SecureTrust-PI: A Privacy-Integrity Trust Management Model for Vehicular Edge-Cloud

Shilpa
Department of Computer Science & Engineering, REVA University, Bangalore, India
shilpasadlapur@rediffmail.com (corresponding author)

T. Prasanth
Research Guide Department of Computer Science and Engineering, REVA University, Bangalore, India
dr.tprasanth@gmail.com

Received: 24 April 2025 | Revised: 22 August 2025 | Accepted: 11 September 2025

 DOI: https://doi.org/10.48084/etasr.11697

ABSTRACT

Vehicular Ad-Hoc Networks (VANETs) integrated with Vehicular Edge-Cloud (VEC) frameworks enable seamless Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, enhancing both traffic safety and efficiency. However, VANET-enabled VEC environments are highly vulnerable to cyber threats, including unauthorized access, data tampering, and identity spoofing. Meanwhile, existing security solutions primarily focus on authentication and privacy, often neglecting data integrity, which leaves the system susceptible to manipulation attacks. To address this limitation, we propose the SecureTrust-PI model, which incorporates attack detection and misclassification minimization while optimizing network performance through efficient trust evaluation and integrity-preserving mechanisms. The model's performance was validated on an Internet of Vehicles (IoV) attack dataset under six adversarial scenarios ranging from 5% to 30% attack intensity and was compared against Practical Byzantine Fault Tolerance (PBFT). Results demonstrate that SecureTrust-PI consistently outperforms PBFT, achieving improvements of 26.16% in attack detection, 25.96% in misclassification reduction, 14.58% in throughput, 23.63% in delay, and 35.08% in energy efficiency.

Keywords-attack detection; integrity; privacy; security; trust model; Vehicular Ad-Hoc Networks (VANETs); vehicular edge cloud

I. INTRODUCTION

Vehicular Ad-Hoc Networks (VANETs) are increasingly recognized as the backbone of next-generation Intelligent Transportation Systems (ITS), enabling vehicles to exchange information using Vehicle-to-Vehicle (V2V) communication [1], with infrastructure using Vehicle-to-Infrastructure (V2I) communication [2], and with other entities using Vehicle-to-Everything (V2X) communication [3] in real time. These networks facilitate road safety applications such as collision avoidance, emergency message dissemination, and dynamic traffic management. Despite their potential, VANETs face significant challenges related to security, trust, privacy, and data integrity, which hinder their large-scale deployment, especially when integrated with Vehicular Edge-Cloud (VEC) frameworks.

Unlike traditional wireless networks, VANETs operate in a highly dynamic environment where rapid vehicle movement leads to frequent topology changes and intermittent connectivity, which complicates authentication, trust management, and message verification [4]. Moreover, the absence of centralized control increases susceptibility to malicious activities such as Sybil attacks [5], where a single adversary assumes multiple identities; spoofing [5], where a malicious node falsifies its identity or location to mislead other vehicles and disrupt secure communication; Denial-of-Service (DoS) attacks [6], which flood the communication channel; and message tampering [7], which compromises the integrity of safety-critical data [8]. These threats not only degrade network performance but also endanger human lives, making robust security and trust mechanisms indispensable [9].

In recent years, several approaches have been developed to address these challenges in VANETs and the broader Internet of Vehicles (IoV) [10]. For instance, the traditional Public Key Infrastructure (PKI) and digital signatures have been used, providing a baseline for authentication; however, they often fail to assess the dynamic trustworthiness of nodes [11]. Additionally, PKI systems are computationally intensive and do not prevent insider attacks from previously authenticated but malicious vehicles [12]. Consequently, there is a growing consensus that VANET security must extend beyond cryptographic primitives to include adaptive trust and privacy-preserving mechanisms [13].

For instance, in [14], a blockchain-based authentication model has been introduced that leverages a Bayesian-Directed Acyclic Graph (B-DAG). By dividing the network into grid-

like structures and utilizing edge-assisted roadside units, the model optimized trust computation using metaheuristic algorithms, while cryptographic techniques were used to generate virtual identities. This approach significantly reduced computation overhead and improved packet delivery, but its dependency on blockchain infrastructure results in higher resource consumption and deployment costs in real-world VANETs [14].

In another line of work in [15], multi-phase protocols that generate session keys for secure communication were employed, demonstrating lower communication and computation costs while maintaining privacy; however, these methods primarily focus on sender-receiver authentication and do not fully address large-scale attacks such as Distributed Denial of Service (DDoS). To address this gap, enhanced protocols were later introduced that integrated dynamic windowing techniques and unidentifiable credentials, showing improved resilience against DDoS attacks while preserving anonymity [16].

Trust-based methods have also been explored using federated learning to predict vehicle reliability before and during communication. These solutions ensured both pre- and post-communication trust by leveraging collaborative learning without central data storage. Although they improved security and reduced overhead, their reliance on federated models raises concerns regarding latency and data synchronization across dynamic vehicular environments [17].

Blockchain-based trust management schemes have also been proposed, employing smart contracts for vehicle registration and message alerting to enhance reliability. These solutions improve transparency and traceability but often suffer from high energy consumption and computational overhead due to continuous blockchain operations [18]. Similarly, trust-aware frameworks combining blockchain and networking techniques have been shown to reduce bandwidth usage, enhance throughput, and improve content delivery; however, integration complexity and storage requirements remain key challenges [19].

Other works have introduced trust-incentive mechanisms based on game theory, rewarding reliable nodes and penalizing malicious ones. These mechanisms reduce false data dissemination and improve overall ecosystem security but rely heavily on accurate trust feedback and sufficient blockchain storage [20]. Additionally, consensus-based blockchain models using Practical Byzantine Fault Tolerance (PBFT) mechanisms have also been implemented to minimize communication delays and improve authentication efficiency. Although effective, they introduce consensus-related delays under high network loads [21]. Lastly, cryptographic pseudonym-based frameworks have achieved secure group communication and low-cost authentication, yet such methods face challenges in managing large-scale pseudonym changes in dynamic vehicular scenarios [22].

This work proposes the SecureTrust-PI model, which integrates security, trust, privacy, and integrity into a unified architecture for VANETs in order to address several limitations of previously proposed models. The core contributions of the SecureTrust-PI model are as follows:

- Dynamic Trust Management: Establishes and continuously updates trust levels of vehicles and roadside infrastructure based on historical interactions, preventing unauthorized access and mitigating malicious behaviors.
- Secure Data Transmission: Employs graph-theory-based trust evaluation and secure message filtering to ensure data integrity, prevent identity forgery, and protect against unauthorized tracking.
- Anomaly and Threat Detection: Detects abnormal communication patterns, isolates compromised nodes, and safeguards network resilience against cyberattacks.
- Lightweight and Scalable Framework: Unlike PBFT, SecureTrust-PI minimizes computational and communication overhead.

II. METHODOLOGY

A. *Architecture*

The architecture of the SecureTrust-PI model, shown in Figure 1, enables secure, trustworthy, and private communication among vehicles and infrastructure through V2V, V2I, and V2X interactions. To achieve that, the security-trust model and privacy-integrity mechanism operate in parallel.

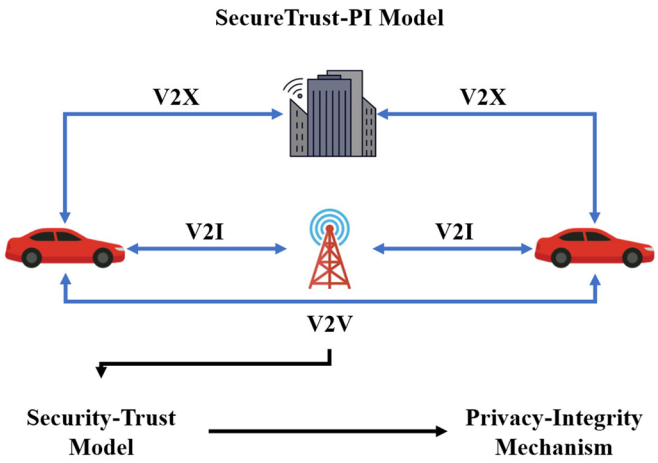

Fig. 1. SecureTrust-PI model architecture.

B. *Security-Trust Model*

The process of trust-based communication in V2V, V2I, and V2X interactions is presented in Figure 2. The SecureTrust-PI model establishes trust between vehicles to ensure that data exchange occurs only among reliable nodes.

Each interaction undergoes a multi-step trust-building process illustrated in Figure 3:

- Establish Security Trust: assigns an initial trust level (assumes trustworthy at first interaction), later refined through interaction history.

- Direct Trust: evaluates trust directly between nodes based on previous exchanges.
- Indirect Trust: computed through intermediary nodes when direct trust is unavailable.
- Recent and Past Trust: evaluates trustworthiness using short-term and long-term interaction histories.
- Future Trust: anticipates trustworthiness based on behavioral trends, enabling proactive defense.
- Establish Security: activates protective measures to isolate malicious or untrustworthy nodes.

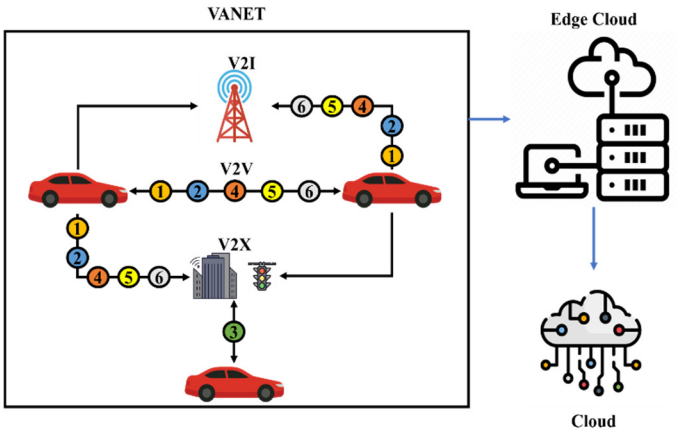

Fig. 2. SecureTrust PI Trust-based communication in V2V, V2I, and V2X interactions.

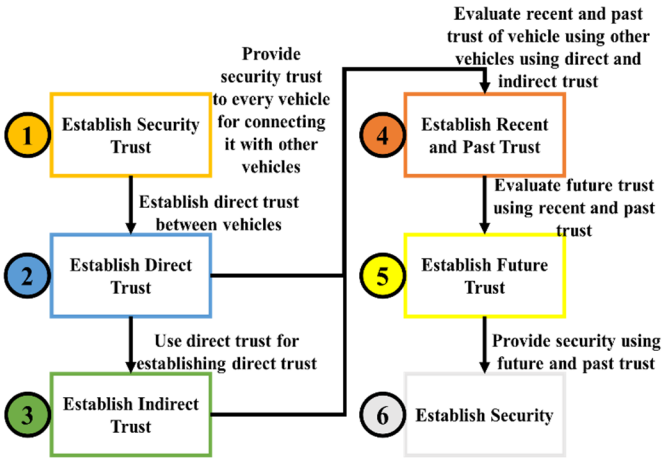

Fig. 3. Flow of trust-based communication and security establishment in VANET-enabled VEC.

C. Privacy-Integrity Mechanism

The proposed privacy-integrity mechanism reinforces privacy and data integrity by filtering unsafe or abnormal data transmissions and by preventing malicious manipulation within VANETs. For filtering malicious activity, the privacy-integrity mechanism leverages graph theory.

1) Graph-Based Representation of Vehicular Interactions

The proposed privacy-integrity mechanism models the vehicular network as a directed interaction graph $H = \{E, V\}$, in which E denotes interactions/connections among vehicles and V denotes vehicles in VANET-enabled VECs. A directed edge $(j, k) \in E$ indicates that the vehicle j transmits data that is exclusively received by the vehicle k. Trust between vehicles updates only through such direct interactions, ensuring that trust values evolve based solely on actual communications.

2) Initial Data State and Session-Based Transmission

At the beginning of each data transmission session l, the initial data position of a vehicle j is denoted by $y_j(0)$. Across sessions, the privacy-integrity mechanism ensures that all states $y(l)$ converge to a stable consensus value $\hat{y}$.

3) Randomized Data Injection for Privacy

For achieving $\hat{y}$ to prevent an adversary from inferring real data patterns, every vehicle first transmits random data as $w_j(l)$, where data follows a uniform distribution with mean 0 and variance 1. This randomized component masks the true communication state during the early phases of interaction.

4) Noise Modeling in Vehicular Communication

Due to the vehicular communication nature and dynamic mobility, noise is introduced during data transmission, which can be denoted as $x_j(l)$:

Case 1: Initial session ($l = 0$) where noise equals the transmitted random data:

$$x_j(l) = w_j(o) \quad (1)$$

Case 2: Subsequent sessions ($l > 0$):

$$x_j(l) = \beta^l w_j(l) - \beta^{l-1} w_j(l-1) \quad (2)$$

where $0 \leq \beta \leq 1$ is a decay constant unique to each vehicle, with a larger β indicating slower fading of previous noise contributions. This exponentially weighted noise model ensures controllable privacy while guaranteeing vanishing long-term noise influence.

5) Local State Update under Security-Trust Dynamics

Each vehicle updates its internal data state (or "transmission position") by incorporating both its previous position and the current noise:

$$y_j''(l+1) = b_{jj} y_j''(l) + x_j(l) \quad (3)$$

where $y_j''(l)$ is the previous data position of vehicle j, b_{jj} is a self-weighting coefficient, controlling how much a vehicle trusts its previous state versus the new incoming signal.

6) Interaction with Neighboring Vehicles

After updating its internal state, each vehicle interacts with its immediate neighbors $O(j)$, updating its value using an average-based strategy:

$$y_j(l+1) = b_{jj} y_j''(l) + \sum_{k \in O(j)} b_{jk} y_k''(l) \quad (4)$$

where b_{jk} is the weight assigned to neighbor k, while the weights b_{jj} and b_{jk} form a row-stochastic trust matrix (rows sum to 1). This cooperative update ensures privacy-preserved consensus among vehicles. The formulas in (3) and (4) are compactly represented in matrix form as:

$$y(l+1) = By''(l) = B\big(y(l) + x(l)\big) \quad (5)$$

where B is the global weighting (trust) matrix.

7) Ensuring Secure Convergence through Dynamic Probability and Covariance Control

For the SecureTrust-PI model to converge to a stable and privacy-preserving final state $\hat{y}$, the cumulative effect of noise must asymptotically vanish. To achieve this, the mechanism employs a dynamic probability method guided by an exponentially decayed covariance matrix. This process controls i) how noise evolves over each communication round, ii) handles both Gaussian and general (non-Gaussian) noise patterns, and iii) adjusts each vehicle's noise contribution based on interaction frequency, distance between vehicles, and channel reliability. As a result, each vehicle can estimate $x_j(l)$ robustly and update its data state without leaking private information or compromising trust.

8) Attack Detection via Position Evaluation

The SecureTrust-PI model evaluates the total number of interactions a vehicle x establishes with the vehicle y over a given period, along with the average interaction time between each vehicle and the surrounding infrastructure. Using this interaction-based position evaluation, the model detects malicious behavior and identifies the specific node at which an anomaly occurs.

When transmitted data is potentially manipulated during communication, the SecureTrust-PI model applies a state-changing detection mechanism. Two transmission scenarios are considered:

- S_0: Data transmitted securely with no attack.
- S_1: Data transmitted securely, but an attack may occur.

In scenario S_1, the attack is detected by monitoring state changes within transmitted data based on evolving trust. Normal states are given as $P_n = P(S_1|S_0)$ and attack states are given as $P_a = P(S_0|S_1)$. To determine whether the data is normal or malicious, SecureTrust-PI evaluates the variance N between the original transmission and the noise-adjusted transmission using

$$N = \| \, y_j(l) - \hat{y}_j(l) \, \|^2 \quad (6)$$

An attack is identified using the decision rule in:

$$N \lessgtr_{S_1}^{S_0} (\vartheta) = \begin{cases} S_0, & N \le \vartheta \\ S_1, & N > \vartheta \end{cases} \quad (7)$$

The threshold ϑ is adaptively determined based on prior probability distributions and acceptable false alarm rates, ensuring accurate discrimination between normal and malicious transmission behaviors. If anomaly thresholds are exceeded, the transmitting vehicle is classified as malicious; otherwise, it is considered trustworthy within the proposed lightweight blockchain-based framework.

III. RESULTS AND DISCUSSION

The SecureTrust-PI model was evaluated using the IoV attack dataset obtained from the Canadian Institute of Cybersecurity [23, 24]. To ensure a fair comparison, similar simulation parameters as those used in the PBFT method were adopted [21, 22], and both SecureTrust-PI and PBFT were implemented using the NS3-based SIMITS simulator developed in C# [25, 26]. The evaluation process involved six different test scenarios, where the attack percentage was varied at 5% (100 total attacks), 10% (200 total attacks), 15% (300 total attacks), 20% (400 total attacks), 25% (500 total attacks), and 30% (600 total attacks) and their performance was assessed based on attack detection rate, attack misclassification rate, throughput, delay, and energy consumption.

A. Attack Detection Rate

The attack detection rate results indicate that the SecureTrust-PI model consistently outperformed the PBFT model across all attack percentage scenarios, as shown in Figure 4. At a 5% attack rate, PBFT achieved a detection rate of 72%, while SecureTrust-PI achieved 78%, representing an 8.33% improvement. The performance gap widens as attack levels rise. For instance, at a 20% attack rate, PBFT detects 50% of attacks, whereas SecureTrust-PI detects 64%, corresponding to a 28% improvement. Even at the highest attack level (30%), SecureTrust-PI maintains a detection rate of 58%, significantly surpassing PBFT's 40%, achieving a 45% improvement. Overall, SecureTrust-PI delivers an average improvement of 26.16% compared to the PBFT model.

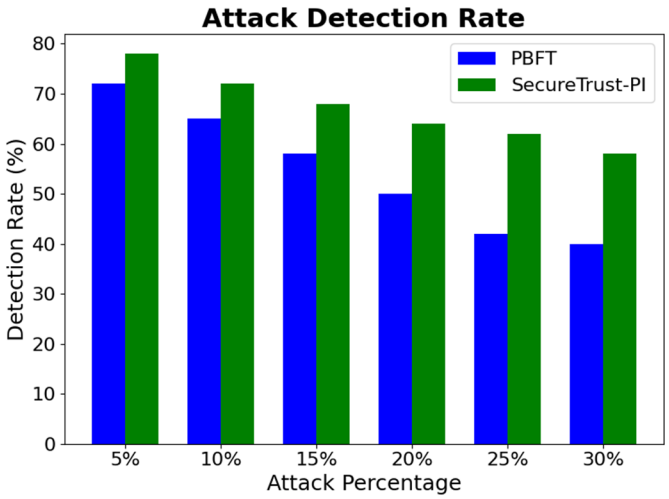

Fig. 4. Attack detection rate evaluation considering SecureTrust-PI and PBFT.

B. Attack Misclassification Rate

The results show that the SecureTrust-PI model significantly reduces the misclassification rate compared to PBFT across all attack percentages, as shown in Figure 5.

At a 5% attack rate, PBFT misclassifies 28% of the attacks, while SecureTrust-PI misclassifies 20% of the attacks, showing an improvement of 28.57%. As the attack percentage increases, PBFT's misclassification rate rises sharply, reaching 58% misclassified attacks at a 30% attack rate, whereas SecureTrust-PI maintains a comparatively lower rate of 42% misclassified attacks, reflecting a 25.96% improvement. On average, the SecureTrust-PI model reduces the attack misclassification rate by 25.96% compared to PBFT, indicating that it is more efficient in differentiating between legitimate and malicious activities.

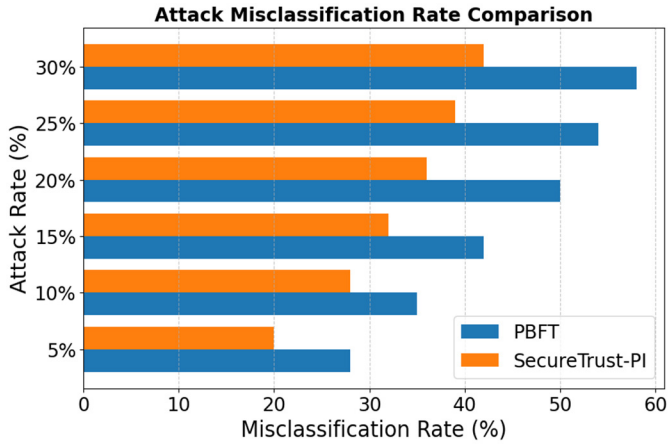

Fig. 5. Attack misclassification rate evaluation considering SecureTrust-PI and PBFT.

C. Throughput

Throughput is a significant performance metric that measures the efficiency of data transmission in VANET environments. The results indicate that the SecureTrust-PI model consistently outperforms PBFT across all attack percentages (Figure 6), demonstrating its ability to maintain a higher rate of successful data delivery even under increasing attack levels.

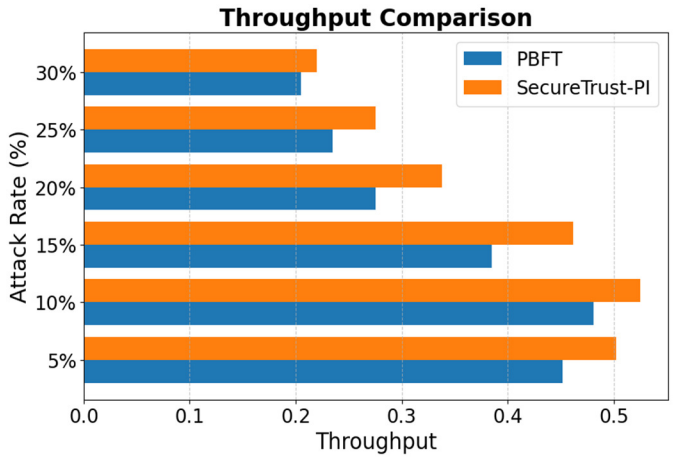

Fig. 6. Throughput evaluation considering SecureTrust-PI and PBFT.

At a 5% attack rate, PBFT achieves a throughput of 0.452, whereas SecureTrust-PI achieved 0.502, reflecting a 11.06% increase. As the attack percentage rises, PBFT's throughput declines significantly, reaching 0.205 at a 30% attack rate, while SecureTrust-PI maintains a comparatively higher throughput of 0.2201, indicating a 7.36% improvement. On average, the SecureTrust-PI model enhances throughput by 14.58% compared to PBFT, demonstrating its ability to handle network congestion and maintain efficient data flow even in the presence of attacks.

Additionally, the higher throughput values show that SecureTrust-PI improves communication reliability, reduces packet loss, and ensures smoother vehicular data exchange, which is essential for real-time applications in VANET-enabled VECs. Additionally, since the performance gap between the two models widens as the attack percentage increases, it further validates that SecureTrust-PI is more resilient in high-attack environments, preventing severe data transmission degradation.

D. Delay

Delay plays an important role in vehicular networks due to the need for fast communication and real-time decision-making. As shown in Figure 7, the SecureTrust-PI model significantly reduces delay compared to PBFT across all attack percentages, indicating its higher efficiency in processing and transmitting messages.

At a 5% attack rate, PBFT exhibits a delay of 71.60 ms, while SecureTrust-PI achieves a much lower 56.14 ms, reflecting a 21.58% reduction. As the attack percentage increases, PBFT's delay remains higher, reaching 61.40 ms at a 30% attack rate, whereas SecureTrust-PI sustains its efficiency with a reduced delay of 45.94 ms, showing an overall delay reduction of 25.16%. On average, SecureTrust-PI achieves a 23.63% reduction in delay compared to PBFT.

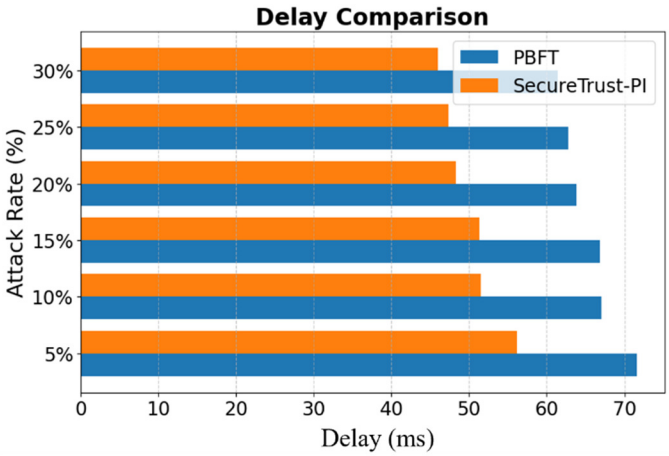

Fig. 7. Delay evaluation considering SecureTrust-PI and PBFT.

E. Energy Consumption

Energy consumption is also important in VANETs, as lower energy usage ensures longer operational times for vehicular communication devices and reduces overall network strain. The results indicate that SecureTrust-PI significantly

reduces energy consumption compared to PBFT across all attack scenarios (Figure 7).

At a 5% attack rate, PBFT consumes 3.54 J, whereas SecureTrust-PI consumes 2.34 J, showing an energy reduction of approximately 33.86%. As attack percentages increase, PBFT's energy consumption remains higher, reaching 3.26 J at a 30% attack rate, while SecureTrust-PI maintains lower consumption at 2.06 J, reflecting an overall reduction of 36.74%. On average, SecureTrust-PI achieves a 35.08% reduction in energy consumption compared to PBFT, emphasizing its lightweight computational requirements and optimized authentication mechanisms.

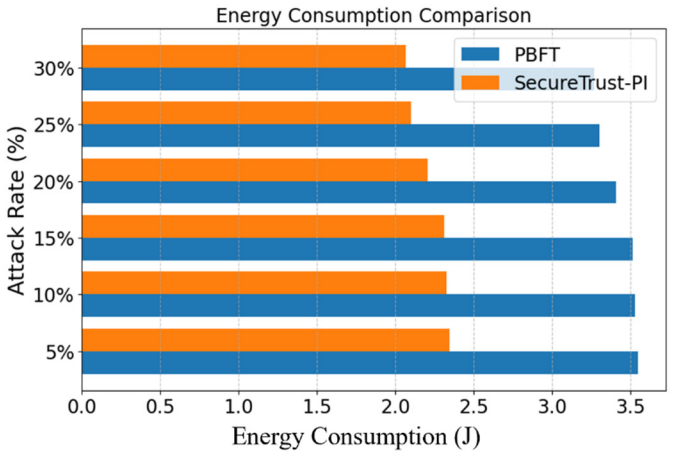

Fig. 8. Energy consumption evaluation considering SecureTrust-PI and PBFT.

IV. CONCLUSION

This study proposed the SecureTrust-PI model, designed to enhance security, privacy, and integrity in Vehicular Ad-Hoc Networks (VANET)-enabled Vehicular Edge-Cloud (VEC) environments. The model was evaluated using the Internet of Vehicles (IoV) attack dataset and benchmarked against the Practical Byzantine Fault Tolerance (PBFT) consensus method. Both models were implemented in identical conditions, and their performance was assessed across six attack scenarios with varying attack rates (5%-30%) using metrics such as attack detection rate, attack misclassification rate, throughput, delay, and energy consumption.

The results demonstrated that SecureTrust-PI achieved significantly higher attack detection accuracy and lower misclassification rates than the PBFT. Additionally, SecureTrust-PI improved network throughput while effectively reducing communication delay and energy consumption, confirming its suitability for real-time, resource-constrained vehicular environments. Collectively, these findings establish SecureTrust-PI as a robust, efficient, and scalable solution for ensuring secure, trustworthy, and privacy-preserving communication in VANET-enabled VEC architectures.

Future work will focus on integrating artificial intelligence and machine learning techniques to further enhance real-time attack detection and adaptive security mechanisms for VEC environments.

ACKNOWLEDGMENT

We sincerely thank REVA University for granting us the opportunity to carry out this research. The encouragement and support provided by the University greatly contributed to this work.

REFERENCES

[1] W. Arellano and I. Mahgoub, "A VANET, Multi-Hop-Enabled, Dynamic Traffic Assignment for Road Networks," *Electronics*, vol. 14, no. 3, Jan. 2025, Art. no. 559, https://doi.org/10.3390/electronics14030559.

[2] Y. Gan, X. Xie, and Y. Liu, "A Privacy-Preserving V2I Fast Authentication Scheme in VANETs," *Electronics*, vol. 13, no. 12, Jun. 2024, Art. no. 2369, https://doi.org/10.3390/electronics13122369.

[3] H. Alabdouli, M. S. Hassan, and A. Abdelfatah, "Enhancing Route Guidance with Integrated V2X Communication and Transportation Systems: A Review," *Smart Cities*, vol. 8, no. 1, Feb. 2025, Art. no. 24, https://doi.org/10.3390/smartcities8010024.

[4] C. Gheorghe and A. Soica, "Revolutionizing Urban Mobility: A Systematic Review of AI, IoT, and Predictive Analytics in Adaptive Traffic Control Systems for Road Networks," *Electronics*, vol. 14, no. 4, Feb. 2025, Art. no. 719, https://doi.org/10.3390/electronics14040719.

[5] Z.-R. Tzoannos, D. Kosmanos, A. Xenakis, and C. Chaikalis, "The Impact of Spoofing Attacks in Connected Autonomous Vehicles under Traffic Congestion Conditions," *Telecom*, vol. 5, no. 3, pp. 747–759, Aug. 2024, https://doi.org/10.3390/telecom5030037.

[6] N. Khatri, S. Lee, and S. Y. Nam, "Sybil Attack-Resistant Blockchain-Based Proof-of-Location Mechanism with Privacy Protection in VANET," *Sensors*, vol. 24, no. 24, Dec. 2024, Art. no. 8140, https://doi.org/10.3390/s24248140.

[7] O. Polat, S. Oyucu, M. Türkoğlu, H. Polat, A. Aksoz, and F. Yardımcı, "Hybrid AI-Powered Real-Time Distributed Denial of Service Detection and Traffic Monitoring for Software-Defined-Based Vehicular Ad Hoc Networks: A New Paradigm for Securing Intelligent Transportation Networks," *Applied Sciences*, vol. 14, no. 22, Nov. 2024, Art. no. 10501, https://doi.org/10.3390/app142210501.

[8] A. Borah and A. Paranjothi, "Enhancing VANET Security: An Unsupervised Learning Approach for Mitigating False Information Attacks in VANETs," *Electronics*, vol. 14, no. 1, Dec. 2024, Art. no. 58, https://doi.org/10.3390/electronics14010058.

[9] Y. Zhan, W. Xie, R. Shi, Y. Huang, and X. Zheng, "Dynamic Privacy-Preserving Anonymous Authentication Scheme for Condition-Matching in Fog-Cloud-Based VANETs," *Sensors*, vol. 24, no. 6, Mar. 2024, Art. no. 1773, https://doi.org/10.3390/s24061773.

[10] Z. S. Alzaidi, A. A. Yassin, Z. A. Abduljabbar, and V. O. Nyangaresi, "A Fog Computing and Blockchain-based Anonymous Authentication Scheme to Enhance Security in VANET Environments," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19143–19153, Feb. 2025, https://doi.org/10.48084/etasr.8663.

[11] Y. Li, R. Bi, N. Jiang, F. Li, M. Wang, and X. Jing, "Methods and Challenges of Cryptography-Based Privacy-Protection Algorithms for Vehicular Networks," *Electronics*, vol. 13, no. 12, Jun. 2024, Art. no. 2372, https://doi.org/10.3390/electronics13122372.

[12] S. Wang, Z. Fan, Y. Su, B. Zheng, Z. Liu, and Y. Dai, "A Lightweight, Efficient, and Physically Secure Key Agreement Authentication Protocol for Vehicular Networks," *Electronics*, vol. 13, no. 8, Apr. 2024, Art. no. 1418, https://doi.org/10.3390/electronics13081418.

[13] X. Xu *et al.*, "Hybrid Trust Model for Node-Centric Misbehavior Detection in Dynamic Behavior-Homogeneous Clusters," *Applied Sciences*, vol. 15, no. 4, Feb. 2025, Art. no. 2020, https://doi.org/10.3390/app15042020.

[14] I. S. Alkhalifa and A. S. Almogren, "Enhancing Security and Scalability in Vehicular Networks: A Bayesian DAG Blockchain Approach With

Edge-Assisted RSU," *IEEE Access*, vol. 12, pp. 116558–116571, 2024, https://doi.org/10.1109/ACCESS.2024.3429184.

[15] S. J. Ibrahim and H. Beitollahi, "PPA6-IoV: A Six-Step Privacy-Preserving Authentication Protocol for the Internet of Vehicles," *IEEE Access*, vol. 12, pp. 168120–168134, 2024, https://doi.org/10.1109/ACCESS.2024.3459948.

[16] S. Jamal Ibrahim and H. Beitollahi, "PPAD-W: A Novel Privacy-Preserving Authentication With Dynamic IPs Window for IoV Networks," *IEEE Access*, vol. 12, pp. 164737–164749, 2024, https://doi.org/10.1109/ACCESS.2024.3493624.

[17] M. M. Alshahrani, "A Verifiable Discrete Trust Model (VDTM) Using Congruent Federated Learning (CFL) for Social Internet of Vehicles," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 1441–1456, 2024, https://doi.org/10.1109/OJVT.2024.3468164.

[18] S. Hussain, S. Tahir, A. Masood, and H. Tahir, "Blockchain-Enabled Secure Communication Framework for Enhancing Trust and Access Control in the Internet of Vehicles (IoV)," *IEEE Access*, vol. 12, pp. 110992–111006, 2024, https://doi.org/10.1109/ACCESS.2024.3431279.

[19] A. Bibi *et al.*, "TR-Block: A Trustable Content Delivery Approach in VANET Through Blockchain," *IEEE Access*, vol. 12, pp. 60863–60875, 2024, https://doi.org/10.1109/ACCESS.2024.3386461.

[20] H. Han, M. Zhang, Z. Xu, X. Dong, and Z. Wang, "Decentralized Trust Management and Incentive Mechanisms for Secure Information Sharing in VANET," *IEEE Access*, vol. 12, pp. 124414–124427, 2024, https://doi.org/10.1109/ACCESS.2024.3453368.

[21] Z. Ma *et al.*, "A Blockchain-Based Secure Distributed Authentication Scheme for Internet of Vehicles," *IEEE Access*, vol. 12, pp. 81471–81482, 2024, https://doi.org/10.1109/ACCESS.2024.3409361.

[22] S. Naskar, G. Hancke, T. Zhang, and M. Gidlund, "Pseudo-Random Identification and Efficient Privacy-Preserving V2X Communication for IoV Networks," *IEEE Access*, vol. 13, pp. 1147–1163, 2025, https://doi.org/10.1109/ACCESS.2024.3523358.

[23] *CIC IoV dataset*. (2024), E. C. P. Neto, H. Taslimasa, S. Dadkhah, S. Iqbal, P. Xiong, T. Rahmanb, and A. A. Ghorbani. [Online]. Available: https://www.unb.ca/cic/datasets/iov-dataset-2024.html.

[24] E. C. P. Neto *et al.*, "CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus," *Internet of Things*, vol. 26, Jul. 2024, Art. no. 101209, https://doi.org/10.1016/j.iot.2024.101209.

[25] N. Ababneh and J. N. Al-Karaki, "On the Lifetime Analytics of IoT Networks," in *2020 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, India, Jul. 2020, pp. 1086–1090, https://doi.org/10.1109/ICCSP48568.2020.9182272.

[26] N. Gadde, B. Jakkali, R. B. H. Siddamallaih, and G. Gowrishankar, "Quality of experience aware network selection model for service provisioning in heterogeneous network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 2, pp. 1839-1848, Apr. 2022, https://doi.org/10.11591/ijece.v12i2.pp1839-1848.