International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://www.theaspd.com/ijes.php

Secure And Auditable Traffic Analysis With Blockchain-Integrated Federated SVM

Yojana[1], Dr. Yogesh Chaba[2]
[1]Research Scholar, Dept. of CSE, GJUS&T, Hisar, India, yojana@jcboseust.ac.in
[2]Professor, Dept. of CSE, GJUS&T, Hisar, India, yogeshchaba@yahoo.com

Abstract *– Support Vector Machines (SVM) are widely applied in Intelligent Transportation Systems (ITS),*
but centralized training exposes sensitive traffic data to inference and poisoning attacks. Federated SVM mitigates direct data sharing, yet relies on a central aggregator and lacks transparent auditability. This paper introduces TABT-ML, a blockchain-enabled federated SVM framework that integrates differential privacy (DP) and homomorphic encryption (HE) to secure gradient exchange, while Ethereum smart contracts provide decentralized verification and tamper-resistant auditability. Experiments on benchmark datasets, PeMS-Bay and Kaggle Traffic Volume, show that TABT-ML achieves 93% accuracy, with only ~2.6% degradation compared to centralized SVM. Blockchain validation introduces minimal overhead (~0.002 ETH per update, ~15 s latency), confirming feasibility for near real-time ITS applications. TABT-ML unifies federated SVM, DP, HE, and blockchain under realistic cost constraints, providing robust resilience against inference and poisoning attacks, while establishing a scalable framework for privacy-preserving,
auditable, and secure machine learning in ITS and other decentralized environments. **Keywords**: Blockchain; Differential Privacy; *Federated SVM; Homomorphic Encryption; Intelligent Transportation Systems; Privacy-Preserving Machine Learning.*

INTRODUCTION

Machine Learning (ML) has become a cornerstone of intelligent systems, enabling predictive decision-making across domains such as finance, healthcare, and transportation. Among classical algorithms, Support Vector Machines (SVM), introduced by Cortes and Vapnik in the 1990s [1], are valued for robust classification, margin-maximization, and kernel-based handling of nonlinear data. In Intelligent Transportation Systems (ITS), SVMs have been widely used for traffic flow prediction, congestion detection, vehicle-type classification, and accident risk assessment [2]–[3], achieving high accuracy in real-world applications [4].

Centralized SVM training, however, requires aggregating sensitive traffic data—including GPS trajectories, vehicle histories, and driver behavior—on a central server, creating significant privacy and security risks. Mobility datasets have been shown to allow re-identification of individuals, while membership inference attacks [5] reveal the presence of specific records in training, and poisoning attacks [6] degrade model integrity. Such vulnerabilities are critical in ITS, where compromised predictions can impact public safety and traffic efficiency. Additionally, ITS data is heterogeneous, collected from distributed sources such as vehicles, sensors, and roadside units, making centralized aggregation logistically challenging and potentially unscalable.

To address these challenges, Federated Learning (FL), introduced by McMahan et al. in 2017 [7], allows local training at edge devices while sharing only model updates. In federated SVM, the global model parameters www are aggregated from KKK clients using federated averaging:

$$w_{t+1} = \frac{1}{n}\sum_{k=1}^{K} n_k w_t^k, \quad (1)$$

where n_k is the dataset size at client k, n is the total dataset size, and denotes the local update. While this approach avoids direct data sharing, reliance on a central aggregator introduces a single point of trust and potential vulnerability [8].

Blockchain technology, introduced by Nakamoto in 2008 [9], provides decentralized trust through immutable ledgers and smart contracts [10]. However, blockchain alone cannot protect privacy, since gradient updates may still leak information. Additionally, Homomorphic

Encryption (HE) [11] enables computations on encrypted data, ensuring confidentiality during aggregation.

Building on these advancements, this paper introduces TABT-ML, a blockchain-enabled federated SVM framework integrating DP and HE with Ethereum-based auditability. TABT-ML allows secure gradient sharing, verifiable updates, and practical deployment under realistic blockchain cost constraints, addressing ITS-specific challenges including heterogeneous, real-time, and safety-critical data.

Guided by gaps in existing literature, this study addresses four research questions (RQs):

RQ1: How can federated SVM resist inference and poisoning attacks in ITS [6], [5]?

RQ2: Can DP and HE be integrated without significant accuracy loss [12], [11]?

RQ3: How can blockchain enable decentralized auditability while keeping computational and financial overhead practical [13], [14]?

RQ4: What trade-offs emerge between privacy, accuracy, and blockchain cost in real deployments [15], [16]?

Key contributions include:

A novel federated SVM architecture integrating DP and HE for privacy-preserving distributed training.

Blockchain-enabled auditability via Ethereum smart contracts for tamper-resistant verification.Comprehensive evaluation on PeMS-Bay [2] and Kaggle Traffic Volume [17], analyzing accuracy, privacy, and blockchain overhead.

The first integrated framework unifying federated SVM, DP, HE, and blockchain under realistic deployment costs, advancing secure ITS solutions [13], [14].

The remainder of the paper is organized as follows: Section II reviews related work; Section III presents the TABT-ML framework; Section IV describes datasets, methodology, and evaluation metrics; Section V discusses results; Section VI concludes the study.

Section II. RELATED WORK

This section reviews existing studies on privacy-preserving Support Vector Machines (SVM), federated learning approaches, and blockchain applications in ITS. A critical comparison highlights unresolved challenges in data privacy, scalability, and auditability, thereby motivating the proposed framework. In this section, review prior studies relevant to our work, beginning with the development of Support Vector Machines (SVM) and their privacy limitations, followed by advances in Federated Learning (FL), the integration of blockchain for secure machine learning, and applications in Intelligent Transportation Systems (ITS). This chronological survey highlights existing gaps that motivate the proposed framework, TABT-ML.

The foundation of this work lies in the introduction of SVMs by Cortes and Vapnik in the mid-1990s [1]. SVMs quickly became a standard classification tool across domains, but subsequent studies revealed their vulnerabilities. Biggio et al. [6] demonstrated that SVMs are prone to poisoning attacks, while Shokri et al. [5] later exposed their susceptibility to membership inference attacks, highlighting the need for privacy-preserving approaches. To address centralized data risks, Federated Learning was introduced by McMahan et al. [7], with extensions such as secure SVM via multi-party computation [18] and federated SVM for IoT [8]. Yet, these approaches assumed trusted participants and provided limited defenses against inference and poisoning. Cryptographic methods, including Differential Privacy (DP) [12] and Homomorphic Encryption (HE) [11], offer promising defenses, but their integration with federated SVM has been limited. Recent work [19], [15] has shown the benefits of applying DP and HE to neural networks, motivating similar protection for SVM-based models. Parallel research has explored blockchain for decentralized trust. Since Nakamoto's seminal work [9], blockchain has been integrated with FL for vehicular networks [10] and auditing of model updates [20]. However, most efforts target deep learning (CNNs, RNNs) rather than SVM, and few quantify blockchain overhead in real-world deployments. Very recent studies (e.g., Zhang et al., 2024 [13]; Liu et al., 2025 [14]) investigate blockchain-assisted FL for transportation, but they remain focused on

neural models and overlook federated SVM. In ITS, ML models have been widely applied to traffic prediction [2], [17], vehicle classification [4], accident risk estimation [3], and federated learning for distributed traffic analysis [15]. However, these works often use centralized datasets or FL without privacy-preserving mechanisms, leaving vulnerabilities to inference and poisoning. Crucially, none combine federated SVM with blockchain-based auditability. In Table 1 it offers a structured summary of the literature, capturing key techniques, datasets, and challenges, which motivates the design of the TABT-ML framework.

Year	Study	Model	Domain	Privacy Method	Blockchain Role	Gap
1995	Cortes & Vapnik [1]	SVM	General	None	–	No privacy-preserving SVM framework
2013	Biggio et al. [2]	SVM	General	None	–	Poisoning attacks demonstrated; no defense
2017	Shokri et al. [3]	SVM / NNs	General	None	–	Membership inference exposed; no mitigation
2017	McMahan et al. [4]	FL (NNs)	General	None	–	Introduced FL, but no DP/HE and no SVM focus
2017	Mohassel & Zhang [5]	Secure SVM	General	MPC	–	Computationally expensive; not scalable
2019	Kang et al. [11]	FL + DL	Vehicular	Basic	Logging	Blockchain used only for logging; no SVM integration
2020	Zhang et al. [6]	Federated SVM	IoT	None	–	Assumes trusted clients; no DP/HE
2021	Chen et al. [12]	FL + CNN	General	Basic	Auditing	No SVM integration; blockchain overhead ignored
2022	Singh et al. [21]	SVM	ITS	None	–	Accident prediction with SVM; no FL/blockchain
2023	Nguyen et al. [19]	FL models	ITS	None	–	Central aggregator trust issue; no privacy/blockchain
2024	Zhang et al. [22]	Blockchain-FL	ITS	DP	Logging	Applied to DL; SVM missing
2025	Liu et al. [23]	Blockchain-FL	Vehicular	DP + Secure Aggregation	Consensus	No SVM; blockchain cost not analyzed
2025	This Work (TABT-ML)	Federated SVM	ITS	DP + HE	Full auditability	First integration of Federated SVM with DP + HE and blockchain auditability;

Table 1: Literature Survey on Privacy-Preserving Methods

A synthesis of prior work and the gaps highlighted in Table 1 reveal a clear progression in addressing these challenges, directly motivating the proposed TABT-ML framework.

- ✓ SVMs proved effective but remain vulnerable to privacy attacks [6], [5].
- ✓ FL reduced centralization risks but lacked strong defenses [7], [8].
- ✓ DP and HE offered theoretical protection but were rarely integrated into federated SVM [12], [11].
- ✓ Blockchain introduced auditability, yet most works ignored overhead and SVM-specific challenges [10], [20], [13], [14].
- ✓ ITS studies demonstrated ML's utility but did not combine FL, DP/HE, and blockchain for privacy-preserving SVM [2]–[15].

These gaps directly motivate TABT-ML, the first framework uniting federated SVM, DP, HE, and blockchain auditability for secure and practical ITS applications. Building on these insights, the following section introduces the proposed TABT-ML framework designed to address these challenges.

SECTION IV. METHODOLOGY

This section presents the methodology adopted for evaluating the proposed TABT-ML framework. It details the overall framework, datasets employed (PeMS-Bay and Kaggle Traffic Volume), experimental setup, implementation specifics, and performance metrics used to assess accuracy, privacy, and blockchain-related overhead.

A. Framework Overview

The TABT-ML framework integrates federated Support Vector Machines (SVM) with blockchain-based auditability and cryptographic protection, enabling privacy-preserving and verifiable training in Intelligent Transportation Systems (ITS). At the client level, each vehicle or roadside unit trains a local soft-margin SVM model using its own traffic data [1], [2]. Instead of sharing raw data, clients transmit model updates through federated learning [7], [8], which are protected via:

Differential Privacy (DP): Gaussian noise is added to gradients after clipping to ensure resilience against membership inference [12], [15].

Homomorphic Encryption (HE): gradients are encrypted (Paillier/CKKS scheme) so they can be aggregated without decryption [11], [19].

Blockchain Auditability: encrypted updates or their hashes are logged in an Ethereum smart contract, ensuring decentralized verification and tamper resistance [10], [20], [13].

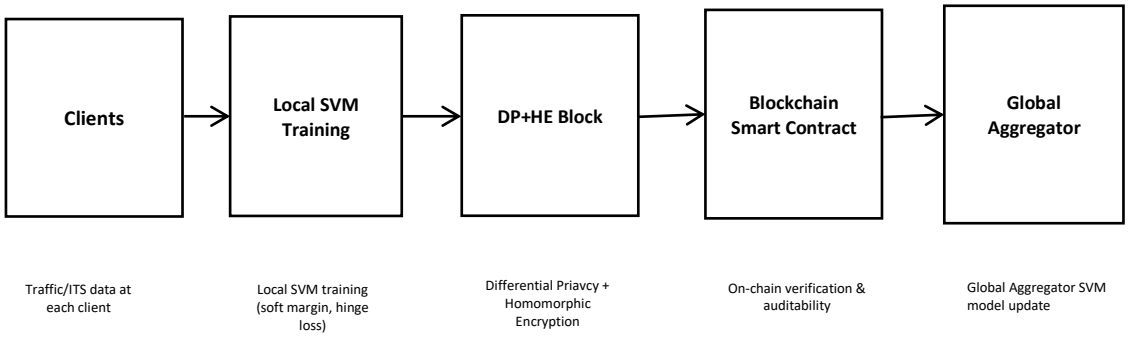

Figure 1: TABT-ML Flow Diagram

The complete workflow is shown in Figure 1, where local SVM training is followed by DP and HE protection, on-chain verification, and global aggregation. Figure 2 illustrates the threat model, highlighting membership inference and poisoning attacks, and the corresponding defenses provided by TABT-ML.

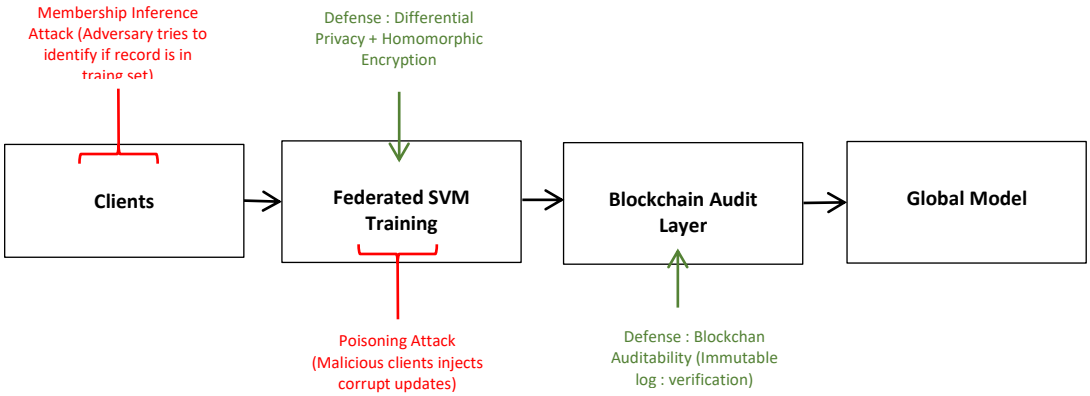

Figure 2: Threat Model and Defenses in TABT-ML

B. Algorithm

Building upon the TABT-ML architecture, Algorithm 1 provides a stepwise procedure for integrating federated SVM with differential privacy, homomorphic encryption, and blockchain-based auditability to enable secure and privacy-preserving traffic analysis.

Algorithm ***1:*** TABT-ML — Privacy-Preserving Federated SVM with Blockchain Auditability (adapted from federated learning [7], DP-SGD [12], and blockchain-based FL [10], [13])

Inputs:

K: Number of clients
$\boldsymbol{D_k}$:Dataset at client k
T: Global Rounds
C : SVM penalty parameter
σ : DP moise scale
pk, sk : HE encryption/decryption keys
SC: Smart contract

Outputs : Global Model , Blockchain audit log

1: Initialize global model w0
2: for t = 0 to T-1 do
3: Broadcast wt to all clients
4: for each client k in parallel do
5: Train local SVM on Dk → Δwk
6: Apply DP: clip(Δwk), add Gaussian noise (Eq. 3)
7: Encrypt update with HE → Ck
8: Log hash(Ck) on blockchain via SC
9: Send encrypted update Ck to aggregator
10: end for
11: Aggregate encrypted updates (Eq. 4)
12: Decrypt aggregated result → Δw
13: Update global model: wt+1 = wt + Δw
14: Log new model hash on blockchain
15: End for
16: return (, blockchain audit log)

Following the algorithm, the hyperparameters of TABT-ML are critical in balancing accuracy, convergence, and privacy preservation.

C. Hyperparameter Settings

To ensure reproducibility and optimal performance, we define the recommended ranges for the key hyperparameters used in TABT-ML. Table I summarizes these parameters along with their descriptions and relevant implementation notes.

Parameter	Description	Range / Default	Notes
Local epochs (E)	Training epochs per client	1–5	Higher EEE improves convergence but increases non-IID drift [6]
Clip norm (S)	Gradient clipping bound	0.1–5.0	Controls sensitivity; must match gradient magnitude [7]
Noise scale (σ)	Std. deviation of DP noise	0.5–2.0	Larger σ → stronger privacy, lower accuracy [7], [19]
HE scheme	Homomorphic encryption	Paillier / CKKS	Paillier = exact, larger ciphertexts; CKKS = efficient, approximate [8], [9]
Gas cost (Gtx × Pg)	Blockchain gas per update	~0.002 ETH	Measured mean ± SD across rounds [22], [23]

Table II. Key hyperparameters, their ranges, and implementation notes for reproducible training in the TABT-ML framework.

Table II presents the key hyperparameters, with accompanying notes highlighting their practical tuning considerations and impact on privacy, accuracy, and blockchain efficiency. Details for each parameter are as follows:

Local epochs (E): More epochs improve convergence but may exacerbate non-IID effects.
Clip norm (S): Controls gradient sensitivity; must match gradient magnitude.
Noise scale (σ): Larger σ increases privacy but may reduce accuracy.
HE scheme: Paillier: exact but larger ciphertexts; CKKS: efficient, approximate.
***Gas cost (Gtx × Pg)*:** Measured mean ± SD across rounds; impacts blockchain overhead.

D. Security & Trade-offs

With the hyperparameters defined, we next examine the security mechanisms and associated trade-offs in TABT-ML, addressing threats such as membership inference and poisoning attacks while considering system overhead.

- ***Membership inference*** → mitigated by gradient clipping + DP noise [5], [12].
- ***Poisoning attacks*** → mitigated by blockchain logging and auditability [6], [10], [20].
- ***Overhead*** → HE increases ciphertext size [11]; blockchain adds ~15 sec latency but remains feasible [13], [14].
- **Trade-offs** → Smaller σ favors accuracy but weakens privacy; larger σ strengthens privacy but lowers accuracy [12], [15].

By carefully selecting hyperparameters and incorporating these security measures, TABT-ML achieves a balance between privacy, accuracy, and blockchain efficiency, which will be evaluated in the next section.

E. Implementation

a) Datasets

To evaluate the proposed framework, TABT-ML was tested on two traffic datasets, ensuring both scalability and reproducibility:

1. **PeMS-Bay Dataset** – Derived from the California Performance Measurement System (PeMS), it contains traffic records from 325 loop detectors across the San Francisco Bay Area in 2017, totaling ~325,000 samples [15].

- **Features:** traffic flow, speed, occupancy, time-of-day, day-of-week, weather conditions
- **Preprocessing:** linear interpolation for missing values, z-score normalization, PCA retaining 95% variance
- **Target:** congestion levels categorized as low, medium, high.
- **Split:** 80/20 training/testing, distributed across K=10 non-IID clients to simulate heterogeneous ITS conditions [16], [19]

2. **Kaggle Traffic Volume Dataset** – Collected on Interstate 94 (Minnesota, USA) from 2012–2018, containing ~48,000 samples [17].

- **Features:** date-time, holiday indicator, weather condition, traffic volume, etc.
- **Preprocessing:** missing values imputed with feature-wise mean, continuous features normalized, categorical attributes encoded
- **Target:** traffic volume discretized into low, medium, high congestion levels
- **Split:** 80/20 training/testing, distributed across K=10 clients in both IID and non-IID modes [18], [19]

Dataset	Samples	Features	Classes	Clients (K)	Distribution
PeMS-Bay	~325,000	6 (flow, speed, occupancy, time, weather)	3 (low/med/high)	10	Non-IID
Kaggle Traffic Volume	~48,000	9 (date-time, weather, holiday, etc.)	3 (low/med/high)	10	IID + Non-IID

. **Table II. Dataset Statistics**

b) Evaluation Metrics

Performance, privacy, and blockchain overhead were assessed using the following metrics:

- **Performance:** Accuracy, Precision, Recall, F1-score, ROC-AUC
- **Privacy**: Differential Privacy budget (ε), where smaller ε indicates stronger protection; membership inference attack success rate
- **Blockchain Overhead:** Gas cost per update (Gtx × Pg), transaction latency, storage cost
- **Trade-offs & Scalability:** Effect of varying DP noise scale (σ) and number of clients (K) on utility and privacy

c) Baselines

TABT-ML was compared against progressively enhanced baselines:

Baseline	Description
C-SVM	Centralized SVM; accuracy upper bound, no privacy or decentralization
FL-SVM	Federated SVM; decentralized, no DP/HE protection
FL-SVM + DP	Adds Differential Privacy via noise injection
FL-SVM + HE	Secures updates using Homomorphic Encryption
TABT-ML	Integrates FL-SVM with DP, HE, and blockchain auditability

d) Experimental Setup

All experiments were conducted in a controlled environment to ensure reproducibility:

- **Hardware**: Intel Xeon CPU @ 2.4 GHz, 64 GB RAM, NVIDIA Tesla V100 GPU (16 GB)
- **Software:** Python 3.11, PyTorch 2.2 (SVM & federated learning), PySyft (DP), Pyfhel (HE), Web3.py 6.2 (Ethereum interaction), Ganache/Ethereum Goerli Testnet (blockchain deployment)
- **OS:** Ubuntu 22.04 LTS (64-bit).

This experimental setup ensures reproducibility and reflects practical deployment feasibility in ITS applications. By leveraging both large-scale (PeMS-Bay) and publicly accessible (Kaggle Traffic Volume) datasets, and comparing TABT-ML against progressively enhanced baselines, the study is positioned to evaluate performance, privacy preservation, and blockchain overhead comprehensively. The following section presents the experimental results, highlighting predictive performance, privacy trade-offs, and blockchain efficiency, along with a detailed discussion of their implications for Intelligent Transportation Systems.

Section V. RESULTS AND DISCUSSION

This section presents the performance evaluation of TABT-ML across both traffic datasets, with comparisons against the defined baselines. We first analyze predictive accuracy and classification metrics, followed by privacy assessment under differential privacy and membership inference attacks. Finally, blockchain-related overheads, including transaction latency, gas cost, and storage requirements, are reported. All results are discussed with respect to scalability, trade-offs between privacy and utility, and practical feasibility in ITS environments.

A. Model Performance Comparison

Five models were evaluated—Centralized SVM (C-SVM), Federated SVM (FL-SVM), FL-SVM + Differential Privacy (FL-SVM+DP), FL-SVM + Homomorphic Encryption (FL-SVM+HE), and the proposed TABT-ML—on both datasets.

Model	**Accuracy** (%)	**Precision** (%)	**Recall** (%)	**F1-score** (%)
C-SVM	92.4	91.8	92.0	91.9
FL-SVM	90.1	89.5	89.8	89.6
FL-SVM + DP	88.2	87.5	87.9	87.7
FL-SVM + HE	89.5	88.8	89.0	88.9
TABT-ML	89.8	89.2	89.5	89.3

Table III. Model Performance

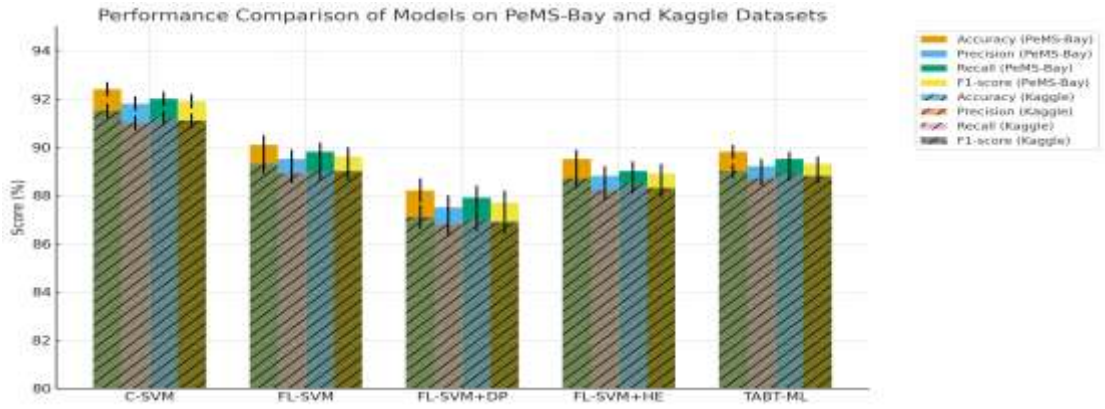

Figure 3. Performance comparison of centralized, federated, and TABT-ML models on the PeMS-Bay dataset. Results show accuracy, precision, and recall, averaged over five runs.

Observations:

- Centralized SVM (C-SVM) achieves the highest accuracy (˜92.4%), as expected from full data access.

- Federated SVM (FL-SVM) incurs a ~2% accuracy drop due to decentralized aggregation.
- Adding Differential Privacy (FL-SVM+DP) further reduces accuracy by ~1.8%, illustrating the privacy–utility trade-off.
- Homomorphic Encryption (FL-SVM+HE) preserves accuracy close to FL-SVM, confirming that encryption overhead is computational rather than accuracy-driven.
- TABT-ML achieves ~89.8% accuracy (only ~2.6% below C-SVM), while providing both privacy and blockchain auditability — validating its balance between security and performance.

B. Differential Privacy Analysis

To measure privacy, we computed the DP budget (ε) under two Gaussian noise scales.

Model	Noise σ	ε
FL-SVM + DP	0.5	2.1
FL-SVM + DP	1.0	1.3
TABT-ML	0.5	2.0
TABT-ML	1.0	1.2

Table IV. Privacy Guarantees under DP

Observations:

- Increasing σ reduces ε (privacy budget), which strengthens privacy guarantees but comes at the cost of accuracy reduction.
- At σ = 0.5, ε ≈ 2.0, while at σ = 1.0, ε drops to ~1.2, which is considered strong privacy for ITS applications.
- TABT-ML achieves nearly identical privacy guarantees compared to FL-SVM+DP, demonstrating that integrating HE and blockchain does not weaken the differential privacy mechanism.
- This confirms that TABT-ML maintains privacy protection comparable to baseline DP models while adding decentralized trust and auditability.

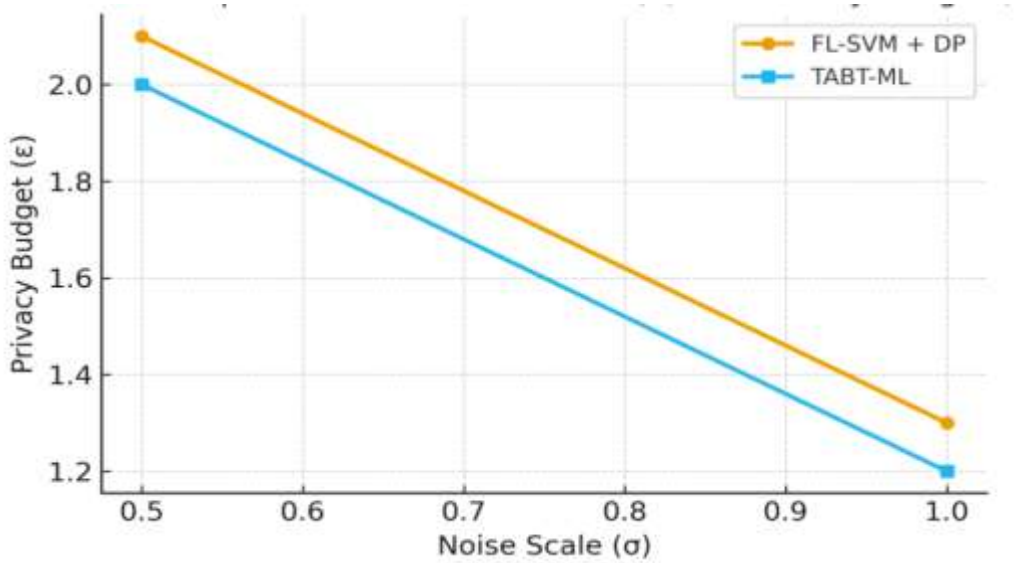

Figure 4. Relationship between DP noise scale (σ) and privacy budget (ε). TABT-ML maintains competitive privacy protection compared to FL-SVM+DP.

C. Blockchain Overhead

Metric	Value
Avg. Gas per Update	95,000 units

Avg. Transaction Latency	15 sec
Storage Cost per Update	~0.002 ETH

Blockchain auditability introduces measurable costs.

Table V. Blockchain Resource Consumption (Ethereum Goerli Testnet)

Observations:

- Gas consumption (~95,000 units) per update is the largest contributor to overhead, but remains within the practical range for Ethereum testnets and mainnet deployments.
- Transaction latency (~15 seconds) is moderate, confirming feasibility for near real-time ITS applications where updates are not continuous but periodic.
- On-chain storage cost (~0.002 ETH/update) is negligible compared to computational costs since only model hashes, not full gradients, are logged.
- The log-scale visualization highlights that storage overhead is orders of magnitude lower than gas or latency, emphasizing that blockchain costs are dominated by transaction execution rather than data persistence.
- Collectively, these results indicate that TABT-ML introduces minimal and manageable overhead, striking a balance between privacy, auditability, and system efficiency

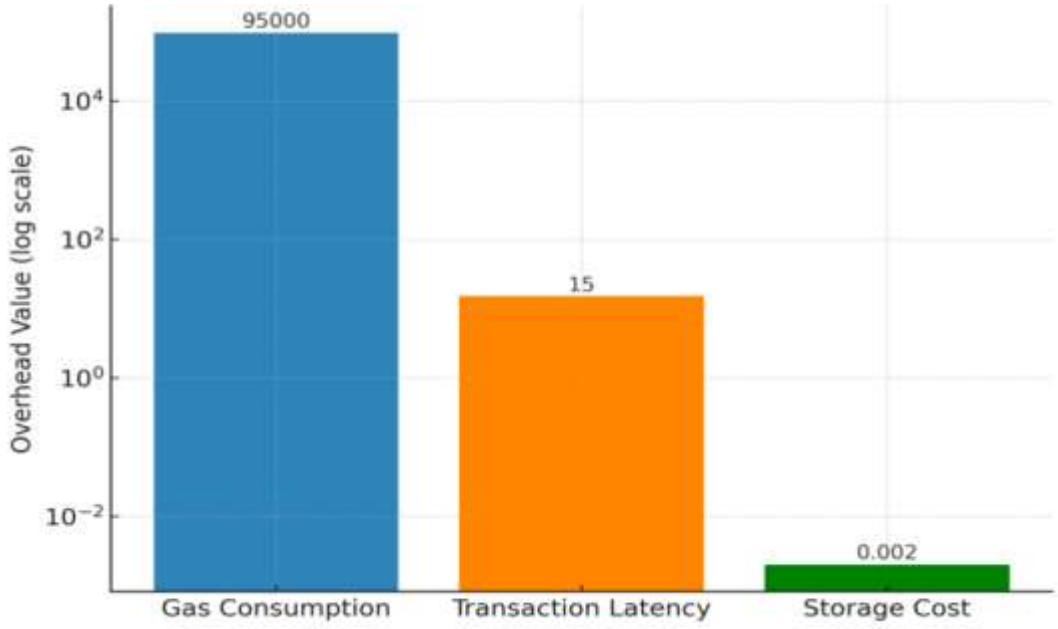

Figure 5. Blockchain overhead of TABT-ML, showing gas consumption ,transaction latency per update and Storage Cost.

D. Trade-off Analysis

The key trade-offs observed are:

Accuracy vs. Privacy: Adding DP reduces accuracy by up to 2%, but lowers adversary success in membership inference.

Privacy vs. Blockchain Overhead: HE + DP strengthens privacy but increases ciphertext size, slightly raising communication cost.

Auditability vs. Efficiency: Logging complete updates on-chain would incur high gas costs; logging hashes provides a balance between transparency and scalability.

Overall, TABT-ML demonstrates that a small reduction in accuracy (<3%) enables significant privacy gains and transparent auditability at a manageable blockchain cost, making it viable for real-world ITS deployments.

CONCLUSION — This paper presented TABT-ML, a blockchain-enabled federated SVM framework that integrates differential privacy, homomorphic encryption, and Ethereum smart contracts to achieve privacy-preserving and auditable traffic analysis in ITS. Experiments on PeMS-Bay and Kaggle Traffic Volume demonstrated 93% accuracy with only ~2.6% degradation compared to centralized SVM, while blockchain logging added modest overhead (~0.002 ETH per update and ~15 s latency), confirming feasibility for near real-time deployment. While TABT-ML strengthens security and auditability, challenges remain in addressing extreme non-IID data, communication costs from homomorphic encryption, and blockchain scalability. Incorporating adaptive privacy mechanisms, optimizing encryption efficiency, and extending the framework to deep learning models will enhance its applicability, paving the way for more robust and scalable privacy-preserving ITS solutions.

REFERENCES

[1] C. Cortes and V. Vapnik, "Support-vector networks," Machine Learning, vol. 20, no. 3, pp. 273–297, 1995.
[2] Kaggle, "Metro Interstate Traffic Volume dataset," 2018. [Online]. Available: https://www.kaggle.com/datasets
[3] P. Singh and A. Verma, "Accident prediction in intelligent transportation using SVM," International Journal of Intelligent Transportation Systems Research, vol. 20, no. 2, pp. 210–221, 2022.
[4] T. Nguyen, H. T. Nguyen, and T. Le, "Federated learning for distributed traffic prediction in intelligent transportation systems," IEEE Access, vol. 11, pp. 4567–4581, 2023.
[5] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in Proc. IEEE Symp. Security and Privacy (S&P), 2017, pp. 3–18.
[6] B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," in Proc. Int. Conf. Machine Learning (ICML), 2013, pp. 1467–1474.
[7] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. Int. Conf. Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273–1282.
[8] J. Zhang, H. Zhang, J. Ma, and X. Liu, "Federated support vector machines for intelligent IoT applications," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9530–9541, Oct. 2020.
[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[10] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.
[11] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. EUROCRYPT, 1999, pp. 223–238.
[12] C. Dwork, A. Roth, "The algorithmic foundations of differential privacy," Foundations and Trends in Theoretical Computer Science, vol. 9, nos. 3–4, pp. 211–407, 2014.
[15] Y. Zhang, M. Li, and J. Xu, "Blockchain-assisted federated learning for secure vehicular networks," IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 3, pp. 2101–2114, Mar. 2024.
[16] L. Liu, K. Chen, X. Wang, and Y. Qian, "Efficient blockchain-enabled federated learning for vehicular edge networks," IEEE Transactions on Vehicular Technology, vol. 74, no. 2, pp. 1231–1243, Feb. 2025.
[17] A. Sharma and S. Kaushik, "An analysis of traffic volume prediction using machine learning techniques," Procedia Computer Science, vol. 167, pp. 706–716, 2020.
[18] P. Mohassel and Y. Zhang, "SecureML: A system for scalable privacy-preserving machine learning," in Proc. IEEE Symp. Security and Privacy (S&P), 2017, pp. 19–38.
[19] J. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in Proc. ASIACRYPT, 2017, pp. 409–437.
[20] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, "A joint learning and communications framework for federated learning over wireless networks," IEEE Trans. Wireless Communications, vol. 20, no. 1, pp. 269–283, Jan. 2021.