Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 01 – April 2025

Privacy-Preserving and Decentralized Authentication for IoV Using Federated Learning and Blockchain

Santhosh Jayagopalan[1*]
[1*]School of Computing, British Applied College, Umm Al Quwain, United Arab Emirates (UAE).
[1*]Santhosh.j@acuq.ae
Corresponding Author E-mail ID: Santhosh.j@acuq.ae

Abstract:
The Internet of Vehicles (IoV) is a rapidly evolving field, and it is imperative to safeguard user privacy while ensuring effective and secure authentication. Conventional centralized authentication methods are susceptible to single points of failure, privacy issues, and data breaches. This study presents an innovative decentralized authentication method utilizing federated learning and blockchain technology to address these concerns. Federated learning safeguards private data by allowing vehicles to collectively develop authentication models locally, hence eliminating the need for data transfer to centralized servers. Blockchain offers a secure, immutable ledger for documenting authentication activities, enhancing transparency and minimizing manipulation. Our privacy-preserving methodology reduces communication overhead and computational expenses while providing real-time, scalable, and tamper-resistant authentication for IoV scenarios. The proposed technique outperforms conventional methods for computational expense, communication costs, throughput, and security robustness. This methodology integrates the advantages of federated learning and blockchain technology to provide a strong solution to the increasing security demands of IoV networks.

Keywords: *IoV, Privacy, Authentication, Blockchain, Federated Learning*

1. INTRODUCTION

The Internet of Vehicles (IoV) is becoming an essential element of intelligent transportation systems, linking vehicles, infrastructure, pedestrians, and service providers in a dynamic and interactive setting. The expansion of linked vehicles and the advancement of autonomous driving technologies are augmenting the complexity of IoV networks. These networks manage substantial data volumes and offer services such as remote diagnostics, road safety notifications, autonomous decision-making, real-time traffic information, and vehicle-to-infrastructure connectivity. Authentication is a crucial responsibility for ensuring the reliability and integrity of IoV networks, as these services depend significantly on secure and efficient communication between vehicles and other entities [1].

Authentication safeguards network resources by permitting access solely to authorized vehicles and users, thereby mitigating risks such as identity impersonation, illicit data access, and man-in-the-middle attacks. Traditional centralized authentication methods are inadequate for Internet of Vehicles (IoV) systems as they often necessitate a singular authority to validate the credentials of each network entity. The risks of single points of failure, heightened computational and communication expenses, and the threat of privacy infringements stemming from the centralized processing and storage of sensitive information are among the disadvantages of these methods [2]. The increasing quantity of linked vehicles in centralized systems

DoI: https://doi.org/10.63949/crinfo.v1i1.004

presents considerable scaling issues, resulting in performance constraints and delays in processing authentication requests.

Decentralized authentication methods are becoming recognized as a more dependable and scalable solution to the challenges faced by IoV networks. A decentralized approach enhances scalability and mitigates the risk of systemic failures by distributing authentication responsibilities throughout the network and eliminating dependence on a singular central authority. Decentralization, however, introduces additional challenges, especially with the safeguarding of privacy and trust. In a decentralized framework, vehicles must verify one another and other entities while safeguarding personal information, including location data, driving behaviors, and identification details. Securing and privatizing authentication in extensive IoV networks poses significant challenges in terms of scalability and efficiency [3].

Federated learning has thus emerged as a viable solution to address the privacy concerns associated with IoV authentication. Federated learning is a decentralized machine learning approach that enables several entities, such as vehicles, to jointly train a global model while preserving the confidentiality of their local data. Rather than transmitting raw data to a central server, each entity constructs a local model utilizing its own data and subsequently transmits the model modifications (parameters) to the central server, where they are aggregated to enhance the global model. This method safeguards privacy by guaranteeing that private data remains within the vehicle and is inaccessible to external entities. Federated learning is especially advantageous in the Internet of Vehicles contexts, where privacy is a significant issue, and vehicles produce substantial data via sensors, cameras, and many sources [4].

Although federated learning mitigates privacy concerns associated with decentralized authentication, it does not intrinsically resolve trust and security challenges within the system. In this instance, blockchain technology serves an extra purpose. A decentralized ledger technology known as blockchain offers an immutable, transparent, and secure method for recording transactions inside a distributed network. In IoV authentication, blockchain is employed to document authentication events, guaranteeing that all transactions are verifiable, immutable, and resistant to manipulation by nefarious entities. Each authentication attempt on the Blockchain is documented as a transaction. It transforms into an immutable record that may be scrutinized at any point subsequent to verifying and incorporating into the ledger. A robust security framework that fosters trust in the authentication process among all entities within the IoV network is created by ensuring the validity and immutability of authentication data [5].

The integration of blockchain technology with federated learning can proficiently resolve issues related to decentralized authentication in the IoV. Federated learning safeguards privacy by retaining sensitive data within the vehicle, whereas blockchain offers a transparent and secure ledger for documenting and authenticating events, enhancing accountability and trust. When integrated, these technologies provide a decentralized, scalable, and privacy-preserving authentication system, ideally suited for the intricate and dynamic characteristics of IoV networks.

The Internet of Vehicles poses distinct issues that complicate authentication compared to conventional networks. Mobility constitutes a primary concern. Vehicles within an Internet of Vehicles (IoV) network are perpetually in motion and frequently engage in simultaneous communication with other entities, including other vehicles, roadside infrastructure, and cloud services. In this dynamic environment, authentication systems must consider sudden changes, intermittent connectivity, and differing levels of trust among entities. Due to autos possessing a limited connectivity range compared to permanent

DoI: https://doi.org/10.63949/crinfo.v1i1.004

infrastructure in conventional networks, prompt and efficient authentication processes are essential to prevent service disruptions.

A significant difficulty is scalability. Internet of Vehicles networks must manage millions of simultaneous authentication requests as the number of linked vehicles increases. Centralized authentication methods depend on a singular authority for request verification, rendering them susceptible to bottlenecks and potential overload, particularly during surges in network traffic. A decentralized method is essential to

share the authentication workload across the network and maintain system performance as the number of vehicles increases.

Privacy is an essential element of the authentication process in the Internet of Vehicles. Vehicles furnish a plethora of sensitive information, encompassing location data, driving behaviors, and personal identification. Centralized systems that store and process data provide substantial privacy concerns due to their attraction for hackers seeking to compromise user information. A decentralized authentication system must safeguard critical data while enabling vehicles to authenticate without disclosing extraneous information to external entities.

Security constitutes a significant impediment. A variety of cyberthreats, such as Distributed Denial of Service (DDoS) attacks, data manipulation, and identity impersonation, can impact Internet of Vehicles networks. An assailant may impersonate a valid vehicle to gain unauthorized access to services or modify authentication data to manipulate system behavior. Consequently, while verifying vehicle IDs, the authentication system must guarantee that all transactions are secure, unaltered, and resistant to malicious attacks [6].

The integration of Blockchain with Federated Learning enhances privacy, scalability, security, and trust in the authentication of Internet of Vehicles. Federated Learning enables vehicles to collaborate in developing a global authentication model while safeguarding the anonymity of their local data, hence enabling distributed model training. This guarantees that essential data is retained within the vehicle, hence significantly diminishing the likelihood of privacy breaches. Federated learning reduces communication overhead and enhances system scalability by transmitting model modifications instead of raw data.

This study will cover the intricate architecture of the proposed system, the particular authentication approaches employed, and the performance assessment of the model for computational cost, communication overhead, and security robustness. The findings demonstrate the efficacy of the proposed solution in resolving the primary issues associated with IoV authentication and underscore its potential extensive applicability in future intelligent transportation systems.

2. RELATED WORK

Blockchain, a decentralized digital ledger, is particularly advantageous for broad applications such as the Internet of Things and the Internet of Vehicles. This is due to the utilization of cryptographic techniques, such as hash algorithms and zero-knowledge proofs, to ensure the immutability of records [7,8]. A blockchain-based approach inside a zero-trust architecture that incorporates a redundant arithmetic incentive mechanism to enhance vehicle authentication at edge servers. The vehicle authentication method for RSUs is straightforward. Babbga et al. [9] introduced an efficient mass authentication method

DoI: https://doi.org/10.63949/crinfo.v1i1.004

enabling the aggregation of many vehicles. RSUs solely verify with the group administrator during inter-member authentication. Upon authentication, the complete vehicle cohort gains access to the vehicular network. Mutual authentication among all group members is essential for the security of this system, albeit at a significant expense. Kumar et al. [10] employed deep learning and blockchain technologies to develop a data interchange method for the Internet of Vehicles (IoV). This method enables secure data sharing inside the Internet of Vehicles (IoV) framework by employing deep learning to identify vulnerabilities in shared data and utilizing blockchain for the mutual authentication of IoV devices. Nonetheless, there exists a considerable authentication burden owing to its substantial dependence on public key cryptographic primitives. Dwivedi S. K. et al. [11] developed an event-sharing protocol for the

Internet of Vehicles utilizing IPFS and blockchain technologies. The protocol employs blockchain technology to facilitate mutual authentication between the cloud server and the vehicle. Nonetheless, it is ill-suited for the vehicle's high velocity and may become a singular point of failure.
Cheng J et al. [12] introduced a blockchain-based collaborative attack detection method that employs Intel Software Protection Extension technology to encrypt the developed attack detection model. A content identifier (CID) is generated and uploaded to the Inter-Planetary File System (IPFS) following the upload of the encrypted model. While the technique does not delineate the matching detection model, it facilitates the rapid dissemination of the detection model, hence enhancing collaborative detection efficacy. Hayat R F et al. [13] proposed a multi-tiered mitigation solution for Distributed Denial of Service (DDoS) assaults utilizing consortium chain and smart contract technologies. This method mitigates DDoS attacks by eliminating malicious devices from IoT ecosystems; nonetheless, it is inadequate against assaults initiated by extensive botnets. Wang et al. [14] developed a deep learning-based verification model to assess the dependability of vehicular communications, compute a vehicle trustworthiness score, and detect malicious vehicles based on the results. Nonetheless, the technique's generalizability is constrained due to its lack of testing on a publicly accessible dataset. Saba T et al. [15] developed an intrusion detection model utilizing a convolutional neural network (CNN) on the BoT-IoT dataset, achieving a detection accuracy of 92.85%, indicating potential for enhancement. To efficiently identify intrusions in IoT networks while adhering to resource limitations, Roy S et al. [16] proposed a dual-layer intrusion detection approach utilizing deep learning and fog computing. The strategic deployment of the deep learning model in the fog cloud infrastructure effectively optimizes resources inside the IoT fog layer. This solution efficiently minimizes IoT resource usage while maintaining the precision of the detection model, despite the detection accuracy being influenced by network quality.

A privacy-centric conditional safe access control system for vehicular ad hoc networks (VANETs) [17]. In contrast to existing methods, our approach does not necessitate the presence of the TA during the vehicleto-RSU verification procedure. Furthermore, our system employs pseudonym approaches to ensure conditional privacy, enabling the monitoring of hostile vehicles while maintaining anonymity for legitimate ones. Both formal and informal security investigations endorse our suggested approach, which has demonstrated resilience against various recognized VANET threats. secure and dependable vehicle-tofacility authentication system (VFAS) [18] that doesn't require a trusted authority's (TA) present presence in real time to function. The car's memory load is significantly reduced because it generates pseudonyms and entire private keys on its own instead of storing them beforehand. In order to ensure

DoI: https://doi.org/10.63949/crinfo.v1i1.004

reliability and anonymity, FN also collects road data from more than 50 different vehicles that has been encrypted using session keys.

The identity and private information of vehicles can be effectively safeguarded during the identification process by existing IoV authentication initiatives. Reconciling resource expenditure with security remains a significant challenge. Moreover, employing ensemble learning approaches for the implementation of intrusion detection models on IoV devices can more efficiently identify hostile activities, thereby mitigating the risk of identity authentication information theft and improving the security of authentication procedures. This is due to the fact that RSUs and vehicles are located in edge environments and are vulnerable to cyberattacks.

3. PRIVACY-PRESERVING AUTHENTICATION MODEL

The proposed authentication security method in the IoV context integrates two advanced technologies, blockchain, and federated learning, to address the unique security and privacy challenges of IoV networks. Federated Learning enhances the effectiveness of a global authentication approach by enabling vehicles to train machine learning models locally while protecting occupant privacy by restricting the transmission of personal data outside the vehicle. This approach preserves anonymity while enabling vehicle identification and authentication through behavioral patterns. Blockchain technology improves authentication by providing an immutable, transparent, and decentralized ledger that records each authentication attempt, preventing fraudulent alteration of authentication data. This approach improves authentication through collaborative learning across distributed vehicles, increasing the overall security of Internet of Vehicles systems. This increases the scalability of the systems as the network expands and their resilience to threats. In addition, blockchain ensures accountability and traceability by documenting each authentication event in an irreversible ledger, thereby promoting transparency and trust within the IoV ecosystem.

Federated Learning is a computational method that protects personal data while facilitating collaboration among devices, including automobiles, to improve model development. Federated Learning enables vehicles to develop authentication models from their own data, including sensor data, driving patterns, and vehicle-specific information. In the context of the IoV, this keeps data on the device and improves privacypreserving authentication.

The key advantage of federated learning for IoV identification is its ability to preserve user privacy by keeping raw data in the vehicle. A global model is created by sending only model adjustments, including weights or gradients, to a central aggregator. The global model is then distributed to each participating vehicle. Our decentralized learning methodology allows anyone to contribute to model training while maintaining their identity.

$w_1, w_2, ..., w_N$: The local models trained on the N vehicles.

w_{global}: The global model, which is the weighted average of local models.

DoI: https://doi.org/10.63949/crinfo.v1i1.004

w_i: The weight vector (parameters) of the local model trained on the i^{th} vehicle.

Local data collection and pre-processing: Each vehicle collects and processes authentication-related data, including driving patterns, sensor readings, and vehicle identification. This data is used to create the unique model of each vehicle. The vehicle maintains the confidentiality of this information and does not share it.

Model initialization: The central server or aggregator can create a global model and distribute it to all vehicles in the network. Based on previous data, this model can be a basic neural network or an alternative machine learning model designed to classify a vehicle's behavior as either legitimate or suspicious.

Local model training: The model is developed using unique data from each vehicle. This training typically involves the vehicle recognizing patterns, including a particular driver's unique driving style (e.g., average

speed, route selection, stopping habits, etc.). The local model's weights and biases are modified based on the data it processes.

Gradient calculation and transmission: After local data training, each vehicle calculates the gradients (model weight modifications) instead of sending unprocessed data to the central aggregator.

$$\Delta_{!"} = w" - w_{\#} \quad (1)$$

Model aggregation: The central aggregator consolidates all changes (gradients or model weights) from each vehicle. A new global model is created by integrating the changes through an aggregation method, such as federated averaging. This aggregation ensures that each local model contributes to a unified global model that can be successfully applied to the entire fleet of vehicles.

$$w_{\$\%\&'(\%} = \frac{1}{N}\sum_{i=1}^{N} w" \quad (2)$$

Global model deployment: The latest consolidated model is distributed to each vehicle and can then be used for authentication. The model is continuously improved through multiple localized training and aggregation iterations performed by the vehicles.

Imagine a scenario where cars wish to authenticate themselves in order to gain access to an intelligent parking system. To verify a vehicle's access request, the system continuously evaluates driving habits and vehicle performance using historical data. Every vehicle generates a localized model to direct common driving practices. By using driving patterns or vehicle identification, the global model is better able to detect anomalous actions, including auto theft or unauthorized entry, particularly when there are more vehicles on the road.

Blockchain is crucial for safeguarding authentication and ensuring unchangeable data inside the Internet of Vehicles (IoV) ecosystem because of its decentralized, transparent, and secure characteristics. Through the recording of every authentication attempt made by a vehicle as a Blockchain transaction, an IoV system guarantees that no one entity may possess or alter the data. Time stamps, authentication results,

DoI: https://doi.org/10.63949/crinfo.v1i1.004

vehicle unique identifiers, and other important information found in every transaction are validated and then combined into blocks. By joining these blocks in a chain and distributing it to every network node, a permanent ledger is produced. Once recorded on the Blockchain, an authentication event cannot be undone, guaranteeing a transparent record of every access attempt and thwarting fraudulent alterations. Because no single entity controls the data and all participants rely on a consensus method to validate transactions, the distributed architecture of blockchain improves system trust. By giving everyone involved—vehicle owners, service providers, and regulatory bodies—access to data at any time, this ensures system integrity against manipulation.

The Internet of Vehicles (IoV) authentication process is enhanced by blockchain's capacity to improve security through Smart Contracts, which are self-executing code that automatically enforces predetermined rules upon the fulfillment of particular criteria. The associated smart contract might allow access to services like charging stations, smart parking, and toll payments if the car's Federated Learning model approves its authentication request. The smart contract may limit access, mark the vehicle for re-authentication, or notify security personnel in the event that an authentication attempt is rejected. By automating the process, smart contracts reduce the possibility of human error and ensure consistent implementation of identity criteria. Additionally, because smart contracts are stored on the Blockchain, they are auditable and unchangeable, guaranteeing adherence to security and regulatory requirements and preventing unwanted changes. The efficiency and security of the IoV system are improved by this automated, trustless authentication standard, which guarantees that vehicles are permitted without the possibility of fraud or unauthorized entry.

Blockchain's capacity to offer quick, safe, and transparent authentication processes is one of its main benefits for IoV authentication. As cars continuously interact with various IoV services, such parking systems and toll booths, blockchain ensures that every identification attempt is processed promptly, reducing delays and improving system performance. Blockchain architecture's ability to eliminate single points of failure improves the system's resistance against cyberattacks including distributed denial of service (DDoS) attacks and data manipulation. By guaranteeing that only valid transactions are entered into the Blockchain, the consensus process safeguards the entire system—even when hacked nodes are present. Any authorized participant may quickly track the history of a vehicle's authentication attempts, spot fraudulent activity, and preserve system integrity thanks to the transparent and verifiable nature of blockchain data. Transparency, security, and decentralization are critical criteria in the quickly developing Internet of Vehicles ecosystem, where a large number of vehicles and devices must safely connect and authenticate without endangering privacy or confidence.

4. PERFORMANCE EVALUATION

The main objectives of evaluating the performance of the proposed Internet of Vehicles (IoV) authentication system that combines blockchain with federated learning are efficiency, scalability, accuracy, security, and privacy protection. Several evaluations are performed in simulated IoV scenarios to compare the proposed method with other sophisticated privacy-preserving strategies and conventional centralized authentication systems. The evaluation includes computation cost, communication cost, and throughput.

The proposed method is significantly more efficient when comparing the computational costs of the VFAS Model with the CPACP Model shown in figure 1. The proposed model exhibits the lowest

DoI: https://doi.org/10.63949/crinfo.v1i1.004

computational cost at 5.1 milliseconds (ms), whereas the CPACP model has the highest at 12 ms, and the VFAS model follows at 7.8 ms. The reduced computing expenses are primarily associated with the increasing integration of Federated Learning with Blockchain, facilitating distributed model training and secure, efficient transaction processing. Blockchain facilitates this through its reduced computational expenses. Federated learning minimizes data transfer and computational demands on centralized servers by implementing local model updates on individual cars, hence decreasing the necessity for centralized data processing. Simultaneously, the Blockchain layer ensures dependable, immutable transaction records at a reduced computational expense using a streamlined consensus method known as Proof of Authority (PoA). The recommended solution is the most computationally efficient for secure authentication inside the Internet of Vehicles ecosystem due to good authentication process management and the scalability of Federated Learning, which significantly reduces response time. Thus, the reduced computational expense of the proposed approach signifies its capacity to provide both efficiency and security, rendering it optimal for real-time Internet of Vehicles applications that require reliable, rapid authentication.

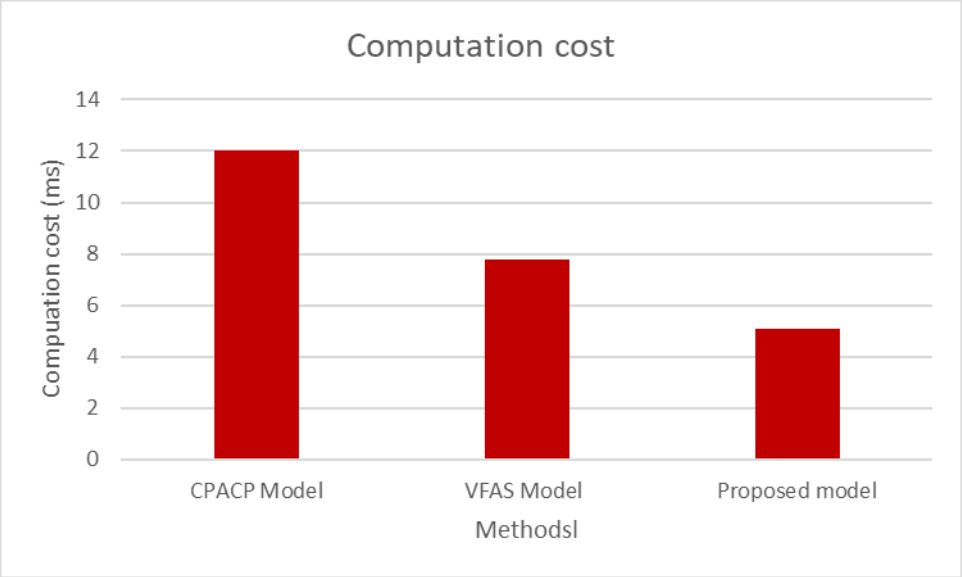

Figure 1: Computation cost analysis

DoI: https://doi.org/10.63949/crinfo.v1i1.004

Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 01 – April 2025

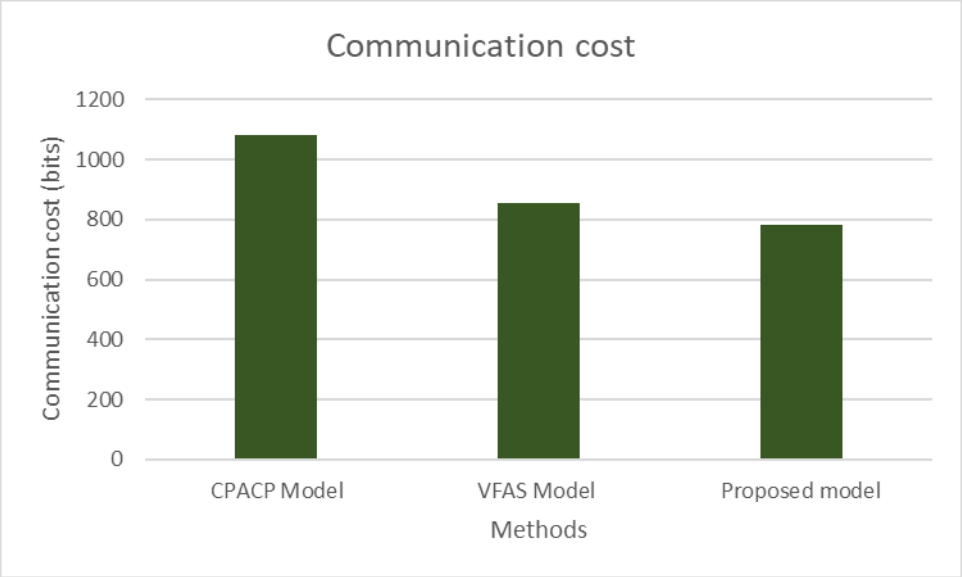

Figure 2: Communication cost analysis

The examination of communication expenses for the proposed VFAS Model and the CPACP Model illustrates the enhancement of data transmission efficiency by the recommended approach shown in figure 2. The proposed model exhibits the minimal communication cost at 783 bits, whereas the CPACP model incurs the maximum cost at 1084 bits, succeeded by the VFAS model. The decrease in communication overhead mostly results from Federated Learning's decentralized architecture, which conveys only model updates rather than raw data between vehicles and the central server. The proposed framework lowers the

amount of data transmitted during authentication by obviating the necessity to convey extensive quantities of sensitive information.

DoI: https://doi.org/10.63949/crinfo.v1i1.004

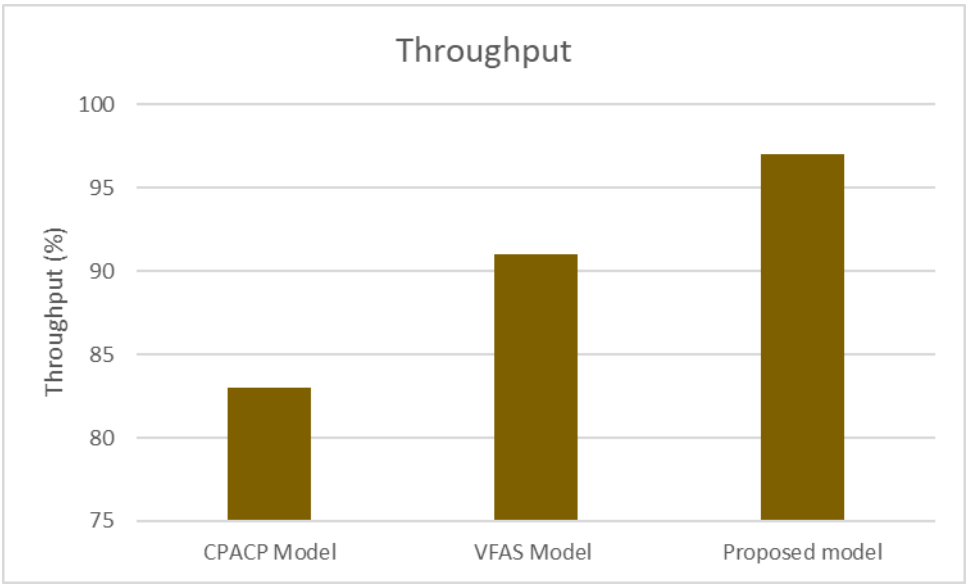

Figure 3: Throughput analysis

The throughput analysis of the CPACP, VFAS, and proposed models illustrates that the recommended technique markedly enhances system efficiency, as shown in Figure 3. The CPACP model attains 83% throughput, but the VFAS model reaches 91%. The suggested solution demonstrates exceptional performance and efficient management of authentication requests in the IoV ecosystem, achieving a throughput of 97%. Federated learning and blockchain provide rapid, decentralized processing and authentication, enhancing throughput by preventing system overload from unprocessed data or prolonged transaction validation delays.

5. CONCLUSION

The integration of blockchain and federated learning in the proposed privacy-preserving distributed authentication system for the Internet of Vehicles provides a secure, efficient, and scalable alternative for vehicle authentication. Federated learning enables vehicles to train local models while preserving private data collaboratively, thus ensuring privacy and achieving high authentication accuracy. Blockchain ensures the confidentiality and permanence of authentication events, prevents unauthorized access, and provides a transparent audit trail. Performance evaluations show that the proposed method significantly reduces transmission and computation costs, while increasing throughput by outperforming traditional centralized authentication methods. In addition, the system demonstrates significant resilience to various intrusions, including data manipulation and model poisoning. This method facilitates the implementation of more secure and private authentication mechanisms in large-scale IoV ecosystems, thus promoting the development of safer and more efficient intelligent transportation systems.

DoI: https://doi.org/10.63949/crinfo.v1i1.004

REFERENCES

[1] Wang X, Zeng P, Patterson N, Jiang F, Doss R. An improved authentication scheme for internet of vehicles based on blockchain technology. IEEE access. 2019 Apr 3;7:45061-72.
[2] Abbas S, Talib MA, Ahmed A, Khan F, Ahmad S, Kim DH. Blockchain-based authentication in internet of vehicles: A survey. Sensors. 2021 Nov 27;21(23):7927.
[3] Bagga P, Das AK, Wazid M, Rodrigues JJ, Park Y. Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. Ieee Access. 2020 Mar 17;8:54314-44.
[4] Hemmati A, Zarei M, Souri A. Blockchain-based internet of vehicles (BIoV): a systematic review of surveys and reviews. Security and Privacy. 2023 Nov;6(6):e317.
[5] Mollah MB, Zhao J, Niyato D, Guan YL, Yuen C, Sun S, Lam KY, Koh LH. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. IEEE Internet of Things Journal. 2020 Oct 2;8(6):4157-85.
[6] Taslimasa H, Dadkhah S, Neto EC, Xiong P, Ray S, Ghorbani AA. Security issues in Internet of Vehicles (IoV): A comprehensive survey. Internet of Things. 2023 Jul 1;22:100809.
[7] Guo J, Liu Z, Tian S, Huang F, Li J, Li X, Igorevich KK, Ma J. TFL-DT: A trust evaluation scheme for federated learning in digital twin for mobile networks. IEEE Journal on Selected Areas in Communications. 2023 Aug 30.
[8] Liu Z, Wan L, Guo J, Huang F, Feng X, Wang L, Ma J. PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks. IEEE Transactions on Vehicular Technology. 2023 Dec 8.
[9] Bagga P, Sutrala AK, Das AK, Vijayakumar P. Blockchain-based batch authentication protocol for Internet of Vehicles. Journal of Systems Architecture. 2021 Feb 1;113:101877.
[10] Kumar R, Kumar P, Tripathi R, Gupta GP, Kumar N. P2SF-IoV: A privacy-preservation-based secured framework for Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems. 2021 Aug 11;23(11):22571-82.
[11] Dwivedi SK, Amin R, Vollala S, Chaudhry R. Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities. Computers & Electrical Engineering. 2020 Sep 1;86:106719.
[12] Cheng J, Yao X, Li H, Lu H, Xiong N, Luo P, Liu L, Guo H, Feng W. Cooperative Detection Method for DDoS Attacks Based on Blockchain. Comput. Syst. Sci. Eng.. 2022 Oct 1;43(1):103-17.
[13] Hayat RF, Aurangzeb S, Aleem M, Srivastava G, Lin JC. ML-DDoS: A blockchain-based multilevel DDoS mitigation mechanism for IoT environments. IEEE Transactions on Engineering Management. 2022 May 13.
[14] Wang S, Hu Y, Qi G. Blockchain and deep learning based trust management for internet of vehicles. Simulation Modelling Practice and Theory. 2022 Nov 1;120:102627.
[15] Saba T, Rehman A, Sadad T, Kolivand H, Bahaj SA. Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering. 2022 Apr 1;99:107810.
[16] Roy S, Li J, Bai Y. A two-layer fog-cloud intrusion detection model for IoT networks. Internet of Things. 2022 Aug 1;19:100557.

DoI: https://doi.org/10.63949/crinfo.v1i1.004

[17] Saleem MA, Li X, Mahmood K, Shamshad S, Ayub MF, Bashir AK, Omar M. Provably secure conditional-privacy access control protocol for intelligent customers-centric communication in vanet. IEEE Transactions on Consumer Electronics. 2023 Oct 16.
[18] Cheng H, Yang J, Shojafar M, Cao J, Jiang N, Liu Y. VFAS: Reliable and privacy-preserving V2F authentication scheme for road condition monitoring system in IoV. IEEE transactions on vehicular technology. 2023 Feb 22;72(6):7958-72

DoI: https://doi.org/10.63949/crinfo.v1i1.004