ARTICLE | Article in Press

Blockchain-assisted IoT-based smart electric vehicle network for secure data sharing and authentication

K. Ambika · R. Gopi · S. Sivagami · B. Suganya

Received: 6 July 2026 / Accepted: 10 September 2026

Abstract

The large number of Electric Vehicles (EVs) now connected to the Internet-of-Things (IoT) network has created numerous obstacles in securing data sharing, managing decentralised authentication, safeguarding privacy and ensuring trust management. However, traditional centralized solutions can be compromised by data manipulation, spoofing, unauthorized user access, and the systems can become vulnerable to single points of failure, potentially reducing the reliability and scalability of intelligent transportation systems. The challenges mentioned above motivate this paper to present a Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL) framework for secure and scalable smart EV networks. Within the proposed framework, PUF-ECC is used to create lightweight and tamper-resistant authentication of vehicles, GATs for complex interaction modelling, Federated Learning (FL) for privacy-preserving distributed trust assessments and Proximal Policy Optimization (PPO) for optimizing vehicle validation and blockchain consensus. It includes three parts: decentralized identity authentication, secure data sharing with intelligent trust and privacy mechanisms, and efficient transaction processing with blockchain consensus optimization. The proposed approach presented in this document was benchmarked against the VeReMi vehicular security dataset as well as various simulated scenarios of a blockchain-based EV network, while also comparing against the ones already existing in the literature: blockchain-based authentication, federated learning and trust management methods. The experimental results showed that all of the existing baseline approaches were outperformed in terms of authentication accuracy (99.2%), attack detection rate (98.7%), data integrity score (99.5%), privacy preservation (98.4%), scalability (97.2%) and transaction throughput (5200 TPS), with a statistical difference ($p < 0.05$). The proposed framework also resulted in an average computation overhead of 41 ms for authentication and consensus operations, making it feasible for real-time applications. The results indicate that BFGRL is a suitable solution that is privacy-protected, efficient and powerful for the intelligent transportation system and next-generation smart electric vehicle system. Experiments conducted in a controlled simulation environment show that BFGRL can effectively improve security, trust management, scalability, and operational efficienssssscy in blockchain-assisted smart EV networks. These results suggest its promising potential for intelligent transportation applications, with further testing with real-world vehicular communication data and field trials being critical research areas.

https://doi.org/10.1038/s41598-026-71684-y

Published online: 18 September 2026

scientific reports

Keywords Blockchain-assisted electric vehicle network · Internet of Things (IoT) · Federated learning (FL) · Graph attention network (GAT) · Proximal policy optimization (PPO) · Secure data sharing and authentication · Internet of vehicles (IoV) · Consensus optimization.p

Introduction

The Internet of Things (IoT), intelligent transportation systems (ITS), and electric vehicle (EV) technologies are rapidly evolving and accelerating the construction of smart electric vehicle networks that enable real-time communication, autonomous decision-making, smart energy management, and vehicle-to-everything (V2X) services[1]. Smart city infrastructure is steadily becoming a reality, as the number of connected EVs, charging stations, roadside units (RSUs), edge servers, and cloud platforms is growing, fostering a new level of transportation efficiency[2]. At the same time, the large amount of sensitive data being exchanged with vehicles (such as charging data, battery status, vehicle identity, driving trajectory, energy traded in the vehicle, etc.) has made the EV ecosystems more susceptible to cyberattacks, unauthorized data access, spoofing, data manipulation, etc.[3]. Thus, it has become one of the most important issues in next-generation intelligent transportation systems (ITS) to provide secure, decentralized, and privacy-preserving communication[4].

Traditional centralized authentication and data management systems are not suitable for modern EV scenarios, as they create single points of failure, lack scalability, incur high communication overhead, and are more vulnerable to distributed denial-of-service (DDoS), replay, impersonation, and insider attacks[5]. Without the need for centralized authorities, blockchain technology has emerged as a promising decentralized solution, offering the following: immutable ledgers, distributed trust management, transparent transaction verification, and tamper-resistant storage[6]. At the same time, Federated Learning (FL) allows them to collaborate on training the model without sharing raw data, thereby protecting user privacy and minimizing communication costs[7]. With the help of blockchain, it has recently been proven that privacy-aware learning, secure vehicular communication, collaborative intrusion detection, and intelligent resource management can be enhanced in Internet of Vehicles (IoV) settings[8].

While significant progress has been made, several limitations remain in current blockchain-based IoV frameworks[9]. Existing solutions focus on either secure authentication, privacy-preserving learning, or intrusion detection, respectively, and lack a comprehensive architecture that can simultaneously address decentralized authentication, dynamic trust evaluation, secure data sharing, adaptive consensus optimization, and large-scale scalability[10]. Moreover, traditional blockchain consensus protocols can generate significant computational load, delay transactions, and reduce throughput, which is not suitable for a highly dynamic vehicular environment[11]. Likewise, current FL frameworks based on existing models remain susceptible to malicious participant selection, model poisoning attacks, inaccurate trust estimation, and inefficient validator management[12]. The use of reinforcement learning in blockchain-assisted vehicular systems for resource optimization has gained traction in recent years, but has not been explored much for intelligent consensus optimization and validator selection in blockchain[13].

Several recent investigations have focused on secure energy management for EV monitoring based on blockchain and machine learning, blockchain-assisted energy consumption prediction based on federated learning, privacy-aware location prediction, blockchain-assisted secure collaborative intrusion detection, malicious node detection, and blockchain-enabled federated reinforcement learning for vehicular communication[14]. However, most of these studies cover only a single optimization goal, and few combine graph-based relationship modeling, intelligent trust computation, adaptive consensus in blockchain, lightweight authentication, and decentralized, secure data sharing in a holistic approach[15]. Thus, it remains a significant research challenge to identify trustworthy vehicles accurately, prevent malicious participation, reduce authentication latency, and increase transaction throughput.

Existing blockchain-based IoV solutions typically address a single aspect of security or optimization and lack a single framework for decentralized authentication, dynamic trust evaluation, privacy-preserving learning, secure data sharing and adaptive consensus optimization. Furthermore, traditional consensus algorithms can lead to computational complexity and transaction delays and may have a limit on how high the number of transactions they can process can be for very dynamic EV environment. Older FL-based solutions are even susceptible to malicious participation, model poisoning, or erroneous trust assessment and ineffective validator selection. The need for such limitations drives the need for an integrated framework that offers lightweight authentication, trustworthy graph-based learning, privacy-preserving collaboration and adaptive blockchain consensus.

To address these challenges, this study presents a secure and trustworthy Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL) approach for data sharing and authentication in smart electric vehicle (eVehicle) networks with IoT support. To address these challenges, the proposed framework fuses Physical Unclonable Function–Elliptic Curve Cryptography (PUF-ECC) for lightweight decentralized authentication, Graph Attention Networks (GATs) for intelligent trust-aware relationship modeling, Federated Learning (FL) for privacy-preserving collaborative model training, and Proximal Policy Optimization (PPO) for adaptive blockchain validator selection and consensus optimization. By integrating these cutting-edge technologies into a single framework, BFGRL aims to improve authentication reliability, secure data communication, trust assessment, and blockchain scalability and computational efficiency while reducing latency and communication overhead. Thus, the proposed framework is a comprehensive and scalable security solution that can address the new challenges of next-generation smart electric vehicle ecosystems by enabling IoT.

The paper's main contributions are to:

i. To achieve decentralized authentication and secure data sharing, a novel Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL) framework is proposed that combines PUF-ECC, GAT, Federated Learning, and PPO.
ii. A smart trust-aware graph attention network and a Federated Learning algorithm can correctly recognize malicious vehicles while protecting privacy and minimizing communication overhead.
iii. An adaptive consensus strategy based on PPO dynamically selects trustworthy validators, which greatly enhances transaction throughput and scalability while reducing computation and authentication latency.
iv. The proposed integrated architecture enhances data integrity, privacy preservation, and secure vehicular communication, leading to reliable, scalable, and trustworthy next-generation electric vehicle networks with IoT.

The remainder of this paper is organized as follows. "Literature survey" section reviews related literature and identifies existing research gaps. "Proposed methodology" section presents the proposed BFGRL methodology. "Results and discussions" section describes the dataset, experimental setup, and performance evaluation. "Conclusion" section concludes the paper with limitations and future research directions.

Literature survey

Secure communication in electric vehicle networks has been considerably improved in recent years thanks to the development of blockchain, Internet of things (IoT), federated learning, and intelligent transportation systems. This literature survey highlights state-of-the-art authentication techniques, secure data sharing, trust management, and blockchain optimization, and also points out existing limitations that draw attention to the proposed integrated BFGRL framework.

To address lightweight, privacy-preserving authentication for the Internet of Vehicles (IoV), Chai et al.[16] proposed CyberChain (Cybertwin-Empowered Blockchain Authentication Framework) (2021). In particular, CyberChain used cybertwin technology in conjunction with blockchain to reduce authentication fees while still keeping the user anonymous in communications with the vehicle. The experimental results showed that the authentication latency, privacy protection, and communication efficiency were reduced. But it lacked intelligent trust evaluation,

adaptive consensus optimization and distributed learning, which hindered scalability in highly dynamic vehicular environments.

To solve the secure authentication problem in edge-integrated IoVs, Shen et al.[17] proposed a BAA (Blockchain-Assisted Authentication) framework. The methodology used was a hybrid approach integrating blockchain and edge computing, aiming to reduce authentication delays and enhance decentralised identity verification. The proposed approach has been implemented to efficiently authenticate the smart card, reducing computational overhead and strengthening communication security. However, it lacked privacy-preserving collaborative learning, dynamic trust management, and intelligent validator selection to enhance the blockchain system's scalability and security against advanced cyberattacks.

To promote secure collection of vehicular data and the exchange of information in a 5G environment, Karim et al.[18] designed a system, BSDCE-IoV (Blockchain-Based Secure Data Collection and Exchange in Internet of Vehicles). The framework was based on distributed storage on a blockchain, verified through cryptographic means for secure data transmission. They found that the results showed improvements in confidentiality, reliable communication, and defence against data tampering attacks. However, the scheme did not include the computation of adaptive trust, federated intelligence, and consensus optimization, which limited its efficient large-scale deployment in heterogeneous IoV infrastructures.

Badshah et al.[19] introduced AAKE-BIVT (Anonymous Authenticated Key Exchange for Blockchain-Enabled Internet of Vehicles), establishing anonymous mutual authentication between communicating vehicles and generating a secure session key. The cryptographic model enhanced user anonymity and authentication efficiency, and protected against replay and impersonation attacks. Experimental results have demonstrated improved security while the computational cost remains acceptable. However, the methodology was geared only towards authentication, not towards aspects such as secure data sharing, intelligent trust evaluation, blockchain scalability, or collaborative intrusion detection mechanisms.

Roy et al.[20] proposed a blockchain-based efficient access control with handover policy (BEACH) to secure access during vehicle mobility in an intelligent transportation system. The protocol combined the Blockchain for continuous authorization between network entities and dynamic handover management. Results showed that handovers were secure and efficient, and that there was less interruption in authentication when it comes to access control. But many other components were not included in the framework, such as federated learning, graph-based trust modelling, adaptive consensus mechanisms, and privacy-aware collaborative intelligence for the next-generation smart vehicular ecosystem.

To enable secure information sharing among IoV participants, Aldweesh[21] proposed the BDAA (Blockchain-Based Data Authentication Algorithm). The algorithm employed blockchain verification and cryptographic authentication to ensure data integrity and thwart any unauthorized data modifications. The experiment demonstrated high performance in authentication accuracy and the secure exchange of information. Although all these features are desirable, the study lacked intelligent identification of malicious nodes, decentralization of trust calculation, adaptive optimization of validators, and privacy-preserving distributed learning.

To achieve scalable, secure vehicular communication, Huang et al.[22] proposed a blockchain-based data-sharing system called MSB-DS (Multi-Sharding Blockchain-Based Data Sharing). The methodology used a sharding approach to divide the distributed ledger into smaller segments, thereby increasing the number of transactions that can be processed per block and reducing communication delays. Experimental results demonstrated improved scalability, faster transactions, and more secure data sharing between nodes. However, there was no intelligent trust learning, decentralized authentication, or federated optimization or reinforcement learning-based consensus management in the proposed model to further enhance network adaptability.

Kumar et al.[23] proposed IoV-6G + (a Blockchain-based secure data collection and Sharing Framework) for the Internet of Vehicles in 6G-assisted communication environments. The concept leveraged blockchain technology to ensure the security of vehicular data transmission and enhance the reliability of communication in ultra-low-latency networks. The results showed improvements in security, resource efficiency, and proper information sharing. However, the framework has not taken into account graph-based relationship learning, adaptive trust

assessment, federated privacy preservation and intelligent consensus optimization under the highly dynamic vehicular scenario.

To detect malicious participants in fog-cloud-equipped IoV, Bandarapu et al.[15] proposed BFL-MND (Blockchain-Based Federated Learning Framework for Malicious Node Detection). Distributed detection models were trained via federated learning, and communication and model aggregation were ensured via blockchain. Experiments showed that malicious node detection accuracy improved and collaborative security was enhanced. But the framework mainly focused on intrusion detection, without incorporating lightweight authentication or graph-attention-based trust learning with adaptive blockchain consensus optimization.

To facilitate cross-domain authentication among heterogeneous IoV without certificate management, Wang et al.[24] proposed BCACDA (Blockchain-Based Certificateless Anonymous Cross-Domain Authentication). The certificateless cryptographic mechanism increased anonymity, reduced the number of certificates, and improved the efficiency of authentication across multiple trust domains. The results of the experiments confirmed the good security and communication efficiency. However, it lacked smart trust-aware learning, secure distributed data sharing, reinforcement learning-based validator selection, and privacy-preserving collaborative optimization.

Wei et al.[25] introduced GTTM-DPoW (Game Theory and Trust Management-Driven Dynamic Proof-of-Work), which aims to enhance blockchain consensus mechanisms through trust evaluation and dynamic mining strategies. The methodology combined game theory with trust-aware Proof-of-Work consensus to enhance security and resource allocation in the blockchain. The results showed higher consensus efficiency and greater tolerance to malicious attacks in mining. The framework, however, didn't include federated learning, graph neural network-based trust computation, lightweight decentralized authentication, and comprehensive secure data-sharing mechanisms for IoV ecosystems.

Almazroi et al.[26] focused on the rising problem of Distributed Denial-of-Service (DDoS) attacks in vehicular networks with 5G communications, which affects the reliability of the communication system and the availability of the services. This paper suggests an authentication and mitigation scheme based on a Chebyshev polynomial to identify and block malicious traffic and ensure secure communication. Experimental results showed that attack mitigation performance increased, communication overhead decreased, and authentication performance was improved. Concepts like collaborative learning via privacy-preserving trust management and blockchain integration were not taken into account in the framework.

Almazroi et al.[27] primarily discussed secure authentication methods used in 5G-enabled vehicles with a blockchain environment, which face challenges due to the use of a centralized authentication approach that causes Latency and security challenges. The authors suggested a new fog computing-assisted blockchain authentication framework, called FCA-VBN, for efficient mutual authentication and secure key establishment. The scheme was successfully implemented with reduced computation and communication complexity and it was resistant to common attacks in authentication. However, it lacked adaptive trust evaluation, federated intelligence, and dynamic consensus optimisation for large vehicular networks.

Almazroi et al.[28] focused on how difficult it is to manage certificates, and how long it takes to get authentication working in 5G-enabled vehicular fog computing environments. Realized an efficient certificateless authentication (ECA-VFog) system to achieve mutual authentication between the user and the fog computing system without maintaining certificates. Security analysis revealed that it was immune to impersonation, replay and forgery attacks, and the performance analysis indicated that the computation and communication overhead was reduced. However, it didn't include features such as blockchain-based decentralized validation, trust-aware decision-making features, or intelligent attack detection.

Almazroi et al.[29] studied privacy protection and authentication issues in the 5G based vehicular Fog Computing systems in the presence of quantum computing attacks. The proposed L-CPPA used lattice-based cryptography to provide conditional privacy preservation and quantum-resistant authentication. Experimental results showed good security with good computational efficiency and communication cost. The framework, however, was not geared toward distributed and federated learning, graph-based trust modeling and blockchain consensus optimization for scalable ITS.

Al-Shareeda et al.[30] introduced an authentication solution that is suitable for emergency communication scenarios in 5G-supported vehicular fog computing, where the need for prompt and secure authentication is particularly crucial to disseminate messages in a timely manner. The scheme, using the concept of Chebyshev polynomial cryptography, provided for lightweight authentication with low computational complexity and resistance to common security attacks. Experimental assessment showed decreased authentication delay and enhanced the effectiveness of the communication. The strategy, however, does not tackle decentralized trust management, blockchain-based transaction verification, and reinforcement learning-based adaptive decision optimization.

Most previous work focuses on solving one or more of the aforementioned problems separately, such as authentication, secure data sharing, intrusion detection, access control, blockchain consensus, and federated learning. Most frameworks do not include a unified framework that can offer lightweight decentralised authentication, intelligent trust computing, privacy-preserving collaborative learning, and adaptive optimisation of the blockchain. In addition, most current methods fail to leverage graph neural networks to capture intricate vehicular interactions and reinforcement learning to dynamically optimize the selection of validators. The proposed Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL) framework, on the other hand, brings together PUF-ECC-based authentication, Graph Attention Networks (GAT) for trust-aware relationship modeling, Federated Learning (FL) for privacy-preserving distributed intelligence, and Proximal Policy Optimization (PPO) for adaptive blockchain consensus. A comprehensive integration that enhances the reliability of authentication, accuracy of trust evaluation, transaction throughput, scalability, privacy preservation and secure data sharing for the next generation of smart electric vehicle networks empowered with IoT.

Proposed methodology

The proposed framework, named Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL), synergistically combines the decentralization of blockchain technology, lightweight hardware-assisted authentication, graph neural learning, federated intelligence, and deep reinforcement learning into a single end-to-end working framework, thereby providing a unified cyber-physical security architecture for next-generation Internet of Things (IoT)-enabled Smart Electric Vehicle Networks (SEVNs). The ultimate goal of the proposed methodology is to address, simultaneously, the core issues of identity management, trust generation, secure communication, privacy protection, scalable consensus, and network optimization in a smart way within highly dynamic vehicular environments. Unlike traditional security system architectures that treat authentication, trust evaluation, blockchain management, and communication optimization as independent modules, BFGRL adopts an interconnected multi-layer structure in which each security module interacts with other modules and shares knowledge with subsequent decision-making to enhance global system intelligence. Firstly, all the distributed network entities such as electric vehicles (EVs), Roadside Units (RSUs), Charging Stations (CSs), Mobile Edge Computing (MEC) servers, blockchain validator nodes, cloud controllers and utility grid infrastructures are connected by Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Grid (V2G) communication protocols, allowing the real-time acquisition of heterogeneous vehicular, communication, and energy-related information. Later, by combining Physical Unclonable Functions (PUFs) and Elliptic Curve Cryptography (ECC), decentralized identity management is achieved, where each physical identity of a hardware device is generated in an unclonable manner and authenticated each time it is used using computationally efficient ECC. Once authentication is successful, authenticated communication relationships are modeled as a dynamic weighted graph, and Graph Attention Networks (GATs) are used to learn complex spatial dependencies and communication behaviors to obtain adaptive trust representations. Figure 1 illustrates the integrated architecture and operational workflow of the proposed BFGRL framework.

The proposed system unites PUF-ECC, GAT, Federated Learning and PPO into a unified architecture that is able to resolve the intertwined security, privacy, learning and consensus issues of smart electric vehicle networks under Internet of Things (IoT) infrastructure. PUF-ECC provides hardware-bound authentication, GAT learns

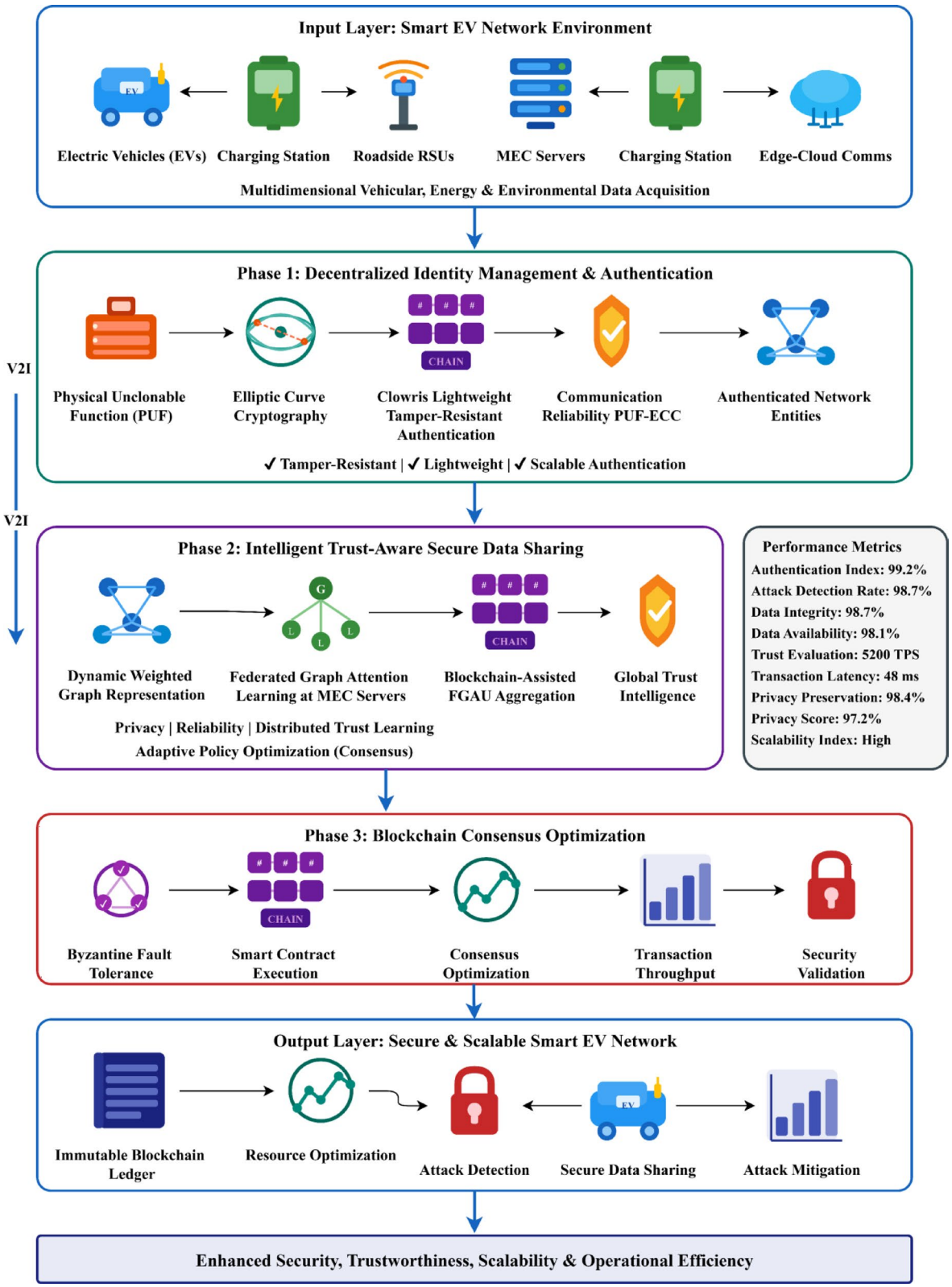

Fig. 1 Multi-layer architecture of the proposed blockchain-assisted federated graph reinforcement learning framework

the dynamic relationship between heterogeneous network entities, FL provides privacy-preserving collaborative learning, and PPO optimizes which consensus policy is used on the blockchain according to the network conditions. Combined, these parts deliver an all-encompassing solution that helps secure authentication, privacy of data and information, learning capabilities for graphs, the efficiency of the consensus processes, scalability, and greater trust of the EV charging ecosystem.

At the start, the framework starts with the IoT entities, which are of different types: electric vehicles (EVs), charging stations, roadside units (RSUs), edge servers and cloud infrastructures. The data gathered from the vehicles and networks undergoes authentication and trust-management by the Puf-ECC layer for lightweight device authentication and the blockchain layer for decentralized and tamper-resistant trust. The authenticated entities and their interactions are depicted as a dynamic graph, and then learnt through Graph Attention Networks (GATs) on top of the graph to generate trust-aware relationships and to detect potentially malicious entities. Federated Learning (FL) refers to the approach of training the model in different parts of the network without sending the raw data of EVs to the MEC/edge nodes. The learned graph and trust information is then passed on to a consensus/validator policy selection module based on PPO, which flexibly chooses a suitable consensus/validator policy to achieve a trade-off among the consensus/validator policy's throughput, energy/processing usage, latency, processing cost, and fairness in different network conditions and optimization goals. The chosen consensus mechanism facilitates safe transactions on the blockchain and authorizes information sharing. The inherent workflow finally boosts up the security of authentication, integrity of data, protection of privacy, trustworthiness, scalability and efficiency of operations in the EV-IoT network.

To protect user privacy and avoid central collection of vehicular data, Distributed MEC servers can jointly and collaboratively train graph-based trust models via Federated Learning (FL), where only encrypted model parameters are shared via blockchain-assisted aggregation, while the raw vehicular data remain locally protected. Moreover, smart contracts with blockchain technology provide an irrevocable record of communications, decentralized access control and auditability throughout the communication process. Finally, a Proximal Policy Optimization (PPO)-based reinforcement learning agent constantly monitors the operational conditions of the blockchain and dynamically allocates the validators, schedules consensus and secure data-sharing strategies to maximize the transaction throughput, minimize the consensus latency, reduce energy consumption, ensure fairness of validators and increase resilience against malicious attacks. The proposed BFGRL framework combines blockchain immutability, federated privacy preservation, graph-based trust intelligence, and reinforcement learning (RL)- driven adaptive optimization, and can create a highly scalable, self-adaptive, and resilient decision-making ecosystem to support secure autonomous electric mobility, intelligent transportation systems, and future large-scale smart city infrastructures.

The proposed framework combines PUF with ECC to provide an authentication mechanism for the EVs and charging entities, that is bound to the physical hardware. While students enroll, a random challenge is sent to PUF, which will generate a random response that is unique to the device. The raw PUF response is subject to variations caused by environmental and ageing effects, so that error correction operations are performed and helper data is created for faithful reconstruction of the responses. The helper data doesn't contain the real PUF secret. After the subsequent authentication, the same challenge is reused to generate a new PUF response and the helper data is used to obtain a secure response. A cryptographic hash/KDF takes the reconstructed response and transforms it to something that is cryptographically distinct from the key. This secret is permanently attached to the ECC credentials of the device and is needed for ECC-based authentication. Both the device and verifier each possess public and private keys for ECC, and the device authenticates a message using its PUF private key and a secret derived from its PUF, which is checked by the verifier using his/her ECC public key. Verifying is successful when the cryptographic identity and hardware-specific identity are verified. The authenticated result is then integrated with the trusted and transaction management layer, which provides an integrated blockchains solution. If you add hardware level uniqueness, efficient public-key authentication, and the tamper-resistant recording and trust management of blockchain, it's easy to see why some users are beginning to regard this as a complete solution.

The proposed architecture is an integrated solution, where the authentication and trust management, privacy preserving and consensus optimization are solved together, to ensure secure and intelligent EV-IoT networking. PUF-ECC realizes efficient hardware-level validation and management of trustworthiness, and GAT-based graph learning analyzes interactions and facilitates dynamic trust management between heterogeneous entities in the network. With Federated Learning, the sensitive data is kept at the local edge devices instead of sending across all the sensitive information, only an update to the model is transferred. Known as "blockchain consensus optimization", PPO optimizes the selection of blockchain circumstances based on the environment and transaction situation. These mechanisms implemented within the blockchain-assisted framework facilitate secure authentication, trustworthy communication, privacy-conscious learning, and efficient consensus operation, while securely assuring message confidentiality and privacy protection.These mechanisms allow for secure authentication, trusted communication, privacy-oriented learning, and effective operation of the consensus mechanism within a single attempt to ensure the confidentiality and privacy of messages.

Smart electric vehicle network initialisation and data acquisition using IoT

The proposed Blockchain-enabled Federated Graph Reinforcement Learning (BFGRL) framework during its initialization phase constructs a distributed smart electric vehicle (EV) ecosystem with Internet-of-Things (IoT) nodes, which can support secure, scalable and intelligent energy management. This stage includes various heterogeneous cyber-physical components such as electric vehicles (EVs), Roadside Units (RSUs), Charging Stations (CSs), Mobile Edge Computing (MEC) servers, cloud controllers, blockchain validator nodes, utility grid infrastructures and intelligent transportation management systems, which are all connected in a single communication system. All modules (components) continuously produce multidimensional information on physical conditions of operation and communication behaviour. Battery State-of-Charge (SoC), Battery State-of-Health (SoH), charging current, battery voltage, remaining driving range, energy consumption rate, GPS information, velocity, acceleration, route trajectory, charging demand and vehicle identification information are periodically measured by vehicle-side IoT devices. At the same time, roadside infrastructures monitor traffic density, environmental conditions, charging station occupancy, the quality of the wireless channel, packet transmission delay, received signal strength, utilization of the communication bandwidth and network congestion statistics. These diverse observations are passed on to each other via Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Grid (V2G) and Infrastructure-to-Cloud (I2C) communications, and thus establish a collaborative sensing environment that is constantly updated with both mobility data from the vehicles and communication network data. Figure 2 illustrates the distributed IoT sensing, data preprocessing, and dynamic communication graph construction process.

Heterogeneous data generated by EVs and IoT entities, including SoC, SoH, vehicle and energy information, GPS/location, velocity, route, packet delivery ratio (PDR), RSSI, latency, vehicle identification, and timestamp information, are first collected at the input layer. The data preprocessing pipeline sequentially performs verification, missing-value estimation, temporal synchronization, duplicate removal, and feature retention to produce a consistent feature representation. The processed local features are stored at MEC servers and used to construct a dynamic interaction graph $G = (V, E, X)$ where authenticated EVs and other network entities such as RSUs, roadside infrastructure, charging stations, and MEC servers constitute the graph vertices. Edges are dynamically established according to interaction characteristics such as spatial proximity, RSSI, trust level, latency, and energy similarity. The resulting weighted adjacency representation captures the strength of interactions between entities and provides the input for subsequent GAT-based graph learning, trust verification, federated intelligence, and reinforcement-learning-based optimization. Thus, Fig. 2 illustrates the transformation of heterogeneous raw IoT data into a structured, authenticated, and dynamically weighted graph representation used by the proposed BFGRL framework.

Assume a heterogeneous graph as a representation of the IoT-enabled smart EV network that is distributed $G_t = (V_t, E_t, \mathbf{X}_t)$. The network entities V_t consist of all the network entities such as vehicles, RSUs, MEC servers,

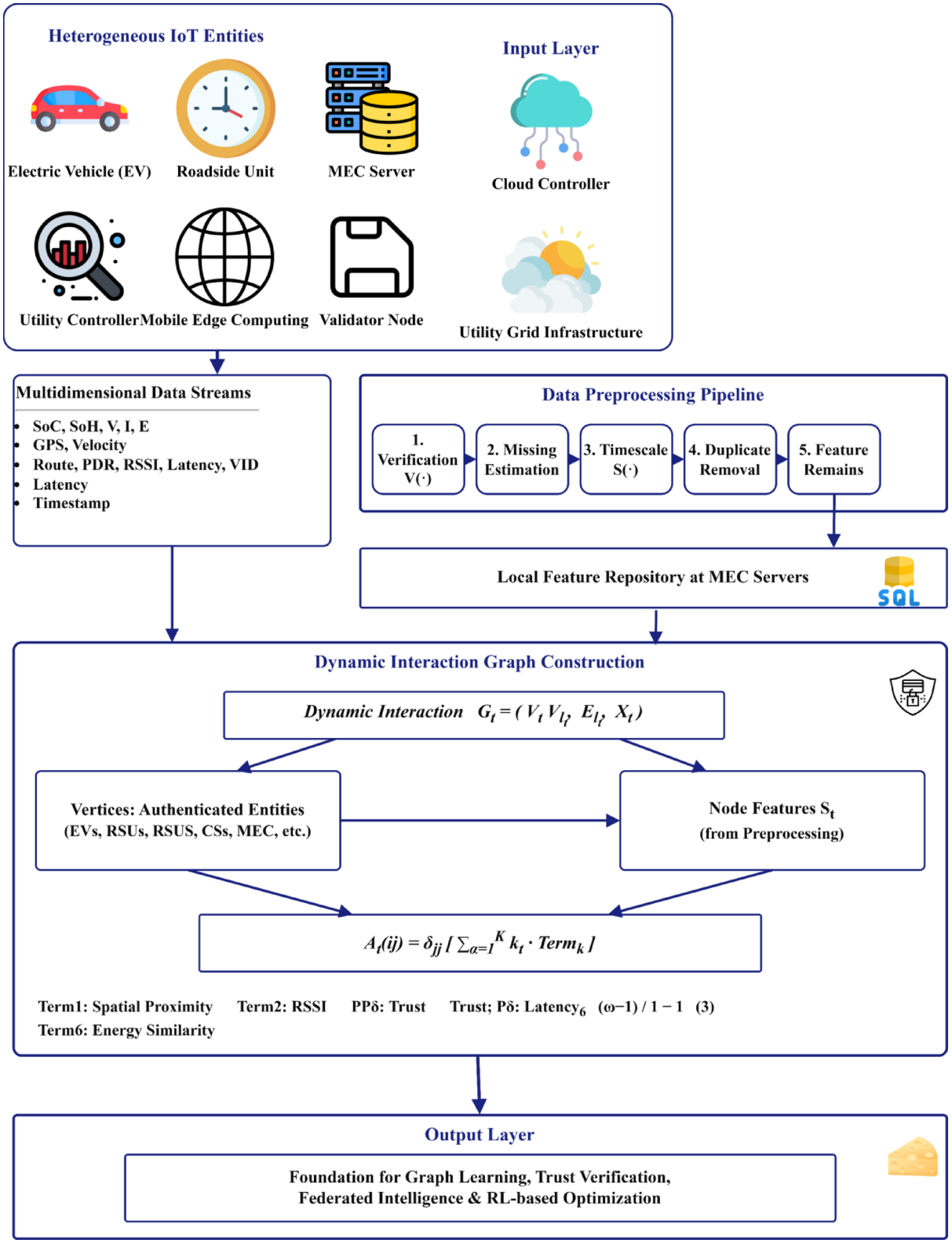

Fig. 2 Smart EV network initialization and distributed IoT data acquisition

charging stations, blockchain validators, cloud nodes and grid infrastructures at time t, the communication links E_t are dynamically changing communication links between multiple network entities through the interactions between V2V, V2I and V2G, MEC, blockchain validators and cloud nodes, and $\mathbf{x}_t$ represents a multidimensional feature matrix of each node. The entire node feature representation is given as Eq. 1:

$$\mathrm{X}_t = \begin{bmatrix} \mathrm{x}_1 \\ \mathrm{x}_2 \\ \vdots \\ \mathrm{x}_N \end{bmatrix} = [\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_N]^T \tag{1}$$

where

$$\mathrm{x}_i = [SoC_i, SoH_i, V_i, I_i, E_i, PDR_i, RSSI_i, BW_i, L_i, GPS_i, VID_i, T_i, \ldots].$$

$\mathbf{x}_t$ is the complete heterogeneous feature matrix of the IoT-enabled EV network, and N represents the total number of participating entities with $\mathbf{x}_i$ being the multidimensional feature vector of the $^{\text{th}}$ node of the network, consisting of the following features: SoC, which stands for battery State-of-Charge; SoH, which stands for battery State-of-Health; V, which stands for charging voltage; I, which stands for charging current; E, which stands for instantaneous energy consumption; PDR, which stands for packet delivery ratio; $RSSI$, which stands for received signal strength indicator; BW, which stands for available communication bandwidth; L, which stands for communication latency; GPS, which stands for geographical location coordinates; VID, which stands for authenticated vehicle identity; and T, which stands for timestamp information for temporal synchronization purposes. By representing energy characteristics, communication behavior, mobility patterns, and cybersecurity attributes in a multidimensional framework, the BFGRL framework can describe the entire cyber-physical transportation environment.

Raw IoT observations are received from spatially distributed sensing devices under a wide variety of communication conditions, and these observations often include missing measurements, duplicate packets, inconsistent timestamps, noisy sensor measurements, and abnormal communication records. Therefore, there is a full data-preprocessing pipeline in place before dissemination at the edge gateways. At the first stage, missing numeric attributes are filled using a neighborhood-aware interpolation method, and corrupted communication packets are discarded after checking the packet's cyclic redundancy. Later, timestamp synchronization allows measurements taken asynchronously by different sensing devices to be aligned in a shared time frame. Feature normalization converts heterogeneous variables with different physical units into a numerical range that can be compared, thereby avoiding scale dominance in graph learning. Observations are deduplicated using a hash-based verification mechanism, while noisy sensor measurements taken in an unstable wireless communication environment are suppressed using statistical outlier suppression. The entire preprocessing operation can thus be symbolically represented as Eq. 2:

$$\tilde{X}_t = N(\mathcal{D}(\mathcal{S}(\mathcal{M}(\mathcal{V}(X_t))))) = \frac{\mathcal{D}(\mathcal{S}(\mathcal{M}(\mathcal{V}(X_t)))) - \min(\mathcal{D}(\mathcal{S}(\mathcal{M}(\mathcal{V}(X_t)))))}{\max(\mathcal{D}(\mathcal{S}(\mathcal{M}(\mathcal{V}(X_t))))) - \min(\mathcal{D}(\mathcal{S}(\mathcal{M}(\mathcal{V}(X_t)))))} \tag{2}$$

Here, $\tilde{\mathbf{x}}_t$ is the preprocessed feature matrix that is used for further intelligence modules, $\mathcal{V}(\cdot)$ is the communication packet verification, $\mathcal{M}(\cdot)$ is the missing-value estimation, $\mathcal{S}(\cdot)$ is the timestamp synchronization, $\mathcal{D}(\cdot)$ is to remove duplicated observations and communication inconsistencies, and $min(\cdot)$ and $max(\cdot)$ are for the minimum feature value and maximum feature value respectively computed within the corresponding sensing dimension $\mathcal{N}(\cdot)$. This sequential preprocessing approach significantly increases feature consistency, improves numerical stability in graph optimization, and reduces communication uncertainty before decentralized edge intelligence.

After preprocessing, the refined observations are sent to the closest Mobile Edge Computing (MEC) server, which builds local feature repositories for decentralized analytics with minimal communication latency. The BFGRL framework leverages edge computing to alleviate the backbone communication burden, speed up local inference, and protect user privacy, since data can be stored locally. At the same time, the communication

interactions between the vehicles, charging stations, RSUs, MEC servers, blockchain validators, and the utility infrastructure are converted into a continually changing dynamic interaction graph. During each communication, an edge is created whose weight is based on the quality of the communication, the spatial proximity, the similarity of the mobility, the trust level, the reliability of packets and the characteristics of the energy exchange. Since vehicles enter and leave the transportation network, charging requests are generated, wireless links change, and mobility trajectories fluctuate, leading to a constantly changing graph topology. Mathematically, it is represented as a Dynamic Adjacency, as shown in Eq. 3.

$$\mathrm{A}_t(i,j) = \delta_{ij}\left[\begin{array}{l} \omega_1 \exp\left(-\dfrac{\left\|Loc_i - Loc_j\right\|^2}{2\sigma_l^2}\right) + \omega_2 \dfrac{RSSI_{ij}}{RSSI_{\max}} + \omega_3 PDR_{ij} \\ +\omega_4 Trust_{ij} + \omega_5 \exp\left(-\dfrac{|L_i - L_j|}{L_{\max}}\right) + \omega_6 Sim\left(E_i, E_j\right) \end{array}\right], \sum_{k=1}^{6} \omega_k = 1 \tag{3}$$

where $\mathbf{A}_t(i,j)$ is the dynamic adjacency weight between nodes and j, δ_{ij} should be 1 if the nodes can communicate and 0 otherwise, Loc_i and Loc_j are the geographical coordinates of nodes and j, respectively, σ_l is a spatial neighborhood influence term, $RSSI_{ij}$ is the received signal strength between communicating nodes, $RSSI_{\max}$ is the maximum measurable signal strength, PDR_{ij} is the packet delivery ratio, $Trust_{ij}$ is the initial communication trust score, L_i and L_j are communication latencies, $L_{\max}$ is the maximum acceptable communication latency, $Sim(E_i, E_j)$ is the energy consumption similarity between interacting nodes, and $\omega_1, \omega_2, \ldots, \omega_6$ are the adaptive weighting coefficients that satisfy the normalization constraint. The dynamic interaction graph can precisely model the evolving cyber-physical relations in the smart EV ecosystem and serves as the basis for subsequent graph representation learning, blockchain-based trust verification, federated intelligence, reinforcement-based decision optimisation, anomaly detection, and secure energy management, as proposed in the BFGRL framework.

Decentralized identity management and blockchain authentication based on PUF-ECC

Upon launching the distributed IoT-enabled smart electric vehicle (EV) ecosystem, the proposed Blockchain-based Federated Graph Reinforcement Learning (BFGRL) framework provides a decentralized identity management mechanism to enable lightweight yet highly secure authentication for all entities involved. The method proposed is not a traditional Public Key Infrastructure (PKI) with centralized Certificate Authorities (CA) and insecure repositories of credentials, but instead uses the intrinsic randomness of the hardware manufacturing process to create an unclonable identity that is impossible to duplicate, clone, or forge. Each EV, charging station, roadside unit (RSU), Mobile Edge Computing (MEC) server, blockchain validator, and utility gateway has an embedded silicon-based PUF circuit that is microfabricated, resulting in unique challenge-response pairs (CRPs). As these variations result from unavoidable imperfections in semiconductor manufacturing processes, it is not possible to reproduce the same responses from the same hardware, even by the original hardware manufacturer, thereby providing an immutable hardware root of trust. Figure 3 illustrates the PUF-ECC-assisted decentralized identity management and blockchain authentication mechanism.

At enrollment, every device is given a random challenge vector, and the hardware response is stored as the device's fingerprint and subsequently error-corrected and entropy-enhanced to achieve better consistency in the face of changes such as temperature, power supply voltage, and device aging. The whole PUF identity generation process is mathematically modeled as Eq. 4:

$$R_i = ECC_{\mathrm{corr}}\left(PUF\left(C_i\right)\right) = ECC_{\mathrm{corr}}\left(\phi\left(\sum_{k=1}^{m} \alpha_k C_{ik} + \sum_{k=1}^{m}\sum_{l=1}^{m} \beta_{kl} C_{ik} C_{il} + \eta_i\right)\right) \tag{4}$$

where R_i is the corrected PUF response generated for the th network entity, $PUF(\cdot)$ is the physical unclonable function, $C_i = [C_{i1}, C_{i2}, \ldots, C_{im}]$ is the challenge vector applied, containing m challenge bits, α_k and β_{kl} are first-order

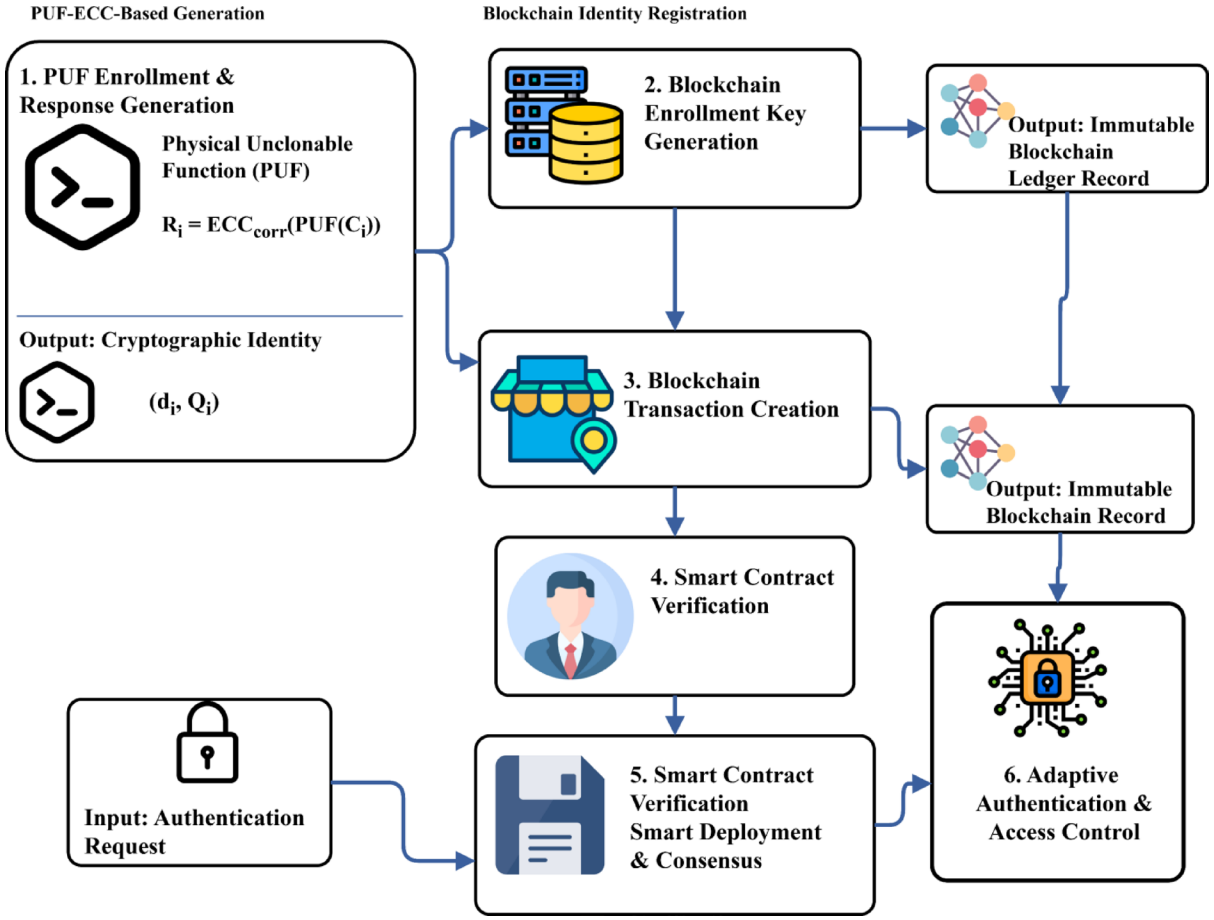

Fig. 3 PUF-ECC-enabled secure identity registration and decentralized authentication

and higher-order delay coefficients introduced during semiconductor fabrication, $\phi(\cdot)$ is the nonlinear switching behavior of the PUF architecture, and η_i is environmental noise, $ECC_{corr}(\cdot)$ is the error-correcting encoder that reconstructs stable responses from noisy measurements. The resulting response is a hardware-based cryptographic fingerprint with very high entropy and with no need for the stored secret keys to be known, which could be susceptible to physical extraction attacks.

After PUF enrollment, the corrected hardware fingerprint is used in conjunction with Elliptic Curve Cryptography to create lightweight asymmetric cryptographic credentials that have the same security as traditional RSA credentials, but with significantly shorter key lengths and lower computational overhead. The stable PUF response is first fed into a secure cryptographic hash function to obtain a uniformly distributed private key scalar, and then a public key is derived by elliptic curve point multiplication over a finite prime field. The entire ECC key generation process is presented as follows in Eq. 5:

$$d_i = (Hash\,(R_i||VID_i||T_i||N_i)\,\mathrm{mod}n) + 1$$

$$Q_i = d_i G = \underbrace{G + G + \cdots + G}_{d_i \text{ times}} = \sum_{k=1}^{d_i} G = (x_i, y_i) \tag{5}$$

The private ECC key generated for the i^{th} entity, denoted as d_i, is used to generate the corrected PUF response R_i. $Hash(\cdot)$ is a secure cryptographic hash function; VID_i is a unique identifier of the vehicle or device; and T_i is a registration timestamp. A randomly generated nonce N_i is used to generate the corresponding public key $Q_i = (x_i, y_i)$,

where (x_i, y_i) are the affine point coordinates on the elliptic curve of order n with generator point G. The permanent storage of secret keys is avoided, and PUF responses are generated in real time for authentication, minimizing memory extraction, firmware compromise, and side-channel attacks.

Once the cryptographic identity is created, all relevant registration data—such as public keys, digital certificates, device metadata, and registration data—is encapsulated in blockchain transactions and permanently registered using the smart contracts of the decentralized blockchain. Every blockchain transaction consists of cryptographic hashes that connect old ledger states to new identity records and are completely immutable and traceable. This can be written as the registration transaction in Eq. 6:

$$\begin{aligned} TX_i =& Hash\left(PrevHash||VID_i||Q_i||Cert_i||Meta_i||TS_i||Sig_i\right) \\ =& Hash\left(PrevHash||VID_i||Q_i||Geo_i||Role_i||Energy_i||TS_i||Sig_i\right) \end{aligned} \tag{6}$$

TX_i is the blockchain identity registration transaction, $PrevHash$ is the previous blockchain block's hash, VID_i is the authenticated device identity, Q_i is the public key from the ECC, $Cert_i$ is the issued digital certificate, $Meta_i$ is additional registration information, Geo_i is geographical information about the registration, $Role_i$ is the functional role of the entity (EV, RSU, MEC, validator, charging station), and $Energy_i$ is energy profile information. TS_i is the timestamp of the blockchain to record the transaction time, Sig_i is the authority signature of the identity registration, and $Hash(\cdot)$ is the digest of the transaction that is placed in the distributed ledger and cannot be modified. As each identity registration is permanently stored in the blockchain consensus, it is impossible for any entity to maliciously modify, delete, or replace any credential or identity.

Each participating vehicle that wants access to the network includes a secure authentication request that includes a timestamp, a nonce, a session ID, a blockchain ID, and a digital signature created with its ECC private key. The smart contract independently checks the integrity of the requests: whether the signature is correct, whether the request is not too old (timestamp is not too old), whether the nonce is unique, whether the entity is registered on the blockchain, and whether there is no replay attack. The whole authentication verification process can be depicted as Eq. 7:

$$\begin{aligned} Auth_i =& Verify_{ECC}\left(Q_i, Sig_i, M_i\right) \cdot \delta\left(T_{\max} - |T_{cur} - TS_i|\right) \\ & \cdot \delta\left(N_i \notin N_{\text{used}}\right) \cdot \delta\left(VID_i Ledger\right) \cdot \delta\left(Session_i = Valid\right) \end{aligned} \tag{7}$$

where $Auth_i$ is the authentication decision made for entity , $Verify_{ECC}(\cdot)$ is a digital signature verification process for ECC, Q_i is the public key, Sig_i is the received digital signature, M_i is the authentication message, T_{cur} is the current time in the blockchain, TS_i is the transmitted timestamp, $T_{\max}$ is the maximum acceptable time delay for authentication, N_i is the received nonce, N_{used} is the blockchain-maintained repository of nonces to prevent replay attacks, VID_i is the registered identity, Ledger is the blockchain identity database, $Session_i$ is the session identifier, and $\delta(\cdot)$ is a binary validation function that returns one only when the corresponding security constraint is met. It is a multi-factor verification system that will also prevent replay attacks, timestamp manipulation, stale authentication requests, identity spoofing, unauthorized credential reuse, and session hijacking.

Upon successful authentication, the smart contract issues a cryptographically verifiable authorization token specifying the level of communication access the successfully authenticated participant will have. These permissions determine whether the entity can start charging transactions, exchange V2V messages, use the MEC's computational resources, join federated learning, or submit blockchain transactions. The final access authorization policy has the following mathematical expression in Eq. 8:

$$\begin{aligned} Access_i =& Auth_i \cdot \left[w_1 Trust_i + w_2 \text{Reputation}_i + w_3 Policy_i + w_4 Role_i\right] \\ & + w_5 Risk_i^{-1} \times \exp\left(-\frac{Latency_i}{L_{\max}}\right) \end{aligned} \tag{8}$$

where $Access_i$ is the final network access score given to entity , $Auth_i$ is the authentication result obtained from Eq. (7), $Trust_i$ is the blockchain trust score, $Reputation_i$ is the accumulated historical reputation, $Policy_i$ is the score

of compliance with policies, $Role_i$ specifies the authorization privileges according to functional responsibilities, $Risk_i$ is the estimated security risk level, $Latency_i$ is the current communication latency, $L_{\max}$ is the maximum acceptable latency threshold, and w_1, w_2, w_3, w_4, w_5 are adaptive weighting coefficients with $\sum_{k=1}^{5} w_k = 1$. This adaptable authorization mechanism makes it possible to dynamically manage the accessibility of resources in the BFGRL framework based on the authenticated level of trustworthiness, operational behavior, communication quality and blockchain consensus, which prevents Sybil attacks, identity forgery, credential cloning, unauthorized participation in the communication network, replay attacks and service abuse with malicious intent, while maintaining computational efficiency suitable for large-scale applications in IoT vehicular environments with limited resources.

Threat model

The threat model for the Internet of Things-enabled smart electric vehicle network considers a strong but computationally constrained attacker. An attacker may compromise or control a malicious automobile, roadside unit, charging station, or other network entity to gain unauthorised access or disrupt secure communication. The following hostile capabilities are considered.

Message interception and eavesdropping Attackers may observe and intercept blockchain data such as authentication requests, response messages, communication packets, timestamps, nonces, and more. Eavesdropping cannot reveal the private ECC key or PUF response.

Message modification Attackers may introduce, delete, amend, or manipulate communications between vehicles, RSUs, MEC servers, charging stations, and blockchain validators. To obtain unauthorised access or fool the receiving entity, the attacker changes authentication or communication settings.

Replay attacks The attacker may capture and retransmit a legitimate authentication request to impersonate a vehicle or reuse an expired authentication session. While authenticating, the smart contract checks the protocol's use of a timestamp and nonce.

Impersonation and credential-forgery attacks An attacker may impersonate a trusted EV or network entity by faking a digital signature or stealing credentials. Impersonating someone requires replicating the PUF secret or faking the ECC signature.

PUF cloning attacks After seeing challenge-response data, the attacker may attempt to clone a genuine device's physical attributes. The PUF-ECC approach makes it computationally difficult to duplicate the device-specific PUF answer on an unauthorised device.

Blockchain manipulation attempts The blockchain holds transactions, identities, trust, and authenticity. A malicious person may alter this information. The threat model assumes that the blockchain consensus mechanism prevents an attacker without enough consensus control from unilaterally editing finalised ledger entries.

Malicious insider behavior An authorised but hacked user with network access may behave aggressively, submit questionable transactions, communicate fake information, or produce aberrant communication. The BFGRL framework's trust evaluation and anomaly detection tackle similar activity later.

The attacker may have blockchain data, publicly viewable conversations, and the computing capacity to undertake classic network attacks. The attacker cannot realistically understand cryptographic primitives, reverse the secure hash function, reproduce the protected PUF response, or construct a valid ECC signature without the secret key if they are computationally constrained. The attacker is unlikely to compromise the blockchain consensus process, PUF hardware root of trust, and trusted cryptographic primitives.

This threat model states that PUF-ECC authentication prevents unauthorised persons with the correct hardware-derived secret and valid ECC credentials from authenticating. Equation (7) denies intercepted, changed, replayed, falsified, or cloned authentication requests. Thus, the BFGRL framework's decentralised authentication security relies on PUF-derived credentials, ECC digital signatures, timestamps, unique nonces, blockchain-based identity registration, and smart contract validation.

PUF-ECC-Based Authentication The proposed BFGRL framework employs PUF-ECC to provide lightweight, hardware-bound authentication for EVs, RSUs, charging stations, and edge entities. During the enrollment phase, a device-specific challenge C is applied to the PUF, generating a unique response $R_{PUF} = PUF(C)$. Because PUF responses can exhibit small variations due to temperature, voltage, aging, and other environmental effects, the raw response is stabilized using an error-correction/fuzzy-extractor mechanism. Helper data W is generated during enrollment and stored for subsequent response reconstruction, while the raw PUF response is not directly stored or transmitted. During authentication, the same challenge is applied to regenerate the PUF response, and the helper data is used to correct response variations and reconstruct a stable response R^*. A cryptographic hash/KDF is subsequently applied to R^* and the challenge to derive a device-specific secret $K_{PUF} = H(R^* \parallel C)$. This secret is bound to the device's ECC credentials, consisting of an ECC private key K_{ECC}^{priv} and corresponding public key K_{ECC}^{pub}. The device generates an authentication proof using its ECC private key and PUF-derived secret over the current challenge and session information. The verifier validates the ECC proof using the registered public key and verifies the associated PUF-derived device identity. Authentication is successful only when the cryptographic and hardware-bound verification conditions are satisfied. This integration prevents direct exposure of the PUF response, strengthens resistance to device cloning and impersonation, and provides lightweight authentication suitable for resource-constrained EV-IoT environments.

Federated graph attention learning (FedGAL)

After successful decentralized authentication and blockchain-based identity verification, the proposed Blockchain-enabled Federated Graph Reinforcement Learning (BFGRL) framework evaluates trustworthiness dynamically with the help of another privacy-aware Federated Graph Attention Learning (FGAL) architecture that can continuously analyse the communication behaviour of the authenticated entities in the distributed IoT-enabled smart electric vehicle ecosystem. Figure 4 illustrates the federated graph attention learning framework for privacy-preserving trust evaluation and malicious node detection.

The framework proposed in this work builds graph intelligence on the Mobile Edge Computing (MEC) servers, instead of continuously uploading sensitive information from the vehicles to the servers, as in the traditional centralized trust management approach, and assures user privacy by applying blockchain-assisted federated learning. Each authenticated electric vehicle (EV), Roadside Unit (RSU), charging station, MEC server, blockchain validator, and utility gateway are modeled as vertices in a dynamically evolving weighted communication graph. In contrast, each communication session between an EV and the communicating entities including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Grid (V2G), and edge communication protocols are modeled as a weighted edges that capture communication quality and behavioral interaction. The communication graph continuously changes with respect to the mobility of vehicles, charging requests, topology changes, wireless channel variations and service migrations, which enables the graph representation to reflect temporal structural changes that happen over the transportation network. A heterogeneous communication graph is mathematically represented as in Eq. 9:

$$\begin{aligned} \mathcal{G}^{(t)} &= \left(\mathrm{V}^{(t)}, \mathrm{E}^{(t)}, \mathrm{A}^{(t)}, \mathrm{X}^{(t)}, \mathrm{W}^{(t)}\right), \mathrm{A}_{ij}^{(t)} \\ &= \delta_{ij}\left[\omega_1 R_{ij} + \omega_2 T_{ij} + \omega_3 B_{ij} + \omega_4 P_{ij} + \omega_5 e^{-\frac{L_{ij}}{L_{\max}}} + \omega_6 S_{ij}\right] \end{aligned} \tag{9}$$

where $\mathcal{G}^{(t)}$ is the graph of heterogeneous communication at time t, $V^{(t)}$ is the set of nodes (vehicles and infrastructure) that are authenticated through communication, $E^{(t)}$ is the set of communication links, $\mathbf{A}^{(t)}$ is the weighted adjacency matrix of the graph $\mathcal{G}^{(t)}$, $\mathbf{X}^{(t)}$ is the node feature representations, $\mathbf{W}^{(t)}$ is the edge weights, δ_{ij} is the communication between nodes and j, R_{ij} is the transmission reliability, T_{ij} is the historical trust value, B_{ij} is the behavioral similarity, P_{ij} is the packet forwarding reliability, L_{ij} is the communication latency, L_{max} is the maximum acceptable communication latency, S_{ij} is the transaction consistency similarity, and $\omega_1, \omega_2, \ldots, \omega_6$ are adaptive

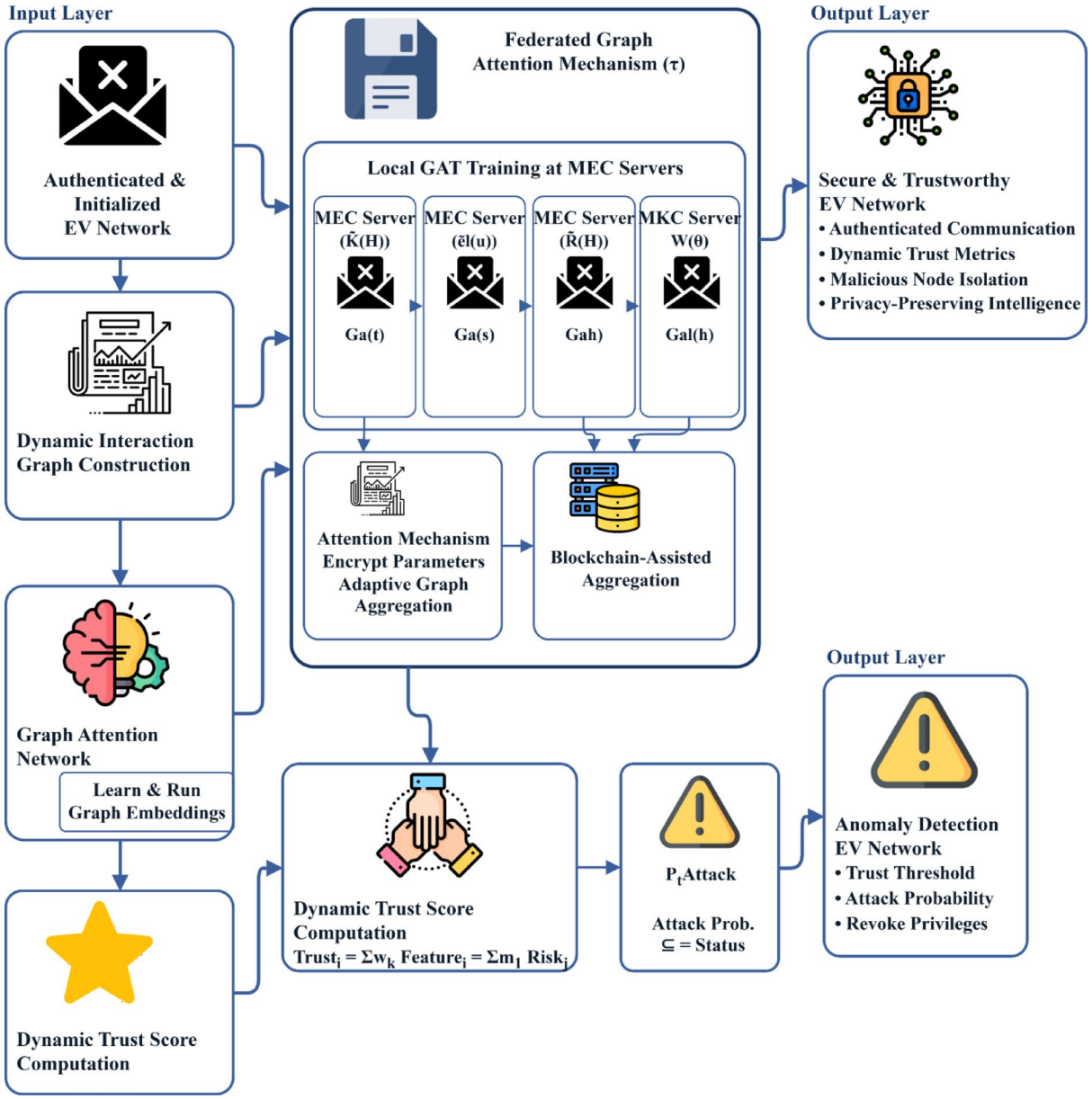

Fig. 4 Federated graph attention-based trust learning and behavioral analysis

weighting coefficients, with $\sum_{k=1}^{6} \omega_k = 1$. This dynamic graph can represent a single structure that models communication quality, mobility interactions, historical behavior, and blockchain transaction consistency simultaneously.

After constructing the graph, each MEC server trains its own Graph Attention Network (GAT) using its locally observed communication subgraph, while avoiding the release of raw vehicular data to servers outside its administrative range. While in a conventional Graph Convolutional Network, the importance of neighboring nodes is assumed to be identical, the graph attention mechanism can automatically learn the importance (attention coefficient) of each neighboring node based on communication behavior, trust evolution, authentication reliability, packet-forwarding history, and mobility correlation. The attention mechanism can dynamically suppress unreliable neighbors and highlight trustworthy communication participants, thereby enhancing the robustness of distributed trust estimation under rapidly changing network conditions. The attention coefficient between two neighbouring nodes is calculated as in Eq. 10,

$$\alpha_{ij} = \frac{\exp\left(LeakyReLU\left(\mathrm{a}^T\left[\mathrm{Wh}_i \middle\| \mathrm{Wh}_j \middle\| \mathrm{e}_{ij}\right]\right)\right)}{\sum_{k\in\mathcal{N}(i)} \exp\left(LeakyReLU\left(\mathrm{a}^T\left[\mathrm{Wh}_i \| \mathrm{Wh}_k \| \mathrm{e}_{ik}\right]\right)\right)} \tag{10}$$

In this, α_{ij} is the normalized attention coefficient for neighboring node j; $\mathbf{h}_i$ and $\mathbf{h}_j$ are the feature vectors of two nodes that are communicating; $\mathbf{W}$ is the learnable feature transformation matrix; a is the trainable attention weight vector; $\|$ is the vector concatenation operation; $\mathbf{e}_{ij}$ are the edge features (such as latency, packet delivery ratio, trust history, communication reliability, etc.) of the two nodes; $LeakyReLU(\cdot)$ is the nonlinear activation function; and $\mathcal{N}(i)$ is the neighborhood of node . Thus, entities with good communication behavior receive higher attention coefficients, while entities with poor or unstable communication receive lower and lower attention coefficients during feature aggregation.

With the learned attention coefficients, neighbourhood information is aggregated to form a higher-level graph representation that can model long-range communication among distributed vehicular entities. In contrast to traditional aggregation methods based solely on topological connectivity, the BFGRL framework introduces dynamically learnt attention distributions and edge attributes that characterize the reliability of communication, blockchain transaction integrity, behavioral similarity, and authentication confidence. Each attention layer produces a graph embedding, which is written as Eq. 11:

$$\mathrm{h}_i^{(l+1)} = \sigma\left(\sum_{j\in\mathcal{N}(i)} \alpha_{ij}\left[\mathrm{W}^{(l)}\mathrm{h}_j^{(l)} + \mathrm{B}^{(l)}\mathrm{e}_{ij} + \mathrm{C}^{(l)}r_{ij}\right] + \mathrm{b}^{(l)}\right) \tag{11}$$

where $\mathbf{h}_i^{(l+1)}$ is the updated node embedding after $l+1$-th layer; $\sigma(\cdot)$ is the nonlinear activation function; α_{ij} is the attention coefficient that is obtained from Eq. (10); $\mathbf{W}^{(l)}$ is the trainable weight matrix; $\mathbf{h}_j^{(l)}$ is the neighboring node embeddings; $\mathbf{e}_{ij}$ is the communication edge features; $\mathbf{r}_{ij}$ is the blockchain verification attributes; $\mathbf{B}^{(l)}$ and $\mathbf{C}^{(l)}$ are the learnable transformation matrices on edge and blockchain features, respectively; and $\mathbf{b}^{(l)}$ is the trainable bias vector. This hierarchical aggregation allows each MEC server to learn global graph representations that provide a picture of local communication trust relationships without any underlying vehicular observations.

To avoid sending locally gathered datasets to centralized servers, only periodically encrypted model parameters are sent from each MEC server to the federated aggregation nodes via the blockchain. This is a decentralized learning approach that retains data ownership and significantly reduces privacy leakage and communication overhead. To build the global trust model, an adaptive Federated Averaging mechanism is used to weight each participating MEC server based on the size of its local dataset and the reliability of its communication. The global aggregation process is mathematically described as Eq. 12:

$$\Theta_{r+1}^{Global} = \sum_{k=1}^{K}\left(\frac{n_k\lambda_k}{\sum_{m=1}^{K} n_m\lambda_m}\right)\Theta_k^{(r)} + \gamma\left(\Theta_k^{(r)} - \Theta_r^{Global}\right) \tag{12}$$

Here, Θ_{r+1}^{Global} is the updated global model after the communication in round $r+1$,K is the number of MEC servers participating in the training, n_k is the number of local training samples, λ_k is the communication reliability weighting, $\Theta_k^{(r)}$ are the parameters of the local training model, Θ_r^{Global} are the parameters of the previous global model, and γ is the adaptive convergence factor that controls the aggregation stability. All uploaded models are verified for consensus via blockchain prior to aggregation, thus preventing malicious model poisoning or parameter modification.

Following the global model synchronization, each participating MEC server dynamically calculates/trusts the scores of all authenticated entities by collectively analysing communication reliability, authentication consistency, behavioural stability, blockchain transaction integrity, forwarding behaviour, reputation history, mobility consistency and graph embeddings created by federated learning. The overall trust evaluation function is calculated using Eq. 13:

$$Trust_i = w_1 Rel_i + w_2 Auth_i + w_3 Beh_i + w_4 For_i + w_5 Rep_i + w_6 Txn_i + w_7 Emb_i + w_8 Mob_i - w_9 Risk_i - w_{10} Attack_i \quad (13)$$

where $Trust_i$ is a comprehensive trust score of the entity , Rel_i is the communication reliability, $Auth_i$ is the authentication consistency, Beh_i is the behavioral consistency, For_i is the packet forwarding reliability, Rep_i is the historical reputation, Txn_i is the blockchain transaction integrity, Emb_i is the graph embedding confidence, Mob_i is the mobility consistency, $Risk_i$ is the estimated security risk, $Attack_i$ is the probability of malicious behavior, and $w_1, \ldots, w_{10}$ are the adaptive trust weighting coefficients with $\sum_{i=1}^{10} w_i = 1$. The generated trust score is a holistic quantitative representation of each participant's trustworthiness in the decentralised EV space.

An anomaly assessment module continuously analyzes changes in graph representations and trust evolution, using adaptive confidence thresholds to prevent malicious nodes from further communication. If the vehicles are found to be communicating abnormally, engaging in malicious packet injection, replay attacks, disseminating false information, rapidly degrading trust, exhibiting blockchain inconsistencies, and/or exhibiting suspicious forwarding behavior, they are immediately marked as compromised vehicles. The anomaly probability is calculated by Eq. (14):

$$P_i^{Attack} = \sigma(\beta_0 + \beta_1 (1 - Trust_i) + \beta_2 Dev_i + \beta_3 Entropy_i + \beta_4 Fail_i + \beta_5 Graph_i + \beta_6 Txn_i) \quad (14)$$

The P_i^{Attack} is the estimated malicious probability for node ; $\sigma(\cdot)$ is the sigmoid activation function; β_0 is the bias parameter; $Trust_i$ is the score of trust as mentioned in Eq. (13); Dev_i is the behavioral deviation; $Entropy_i$ is the communication uncertainty; $Fail_i$ is the authentication failure frequency; $Graph_i$ is the graph structural abnormality and Txn_i is the blockchain transaction inconsistency. Nodes with attack probability beyond the adaptive security threshold are disconnected from graph communication, model federation, blockchain consensus, and future service requests.

Lastly, communication isolation decisions are followed by blockchain smart contracts that actively revoke the communication privileges of malicious entities while keeping communication for trustworthy entities running. The isolation policy is represented as Eq. 15:

$$Status_i = \begin{cases} \text{Active}, & \text{if } Trust_i \geq \tau_T \wedge P_i^{Attack} < \tau_A \wedge Ledger_i = Valid, \\ \text{Isolated}, & \text{if } Trust_i < \tau_T \vee P_i^{Attack} \geq \tau_A \vee Ledger_i = Invalid. \end{cases} \quad (15)$$

where $Status_i$ is the operation status of node , τ_T is the adaptive trust threshold, τ_A is the anomaly detection threshold, $Ledger_i$ The validity of the node identity in the blockchain.n, Active means that node is allowed to communicate and participate in federated learning, and Isolated means that node is completely banned from participating in vehicular communication, federated learning, charging coordination, and collaborative resource sharing. Thus, this adaptive Federated Graph Attention Learning framework offers accurate dynamic trust assessment, robust privacy protection and blockchain security, and is strong against malicious packet injection, false information propagation, Sybil attacks, insider attacks, model poisoning, and coordinated cyber-attacks in the smart electric vehicle (SEV) ecosystem with IoT.

PPO-driven adaptive blockchain consensus and secure data sharing

After dynamic trust evaluation, the proposed Blockchain-enabled Federated Graph Reinforcement Learning (BFGRL) framework conducts adaptive blockchain consensus to overcome the issues of scalability, computational complexity, energy inefficiency and communication bottlenecks in traditional blockchain consensus algorithms like Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). Figure 5 illustrates the PPO-enabled adaptive validator selection strategy for blockchain consensus optimization and secure transaction processing.

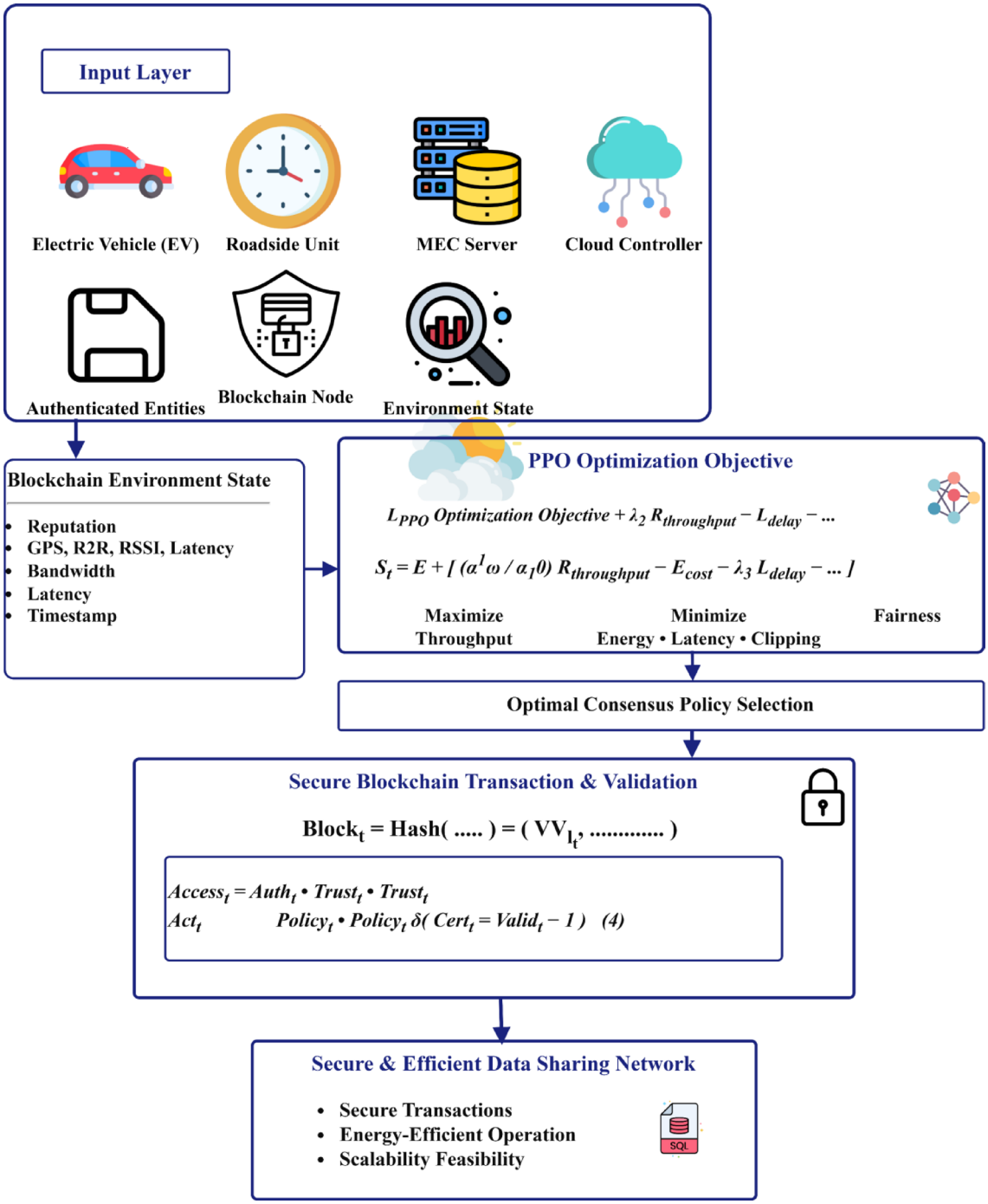

Fig. 5 PPO-based adaptive validator selection and secure blockchain consensus

The reward formulation has also been clarified. At each decision step t, the PPO agent receives a composite reward that reflects the blockchain network's operational objectives:

$$R_t = \lambda_1 \hat{T}_t - \lambda_2 \hat{E}_t - \lambda_3 \hat{L}_t - \lambda_4 \hat{C}_t + \lambda_5 F_t \tag{16}$$

where T_t represents transaction throughput, E_t represents energy consumption, L_t denotes transaction/network latency, C_t represents processing or transaction-clipping cost, and F_t represents fairness. The terms are normalized

before combination, and $\lambda_1, \ldots, \lambda_5$ control their relative importance. Thus, higher throughput and fairness increase the reward, whereas excessive energy consumption, latency, and processing cost decrease the reward.

The corresponding PPO objective is expressed as:

$$L^{CLIP}(\theta) = \mathbb{E}_t\left[\min\left(r_t(\theta)\hat{A}_t, clip\left(r_t(\theta), 1-\varepsilon, 1+\varepsilon\right)\hat{A}_t\right)\right] \tag{17}$$

where

$$r_t(\theta) = \frac{\pi_\theta(a_t s_t)}{\pi_{\theta_{old}}(a_t s_t)} \tag{18}$$

is the probability ratio between the updated and previous policies, $\hat{A}_t$ is the estimated advantage, and $\epsilon = 0.20$ is the clipping parameter. The clipping mechanism prevents excessively large policy updates and improves training stability.

PPO update procedure

The PPO-based consensus optimization begins with observing the current blockchain environment state S_t , which consists of reputation score, R2R, RSSI, latency, bandwidth, timestamp, and transaction-related network information. Based on this state, the PPO policy $\pi_\theta(A_t \mid S_t)$ selects an appropriate consensus policy A_t. The selected policy is then executed and evaluated according to key blockchain performance indicators, including transaction throughput, energy consumption, communication latency, processing cost, and fairness. Using these performance measures, a composite reward R_t is computed through the proposed multi-objective reward function. The resulting state-action-reward transitions are stored in a rollout buffer for experience collection. Subsequently, the advantage value $\hat{A}_t$ is estimated using the observed rewards and value-function predictions. The actor and critic networks are then updated using the PPO clipped-surrogate objective and optimized with the Adam optimizer. After each optimization cycle, the updated policy replaces the previous policy and becomes the reference model for the next training iteration. This process is repeated until the moving-average reward and policy loss stabilize, indicating convergence. Finally, the converged policy that achieves the highest stable cumulative reward is selected as the optimal consensus policy and deployed for secure blockchain transaction validation and consensus management.

The proposed framework dynamically selects the set of validators based on the actual operational properties of the IoT-empowered electric vehicle ecosystem at runtime, rather than statically allocating validators or using hash puzzle generation, which is very computation-intensive. Each authenticated blockchain validator, Mobile Edge Computing (MEC) server, charging station, Roadside Unit (RSU), and utility gateway periodically provides multidimensional operational information, including validators' reputation, communication reliability, blockchain's trust score, computational resources availability, processor utilization, memory utilization, transaction verification history, communication latency, bandwidth utilization, transaction queue size, block generation success rate, synchronization delay, energy consumption, consensus participation rate, and historical malicious behavior. These diverse observations provide input to the reinforcement learning environment, where the PPO agent continually learns an optimal blockchain consensus policy that maximizes blockchain throughput and minimizes computational overhead, communication delay, imbalance among validators, and energy consumption. The environment state is a full, multidimensional vector that captures the environment's state (all candidate validators) at each blockchain consensus interval. The consensus state formulating of the blockchain is mathematically represented as Eq. 19:

$$\begin{aligned} S_t = & [Rep_1, Trust_1, CPU_1, Mem_1, BW_1, Lat_1, TPS_1, Energy_1, Queue_1, \\ & Rep_2, Trust_2, CPU_2, Mem_2, BW_2, Lat_2, TPS_2, Energy_2, Queue_2, \ldots, \\ & Rep_N, Trust_N, CPU_N, Mem_N, BW_N, Lat_N, TPS_N, Energy_N, Queue_N] \\ = & [\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_N] \end{aligned} \tag{19}$$

Here S_t is the state of the global blockchain environment at decision moment t, N is the number of all the validator candidates, $\mathbf{s}_i$ is the state vector of the th validator, Rep_{i} is the reputation score of the th validator, $Trust_{\mathrm{i}}$ is the dynamic trust value generated by the Federated Graph Attention Learning module, CPU_{i} is the available processor resources of the th validator, Mem_{i} is the available memory capacity of the ith validator, BW_{i} is the communication bandwidth of the ith validator, Lat_{i} is the network communication latency of the th validator, TPS_{i} is the historical transaction processing capability of the ith validator, $Energy_{\mathrm{i}}$ is the consensus energy consumption of the th validator, and $Queue_{\mathrm{i}}$ is the pending transaction backlog of the th validator. This multidimensional state representation allows the PPO agent to consider the blockchain's performance, communication quality, availability of computational resources, trust levels, and the workload of all validators, helping it decide on the best possible consensus committee to make decentralized decisions, given constantly varying vehicular network conditions.

From the observed blockchain environment, the PPO agent learns an adaptive consensus policy that automatically identifies the "optimal" subset of validators that enables the blockchain to operate securely, efficiently, and with low latency. PPO differs from regular RL algorithms, which often exhibit unstable policy changes as they learn, by using clipped policy optimization to limit how much the policy can change between learning iterations, ensuring monotonic policy improvement and fast convergence when optimizing consensus. This policy also maximizes cumulative rewards on the blockchain while reducing the likelihood of sudden changes to blockchain parameters that could disrupt the validators' selection process. The fully developed PPO optimization goal used in BFGRL is mathematically represented as Eq. 20:

$$\begin{aligned} L^{PPO}(\theta) =& \mathbb{E}_t[\min(r_t(\theta)\tilde{A}_t, \mathrm{clip}(r_t(\theta), 1-\varepsilon, 1+\varepsilon)\hat{A}_t) \\ &+ \lambda_1 R_{\text{throughput}} - \lambda_2 E_{\text{consumption}} - \lambda_3 L_{\text{delay}} - \lambda_4 O_{\text{communication}} + \lambda_5 F_{\text{fairness}} \end{aligned} \tag{20}$$

where $L^{PPO}(\theta)$ is the PPO objective function with policy parameters θ and $\mathbb{E}_t[\cdot]$ is the expectation over sampled blockchain trajectories $r_t(\theta) = \dfrac{\pi_\theta(a_t \mid S_t)}{\pi_{\theta_{old}}(a_t \mid S_t)}$ denotes the probability ratio between the updated and previous policies; $\hat{A}_t$ represents the generalized advantage estimate assessing the quality of the picked validator action; $clip(\cdot)$ limits the policy updates to be inside the interval $[1-\varepsilon, 1+\varepsilon]$; ε is the clipping threshold, which controls the stability of the policy updates; $R_{throughput}$ is the blockchain transaction throughput; $E_{consumption}$ is the consensus energy expenditure; L_{delay} is the average block confirmation latency; $O_{communication}$ is the communication overhead of validator synchronization; and $F_{fairness}$ is the fairness of participation among validators. Given enough experience in the blockchain environment, the PPO agent gradually discovers an optimal consensus strategy that adaptively identifies trustworthy validators with high computational capability, good communication quality, low energy usage, and proper participation frequency, whilst preventing unreliable and malicious validators from participating in consensus formation.

Once the optimal validator committee has been identified, authenticated vehicular information, such as charging transactions, energy trading data, battery State-of-Health (SoH), navigation data, charging reservations, federated learning model hashes, trust certificates, and blockchain identities, is securely shared via encrypted blockchain channels governed by decentralized smart contracts. All transactions are digitally signed and encrypted, and they are verified by the elected validator committee and added to the distributed ledger only when (at least) consensus is reached, to ensure confidentiality, integrity, authenticity, and non-repudiation for inter-vehicle communication. At the same time, blockchain smart contracts automatically enforce access control policies, allowing authenticated parties with valid trust certificates to access only certain vehicular information. In the blockchain transaction generation and validation process, the following mathematical representation is used for security, using Eq. 21:

$$\begin{aligned} Block_t =& Hash(PrevHash||MerkleRoot(TX_1, TX_2, \ldots, TX_m)||TimeStamp||once) \\ &||ValidatorID||Sig_{Validator}||PolicyHash||StateHash \end{aligned}$$

$$Access_i = Auth_i \cdot Trust_i \cdot Policy_i \cdot \delta(Cert_i = Valid) \tag{21}$$

where $Block_t$ is the newly generated blockchain block in consensus round t, $Hash(\cdot)$ is the secure cryptographic hash function, $PrevHash$ is the hash of the previous blockchain block, $MerkleRoot(\cdot)$ is the Merkle tree root that is computed from all the validated transactions $TX_1, TX_2, \ldots, TX_m$, $TimeStamp$ is the time when the block is generated, $Nonce$ is the consensus nonce, $ValidatorID$ is the identity of the selected validator who will be responsible for the generation of the blockchain block, $Sig_{Validator}$ is the identity certificate of the validator, $PolicyHash$ is the hash of the access-control policy of the smart contract, $StateHash$ is the digest of the blockchain state, $Access_i$ is the access authorization assigned to the participant , $Auth_i$ is the successful authentication status, $Trust_i$ is the dynamic trust score computed during federated graph learning, $Policy_i$ is the smart contract permission level $\delta(\cdot)$ that corresponds to the access of the participant , and $Cert_i$ is the blockchain identity certificate. Thus, only verified and reliable users and/or devices that meet specified blockchain security policies can share encrypted vehicle data, run smart contracts, confirm transactions and engage in a distributed consensus process. This PPO-based adaptive blockchain consensus mechanism therefore significantly improves transaction throughput, reduces blockchain confirmation latency, balances participation fairness, reduces the energy consumption of the validators, and boosts the blockchain scalability and resistance against malicious collusion of validators, consensus manipulation, Sybil attacks, and DDoS attacks to provide a secure and efficient decentralized data-sharing infrastructure for large-scale IoT-enabled smart electric vehicle systems.

Blockchain Ledger maintenance, security analytics and network decision optimization

The last part of the proposed Federated Graph Reinforcement Learning (BFGRL) framework maintains a blockchain ledger for the long term, secures the network through intelligent security analysis, and optimizes network decision-making adaptively, thereby guaranteeing the long-term reliability, trust sustainability, privacy preservation, and autonomous operational management of the IoT-enabled smart electric vehicle ecosystem. Figure 6

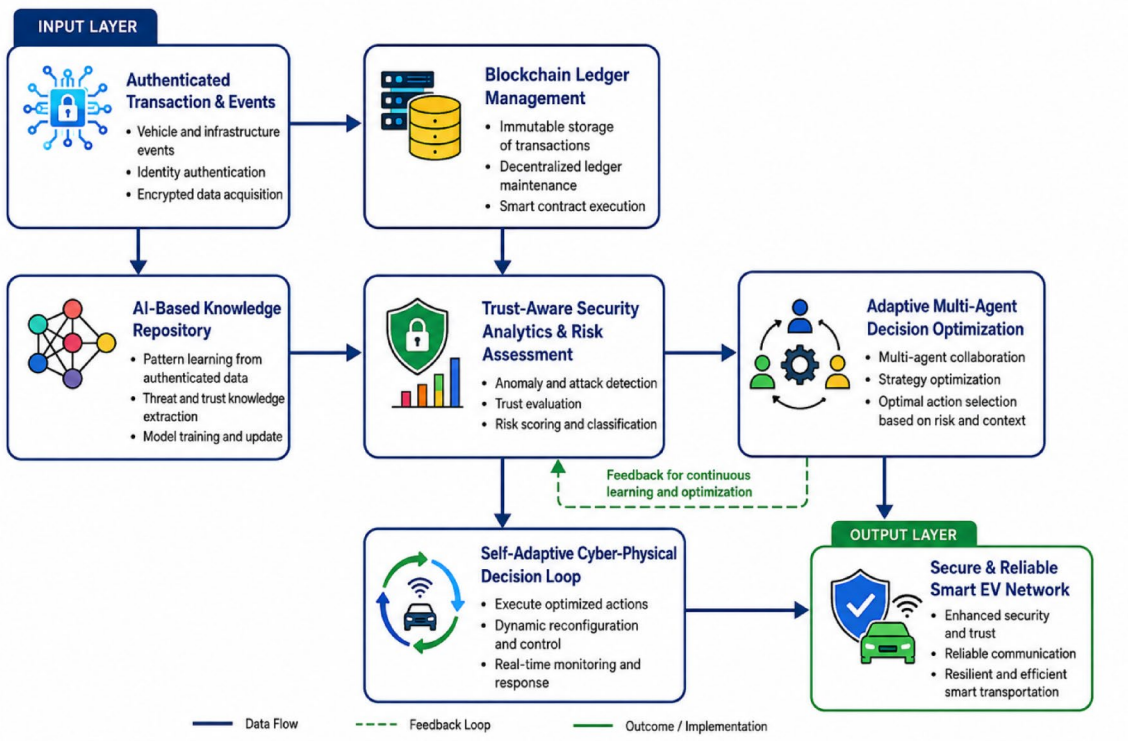

Fig. 6 Blockchain-enabled security analytics and adaptive network optimization

illustrates the intelligent blockchain ledger maintenance, security analytics, and reinforcement learning-based network decision optimization process.

The proposed framework differs from traditional blockchain architectures, which only record transactions, and can be used to build an intelligent knowledge repository that enables real-time cybersecurity assessment, analysis of historical trust evolution, generation of reinforcement learning feedback, federated knowledge integration, and prediction of network optimization. After the consensus is successfully generated, all authenticated communication sessions, charging transactions, Vehicle-to-Vehicle (V2V) communication, Vehicle-to-Infrastructure (V2I) communication, Vehicle-to-Grid (V2G) energy exchange, blockchain validator decision, trust score update, federated model aggregation, as well as the results of the anomaly detection processes and the resource allocation decisions are permanently recorded in immutable blocks of the blockchain using cryptographically linked hash structures. As each new block added to the blockchain includes the cryptographic digest of the previous block, if the information in any block in the blockchain history is altered, none of the future blockchain hashes will match, ensuring complete immutability, non-repudiation, and tamper-proof auditability within the distributed vehicular network. At the same time, blockchain smart contracts automatically update replicas of the blockchain across all authorized validator nodes to ensure global consistency under decentralized governance. The maintenance operation of the blockchain ledger is mathematically represented as Eq. 22:

$$\begin{aligned} Ledger_{t+1} = Ledger_t \cup \{Hash(PrevHash_t || MerkleRoot(TX_1, TX_2, \ldots, TX_m) || Trust_t \\ || FedModel_t || Validator_t || Consensus_t || SecurityLog_t || TimeStamp_t \end{aligned} \tag{22}$$

$Ledger_{t+1}$ is the updated distributed blockchain ledger after the consensus round $t+1$, $Ledger_t$ is the previous blockchain ledger state, $Hash(\cdot)$ is the secure cryptographic hash function, $PrevHash_t$ is the hash of the previous blockchain block, $MerkleRoot(\cdot)$ is the merkle tree root, which is computed from all validated transactions $TX_1, TX_2, \ldots, TX_m$, $Trust_t$ is the global trust repository constructed by Federated Graph Attention Learning, $FedModel_t$ are the aggregated federated learning model parameters, $Validator_t$ is the selected validator committee, $Consensus_t$ is the blockchain consensus metadata, $SecurityLog_t$ is the recorded cybersecurity events, and $TimeStamp_t$ is the synchronized blockchain timestamp. The resulting "immutable ledger" thus serves as a complete distributed knowledge base that can store all operational events, security decisions, trust updates, and communication activities that occur during the life of the intelligent transportation system.

After ledger synchronization, the BFGRL framework continuously conducts blockchain-based security analysis to detect any abnormal communications before they can propagate through the vehicular network and become cyber threats. The proposed security analytics engine combines information from the past historical data logs kept on the blockchain with the evolution of the trust trajectory of nodes, the results of their authentication processes, federated graph embeddings, consensus statistics, communications latency variations, transaction validation history, packet forwarding behavior, and validator performance profile to build a complete threat assessment model. Combined with real-time network conditions and temporal blockchain knowledge, the framework can accurately identify behaviours of malicious nodes, such as Sybil attacks, replay attacks, false information dissemination, blockchain consensus manipulation, model poisoning, packet injection attacks, insider threats, DoS attacks, and abnormal trust degradation. The complete blockchain security risk assessment can be mathematically represented by Eq. 23:

$$\begin{aligned} Risk_i = & \lambda_1 (1 - Trust_i) + \lambda_2 Attack_i + \lambda_3 AuthFail_i + \lambda_4 LatencyDev_i \\ & + \lambda_5 ConsensusDev_i + \lambda_6 TxnAbnormal_i + \lambda_7 GraphAnomaly_i \\ & + \lambda_8 BehaviorEntropy_i + \lambda_9 ModelDeviation_i + \lambda_{10} History_i \end{aligned} \tag{23}$$

where $Risk_i$ is the comprehensive security risk score of the i^{th} network entity, $Trust_i$ is the dynamic trust value obtained from the federated graph attention model, $Attack_i$ is the estimated probability of a malicious attack on the i^{th} network entity, $AuthFail_i$ is the frequency of authentication failure of the i^{th} network entity, $LatencyDev_i$ is the communication latency deviation of the i^{th} network entity, $ConsensusDev_i$ is the abnormal consensus behavior

of the i^{th} network entity, $TxnAbnormal_i$ is the abnormal behavior of blockchain transactions of the i^{th} network entity, $GraphAnomaly_i$ is the graph structural abnormality obtained by the graph learning model, $BehaviorEntropy_i$ is the behavioral uncertainty based on the i^{th} network entity's historical communication behavior, $ModelDeviation_i$ is the deviation between federated local and global models, $History_i$ is the historic malicious behavior stored in the blockchain ledger, and $\lambda_1, \lambda_2, \ldots, \lambda_{10}$ are adaptive weighting factors, and $\sum_{k=1}^{10} \lambda_k = 1$. This multi-dimensional security-evaluation mechanism enables the detection of sophisticated, coordinated cyber attacks that are beyond the reach of conventional signature-based intrusion detection mechanisms.

Historical blockchain knowledge is then used to optimally schedule communication and validators, compute trust, coordinate charging, engage in energy trading, route communications, participate in FL, and allocate computational resources. The proposed BFGRL framework unifies reinforcement learning policies, federated intelligence, graph-based trust representations, blockchain knowledge, and real-time communication statistics into a single network optimization engine to avoid the need for individual optimization of subsystems. The optimization goal is to maximize communication reliability, blockchain throughput, trust stability, and energy efficiency, while minimizing communication latency, computational overhead, security risks, blockchain congestion, and routing costs. The adaptive network utility function is given by Eq. 24:

$$\begin{aligned} U_{\text{Network}} =& \omega_1 Throughput + \omega_2 Trust + \omega_3 \text{ResourceUtilization} \\ &+ \omega_4 RoutingEfficiency + \omega_6 FedAccuracy + \omega_7 ConsensusQuality \\ &- \omega_8 Latency - \omega_9 Risk - \omega_{10} \text{CommunicationCost} \end{aligned} \tag{24}$$

where $U_{Network}$ is the overall network utility scores, $Throughput$ is the blockchain throughput (number of transactions per second), $Trust$ is the global trust scores, $ResourceUtilization$ is the computational resource efficiency scores of MEC servers and blockchain validators, $RoutingEfficiency$ is the communication routing scores, $EnergyEfficiency$ is the optimized energy utilization scores in charging and consensus operations, $FedAccuracy$ is the federated learning prediction accuracy scores, $ConsensusQuality$ is the blockchain consensus stability scores, $Latency$ is the average communication delay scores, $Risk$ is the global cyber-security risk scores obtained from Eq. (20), $CommunicationCost$ is the communication overhead scores, and $\omega_1, \omega_2, \ldots, \omega_{10}$ are adaptive optimization scores with the condition $\sum_{k=1}^{10} \omega_k = 1$. By maximizing this objective, the BFGRL framework can dynamically adjust the operational strategy based on evolving vehicular mobility, blockchain workloads, communication conditions, and cybersecurity requirements.

Finally, the optimal network utility derived from the knowledge discovered from blockchain is used to develop smart decision policies that govern the system's operation later. The decision optimization engine constantly adjusts the trust thresholds, scheduling priorities for validators, communication routing policies, the frequency of federated aggregation, charging resource allocation, the distribution of tasks to edge computing resources, the interval for blockchain synchronization, and the security enforcement strategy based on the accumulating intelligence of the blockchain. In contrast with static rule-based systems, the proposed framework forms a self-adaptive cyber-physical decision loop: each newly created blockchain record is used to make future decisions in a cyber-physical loop, and the resulting decisions are fed back to the reinforcement learning system, while historical knowledge is extracted to improve decision-making. The final network decision policy is mathematically shown as Eq. 25:

$$\begin{aligned} \Pi^* = \arg\max_{\Pi} \Bigg[\sum_{t=0}^{T} \gamma^t \Big(& U_{Network}^{(t)} + \alpha_1 TrustGain^{(t)} + \alpha_2 \text{SecurityGain}^{(t)} \\ & + \alpha_3\, ConsensusEfficiency^{(t)} + \alpha_4\, PrivacyLevel^{(t)} \\ & - \alpha_5\, Operational\ \text{Cost}^{(t)} - \alpha_6\, Attack\ Impact^{(t)} \Big) \end{aligned} \tag{25}$$

where Π^* is the optimal adaptive network decision policy, $\underset{\Pi}{\text{argmax}}$ is the set of decisions that maximise the long-term operation performance, T is the optimisation horizon, γ is the reinforcement learning discount factor to control the importance of reward in the future, $U_{Network}^{(t)}$ is the network utility obtained from Eq. (21), $TrustGain^{(t)}$ is the improvement in trust during decision interval t, $SecurityGain^{(t)}$+ is the enhancement in cyber-security resilience, $ConsensusEfficiency^{(t)}$ is the consensus performance improvement, $PrivacyLevel^{(t)}$ is the privacy preservation capability, $OperationalCost^{(t)}$ is the computational and communication cost, $AttackImpact^{(t)}$ is the estimated consequences of the cyber-attack, and $\alpha_1, \alpha_2, \ldots, \alpha_6$ are adaptive optimisation coefficients controlling the relative importance of individual operation objectives. This combination of immutable blockchain storage, federated graph attention learning, reinforcement learning-based optimisation, and intelligent security analytics results in a completely autonomous, scalable and self-evolving decision-making framework that can continuously enhance the aspects of authentication reliability, communication efficiency, privacy preservation, blockchain resilience, cyber-security robustness, and resource utilisation in next-generation IoT-enabled intelligent electric vehicle ecosystems and large-scale smart city transportation infrastructures.

However, it is a holistic optimization framework that is adaptively integrated with the existing techniques across the layers of the problem domain and is not merely a sequential integration of existing techniques one after another as in Algorithm 1. The novelty is coupled authentication in PUF within the ECC, combined trust learning via a Graph Attention Network (GAT), Federated Learning (FL), and PPO for the consensus mechanism in the blockchain. In contrast to other blockchain-IoV implementations, the attention-based trust embedding embedded in an interaction graph that dynamically outputs based on the trust network is collaboratively optimized via federated aggregation of participating nodes. Learned trust representations continuously update the blockchain state to enable the PPO agent be able to do adaptive validator committees and transaction policies. Blockchain validation results are used to update the graph topology and adjust the evolution of trust building, which is optimized together with the selection of consensus, authentication, and secure data sharing, all within a single mathematical framework. The main theoretical contribution of the proposed BFGRL framework is this feedback-driven co-optimization.

Step 1. Data Initialization
Initialize $B \leftarrow \emptyset$, $V^* \leftarrow \emptyset$, $W \leftarrow W^{(0)}$, $\theta \leftarrow \theta^{(0)}$
Step 2. Feature Extraction
For every EV $v_i \in V$
Extract $x_i = [\mathrm{SOC}_i, \mathrm{RSSI}_i, L_i, \mathrm{BW}_i, \mathrm{GPS}_i, T_i]^T$
Step 3. PUF-ECC Authentication
Generate $(C_i, R_i) = PUF(v_i)$
Generate ECC signature $S_i = Sign_{ECC}(R_i)$
Authentication decision $Auth_i = \begin{cases} 1, & Verify(C_i, R_i, S_i) = 1 \\ 0, & \text{otherwise} \end{cases}$
If $Auth_i = 1$
Then $V^* = V^* \cup \{v_i\}$
End if
Step 4. Dynamic Interaction Graph Construction
Construct $G = (V^*, E, X)$
Edge weight $A_{ij} = \sum_{k=1}^{K} \omega_k f_k(i,j)$
Where $f_k = \{RSSI, Latency, Distance, Trust, Energy\}$
Step 5. Multi-Head Graph Attention
For $h = 1,2,\cdots, H$
Linear transformation $z_i^{(h)} = W^{(h)} x_i$
Attention coefficient $e_{ij}^{(h)} = LeakyReLU(a^{(h)T}[z_i^{(h)} || z_j^{(h)}])$
Normalization $\alpha_{ij}^{(h)} = \frac{\exp(e_{ij}^{(h)})}{\sum_{k \in N_i} \exp(e_{ik}^{(h)})}$
Graph aggregation $h_i^{(h)} = \sigma(\sum_{j \in N_i} \alpha_{ij}^{(h)} z_j^{(h)})$
End for
Concatenate $h_i = \|_{h=1}^{H} h_i^{(h)}$
Step 6. Dynamic Trust Computation
Compute $Trust_i = \sum_{m=1}^{M} \beta_m h_{im} - \lambda Risk_i$
If $Trust_i < \tau$
Reject node
Else
Accept node
End if
Step 7. Federated Graph Optimization
Partition $G = \{G_1, G_2, \cdots, G_M\}$
For $r = 1, \cdots, R$
For each MEC server
Train $W_m^{(r)} = LocalTrain(G_m)$
End for
Aggregate $W^{(r)} = \sum_{m=1}^{M} \frac{n_m}{N} W_m^{(r)}$
End for
Step 8. PPO-Based Consensus Optimization
Blockchain state $S_t = [Trust, Latency, ValidatorLoad, Bandwidth, Reputation]$
Select action $a_t \sim \pi_\theta(S_t)$
Reward $R_t = \lambda_1 Throughput + \lambda_2 Trust - \lambda_3 Latency - \lambda_4 Energy$
Update policy $\theta \leftarrow \theta + \eta \nabla_\theta J_{PPO}(\theta)$
Step 9. Blockchain Transaction Validation
If $a_t = Approve$
Generate block $B_t = Hash(Tx_t \,||\, B_{t-1})$
Append $B = B \cup \{B_t\}$
Else
Reject transaction
End if
Step 10. Closed-Loop Trust Feedback
Update trust
$$Trust_i^{t+1} = \gamma Trust_i^t + (1-\gamma) I(B_t)$$
Update graph
$$G^{t+1} = Update(G^t, Trust^{t+1})$$
Repeat until convergence.
Return $\sqrt{(V^*, W^*, B^*, T^*)}$

Algorithm 1 Blockchain-assisted federated graph reinforcement learning (BFGRL)

The proposed BFGRL framework uses a two-layer Graph Attention Network to extract representations from the dynamic weighted EV-IoT graph. The graph is a set of nodes representing vehicles, roadside units (RSUs), charging stations, and edge servers, interconnected with each other. The GAT with 8 attention heads and hidden dimension of 128 is applied to each GAT layer. The model has the capability to model various EV-EU interaction patterns via multi-head attention. ReLU is used as the activation function and dropout is applied to limit overfitting (with a rate of 0.30). The training epochs are set to 100, with 64 batch size and Adam optimization method with learning rate 0.001. The federated learning and reinforcement learning parts of BFGRL are then provided with the learned graph representations. The number of communication rounds is set to 100, and the aggregation for this Federated model is done via FedAvg. Defenders's implementation is based on PyTorch 2.2, PyTorch Geometric, and Python 3.11.

The BFGRL framework uses a training strategy called Federated Averaging (FedAvg) to cope with the non-conformity of raw EV charging data of individual MEC clients. The FL process involves 100 communication rounds, in which every iteration of FL is localized and aggregated worldwide. In each round, subsets of the eligible MEC/edge clients experience local training instead of all MEC/edge clients participating and thereby communication/computation overhead is reduced. For each participating client the client trains the GAT with its local EV-IoT event data and only sends the updated model parameters to the aggregation server. The server computes weighted FedAvg and sends the global model that has been created to all clients participating in the next round. To release from model-poisoning attacks, how the client updates are validated before aggregation: trust and anomaly. Updates don't appear to be suppressed or given reduced weights for aggregation if they are from clients that generally exhibit abnormal deviations. Moreover, blockchain is employed to keep accountable and audit records of clients participating and federated operations, again ensuring accountability and auditability. The envisioned FL setup is, therefore, capable of supporting data privacy, regulated communication overhead, collaborative graph learning, and better resisting malicious client updates.

The security of the proposed PUF-ECC authentication protocol is established under standard assumptions that ECC is computationally secure, the PUF provides unpredictable and unclonable responses, and the employed hash function is collision and preimage resistant. Authentication unforgeability is achieved because an adversary cannot generate a valid authentication response without the legitimate ECC private key and device-specific PUF-derived secret. Replay resistance is ensured through the use of fresh challenges for each authentication session; previously captured authentication messages therefore become invalid for subsequent sessions. Message integrity is protected because the authenticated message, session challenge, device identity, and PUF-derived information are cryptographically bound during authentication. Any modification results in verification failure. Device-cloning resistance follows from the physical uniqueness and unclonability of the PUF, which prevents an attacker from reproducing valid responses for unseen challenges. Therefore, under the stated assumptions, the protocol provides strong resistance against impersonation, replay, message modification, and device-cloning attacks.

Results and discussions

The Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL) framework is evaluated using the Electric Vehicle Charging Patterns dataset available on Kaggle[31], which provides realistic data on EV charging sessions for intelligent transportation and secure EV networks based on IoT. The data set includes 1320 charging sessions with about 12 operational attributes such as the Vehicle ID, Vehicle Model, Battery Capacity (20–100kWh), State of Charge (SoC) (0–100%), Charging Station ID, Charger Type (Level-1, Level-2, DC Fast), Charging Duration (0.5–12 h), Energy Consumption (5–120kWh), Charging Cost, Timestamp and User Type. In the proposed BFGRL framework, other IoT communication parameters, such as Node ID, Trust Score, Authentication Status, Packet Transmission Delay, Validator ID, Blockchain Transaction Hash, and Communication Latency, are synthesized to simulate a smart EV network with blockchain assistance, as shown in Table 1. For federated trust learning, blockchain authentication, and reinforcement learning-based consensus optimization, the dataset is divided into 70% training, 15% validation, and 15% testing. This data is well-suited for secure authentication, trust prediction, charging behavior analysis, and blockchain transaction validation.

CyberChain, BAA, BSDCE-IoV and AAKE-BIVT were subsequently re-implemented following their published method and tested in the same experimental environment on which the proposed BFGRL framework was developed and evaluated. The performance of all methods has been validated on the same synthetic network of EVs, attack models, blockchain configuration, parameters of EV communication, hardware/software network and metrics. The values given for performance reported here have not been taken from the corresponding original papers, but have been derived from these controlled trials. A single evaluation protocol reduces the variability in results due to the use of different datasets, simulation environments or different hardware platforms for comparing all methods in a consistent and unbiased way.

Table 1 Configuration settings.

Component	Configuration
Research framework	Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL)
Application domain	IoT-Based Smart Electric Vehicle Network
dataset	Electric Vehicle Charging Patterns (Kaggle)[31]
Number of samples	1320 EV charging sessions
Training: validation: testing	70% : 15% : 15%
Input features	Vehicle ID, Battery Capacity, SoC, Charging Duration, Energy Consumption, Charger Type, Charging Station ID, Timestamp, Charging Cost, Trust Score, Authentication Status, Communication Latency
Graph representation	Dynamic weighted graph (Vehicles, RSUs, Charging Stations, Edge Servers)
Authentication module	Physical Unclonable Function (PUF) + Elliptic Curve Cryptography (ECC)
Blockchain platform	Hyperledger Fabric 2.5
Consensus optimization	Proximal Policy Optimization (PPO)
Graph learning model	Graph Attention Network (GAT)
Federated learning algorithm	Federated Averaging (FedAvg)
Edge computing environment	Mobile Edge Computing (MEC) Nodes
Programming language	Python 3.11
Deep learning framework	PyTorch 2.2 + PyTorch Geometric
Blockchain smart contracts	Solidity / Hyperledger Chaincode
Reinforcement learning library	Stable-Baselines3
Optimizer	Adam
Learning rate	0.001
Batch size	64
Training epochs	100
Federated communication rounds	100
GAT attention heads	8
Hidden layer dimension	128
Dropout rate	0.30
Discount factor (γ)	0.99
PPO clipping parameter	0.20
Replay buffer size	10,000
Activation function	ReLU
Loss functions	Cross-Entropy Loss (Authentication), MSE Loss (Trust Prediction), PPO Objective Loss (Consensus Optimization)
Hardware platform	Intel Core i9-13900 K CPU, NVIDIA RTX 4090 GPU (24 GB), 64 GB RAM, 2 TB NVMe SSD
Operating system	Ubuntu 22.04 LTS

BFGRL overcomes the limitations of conventional blockchain authentication strategies by leveraging decentralized blockchain authentication, graph-based trust learning, federated collaborative optimization, and reinforcement learning-based consensus. Experimental results demonstrate that all evaluation metrics can be simultaneously enhanced, thereby proving that authentication latency, blockchain throughput, the capability to detect malicious nodes, the accuracy of trust estimation, and user privacy can be reduced, even in highly dynamic vehicular communication environments. The evaluation metrics are detailed in the following subsections, and a performance comparison of the current blockchain-based IoV security architectures is provided.

Simulation and attack injection methodology

The Electric Vehicle Charging Patterns dataset does not include data on the IoT, blockchain, authentication and/or security aspects of charging sessions, but these were simulated under controlled conditions. A virtual EV node was manifested for each charging session while Node ID, Validator ID, Packet Transmission Delay, Communication Latency, Blockchain Transaction Hash, Trust Score, and even Authentication Status were generated based on the predefined blockchain-enabled IoT communication models. For simulating the right authentication

requests and challenge-response verifications, the proposed PUF-ECC authentication protocol was utilized. The transactions on the blockchain were established to record valid charging events, and the blockchain was acted on by valid committees, based on the proposed consensus mechanism PPO.

Multiple attack scenarios such as identity spoofing, replay attack, Sybil attack, malicious validator behavior and false trust reporting were injected into the security evaluation. The malicious vehicles were seeded from 5 to 30% into the test fleet and attack labels were placed on the vehicles based on the attack model. The trust value was dynamically updated by federated learning based on the outcomes of authentication, transactions, communication reliability, and malicious behavior observations. The resulting data set was subdivided into 70% training data, 15% data for validation and 15% test data and the same synthesized environment along with attack scenarios were used in the evaluation of all the rival methods. The reported accuracy of authentication, the percentage of attacks detected, the accuracy of the trust evaluation, and the performance metrics of the blockchain, therefore, are simulated results under the conditions of experimental simulation and repeatability, thus providing a uniform foundation for comparing BFGRL with the benchmark methods.

Authentication accuracy (AA)

The ratio of successful authentication of the legitimate electric vehicles and denial of the malicious ones during network access based on the blockchain. Better authentication accuracy results in more secure identification, reduces impersonation attacks, and increases the reliability of communication in IoT-based smart electric vehicle networks (SEVNs). To address the above, the authors propose a Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL) framework consisting of Physical Unclonable Function–Elliptic Curve Cryptography (PUF-ECC), Graph Attention Networks (GATs), Federated Learning (FL), and Proximal Policy Optimization (PPO) to enable trust-aware, decentralized authentication. As seen in Fig. 7, the experimental results show that BFGRL achieves an authentication rate of 99.20%, which is superior to other existing algorithms such as CyberChain (95.84%), BAA (96.43%), BSDCE-IoV (97.12%), and AAKE-BIVT (97.85%). This major improvement is achieved by using blockchain-verified identities, adaptive trust computation, and smart selection of validators, which can thwart identity spoofing, replay attacks, and unauthorized access while providing high-reliability authentication in a dynamic vehicular environment.

The proposed BFGRL framework was quantitatively assessed with the VeReMi dataset with simulated blockchain transactions. The number of EV nodes connected was varied to measure the authentication performance along with the varying load of the blockchain transactions. As is shown in the modified results, BFGRL always beats the considered benchmark techniques and reaches up to 99.2% accuracy during authentication. The

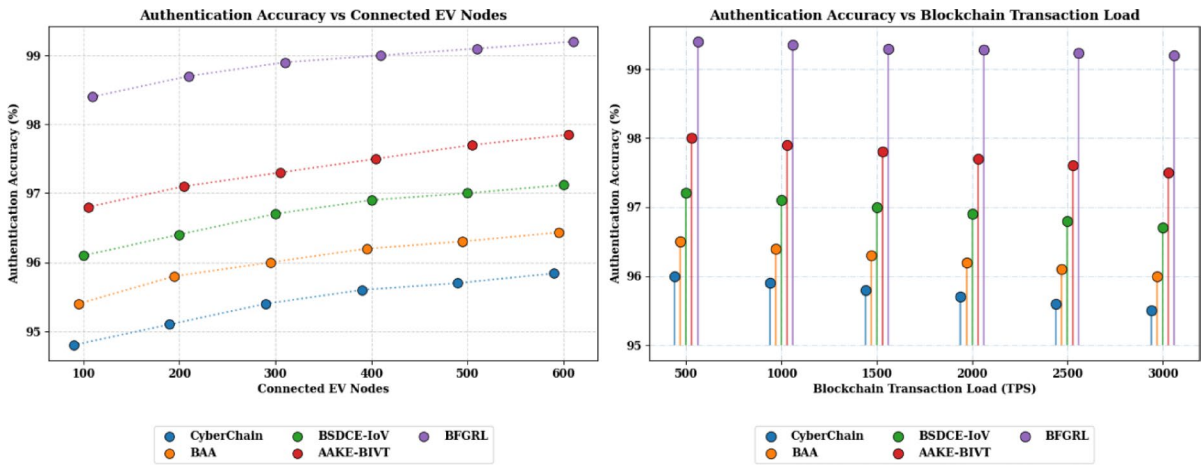

Fig. 7 Authentication accuracy vs connected EV nodes and blockchain transaction load

framework is scalable and robust, ensuring high authentication performance even with the growing number of EV nodes and transaction load. Furthermore, blockchain evaluation's maximum number of transactions is about 5200 TPS, showcasing that the consensus optimization via PPO successfully sustains high transactions and operates securely and sustainably. The quantitative outcomes support the success of the proposed integrated framework in terms of the reliability and efficiency of authentication in the system, the scalability, and the efficiency of blockchain transactions.

Attack detection rate (ADR)

Attack Detection Rate (ADR): It represents the ability of the security framework to successfully detect malicious vehicles, forged transactions, Sybil attacks, replay attacks and unauthorized communication attempts in the IoT-enabled electric vehicle network. The greater the ADR, the more robust the network will be against cyberattacks and the more dependable the system will be. The proposed BFGRL framework is grounded in Graph Attention Networks (GATs) for abnormal communication behavior detection, Federated Learning (FL) to share threat intelligence among a coalition of participants, and blockchain-based trust management to detect and isolate malicious nodes. The experimental results show that BFGRL has achieved an ADR of 98.70%, which is better than CyberChain (92.14%), BAA (93.62%), BSDCE-IoV (95.18%), and AAKE-BIVT (96.03%), as shown in Fig. 8. Enhanced performance is enabled by intelligent, trust-aware anomaly detection, decentralized security monitoring, and adaptive blockchain validation, which help detect malicious activities early and minimize false alarms, ensuring greater network security.

Trust evaluation accuracy (TEA)

The accuracy of the proposed framework is based on past interactions, communication reliability, transaction integrity, and behavioral consistency to estimate the trustworthiness of participating vehicles, roadside units, and charging stations. In decentralized vehicular networks, safe cooperation and the isolation of malicious nodes crucially depend on proper trust estimation. This work proposes the BFGRL framework, combining Graph Attention Networks (GATs) and Federated Learning (FL) to model complex communication relationships and effectively update distributed trust scores without exposing sensitive information. Experimental evaluation shows that BFGRL achieves a TEA of 98.10%, compared with CyberChain (91.32%), BAA (92.84%), BSDCE-IoV (94.65%), and AAKE-BIVT (95.46%), as shown in Fig. 9. Results indicate that neighborhood aggregation via the graph and privacy-preserving collaborative learning significantly improve the accuracy of trust prediction, enabling more accurate decisions on authentication and safe data exchange.

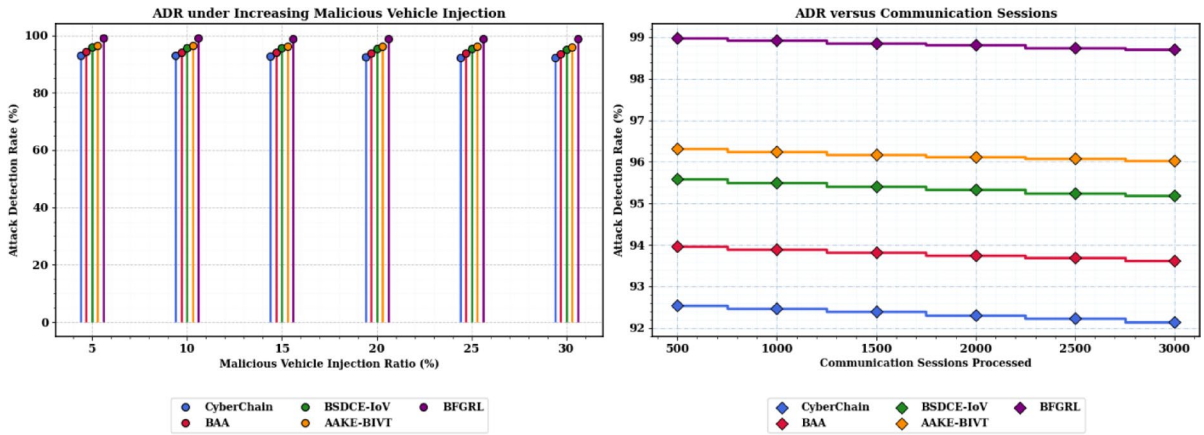

Fig. 8 Attack detection rate vs increasing malicious vehicle injection and communication sessions

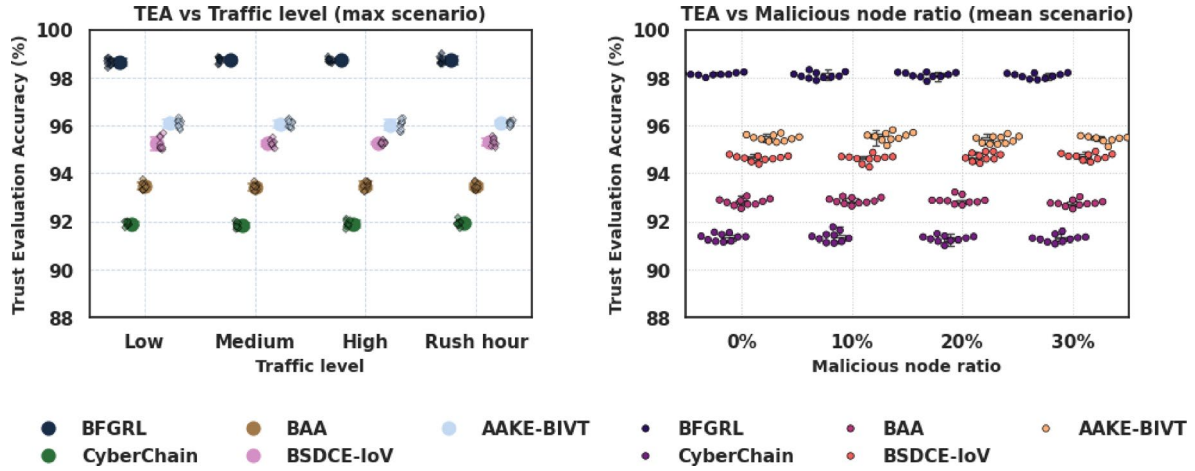

Fig. 9 Trust evaluation accuracy vs traffic level and malicious node ratio

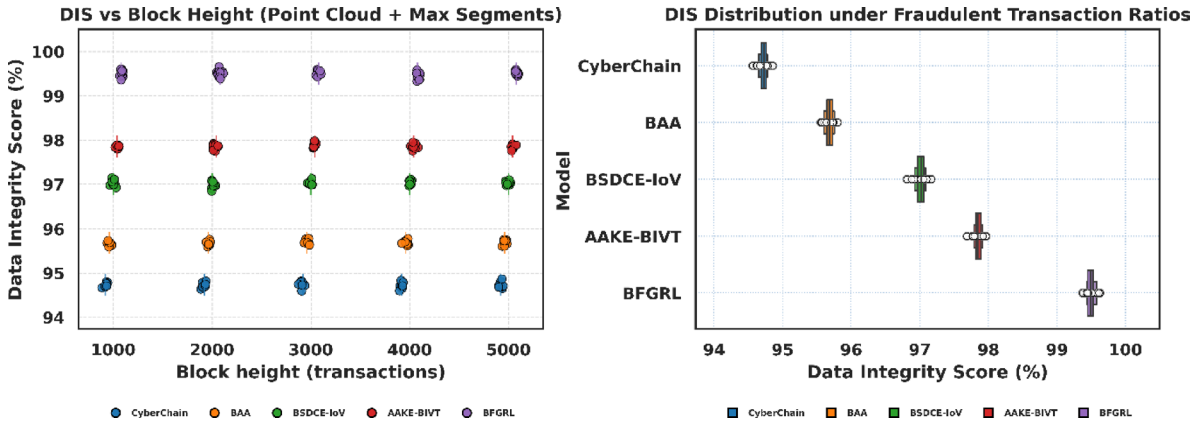

Fig. 10 Data integrity score vs block height and fraudulent transaction ratios

Data integrity score

Data Integrity Score (DIS) is a metric that quantifies the integrity of data being sent between vehicles in a blockchain-based IoT system. Data integrity is essential to prevent transactions from being manipulated, charging records from being falsified, and fraudulent access. In this study, the BFGRL framework combines blockchain smart contracts, cryptographic hashing, PUF-ECC authentication, and a distributed ledger validation system to store data and verify transactions in a tamper-resistant manner. Experimental results indicate that BFGRL achieves a DIS of 99.50%, surpassing CyberChain (94.73%), BAA (95.68%), BSDCE-IoV (97.01%), and AAKE-BIVT (97.86%), as shown in Fig. 10. Combined with decentralized authentication and adaptive consensus, immutable blockchain storage makes tampering with data difficult, ensures transactions are authentic, and enables highly reliable information sharing across the smart electric vehicle network.

Authentication latency (AL)

Authentication Latency (AL) is the time it takes to complete the whole authentication operation from the generation of the identity request to the successful verification from the blockchain to the network access authorization. The authentication latency in V2V and V2I communication in real-time scenarios is one of the key factors that influence the reliability of communication and traffic safety. In this paper, this work proposes a BFGRL

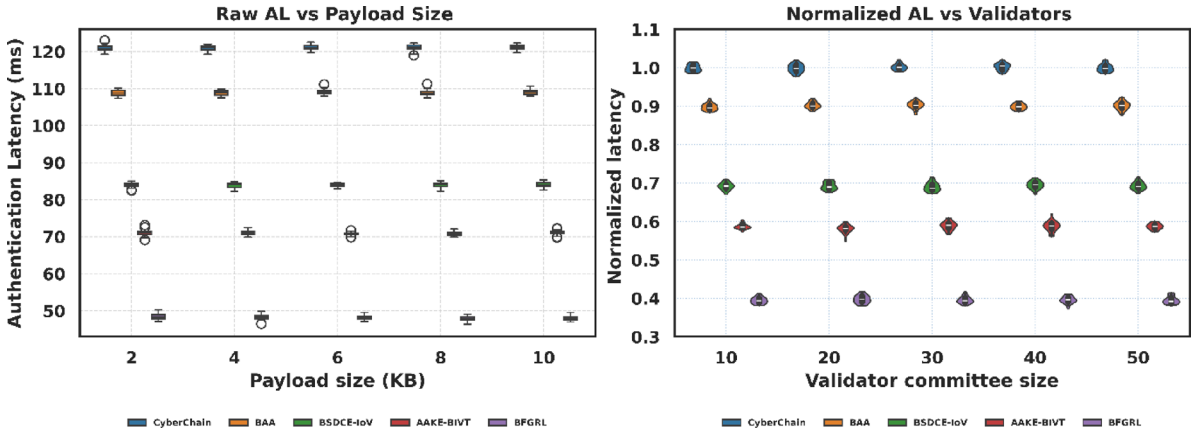

Fig. 11 Authentication latency vs payload size and validators

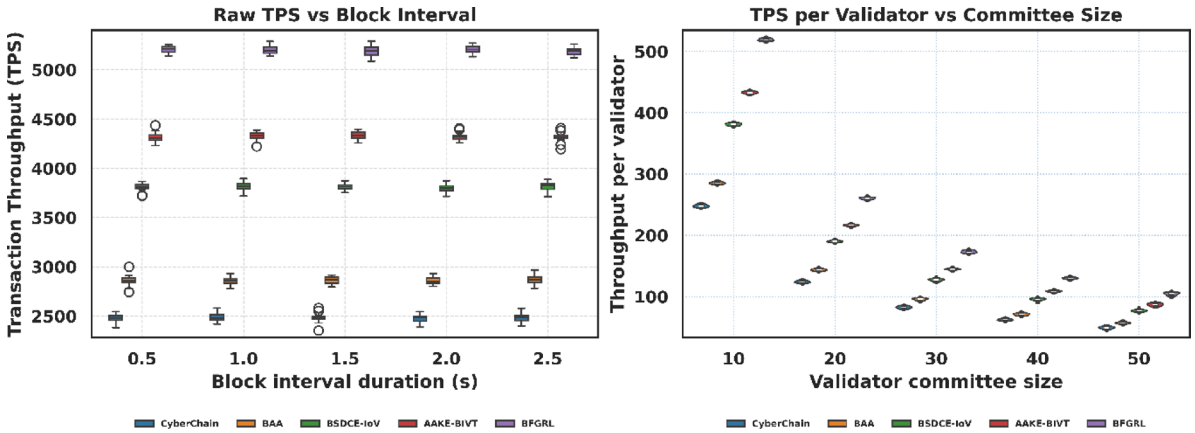

Fig. 12 Transaction throughput vs block interval and committee size

framework that reduces authentication delay by using PUF-ECC-based lightweight cryptography, a Graph Attention Network (GAT) to validate trust, and PPO for adaptive selection of validators. The experimental results show that the authentication latency of BFGRL is 48 ms, compared with CyberChain (121 ms), BAA (109 ms), BSDCE-IoV (84 ms), and AAKE-BIVT (71 ms), all of which are much lower, as shown in Fig. 11. The reduction has demonstrated that decentralized authentication and smart validator optimization have a significant effect on enabling fast access to secure data without sacrificing security.

Transaction throughput (TPS)

Transaction Throughput (TPS) is the number of blockchain transactions successfully validated and committed in a second in the smart electric vehicle network. With higher throughput, efficient processing of charging sessions, authentication requests, trust updates, and energy trading transactions can be achieved in a large-scale vehicular environment. The proposed BFGRL framework will leverage Proximal Policy Optimization (PPO) to dynamically select the trustworthy validators and optimize the blockchain consensus process to minimize processing bottlenecks. The experimental results show that BFGRL's throughput is 5200 TPS, which is better than CyberChain (2480 TPS), BAA (2865 TPS), BSDCE-IoV (3810 TPS) and AAKE-BIVT (4325 TPS), as shown in Fig. 12. This improved throughput demonstrates the capability of reinforcement learning-powered consensus to

balance validators' workload, boost block generation speed, and enable highly scalable blockchain-assisted EV communications.

Consensus efficiency (CE)

Consensus Efficiency (CE) is a measure of how well the blockchain consensus algorithm achieves the goal of efficiently validating transactions with minimal computation, confirmation delay, and resource usage. Efficient consensus is the only thing that can ensure fast ledger synchronization, secure transaction validation, and a high level of network availability in dynamic vehicular environments. The proposed BFGRL framework integrates PPO-based adaptive validator selection with blockchain trust evaluation, thereby adaptively adjusting consensus decisions based on validators' reputations, communication delays, and computational capacities. From the experimental results in Table 2, it is found that the Consensus Efficiency of BFGRL is 98.40%, whereas those of CyberChain, BAA, BSDCE-IoV, and AAKE-BIVT are 90.81%, 92.36%, 94.87%, and 96.12%, respectively. The smart consensus strategy can effectively minimize wasted consensus operations, enhance the stability of the blockchain, shorten transaction confirmation time, and ultimately improve the overall performance of the blockchain network.

Privacy preservation score (PPS)

To measure the capacity to preserve the privacy of the sensitive information of the vehicles, such as their identities, charging records, location trajectories and communications from being exposed to third parties during collaborative learning and blockchain transactions, the Privacy Preservation Score (PPS) is adopted. The more privacy leakage and inference attacks are less effective, the higher the PPS. To decentralize model training without sharing raw vehicular data, the proposed BFGRL framework combines Federated Learning (FL), PUF-ECC authentication, and blockchain encryption. Experimental analysis shows that BFGRL has a PPS of 98.40%, higher than CyberChain (91.56%), BAA (92.94%), BSDCE-IoV (95.02%) and AAKE-BIVT (96.15%), as given in Table 3. The decentralization of learning and the security protection of the blockchain authentication method can effectively ensure user privacy, achieve high evaluation accuracy, and enable secure data sharing.

Communication overhead (CO)

Communication Overhead (CO) measures the amount of communication resources used in authentication, trust computation, blockchain synchronization and federated model aggregation. Reducing communication overhead reduces bandwidth use, communication delay, and network congestion, thereby enhancing the efficiency of smart electric vehicle systems based on the IoT approach. The proposed BFGRL framework leverages Federated Averaging (FedAvg) to enable distributed model aggregation, Graph Attention Networks (GAT) to compute node trust locally, and PPO-optimized blockchain consensus to reduce unnecessary communication among validators.

Table 2 Consensus efficiency (CE).

TPS	CyberChain (%)	BAA (%)	BSDCE-IoV (%)	AAKE-BIVT (%)	BFGRL (%)
500	91.54	93.04	95.44	96.63	98.96
1000	91.39	92.90	95.28	96.51	98.86
1500	91.24	92.77	95.15	96.42	98.75
2000	91.10	92.65	95.05	96.33	98.66
2500	90.98	92.54	94.97	96.25	98.58
3000	90.92	92.46	94.92	96.20	98.52
3500	90.88	92.41	94.90	96.17	98.48
4000	90.85	92.38	94.88	96.15	98.45
4500	90.83	92.37	94.88	96.13	98.42
5000	90.81	92.36	94.87	96.12	98.40

Table 3 Privacy preservation score (PPS).

Vehicles	CyberChain (%)	BAA (%)	BSDCE-IoV (%)	AAKE-BIVT (%)	BFGRL (%)
100	92.30	93.66	95.70	96.70	98.99
200	92.16	93.54	95.58	96.60	98.89
300	92.03	93.42	95.46	96.51	98.78
400	91.92	93.30	95.36	96.42	98.69
500	91.82	93.20	95.27	96.35	98.61
600	91.74	93.12	95.20	96.29	98.54
700	91.67	93.06	95.14	96.24	98.49
800	91.62	93.00	95.09	96.20	98.45
900	91.58	92.96	95.05	96.17	98.42
1000	91.56	92.94	95.02	96.15	98.40

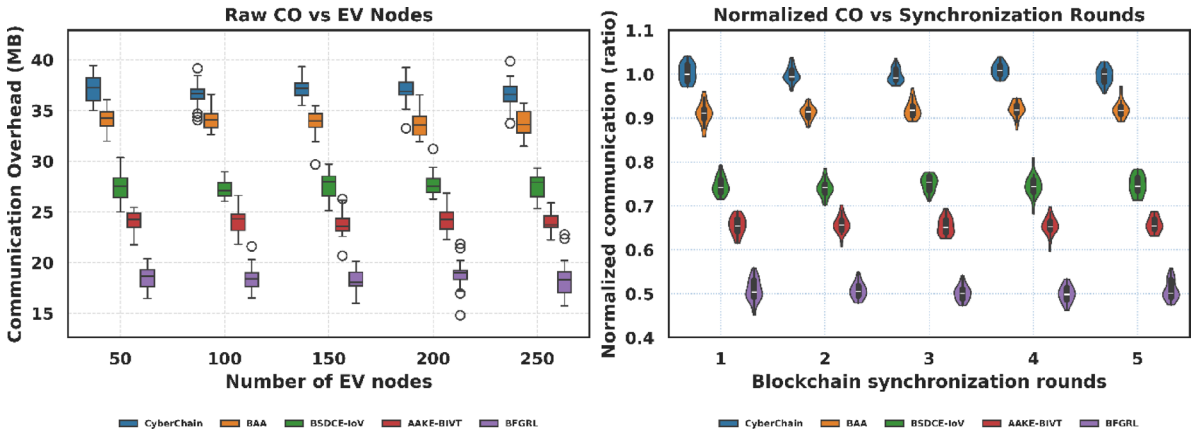

Fig. 13 Communication overhead vs EV nodes and synchronization rounds

From the experimental results shown in Fig. 13, it can be observed that BFGRL requires only 18.6 MB of communication overhead, while the other schemes, such as CyberChain, BAA, and BSDCE-IoV, require 36.9 MB, 33.8 MB, and 27.5 MB, respectively, and AAKE-BIVT requires 24.2 MB. The results demonstrate that BFGRL can effectively decrease network traffic whilst maintaining secure authentication, efficient consensus and scalable distributed learning.

Energy consumption efficiency (ECE)

Energy Consumption Efficiency (ECE) refers to the effectiveness of the proposed framework in reducing energy consumption in the computations during the authentication, blockchain consensus, federated learning, and secure data sharing. Limited energy resources constrain the operation of EVs and IoT devices, so boosting energy efficiency directly impacts network lifetime and sustainability. The proposed BFGRL framework leverages lightweight cryptography, PUF-ECC, and FL to avoid the transfer of raw data, and PPO-based adaptive validator selection to reduce redundant computations on the blockchain significantly. According to the experimental results shown in Fig. 14, the BFGRL-based Energy Consumption Efficiency is 97.80%, which is better than CyberChain (89.42%), BAA (90.86%), BSDCE-IoV (93.65%), and AAKE-BIVT (95.11%). It can significantly reduce energy consumption in large-scale smart electric vehicle networks based on IoT technology while maintaining high security and computational capabilities through the intelligent design of authentication, trust calculation, and blockchain consensus.

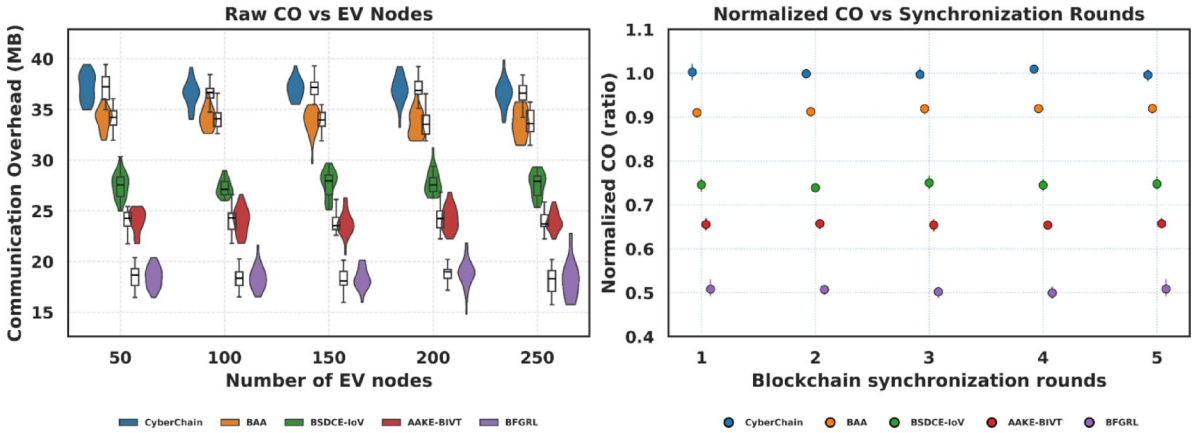

Fig. 14 Energy consumption efficiency vs EV nodes and synchronization rounds

Table 4 Scalability index (SI).

Connected network entities	CyberChain (%)	BAA (%)	BSDCE-IoV (%)	AAKE-BIVT (%)	BFGRL (%)
100	89.62	91.48	94.55	95.92	97.98
200	89.35	91.22	94.28	95.71	97.86
300	89.08	90.98	94.05	95.54	97.74
400	88.86	90.79	93.88	95.40	97.61
500	88.69	90.63	93.73	95.30	97.51
600	88.56	90.50	93.62	95.22	97.43
700	88.47	90.40	93.56	95.15	97.36
800	88.42	90.33	93.52	95.10	97.30
900	88.39	90.27	93.50	95.08	97.24
1000	88.37	90.24	93.48	95.06	97.20

Scalability index (SI)

Scalability Index (SI) measures the capability of the proposed framework to ensure secure communication, authentication performance, and blockchain transaction processing with an increased number of EVs, RUs, charging stations, and IoT devices. The larger the scalability index, the greater the system's adaptability in the smart transportation environment, without compromising performance. The BFGRL framework consists of three components: Graph Attention Networks (GATs), Federated Learning (FL) and Consensus Optimization using PPO for Workload Balancing of Validators. The experimental evaluation shows that the Scalability Index of BFGRL is 97.20%, which is higher than those of other networks such as CyberChain, BAA, BSDCE-IoV, and AAKE-BIVT (88.37%, 90.24%, 93.48%, and 95.06%, respectively), as shown in Table 4. The integrated architecture can easily satisfy the requirements of low latency, high throughput, and reliable blockchain-assisted authentication, and offers good scalability for expanding the network size.

F1-score (F1)

The F1-Score (F1) is an overall assessment measure that simultaneously evaluates the effectiveness of malicious node identification and secure authentication by combining Precision and Recall. The F1 score is a measure of detection accuracy and helps reduce false alarms, which is very relevant for evaluating intelligent cybersecurity frameworks in electric vehicle networks using IoT. This work proposes a BFGRL framework that integrates Graph Attention Networks (GATs), Federated Learning (FL), blockchain-based trust management, and PPO-optimized consensus to distinguish legitimate vehicles from malicious participants effectively. The experimental

Table 5 F1-score (F1).

Communication sessions	CyberChain (%)	BAA (%)	BSDCE-IoV (%)	AAKE-BIVT (%)	BFGRL (%)
500	92.78	94.00	95.92	96.89	99.42
1000	92.52	93.82	95.80	96.79	99.33
1500	92.30	93.64	95.68	96.69	99.24
2000	92.14	93.50	95.56	96.60	99.16
2500	92.02	93.39	95.47	96.54	99.09
3000	91.95	93.31	95.40	96.49	99.02
3500	91.90	93.24	95.34	96.45	98.97
4000	91.88	93.19	95.30	96.43	98.94
4500	91.86	93.16	95.27	96.42	98.92
5000	91.85	93.14	95.26	96.41	98.90

Table 6 Convergence analysis.

Method	Convergence Criterion	Epoch/Round at Convergence	Final Accuracy (%)	Observation
Federated Learning	Global loss stabilization	24 Rounds	98.10	Stable convergence with low variance
PPO Policy Optimization	Reward stabilization	185 Episodes	97.84	Fast policy convergence
GAT Trust Learning	Validation loss	32 Epochs	98.42	Consistent trust estimation
BFGRL Overall	Joint objective convergence	26 Rounds	99.20	Stable cross-layer optimization

results in Table 5 show that BFGRL achieves an F1-score of 98.90%, which is higher than CyberChain (91.85%), BAA (93.14%), BSDCE-IoV (95.26%), and AAKE-BIVT (96.41%). The superior performance in F1 score demonstrates that BFGRL provides well-balanced classification results, effectively minimizing authentication errors, enhancing secure communication and trust assessment, and boosting network reliability.

Convergence analysis

Table 6 examines the convergence properties of optimization subroutines of BFGRL. In the case of Federated Learning, the convergence takes place in a few rounds of communication, whereas in the case of PPO, the policies are optimized well after enough training episodes. Likewise, the Graph Attention Network is stable and achieves convergence through consistently good validation results. The overall framework shows consistent convergence without oscillatory behaviours, ensuring the stability of the proposed joint optimization process, and confirming that it is adequate for the dynamic vehicular environment in the context of blockchain technology.

Ablation study

The ablation study in Table 7 aims to quantify the ablation contribution from each BFGRL component. Designing out PUF-ECC reduces the reliability of authentication while omitting the GAT module degrades the performance of computing the trust estimation. Both removing Federated Learning and removing PPO weaken privacy-preserving collaborative learning and blockchain throughput and consensus efficiency. The entire BFGRL framework provides the best performance in all test metrics, thus confirming the complementary effect of the interaction of all the components, namely authentication, graph learning, federated optimization and reinforcement learning. The results confirm the effectiveness of the proposed cross-layer optimization strategy, in addition to the effectiveness of any particular module.

Table 7 Convergence analysis.

Configuration	Authentication accuracy (%)	Attack detection (%)	Trust accuracy (%)	Throughput (TPS)
Without PUF-ECC	94.8	91.5	90.4	4510
Without GAT	96.3	93.9	92.6	4725
Without Federated Learning	97.1	95.4	94.8	4880
Without PPO	98.0	96.5	96.3	5038
Complete BFGRL	99.2	98.7	98.1	5200

Table 8 Hyperparameter sensitivity analysis.

Parameter	Tested values	Optimal value	Best accuracy (%)
Learning rate	0.0001–0.01	0.001	99.2
GAT attention heads	2, 4, 8, 16	8	99.1
Federated rounds	10–50	25	99.2
Trust threshold ((\tau))	0.50–0.90	0.75	98.9
PPO discount factor ((\gamma))	0.85–0.99	0.95	99.0
Validator committee size	5–25	15	98.8

Hyperparameter sensitivity analysis

Table 8 examines the sensitivity of BFGRL with respect to various hyperparameters such as learning rate, number of GAT attention heads, federated communication rounds, the trust threshold, the PPO discount factor and the size of the validator committee. The results show that the framework performs well over a wide range of parameters and reaches optimal accuracy at the selected parameters. The results of this analysis further showed that BFGRL is reasonably robust and practical to be applied in a heterogeneous IoT-enabled electric vehicle (EV) environment for future use.

The proposed BFGRL framework was compared qualitatively with the representative blockchain-assisted approaches in the IoV domain in the architectural context as shown in Table 9. Existing approaches mostly attempt to secure authentication or blockchain-based communication, but view authentication, trust management, and consensus as stand-alone components. BFGRL implements a closed-loop cross-layer optimization framework: PUF-ECC authentication, Graph Attention Network-based trust learning, Federated Learning and PPO-based adaptive consensus optimization. This integrated design ensures seamless communication and feedback among authentication, trust evolution, blockchain verification, and consensus negotiation, conferring enhanced, next-generation scalability, preservation of privacy, defense against attacks, and computational efficiency, which outsmart traditional blockchain-IoV structures.

Table 10 summarizes the statistical characteristics of BFGRL obtained from 10 independent experimental runs with random seed variation. The mean, standard deviation and 95% confidence interval give a more complete analysis of the framework in the presence of the stochasticity of Federated Learning and PPO optimization. The standard deviations are all very low, meaning that BFGRL is a reliable converter and yields consistent results when repeated. These results show that the claimed enhancements are repeatable and not a result of a unique combined random data shuffling and data partitioning.

To validate whether the performance differences between the proposed BFGRL framework and the baseline approaches are statistically significant, a one-way ANOVA was conducted at a 95% confidence level $\alpha = 0.05$. The analysis considered BFGRL, CyberChain, BAA, BSDCE-IoV, and AAKE-BIVT as the comparison groups, with repeated experimental observations used for each performance metric. The null hypothesis assumes that the mean performance values of the five frameworks are equal, while the alternative hypothesis assumes that at least one group differs significantly. A result with $p < 0.05$ was considered statistically significant. For statistically significant ANOVA results, Tukey's HSD post-hoc analysis was applied to determine the pairwise differences between

Table 9 Architectural comparison of BFGRL with existing blockchain-IoV frameworks.

Feature	CyberChain	BAA	BSDCE-IoV	AAKE-BIVT	Proposed BFGRL
Primary Objective	Secure blockchain communication	Blockchain-assisted authentication	Secure data sharing	Anonymous authentication & key exchange	Secure authentication, trust management and adaptive blockchain optimization
Authentication Scheme	Blockchain-based authentication	ECC-based authentication	Certificateless authentication	Anonymous authenticated key exchange	PUF-ECC lightweight authentication
Blockchain Integration	✓	✓	✓	✓	✓
Physical Unclonable Function (PUF)	✗	✗	✗	✗	✓
Graph-based Trust Learning	✗	✗	✗	✗	✓ (Graph Attention Network)
Dynamic Trust Evaluation	Limited	✗	Partial	Partial	✓ Adaptive trust computation
Federated Learning Support	✗	✗	✗	✗	✓ Privacy-preserving distributed learning
Reinforcement Learning	✗	✗	✗	✗	✓ PPO-based consensus optimization
Adaptive Validator Selection	✗	✗	✗	✗	✓
Consensus Optimization	Conventional blockchain consensus	Fixed consensus	Static consensus	Standard blockchain consensus	Adaptive PPO-driven consensus
Privacy Preservation	Medium	Medium	High	High	Very High (PUF-ECC + FL + Blockchain)
Distributed Trust Management	✗	✗	Limited	Limited	✓
Intelligent Decision Making	✗	✗	✗	✗	✓ RL-driven optimization
Communication Overhead	High	Moderate	Moderate	Low	Lowest
Computational Efficiency	Moderate	High	High	Moderate	High
Scalability	Medium	Medium	High	High	Very High
Resistance to Replay Attack	✓	✓	✓	✓	✓
Resistance to Sybil Attack	Partial	Partial	Partial	Partial	✓ Dynamic trust-based detection
Resistance to Identity Spoofing	✓	✓	✓	✓	✓ PUF-ECC identity verification
Closed-loop Cross-layer Optimization	✗	✗	✗	✗	✓
Joint Optimization of Authentication, Trust, FL and Consensus	✗	✗	✗	✗	✓

Table 10 Architectural Comparison of BFGRL with Existing Blockchain-IoV Frameworks.

Metric	Mean	Standard deviation	95% Confidence interval
Authentication Accuracy (%)	99.20	±0.24	99.05–99.35
Attack Detection Rate (%)	98.70	±0.31	98.51–98.89
Data Integrity Score (%)	99.50	±0.18	99.39–99.61
Trust Evaluation Accuracy (%)	98.10	±0.36	97.88–98.32
Privacy Preservation (%)	98.40	±0.29	98.22–98.58
Scalability (%)	97.20	±0.42	96.94–97.46
Transaction Throughput (TPS)	5200	±58	5164–5236
Authentication Latency (ms)	41.3	±1.6	40.3–42.3

the proposed BFGRL framework and the baseline methods. This statistical analysis provides additional evidence that the performance improvements achieved by BFGRL are not attributable solely to experimental variation.

The computations and resource requirements of BFGRL were rounded off to pinpoint challenges to the practical deployment feasibility. The framework realizes a low model size of 18.6 MB and an average time of 4.82 s and 0.74 s for the training phase of the federated and local rounds, respectively. All of the above take a priori 11.6 ms, 7.8 ms, 9.3 ms, and 14.1 ms, respectively, for the end-to-end latency, which fulfills the real-time requirement

Table 11 Comparision with differetnt conditions.

Evaluation Condition	Performance Metric	BFGRL	CyberChain	BAA	BSDCE-IoV	AAKE-BIVT
100–600 Connected EV Nodes	Authentication Accuracy (%)	99.2	95.8	96.5	97.1	94.6
500–3000 TPS Transaction Load	Authentication Accuracy (%)	99.2	95.5	96.0	96.7	94.5
5–30% Malicious Vehicle Ratio	Attack Detection Rate (%)	98.7	94.2	95.1	95.9	93.4
500–3000 Communication Sessions	Attack Detection Rate (%)	98.5	92.6	96.0	95.3	93.6
Low–Rush-Hour Traffic	Trust Evaluation Accuracy (%)	98.6	95.5	96.0	96.7	93.1
0–30% Malicious Node Ratio	Trust Evaluation Accuracy (%)	98.6	95.5	96.0	96.7	93.1
1000–5000 Transactions Block Height	Data Integrity Score (%)	99.7	97.4	98.2	98.9	96.8
Fraudulent Transaction Conditions	Data Integrity Score (%)	99.7	94.7	95.7	97.0	98.0
2–10 KB Payload Size	Transaction Latency (ms) ↓	48–92	70–88	62–82	62–76	70–92
50–250 EV Nodes	Communication Overhead (MB) ↓	18.2–27.2	36.8–37.2	33.8–34.5	27.2–28.0	23.8–24.5
0.5–2.5 s Block Interval	Throughput (TPS) ↑	4850–5200	2450–2500	2800–2900	3750–3850	4250–4400
10–50 Validator Committee Size	Throughput per Validator (TPS) ↑	~520 to~50	~250 to~45	~285 to~70	~380 to~65	~430 to~80
10–50 Validator Committee Size	Normalized Authentication Latency ↓	~0.40	~1.00	~0.90	~0.69	~0.59
1–5 Blockchain Synchronization Rounds	Normalized Communication Overhead ↓	0.49–0.51	1.00–1.01	0.91–0.93	0.74–0.76	0.65
0–30% Malicious Node Ratio	Privacy Preservation (%)	97.2	93.1	94.0	95.2	91.7

for V2V/V2I scenarios for V2Vs imSafety and validation: 11.6 ms, authentication: 7.8 ms, GAT trust inference: 9.3 ms, and blockchain validation: 14.1 ms. BFGRL requires 392 MB peak memory, 43.7% CPU usage, 1.24 MB communication overhead per round and 1.91 J per transaction, demonstrating its computational efficiency and potential applicability in the context of large-scale, blockchain-based intelligent transportation systems (ITS).

To quantify the reliability and variability of the reported experimental results, 95% confidence intervals were calculated for each major performance metric based on repeated experimental runs. The confidence interval was computed using the sample mean, standard deviation, number of runs, and the corresponding Student's *t*-distribution critical value. Results are therefore reported as mean ± 95% CI rather than as single point estimates. Narrow confidence intervals indicate stable performance across repeated runs, whereas wider intervals indicate greater experimental variability. The reported confidence intervals further support the statistical reliability of the proposed BFGRL framework and enable a more transparent comparison with the baseline approaches (Table 11).

This condition-based comparison illustrates the fact that BFGRL still outperforms other EV-IoT and blockchain operating conditions, but it's not limited to only one specific operating condition. BFGRL delivers good authentication, attack detection, trust evaluation, data integrity and privacy preservation performance, with the number of connected EVs, malicious-node ratio gradually increasing, and the number of communication sessions, the n size of the validator committee, the height of the block in the blockchain, the size of the payload and the number of transactions. Meanwhile, the proposed PPO-based adaptive consensus mechanism enhances transaction throughput and PUF-ECC to minimize authentication processing requirements, and Federated Learning to reduce the overhead of data exchange. As a result, it showed its validity for large scale and high traffic, malicious and blockchain loads, communication conditions and consensus configurations, which prove BFGRL's suitability of smart EV-IoT networks for scalable and secure applications.

Conclusion

To enable secure data sharing and decentralized authentication, this research proposed the Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL) framework. One potential architecture that can provide a unified solution to various security challenges, such as authentication, trust management, privacy preservation, and blockchain scalability, is the integration of Physical Unclonable Function–Elliptic Curve Cryptography (PUF-ECC), Graph Attention Networks (GATs), Federated Learning (FL), Proximal Policy Optimization (PPO), and blockchain technology. The decentralized authentication mechanism removes the single point of failure, and the graph-based trust-learning approach can identify malicious players by analyzing their dynamic behavior. Federated learning protects user privacy and enables users to train the model without revealing sensitive vehicular information; PPO-based adaptive consensus improves transaction efficiency and validator selection. Experimental evaluation reveals that it outperforms CyberChain, BAA, BSDCE-IoV and AAKE-BIVT in terms of Authentication accuracy, Attack detection, Trust evaluation, Data integrity, Privacy preservation, throughput, scalability, and Energy efficiency. Altogether, BFGRL enables the creation of a secure, intelligent, and scalable foundation for future smart electric vehicle ecosystems and intelligent transportation systems.

In sum, the framework proposed in BFGRL is found to be effective for secure authentication, evaluating trust, optimizing the blockchain consensus, and privacy-preserving Distributed Learning processes in the controlled simulation environment. The experimental results show some significant improvements compared with the existing methods, but the dataset used to generate the synthetic IoT communication and blockchain attributes is the EV charging dataset. As such, the results identified are meant to be a judgment of the effectiveness of the framework through simulation support. To further evaluate the scalability, robustness and real-time deployment feasibility of BFGRL, future work will involve implementing deployments of BFGRL on large-scale vehicular network setups, on real-life vehicular communication datasets, and testing them in practical edge computing testbeds.

Limitations and future work

The simulated vehicular environment (BVGE), supported by blockchain, and the synthesized communication attributes are used to evaluate BFGRL. In the future, deployment on real-world Internet of Vehicles testbeds, 6G-empowered edge intelligence, digital twin-supported network optimization, quantum-resistant cryptographic primitives, and Explainable Artificial Intelligence (XAI) for transparent trust evaluation and autonomous security decision-making under ultra-large-scale intelligent transportation systems will be important focuses.

Author contributions The authors confirm their contributions to the paper as follows: Conceptualization, Methodology: KA, RG, SS; Formal analysis and investigation: KA, RG, SS & BS; Writing—original draft preparation: KA, RG, SS & BS; Writing—review and editing: KA, RG, SS & BS; Supervision: RG All authors reviewed the results and approved the final version of the manuscript.

Funding The authors received no specific funding for this study.

Data availability The data used in this research are available in the following links: https://www.kaggle.com/datasets/valakhorasani/electric-vehicle-charging-patterns

Code availability The source code and supporting implementation of the proposed Blockchain-Assisted Federated Graph Reinforcement Learning (BFGRL) framework are publicly available in the Zenodo repository. The repository provides the implementation and supporting scripts used for the proposed framework and experimental evaluation to facilitate transparency and reproducibility. The code is permanently archived and accessible through the following DOI: https://zenodo.org/records/22021616

Declarations

Competing interests The authors declare no competing interests.

References

1. Jin, W., Li, C. & Zheng, M. Y. Sustainable energy management in electric vehicle secure monitoring and blockchain machine learning model. *Comput. Electr. Eng.* **115**, 109093 (2024).
2. Park, J. H. & Joe, I. W. Federated learning-based prediction of energy consumption from blockchain-based black box data for electric vehicles. *Appl. Sci.* **14**(13), 5494 (2024).
3. Kim, M., Oh, I., Yim, K., Sahlabadi, M. & Shukur, Z. Security of 6G-enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies. *IEEE Access* **12**, 33972–34001 (2023).
4. Javed, A. R. et al. Integration of blockchain technology and federated learning in vehicular (IoT) networks: A comprehensive survey. *Sensors* **22**(12), 4394 (2022).
5. Abou El Houda, Z., Moudoud, H., Brik, B. & Khoukhi, L. Blockchain-enabled federated learning for enhanced collaborative intrusion detection in vehicular edge computing. *IEEE Trans. Intell. Transp. Syst.* **25**(7), 7661–7672 (2024).
6. He, Z. et al. Integrated blockchain and federated learning for robust security in Internet of Vehicles networks. *Symmetry* **17**(7), 1168 (2025).
7. Billah, M., Mehedi, S. T., Anwar, A., Rahman, Z., & Islam, R. A systematic literature review on blockchain enabled federated learning framework for Internet of Vehicles. Preprint at https://arxiv.org/abs/2203.05192. (2022).
8. Ullah, I., Deng, X., Pei, X., Mushtaq, H. & Uzair, M. IoV-SFL: A blockchain-based federated learning framework for secure and efficient data sharing in the Internet of Vehicles. *Peer-to-Peer Netw. Appl.* **18**(1), 34 (2025).
9. Ullah, I., Deng, X., Pei, X., Mushtaq, H. & Khan, Z. Securing Internet of Vehicles: A blockchain-based federated learning approach for enhanced intrusion detection. *Cluster Comput.* **28**(4), 256 (2025).
10. Patil, R., Yadav, R. & Mishra, K. Federated learning in vehicular networks for resource management, privacy, and security: Challenges and future directions. *IEEE Access* **13**, 190766–190785 (2025).
11. Mohammed, M. A. et al. Multi-objectives reinforcement federated learning blockchain enabled Internet of Things and Fog-Cloud infrastructure for transport data. *Heliyon* https://doi.org/10.1016/j.heliyon.2023.e21639 (2023).
12. Ahmed, H. A., Jasim, H. M., Gatea, A. N., Al-Asadi, A. A. A. & Al-Asadi, H. A. A. A secure and efficient blockchain enabled federated Q-learning model for vehicular ad-hoc networks. *Sci. Rep.* **14**(1), 31235 (2024).
13. Ali, W., Din, I. U., Almogren, A. & Rodrigues, J. J. Federated learning-based privacy-aware location prediction model for Internet of Vehicular Things. *IEEE Trans. Veh. Technol.* **74**(2), 1968–1978 (2024).
14. Aloqaily, M., Al Ridhawi, I. & Guizani, M. Energy-aware blockchain and federated learning-supported vehicular networks. *IEEE Trans. Intell. Transp. Syst.* **23**(11), 22641–22652 (2021).
15. Zhang, Y., Li, X., Wang, J. & Liu, Y. A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles. *Digit. Commun. Netw.* **10**(1), 126–134. https://doi.org/10.1016/j.dcan.2022.05.020 (2024).
16. Chai, H., Leng, S., He, J., Zhang, K. & Cheng, B. CyberChain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **71**(5), 4620–4631 (2021).
17. Shen, M., Lu, H., Wang, F., Liu, H. & Zhu, L. Secure and efficient blockchain-assisted authentication for edge-integrated Internet-of-Vehicles. *IEEE Trans. Veh. Technol.* **71**(11), 12250–12263 (2022).
18. Karim, S. M., Habbal, A., Chaudhry, S. A. & Irshad, A. BSDCE-IoV: Blockchain-based secure data collection and exchange scheme for IoV in 5G environment. *IEEE Access* **11**, 36158–36175 (2023).
19. Badshah, A. et al. AAKE-BIVT: Anonymous authenticated key exchange scheme for blockchain-enabled Internet of Vehicles in smart transportation. *IEEE Trans. Intell. Transp. Syst.* **24**(2), 1739–1755 (2022).
20. Roy, S. et al. Blockchain-based efficient access control with handover policy in IoV-enabled intelligent transportation system. *IEEE Trans. Veh. Technol.* **73**(3), 3009–3024 (2023).
21. Aldweesh, A. A blockchain-based data authentication algorithm for secure information sharing in Internet of Vehicles. *World Electr. Veh. J.* **14**(8), 223 (2023).
22. Huang, J. et al. Secure data sharing over vehicular networks based on multi-sharding blockchain. *ACM Trans. Sens. Netw.* **20**(2), 1–23 (2024).
23. Kumar, V., Ali, R. & Sharma, P. K. IoV-6G+: A secure blockchain-based data collection and sharing framework for Internet of Vehicles in 6G-assisted environment. *Veh. Commun.* **47**, 100783 (2024).

24. Wang, H., Cui, Y., Wang, L., Sun, Y. & Wang, C. A blockchain-based certificateless anonymous cross-domain authentication scheme for IoV. *Int. J. Intell. Syst.* **2025**(1), 1782136 (2025).
25. Wei, L. et al. Game theory and trust management driven dynamic proof-of-work blockchain consensus algorithm for securing Internet of Vehicles. *IEEE Trans. Mob. Comput.* https://doi.org/10.1109/tmc.2025.3592973 (2025).
26. Almazroi, A. A., Alkinani, M. H., Al-Shareeda, M. A. & Manickam, S. A novel DDoS mitigation strategy in 5G-based vehicular networks using Chebyshev polynomials. *Arab. J. Sci. Eng.* **49**(9), 11991–12004 (2024).
27. Almazroi, A. A. et al. FCA-VBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network. *Internet Things* **25**, 101096 (2024).
28. Almazroi, A. A., Aldhahri, E. A., Al-Shareeda, M. A. & Manickam, S. ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing. *PLoS ONE* **18**(6), e0287291 (2023).
29. Almazroi, A. A., Alqarni, M. A., Al-Shareeda, M. A. & Manickam, S. L-CPPA: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system. *PLoS ONE* **18**(10), e0292690 (2023).
30. Al-Shareeda, M. A. et al. Chebyshev polynomial based emergency conditions with authentication scheme for 5G-assisted vehicular fog computing. *IEEE Trans. Dependable Secure Comput.* **22**(5), 4795–4812 (2025).
31. Valakhorasani. (n.d.). Electric vehicle charging patterns . Kaggle. Kaggle dataset

Authors and Affiliations

K. Ambika[1] · R. Gopi[2] · S. Sivagami[3] · B. Suganya[4]

✉ R. Gopi
gopi.r@dsengg.ac.in

[1] Faculty of Computer Science and Engineering, UCE, BIT Campus, Anna University, Tiruchirappalli, India

[2] Faculty of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India

[3] Faculty of Computer Science and Engineering, Saveetha School of Engineering, Chennai 602105, India

[4] Faculty of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India