A Hybrid Federated Tree-Based Intrusion Detection System for Securing Autonomous Vehicles and V2X Networks Using Adaptive Boosting and Blockchain

Saranya Eeday[1], Sandeep Kosuri[2]
[1,2] *Lakeview Loan Servicing, 4425 Ponce de Leon BLVD,4th floor, Coral Gables, Florida-33146.*[2]*DEF*
(*[1]Saranyaemastermind@gmail.com, [2]Sandeepkscholar@gmail.com*)

***Abstract*—**The increasing reliance on autonomous vehicles and Vehicle-to-Everything (V2X) communication networks has introduced significant cybersecurity risks, particularly in real-time systems like Intelligent Transportation Systems (ITS). Traditional Intrusion Detection Systems (IDS) face challenges in scalability, real-time response, and adapting to evolving attack vectors. This paper proposes a novel Hybrid Federated Tree-Based Intrusion Detection System (IDS) to address these limitations by integrating adaptive boosting, federated learning, and blockchain technologies. The proposed system leverages federated learning to enable distributed training of tree-based models (Random Forests and Gradient Boosting) across autonomous vehicles, ensuring privacy and scalability by keeping data localized. To enhance detection accuracy and adapt to new, sophisticated attacks, the system incorporates adaptive boosting, allowing it to learn from hard-to-detect anomalies. Furthermore, blockchain is employed to securely aggregate and verify model updates from different vehicles, providing resistance to model poisoning attacks. A novel V2V ensemble approach is introduced, enabling vehicles to collaborate in real-time, improving the overall detection accuracy through consensus-based decision-making. The proposed IDS is designed to operate with ultra-low latency, ensuring real-time protection against threats like denial of service (DoS), message tampering, and spoofing attacks. Experimental results demonstrate the system's effectiveness in detecting cyberattacks with high accuracy and low computational overhead, making it a viable solution for securing autonomous vehicles and V2X networks in next-generation transportation systems.

Keywords*—Intelligent Transportation Systems (ITS), Autonomous Vehicles, Intrusion Detection System (IDS), Hybrid Federated Learning,Cybersecurity*

I. INTRODUCTION

The rapid advancement of Intelligent Transportation Systems (ITS) and the increasing deployment of autonomous vehicles have revolutionized the landscape of modern transportation. By enabling seamless communication between vehicles (Vehicle-to-Vehicle, V2V) and between vehicles and infrastructure (Vehicle-to-Infrastructure, V2I), these technologies promise enhanced safety, efficiency, and convenience [1], [2]. However, the integration of communication networks into transportation systems introduces significant cybersecurity vulnerabilities. Cyberattacks targeting autonomous vehicles and V2X networks pose critical risks that can compromise passenger safety, disrupt traffic flow, and undermine public trust in these emerging technologies [2].

Recent incidents have demonstrated that cyber threats, such as denial of service (DoS) attacks, spoofing, and data tampering, can exploit the interconnected nature of ITS, leading to catastrophic consequences [2]. Existing Intrusion Detection Systems (IDS) primarily rely on centralized approaches that face challenges related to scalability, real-time detection, and adaptability to evolving attack patterns [3]. Furthermore, the increasing volume of data generated by autonomous vehicles necessitates a robust detection mechanism capable of operating efficiently in real-time without sacrificing accuracy or privacy [1], [2].

In this paper, we propose a novel Hybrid Federated Tree-Based Intrusion Detection System (IDS) designed to enhance cybersecurity in ITS by leveraging tree-based machine learning models, adaptive boosting techniques, and blockchain technology. Our methodology facilitates distributed learning through federated learning, allowing individual vehicles to maintain data privacy while collaboratively improving the global model [4], [5]. The integration of adaptive boosting enables the system to continuously learn from evolving attack patterns, ensuring that detection capabilities remain effective over time [3]. Additionally, employing blockchain technology provides a secure and transparent means of aggregating model updates, thus safeguarding against model poisoning attacks [4], [5].

The key contributions of this work include the development of a decentralized intrusion detection framework that operates in real-time, a robust V2V collaboration mechanism to enhance detection accuracy, and a comprehensive evaluation of the proposed system's performance in realistic attack scenarios. Through our approach, we aim to address the critical cybersecurity challenges faced by ITS and contribute to the safe deployment of autonomous vehicles and V2X networks Savitha et al. [2].

II. LITERATURE SURVEY

In the field of Intelligent Transportation Systems (ITS) and autonomous vehicles, numerous studies have contributed to understanding various aspects of these technologies, including safety, decision-making, and traffic flow. However, significant gaps remain, particularly concerning the cybersecurity of these systems, which is critical for their safe deployment and public acceptance.

Gao et al. Gao et al. [6] explored longitudinal control for autonomous vehicles, focusing on performance optimization based on driving data. While their work advances vehicle control algorithms, it does not address the cybersecurity implications of such systems. Chan and Chin Chan & Chin [7] provided a comprehensive review of autonomous intelligent vehicles, emphasizing urban driving and parking challenges. However, their analysis lacks a focus on the vulnerabilities introduced by vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, which are essential for the safe operation of autonomous vehicles.

Wang et al. Wang et al. [8] and Wu et al. Wu et al. [9] investigated lane-changing behaviors and trajectory planning, respectively, highlighting the importance of decision-making in mixed traffic environments. Yet, these studies do not consider the potential cyber threats that could manipulate these decision-making processes, leading to unsafe driving conditions. Similarly, while Narayanan et al. Narayanan et al. [10] reviewed shared autonomous vehicle services, they did not address the cybersecurity challenges that could arise from the shared nature of these services.

Recent advancements in connected autonomous vehicles (CAVs) have shown promise in improving traffic safety and efficiency through real-time information sharing [11]. However, the reliance on communication networks exposes these vehicles to various cyberattacks, a concern that has not been sufficiently addressed in the literature. For instance, Alheeti et al. Alheeti et al. [12] discussed intrusion detection systems in vehicular networks but did not propose a comprehensive solution that integrates real-time detection with privacy-preserving techniques.

Moreover, while studies like those by Garg and Bouroche Garg & Bouroche [11] emphasize the cooperative nature of autonomous driving, they often overlook the implications of cybersecurity on cooperation and communication between vehicles and infrastructure. The existing literature primarily focuses on operational efficiency and safety without adequately addressing the cybersecurity frameworks necessary to protect these systems from malicious attacks.

In this paper, we aim to fill these gaps by proposing a Hybrid Federated Tree-Based Intrusion Detection System (IDS) that not only enhances cybersecurity in ITS but also ensures data privacy through federated learning. Our approach leverages adaptive boosting techniques to continuously learn from evolving attack patterns, thus addressing the critical cybersecurity challenges that have been largely neglected in previous research. By integrating blockchain technology, we provide a secure and transparent method for aggregating model updates, which further strengthens the resilience of autonomous vehicle networks against cyber threats.

III. METHODOLOGY

This section outlines the novel Hybrid Federated Tree-Based Intrusion Detection System (IDS) developed to enhance cybersecurity in Intelligent Transportation Systems (ITS) and autonomous vehicles. Our approach leverages distributed machine learning, adaptive boosting techniques, and blockchain technology to create a robust and scalable IDS capable of real-time intrusion detection.

A. Hybrid Federated Learning Framework

The proposed IDS utilizes a Hybrid Federated Learning (HFL) framework to train tree-based models collaboratively across multiple vehicles while ensuring data privacy and minimizing centralized data processing. The HFL framework consists of the following key components:

- Local Model Training: Each vehicle collects and processes local data from its onboard sensors and communication systems. Tree-based models, such as Random Forests and Gradient Boosting, are trained on this local data to identify patterns indicative of intrusions. The choice of tree-based models is motivated by their high interpretability and effectiveness in handling structured data.
- Periodic Model Aggregation: Instead of sharing sensitive raw data, each vehicle periodically sends its model updates (e.g., weights and parameters) to a central server or blockchain network. The server aggregates these updates to create a global model that reflects the learning from all participating vehicles, enhancing detection capabilities across the fleet.

B. Adaptive Boosting for Evolving Attack Patterns

To enhance the IDS's accuracy in detecting new and sophisticated attacks, we integrate Adaptive Boosting (AdaBoost) into our methodology:

- Dynamic Weight Adjustment: AdaBoost assigns higher weights to misclassified instances, allowing the model to focus on hard-to-detect anomalies. This mechanism is crucial in adapting to evolving attack vectors, ensuring that the IDS learns from previous attack attempts and improves its detection capabilities over time.
- Model Retraining: The global model can be periodically retrained based on the newly aggregated data from vehicles, incorporating the latest attack patterns and enhancing its resilience against emerging threats.

C. Blockchain Integration for Secure Model Aggregation

To safeguard the integrity of model updates and protect against potential attacks on the IDS, we implement a blockchain-based system for secure model aggregation:

- Decentralized Verification: The blockchain serves as a decentralized ledger that records all model updates from participating vehicles. This architecture prevents unauthorized access and ensures that only legitimate updates are included in the global model.
- Tamper-Proof Audit Trail: Every update transaction is time-stamped and linked to previous transactions, creating a tamper-proof audit trail that enhances accountability and trust in the model aggregation process.

D. V2V Collaboration Mechanism

Our methodology introduces a novel Vehicle-to-Vehicle (V2V) collaboration mechanism to enhance detection accuracy through collective decision-making:

- Ensemble Decision-Making: Vehicles within close proximity can share their local detection results and collaborate to reach a consensus on potential threats. This ensemble approach allows for improved accuracy, as it reduces the likelihood of false positives and negatives.
- Real-Time Communication: The V2V collaboration is designed to operate in real-time, enabling vehicles to respond quickly to identified threats, such as potential spoofing or jamming attacks.

E. Low-Latency Detection Architecture

To ensure that the proposed IDS can operate effectively in real-time scenarios, we design a low-latency detection architecture:

- Onboard Processing: Lightweight tree-based models are deployed on vehicles, allowing for immediate analysis of incoming data without reliance on cloud processing. This design minimizes latency in detecting intrusions.
- Edge-Cloud Orchestration: In situations requiring more computational power, vehicles can offload complex processing tasks to edge servers or the cloud while maintaining a seamless detection experience.

IV. RESULTS AND DISCUSSION

This section presents the experimental evaluation of the proposed Hybrid Federated Tree-Based Intrusion Detection System (IDS), focusing on its performance in detecting cyber threats within Intelligent Transportation Systems (ITS). The evaluation was conducted using both simulated environments and real-world datasets to assess the system's effectiveness, scalability, and adaptability.

A. Experimental Setup

Datasets: The experiments utilized a combination of public datasets, including the KDD Cup 1999 dataset and simulated V2X communication data representing realistic traffic scenarios. The datasets were chosen to represent various attack types relevant to autonomous vehicles, such as DoS attacks, spoofing, and message tampering.

Simulation Environment: A simulation environment was created to model the interactions between multiple vehicles, with each vehicle equipped with an onboard instance of the IDS. The vehicles communicated through a V2V protocol to share detection results and collaborate on identifying potential threats.

Evaluation Metrics: The performance of the proposed IDS was evaluated using key metrics such as accuracy, precision, recall, F1-score, and latency. These metrics provide insight into the system's ability to detect attacks while minimizing false positives and ensuring timely responses.

B. Detection Performance

1) Accuracy and Precision

The proposed IDS demonstrated high accuracy rates across various attack scenarios. The results are summarized in Table 1, which presents the accuracy, precision, recall, and F1-score for each type of attack:

TABLE I. TABLE STYLES

Attack Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DoS Attack	98.5	97.2	98	97.6
Spoofing	97.8	96.5	96	96.2
Message Tampering	98.2	97.5	97	97.2
Normal Traffic	99	98.8	99.2	99

The results indicate that the system effectively identifies both malicious and benign traffic, achieving overall high performance in distinguishing between normal and attack patterns.

2) Latency Analysis

The latency of the intrusion detection process is critical for real-time applications. Figure 1 illustrates the average detection latency for different attack types under varying vehicle densities (number of vehicles in the network). The proposed IDS maintained low latency levels, averaging around 20 milliseconds, even with increasing vehicle numbers.

Observation: The latency remained consistent across different attack types, demonstrating the efficiency of the onboard processing capabilities and the low-latency architecture.

C. Scalability

To assess scalability, we analyzed the system's performance with an increasing number of vehicles participating in the federated learning process. The IDS successfully handled up to 100 vehicles without a significant drop in detection accuracy or an increase in latency, indicating robust scalability.

D. Adaptability to Evolving Attacks

The integration of Adaptive Boosting significantly improved the IDS's adaptability to new attack patterns. When subjected to previously unseen attack types, the system was

able to learn and adapt after just a few iterations of model updates. The effectiveness of the adaptive boosting mechanism is illustrated in Figure 2, which shows the F1-score improvement over training epochs.

V. CONCLUSION

In this paper, we proposed a Hybrid Federated Tree-Based Intrusion Detection System (IDS) designed to enhance cybersecurity in Intelligent Transportation Systems (ITS), particularly for autonomous vehicles and V2X networks. Our approach integrates federated learning, tree-based machine learning algorithms, and adaptive boosting to create a robust and efficient system capable of detecting various cyber threats in real time.

The experimental results demonstrate the effectiveness of the proposed IDS in accurately identifying malicious activities while maintaining low latency, even as the number of vehicles in the network increases. The system achieved high accuracy rates across multiple attack scenarios, including Denial of Service (DoS), spoofing, and message tampering, showcasing its adaptability to evolving threats. Moreover, the use of federated learning allows individual vehicles to learn from local data while contributing to a shared global model, thereby preserving privacy and reducing the need for data transmission. The findings highlight the potential of our proposed methodology to address the pressing cybersecurity challenges faced by intelligent transportation systems.

Future research can focus on several key areas to further enhance the effectiveness and applicability of the proposed IDS. Real-time implementation of the system in actual traffic environments will provide valuable insights into its performance under varied conditions and attack vectors. Additionally, exploring the integration of other advanced machine learning techniques, such as deep learning, could improve detection accuracy, particularly for complex attack patterns. Developing adaptive learning mechanisms that enable the system to continuously learn and adapt to new threats in real time will significantly bolster its resilience. Investigating and refining V2V communication protocols will enhance data sharing and collaboration among vehicles without compromising security and privacy. Lastly, incorporating contextual information about users and the environment can aid the IDS in making more informed decisions, thereby reducing false positives and improving overall response strategies.

REFERENCES

[1] A. Ferdowsi, U. Challita, & W. Saad, "Deep learning for reliable mobile edge analytics in intelligent transportation systems: an overview", Ieee Vehicular Technology Magazine, vol. 14, no. 1, p. 62-70, 2019. https://doi.org/10.1109/mvt.2018.2883777

[2] P. Savitha, S. Madhu, & S. Arjun, "Cyber security issues in connected autonomous vehicle", International Journal of Research Publication and Reviews, vol. 4, no. 3, p. 929-936, 2023. https://doi.org/10.55248/gengpi.2023.32358

[3] X. Huang and X. Wang, "Detection and isolation of false data injection attack in intelligent transportation system via robust state observer", Processes, vol. 10, no. 7, p. 1299, 2022. https://doi.org/10.3390/pr10071299

[4] X. Guo and X. Guo, "A research on blockchain technology: urban intelligent transportation systems in developing countries", Ieee Access, vol. 11, p. 40724-40740, 2023. https://doi.org/10.1109/access.2023.3270100

[5] V. Elagin, A. Spirkina, M. Buinevich, & A. Vladyko, "Technological aspects of blockchain application for vehicle-to-network",, 2020. https://doi.org/10.20944/preprints202009.0132.v1

[6] H. Gao, X. Zhang, Y. Liu, & D. Li, "Longitudinal control for mengshi autonomous vehicle via gauss cloud model", Sustainability, vol. 9, no. 12, p. 2259, 2017. https://doi.org/10.3390/su9122259

[7] T. Chan and C. Chin, "Review of autonomous intelligent vehicles for urban driving and parking", Electronics, vol. 10, no.