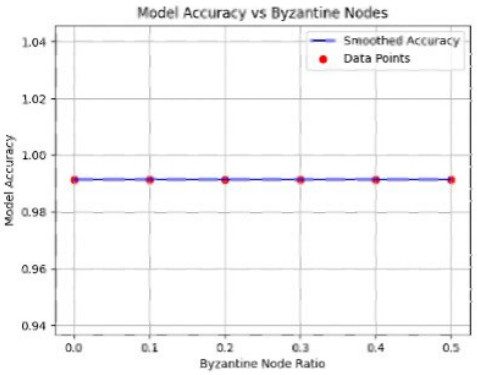

Figure 3. Model Accuracy vs Byzantine Nodes

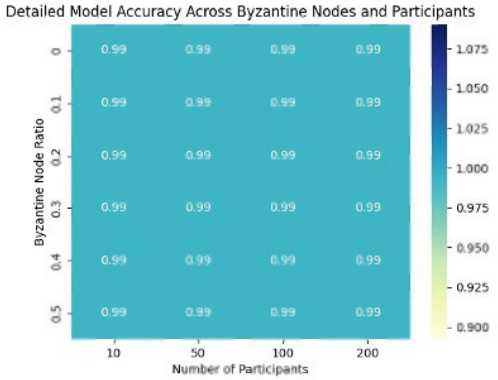

Figure 4: Detailed Model Accuracy Across Byzantine Nodes and Participants (Heatmap)

ensuring the integrity of the global model despite adversarial behavior.

C. *Latency and Throughput Analysis*

Efficiency is critical in federated learning systems, especially in peer-to-peer networks with a decentralized structure. We measured the system's latency and throughput

during multiple communication rounds to evaluate how quickly and efficiently the model updates propagate through the network. Setup: The system was tested over 100 communication rounds, measuring latency (in seconds) and throughput (updates per second). Results and Discussion: Figure 5 shows the latency and throughput comparison of the

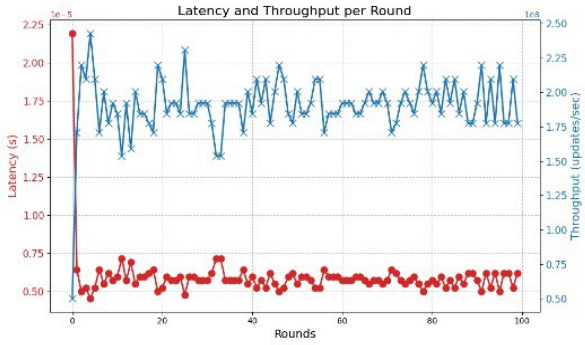

Figure 5: Latency and Throughput per Round

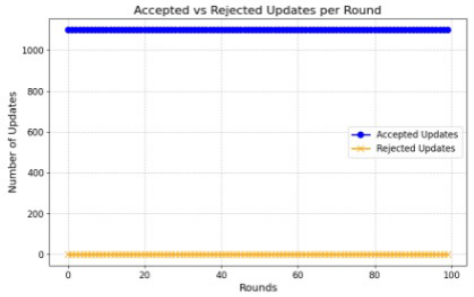

Figure 6: Accepted vs Rejected Updates per Round.

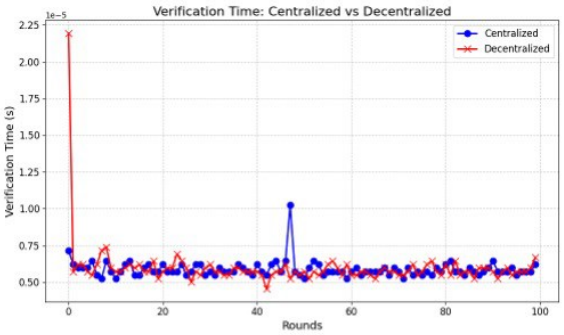

Figure 7: Verification Time: Centralized vs Decentralized.

system with and without lightweight blockchain. The added security layer maintains low latency and optimized throughput, suitable for real-time autonomous vehicle networks.

D. Accepted vs. Rejected Updates

This experiment tracked the number of accepted versus rejected updates per communication round, providing insights into the system's validation process. Setup: We ran 100 communication rounds, logging the number of accepted and rejected updates. Results and Discussion: As shown in Figure 6, nearly all updates were accepted across all rounds, with a negligible number of rejections. This demonstrates the robustness of the Binius ZKP-based verification system in accurately validating model updates and filtering out faulty or malicious contributions.

E. Verification Time: Centralized vs. Decentralized

We compared verification times for both centralized and decentralized approaches, evaluating the impact of using lightweight blockchain and Binius ZKPs for decentralized verification. Setup: The experiment was conducted over 100 rounds, comparing the time required to verify model updates using centralized and decentralized methods.

Results and Discussion: As depicted in Figure 7, verification times for both approaches remained consistent, with the decentralized system averaging around 0.75 seconds per verification. While centralized verification had occasional spikes, the decentralized approach consistently performed well, demonstrating its scalability and reliability.

V. Future Work

The proposed federated learning system combines lightweight blockchain, Binius Zero-Knowledge Proofs (ZKPs), and differential privacy, offering a strong foundation for secure and privacy-preserving decentralized learning. However, several avenues for further enhancement remain:

- Dynamic Privacy Mechanisms: While the system already ensures privacy with differential privacy and ZKPs, future work could explore dynamic, real-time adjustments of privacy budgets to further optimize privacy without sacrificing performance.
- Advanced Consensus Models: Although the current system incorporates lightweight blockchain, future research could focus on developing even more scalable and efficient consensus mechanisms tailored to connected autonomous vehicle (CAV) networks. This would help reduce latency and computational overhead as network complexity increases.
- Enhanced Byzantine Detection: The existing Byzantine fault-tolerant mechanisms could be augmented with advanced machine learning-based techniques to further improve the detection and mitigation of Byzantine failures, enhancing overall system security.

VI. Conclusion

This paper introduces a robust, secure, and privacy-preserving federated learning framework that uniquely integrates Binius Zero-Knowledge Proofs (ZKPs), lightweight blockchain, and differential privacy. The novelty lies in the combination of these technologies, offering an advanced solution for decentralized learning in autonomous vehicle (AV) networks. Binius ZKPs provide efficient, privacy-preserving proof mechanisms that allow vehicles to verify model updates without exposing sensitive data. This novel cryptographic technique ensures the system's privacy and integrity while reducing computational overhead. In conjunction with lightweight blockchain, the framework securely records and verifies model updates, preventing tampering and securing the network from malicious nodes.

The inclusion of Byzantine fault tolerance further strengthens the system, allowing it to detect and reject faulty or malicious updates. The use of differential privacy further enhances the system by introducing noise into the model updates, ensuring that individual data points remain private while still allowing for accurate model training. This combination of privacy and security ensures that the system is not only secure but also scalable and efficient, making it suitable for the fast-paced, decentralized nature of AV networks. Simulations demonstrate the framework's low-latency performance and scalability, showing its potential for real-world applications in AV networks. Beyond AVs, the framework's applicability can extend to sectors such as healthcare, smart cities, and industrial IoT, where privacy-preserving, secure, and decentralized learning is critical. In conclusion, the integration of Binius ZKPs, blockchain, Byzantine fault tolerance, and differential privacy provides a novel, secure, and scalable solution for federated learning in real-time environments, offering significant contributions to both privacy-preserving technology and decentralized learning frameworks.

REFERENCES

[1] S. Sultana, J. Hossain, M. Billah, H. H. Shajeeb, S. Rahman, K. Ansari, and K. F. Hasan. "Blockchain-Enabled Federated Learning Approach for Vehicular Networks." 5th IEEE International Conference on Sustainable Technologies for Industry 5.0, 2023.

[2] Z. Wang, N. Dong, J. Sun, W. Knottenbelt, and Y. Guo. "zkFL: Zero-Knowledge Proof-based Gradient Aggregation for Federated Learning." IEEE Transactions on Big Data, 2020.

[3] H. Lycklama, L. Burkhalter, A. Viand, N. Küchler, and A. Hithnawi. "RoFL: Robustness of Secure Federated Learning." arXiv preprint arXiv:2107.03311v4, January 2023.

[4] Y. Zhu, Y. Wu, Z. Luo, B. C. Ooi, and X. Xiao. "Secure and Verifiable Data Collaboration with Low-Cost Zero-Knowledge Proofs." arXiv preprint arXiv:2311.15310v1, November 2023.

[5] Xu, J., Wang, C., & Jia, X. A Verifiable and Privacy-Preserving Blockchain-Based Federated Learning Approach. Peer-to-Peer Networking and Applications. 2023

[6] Z. Xing, Z. Zhang, M. Li, J. Liu, L. Zhu, G. Russello, and M. R. Asghar. "Zero-Knowledge Proof-based Practical Federated Learning on Blockchain." Journal of Latex Class Files, vol. 14, no. 8, 2015.

[7] V. Buterin, https://vitalik.eth.limo/general/2024/04/29/binius.html, 2024

[8] M. Ghanem, F. Dawoud, H. Gamal, E. Soliman, T. El-Batt, and H. Sharara. "FLoBC: A Decentralized Blockchain-Based Federated Learning

[9] Y. Abuzied, M. Ghanem, F. Dawoud, H. Gamal, E. Soliman, H. Sharara, and T. ElBatt. "A Privacy-Preserving Federated Learning Framework for Blockchain Networks." Cluster Computing, 2024.

[10] Y. Tian, Z. Guo, J. Zhang, and Z. Al-Ars. "DFL: High-Performance Blockchain-Based Federated Learning." Distributed Ledger Technologies: Research and Practice, vol. 2, no. 3, 2023.

[11] Y. Yuan, J. Liu, D. Jin, Z. Yue, T. Yang, and R. Chen. "DeceFL: A Principled Fully Decentralized Federated Learning Framework." National Science Open, vol. 2, 2023.

[12] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan. "A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus." IEEE Network, vol. 34, no. 1, 2021.

[13] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth. "Practical Secure Aggregation for Privacy-preserving Machine Learning." Google Technical Report, 2021.

[14] R. Fotohi, F. S. Aliee, and B. Farahani. "Decentralized and Robust Privacy-preserving Model Using Blockchain-enabled Federated Deep Learning in Intelligent Enterprises." Applied Soft Computing, vol. 161, 2024.

[15] V. Chellapandi, L. Yuan, C. Brinton, S. Zak, and Z. Wang. "Federated Learning for Connected and Automated Vehicles: A Survey of Existing Approaches and Challenges." IEEE Transactions on Intelligent Vehicles, 2023