

BLOCKCHAIN-ENABLED FUZZY MACHINE LEARNING FRAMEWORK FOR CYBERSECURITY IN CLOUD CONNECTED ELECTRIC VEHICLES

J RAVINDRA BABU¹, RAYUDU SRINIVAS², S MANI KUCHIBHATLA³, A PRANEETHA⁴,
M SIVASANKARA RAO⁵, A V KRISHNARAO PADYALA⁶, D N V SATYANARAYANA⁷

¹Associate Professor, Department of Electronics and Communication Engineering,
Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India

²Assistant Professor, Department of Electrical and Electronics Engineering, Aditya university,
Surampalem, Andhra Pradesh, India

³Professor, Department of Electrical & Electronics Engineering, ACE Engineering College, Hyderabad,
Telangana, India

⁴Assistant Professor, Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

⁵Sr Assistant Professor, Department of Electronics and Communication Engineering,
Lakireddy Bali Reddy College of Engineering, Mylavaram, Andhra Pradesh, India

⁶Assistant Professor, Department of Computer Science and Engineering (Data Science),
R.V. R & J.C. College of Engineering, Guntur, Andhra Pradesh, India

⁷Associate Professor, Department of Chemical Engineering, R.V. R & J.C. College of Engineering, Guntur,
Andhra Pradesh, India

E-mail: ¹jrb0009@gmail.com, ²srinivasrayudu245@gmail.com, ³drsmanik21@gmail.com,

⁴nyshpranee@gmail.com, ⁵engineer.shankar@gmail.com, ⁶guntur.krishna@gmail.com,

⁷dvnv2001@gmail.com

ABSTRACT

The increasing connectivity among electric vehicles (EVs), charging infrastructure, in-vehicle networks, and inter-vehicle communication has created new cybersecurity challenges for intelligent transportation and smart-grid environments. This study presents a secure and intelligent cybersecurity framework for EV systems by integrating blockchain technology, cloud-based smart-grid communication, and fuzzy machine learning. A smart-grid-assisted cloud computing architecture is employed to collect, process, and exchange EV-related information, while a Fuzzy Adversarial Q-Stochastic (FAQS) model is developed to identify and assess potentially malicious activities. To further strengthen information protection, role-based access control is incorporated to regulate data access according to user responsibilities and authorization levels. Cryptographic mechanisms are applied during data encryption and decryption to protect sensitive EV information against unauthorized access and manipulation. The proposed framework is experimentally evaluated using representative cybersecurity datasets under multiple performance indicators, including security rate, root mean square error (RMSE), quality of service (QoS), scalability, and energy efficiency. The experimental results demonstrate that the proposed approach achieves approximately 98.4% energy efficiency, 96.8% QoS, 92.3% scalability, and 95.7% security rate, indicating its potential to provide secure, efficient, and scalable communication for interconnected electric vehicle and smart-grid environments.

Keywords: *Electric Vehicles, Cybersecurity, Blockchain, Cloud Computing, Fuzzy Machine Learning, Fuzzy Adversarial Q-Stochastic Model, Smart Grid, Role-Based Access Control, Data Encryption, Intelligent Transportation Systems.*

1. INTRODUCTION

The large-scale deployment of electric vehicle supplies equipment (EVSE) requires continuous interaction among multiple stakeholders and

consumers, resulting in substantial information exchange across transportation, energy, and financial domains. These stakeholders can broadly be categorized into three groups: (i) intelligent transportation system (ITS) and vehicle-to-

everything (V2X) infrastructures, including roadside sensing units, connected and automated vehicles (CAVs), and electric vehicles (EVs); (ii) electric power infrastructure involving generation, transmission, distribution, utilities, protection equipment, relays, and monitoring devices; and (iii) financial service providers, including organizations responsible for processing and managing payment transactions [1]. The interaction among these entities creates significant challenges concerning authorization, administrative privileges, interoperability, and secure information sharing. The absence of universally adopted standards and fully trusted communication environments further complicates the coordination of EVSE-related services. The rapid development of smart-city infrastructure has accelerated the deployment of EV charging stations in many regions. Governments and private organizations are increasingly investing in charging infrastructure to support the growing adoption of electric mobility [2]. Modern electric vehicle charging stations (EVCSs) incorporate intelligent functionalities that enable operators to remotely supervise charging operations and provide users with convenient services. The integration of Internet of Things (IoT) technologies has significantly expanded these capabilities. However, because EVCSs are network-connected IoT-enabled systems, their exposure to communication networks also creates additional cybersecurity vulnerabilities. A successful cyberattack can affect not only the charging station but also EV users and the interconnected electrical grid.

The EVCS ecosystem can generally be viewed as a combination of three major components: the charging infrastructure, the electrical grid, and the end user. Each component communicates with the others through interconnected information and communication technologies, making the complete ecosystem susceptible to different categories of cyber threats [3]. Consequently, cybersecurity must be considered an essential component of EV infrastructure development rather than an additional feature. The availability of large volumes of operational information generated by EV charging facilities through IoT networks enables advanced services such as user authentication, remote supervision, charging-status monitoring, and intelligent scheduling. For example, users can schedule charging during off-peak periods when electricity prices are comparatively lower. Although these capabilities improve operational efficiency and user convenience, they also increase the volume and complexity of network traffic that must be protected. One of the fundamental challenges in

IoT-based EVCS security is the identification of malicious communication among legitimate data exchanges. The EV charging environment represents a complex cyber-physical system in which hardware devices, embedded software, communication networks, and control mechanisms operate in an interconnected manner. An EVCS receives electrical power from the grid and transfers it to the connected vehicle while simultaneously exchanging operational information with cloud platforms and user applications. Public charging stations are commonly supported by cloud-based management systems that facilitate charging-session configuration, transaction processing, usage monitoring, station availability information, and remote control functions. Through these platforms, users can initiate or terminate charging, modify charging parameters, monitor charging status, and access information regarding available charging facilities [4]. The strong interdependence between EVCSs and the electrical grid introduces additional security and reliability concerns. Since charging stations directly consume grid power, disturbances affecting their communication or control systems can potentially influence both charging services and grid operations. Therefore, sensitive information exchanged among mobile applications, EVs, charging stations, and cloud platforms should be appropriately protected through secure communication and cryptographic mechanisms. However, cybersecurity practices adopted by equipment manufacturers, charging-network operators, and regulatory authorities may differ considerably. Such variations can create interoperability and security gaps, particularly when standardized communication and protection mechanisms are not consistently implemented.

Anomaly detection is an important technique for identifying data patterns or communication activities that differ from expected system behavior [5]. It has been extensively investigated across numerous application domains and has become particularly relevant to the cybersecurity of connected vehicles. Within an automotive Controller Area Network (CAN), for example, anomaly detection involves continuously analyzing communication exchanged among electronic control units (ECUs) and identifying deviations that may indicate malicious or abnormal activity. Machine learning (ML) techniques have increasingly been investigated for this purpose because they can learn patterns from communication data and assist in distinguishing legitimate behavior from potentially harmful activities [6]. Despite the progress in EV and IoT

cybersecurity, the increasing integration of EVs, charging infrastructure, cloud platforms, and smart-grid networks requires security frameworks capable of providing trustworthy data exchange, intelligent threat assessment, and controlled access. To address these requirements, this research develops an integrated cybersecurity framework based on blockchain-enabled cloud computing and fuzzy machine learning for electric vehicle environments. Blockchain technology is incorporated to strengthen data integrity and trust during information exchange, while the smart-grid-integrated cloud architecture supports EV data monitoring and communication. The proposed framework employs the Fuzzy Adversarial Q-Stochastic (FAQS) model to evaluate potentially harmful activities and support intelligent cybersecurity assessment. In addition, role-based access control is incorporated to regulate access to system resources according to predefined user responsibilities and authorization levels. Data protection is further supported through encryption and decryption mechanisms to reduce the possibility of unauthorized information disclosure. The effectiveness of the proposed framework is evaluated experimentally using cybersecurity datasets. The assessment considers several performance indicators, including security rate, root mean square error (RMSE), quality of service (QoS), scalability, and energy efficiency. The resulting analysis is used to examine the capability of the proposed approach to provide secure, efficient, and scalable communication and cybersecurity management for interconnected electric vehicle and smart-grid environments.

2. RELATED WORKS

Previous research has extensively examined secure data storage, privacy preservation, and access-control mechanisms for cloud-based environments; however, issues such as unauthorized disclosure and data leakage remain significant concerns. For mobile and cloud computing applications, [7] proposed an outsourced data-security mechanism incorporating trustworthy decryption and attribute-based privacy protection. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has also been investigated as an efficient approach for controlled data decryption. In [8], cryptographic techniques were explored for protecting distributed large-scale data storage while reducing the exposure of sensitive information to cloud service providers. The proposed approach was designed to lower computational requirements during cloud-based security operations. A privacy-oriented encryption framework for big-data applications on mobile cloud platforms was

presented in [9], where a Dynamic Data Encryption Strategy (D2ES) was employed to classify and protect sensitive information under time constraints. Selective encryption was further incorporated to improve privacy while maintaining acceptable processing requirements. Cloud data classification with integrated security mechanisms was investigated in [10] through prototype-based evaluation and simulation. In the area of automotive cybersecurity, [11] integrated a deep neural network (DNN) with an intrusion detection system (IDS) to identify abnormal CAN-bus communications. Likelihood-based feature vectors were extracted from CAN traffic and used for DNN training, allowing legitimate messages to be distinguished from malicious packets. An expert-independent anomaly detection framework was presented in [12], combining one-class and two-class classifiers within an ensemble structure to identify both univariate and multivariate abnormalities. In [13], a Hidden Markov Model (HMM) was employed to identify abnormal patterns in real-world vehicle data by representing vehicle motion as a sequence of probabilistically related events.

Further research has focused on hardware fingerprinting, intelligent fault diagnosis, and battery-health monitoring in connected electric vehicles. A clock-skew-based electronic control unit (ECU) fingerprinting architecture was introduced in [14] for developing a clock-based intrusion detection system. The underlying concept, discussed in [15], utilizes small timing variations known as clock skew, which are inherent characteristics of digital devices and can be used to distinguish individual ECUs. Reference [16] presented a combined deep-learning and blockchain-oriented framework for EV fault identification, targeting conditions such as battery abnormalities, tire-pressure variations, and temperature-related faults. A fault-tree-analysis (FTA) approach was incorporated in [17] to support dependable and scalable defect-detection transactions for electric vehicles. Real-world diagnosis of voltage-related battery abnormalities was investigated in [18] using an EV equipped with a multi-cell battery system, where voltage profiles were analyzed to identify overvoltage conditions in lithium-ion cells. Deep-learning-based battery-failure detection was further explored in [19] using a large EV battery dataset containing charging information obtained from numerous vehicles. Finally, [20] investigated the application of the interclass correlation coefficient (ICC) for identifying battery-related abnormalities. Voltage

measurements obtained from EV operational service and management data were analyzed to calculate ICC values and identify unusual voltage-degradation patterns. Collectively, these studies demonstrate the growing use of cryptography, machine learning, deep learning, blockchain, and statistical techniques for strengthening cloud, automotive, and electric-vehicle cybersecurity and reliability.

3. MODEL OF THE SYSTEM

Cloud service providers typically process and maintain large volumes of information across geographically distributed data centers. The

proposed cloud–fog architecture incorporates multiple fog nodes and cloud-based data centers to support efficient data processing, communication, and service delivery. As illustrated in Fig. 1, the framework is organized into three interconnected layers. The end-user layer, positioned at the bottom, supports the execution of smart-grid (SG) applications and interaction with connected devices. The fog-node layer forms the intermediate level and provides localized processing and communication capabilities closer to end users. At the upper level, the cloud layer contains centralized data centers and cloud services managed by service providers, enabling large-scale storage, computation, and application support.

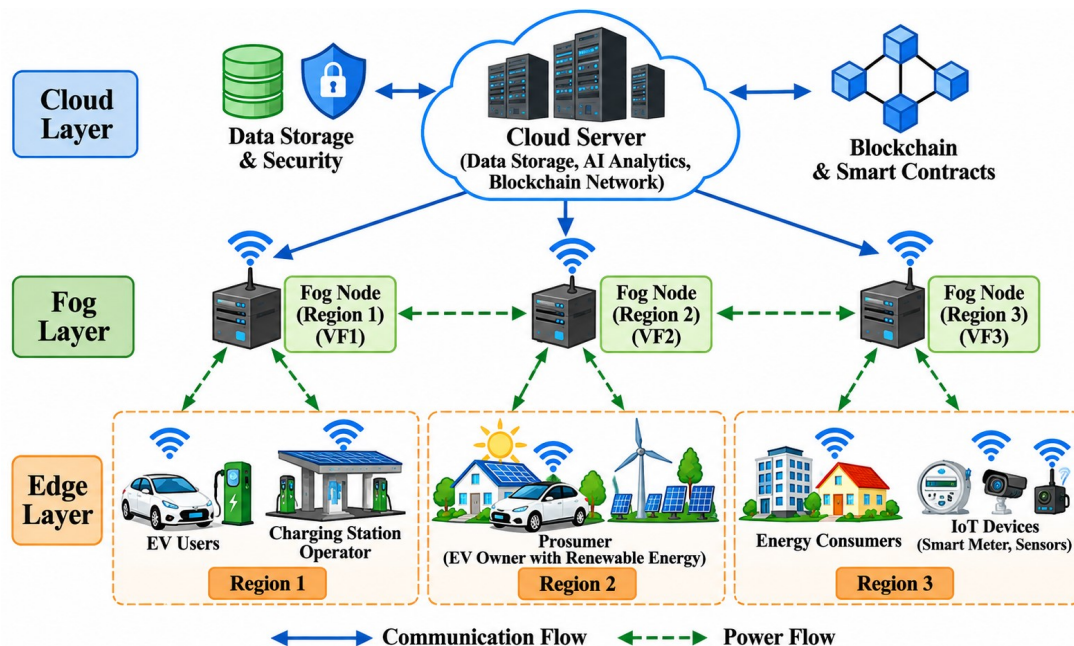


Figure 1. Proposed smart cloud network-based electric vehicle architecture

Smart PHEV charging determines an appropriate charging period by considering electricity price, household demand, battery state of charge (BSOC), available grid capacity, driving requirements, battery capacity, depth of discharge, charging efficiency, and charger rating. When a PHEV is connected to a residential charger, its initial BSOC is estimated from the vehicle's recent travel distance and all-electric driving range. The required charging energy and charging duration are then determined from the battery capacity and charging characteristics. Different PHEV categories, such as PHEV-20, PHEV-30, PHEV-40, and PHEV-60, can be incorporated according to their respective electric ranges and market shares. A probabilistic representation of daily driving

behavior and PHEV market distribution can be used to model variations among vehicles. The resulting charging schedule aims to shift vehicle charging toward economically favorable and grid-supportive periods while satisfying the user's required energy level and departure-time constraints. The proposed Fuzzy Adversarial Q-Stochastic (FAQS) model combines fuzzy representation, adversarial learning, and stochastic optimization to identify potentially malicious activities in electric-vehicle communication environments. The classification mechanism determines an appropriate decision boundary while maximizing separation between normal and abnormal data patterns. Type-2 fuzzy membership functions are employed to represent uncertainty and variations in the input features,

with local statistical characteristics such as mean and standard deviation extracted from neighboring data samples. These fuzzy features are subsequently processed by an adversarial learning mechanism, in which the generator produces representative samples and the discriminator distinguishes legitimate patterns from generated or malicious patterns. A multiclass formulation can further separate genuine observations from anomalous classes. To improve training stability, the optimization process considers stochastic gradient variations and evaluates the distance between the current model parameters and the desired optimum. A Lyapunov-based convergence analysis is employed to characterize the training behavior, while the learning rate and gradient variance are considered important factors affecting convergence. The resulting FAQS framework therefore provides an uncertainty-aware and adaptive mechanism for detecting both known and previously unseen malicious activities in EV communication networks.

Blockchain provides a distributed and tamper-resistant mechanism for recording EV charging, energy, and payment transactions without relying on a centralized intermediary. In the proposed EV ecosystem, a private blockchain with smart contracts is used to automate charging payments and reduce manual intervention. An electronic

wallet is associated with each authorized user, allowing charging charges to be automatically settled according to predefined contractual conditions. Energy prosumers, such as users equipped with photovoltaic generation, can also participate in peer-to-peer energy trading by supplying surplus electricity to charging stations. Smart contracts establish the rules for energy exchange and payment among prosumers, charging-station operators, and EV users, thereby improving transaction transparency and trust. Charging stations are equipped with controllers, meters, load switches, and blockchain-enabled data storage components, while EV applications provide services such as station identification, charging-session management, and charging-history access. As illustrated in Figure 2, when a charging or energy transaction is initiated by an authorized participant, the transaction is recorded and grouped with other transactions to form a new block. Participating blockchain nodes then validate the block through the predefined consensus mechanism. Once verification is completed, the validated block is appended to the distributed ledger, where transaction records are time-stamped and protected against unauthorized modification. This architecture provides a secure foundation for EV charging management, energy trading, payment processing, and trustworthy data exchange.

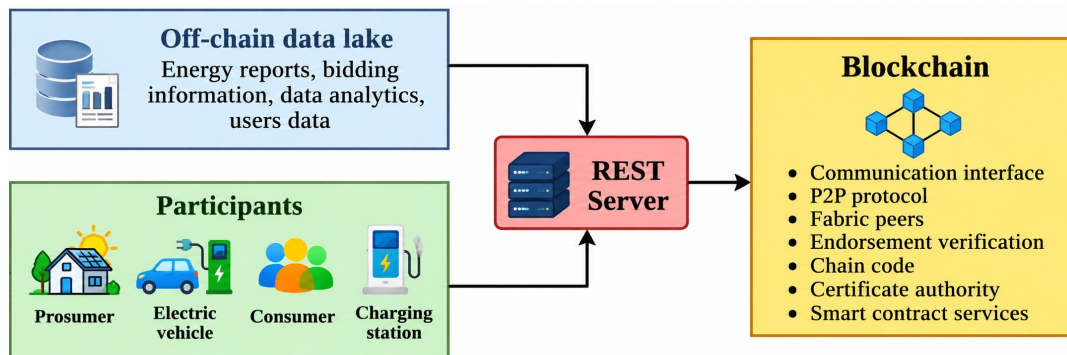


Figure 2. Block diagram of the proposed blockchain-based method

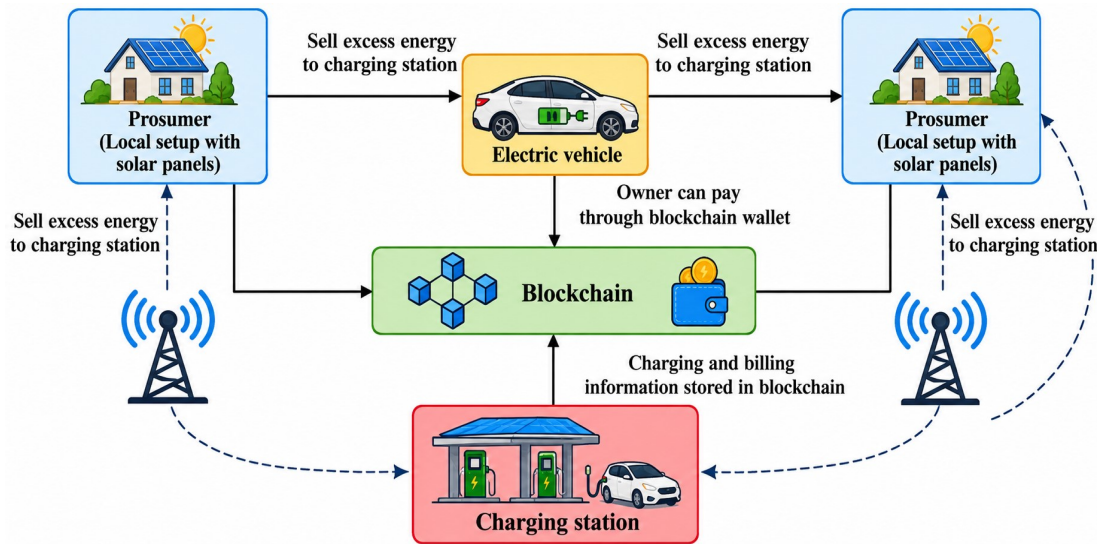


Figure 3. Proposed energy trading and EV charging system

The proposed blockchain-enabled EV ecosystem consists of three principal participants: EV owners or users, charging-station operators, and energy consumers. Each participant registers with the blockchain network and receives a unique set of credentials and private keys through the Membership Service Provider (MSP). EV-related information, charging records, energy transactions, and billing details can be securely maintained on the distributed ledger. As illustrated in Figure 3, solid arrows indicate information or communication flows, whereas dotted lines represent electrical power transfer. An EV owner equipped with a renewable-energy source, such as a photovoltaic system, can function as a prosumer by using locally generated electricity for vehicle charging and transferring surplus energy to a charging station. Smart contracts automate energy trading, billing, and charging-related transactions according to predefined conditions. Smart meters continuously record energy consumption and transfer the relevant measurements to the blockchain network, providing a verifiable transaction history. The Hyperledger Fabric-based infrastructure enables authorized participants to interact with the network without relying on manual intermediaries. Charging stations can record charging sessions, energy consumption, and payment information on the blockchain for subsequent verification. In addition, EV users can employ digital wallets to settle charging costs, with smart contracts automatically calculating and deducting the applicable payment according to the charging duration and energy consumed.

4. RESULTS AND DISCUSSION

The proposed framework was evaluated using an NVIDIA RTX 2080 Ti GPU and a 3.7 GHz AMD Ryzen 7 2700X 8-core processor. The experimental environment included three virtual fog functions and one remote cloud server distributed across five geographical regions. Five non-safety-critical vehicular applications with different delay requirements were considered. CloudAnalyst, based on the CloudSim platform, was used to evaluate cloud-fog resource allocation, communication, and application performance. Four geographical fog units were configured, and lightly loaded cloud resources were deactivated to reduce unnecessary energy consumption. Hyperledger Fabric Composer Playground and Composer CLI were used for blockchain implementation and testing.

The cybersecurity evaluation considered DoS attacks because interruption of communication can adversely affect connected EV services. CAN-bus traffic recorded during a 10-min normal driving period was analyzed to identify characteristic message patterns and detect abnormal communication. A total of 285,000 traffic flows, comprising approximately 74,000 legitimate and 211,000 malicious samples, were used for binary classification. The proposed anomaly-detection mechanism was evaluated using energy efficiency, QoS, scalability, and security rate as the principal performance indicators.

Figure 4 presents the comparison for different numbers of smart-grid entities. The proposed

approach achieved approximately 94% energy efficiency, 92% QoS, 86% scalability, and 90% security rate. LoRaWAN obtained approximately 89%, 88%, 81%, and 86%, respectively, while DRES achieved approximately 91%, 90%, 83%, and 88% for the same four metrics. The results indicate that the proposed framework maintains consistent performance as the smart-grid environment expands.

Figure 5 illustrates the performance comparison for different numbers of EVs. The proposed method achieved approximately 96.5% energy efficiency, 95.5% QoS, 89% scalability, and 92% security rate. LoRaWAN recorded approximately 91%, 91%, 82%, and 86%, respectively, whereas DRES achieved approximately 94.5%, 93%, 86%, and 89%. The results demonstrate that the proposed architecture can accommodate increasing EV participation while maintaining efficient resource utilization and secure communication.

Figure 6 shows the comparative results for different numbers of cloud users. The proposed framework obtained the highest reported values of 98.4% energy efficiency, 96.8% QoS, 92.3%

scalability, and 95.7% security rate, which are consistent with the overall performance values reported in this study. LoRaWAN achieved approximately 93% energy efficiency, 92% QoS, 85% scalability, and 91% security rate, while DRES achieved approximately 95%, 94%, 89%, and 93%, respectively. The results in Figure 6 demonstrate that the proposed framework remains effective under increasing cloud-user demand.

The experimental findings indicate that integrating blockchain with cloud-fog computing can support secure EV charging, energy trading, and transaction management. Blockchain provides tamper-resistant records for charging information, payment transactions, and energy exchanges, while smart contracts can automate billing and reduce manual intervention. The framework can also support EV owners with renewable-energy generation by enabling surplus energy to be exchanged with charging infrastructure. This mechanism can improve the utilization of distributed energy resources and enhance transparency among EV users, charging operators, and prosumers.

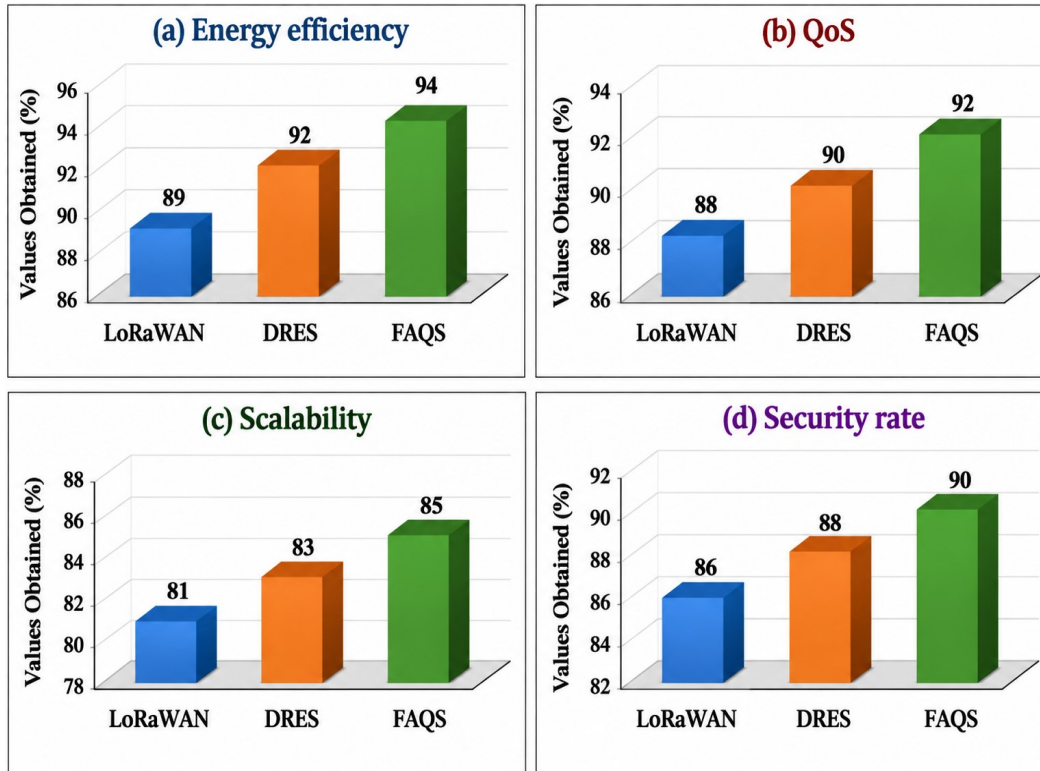


Figure 4. Performance Comparison for Different Numbers of Smart-Grid Nodes.

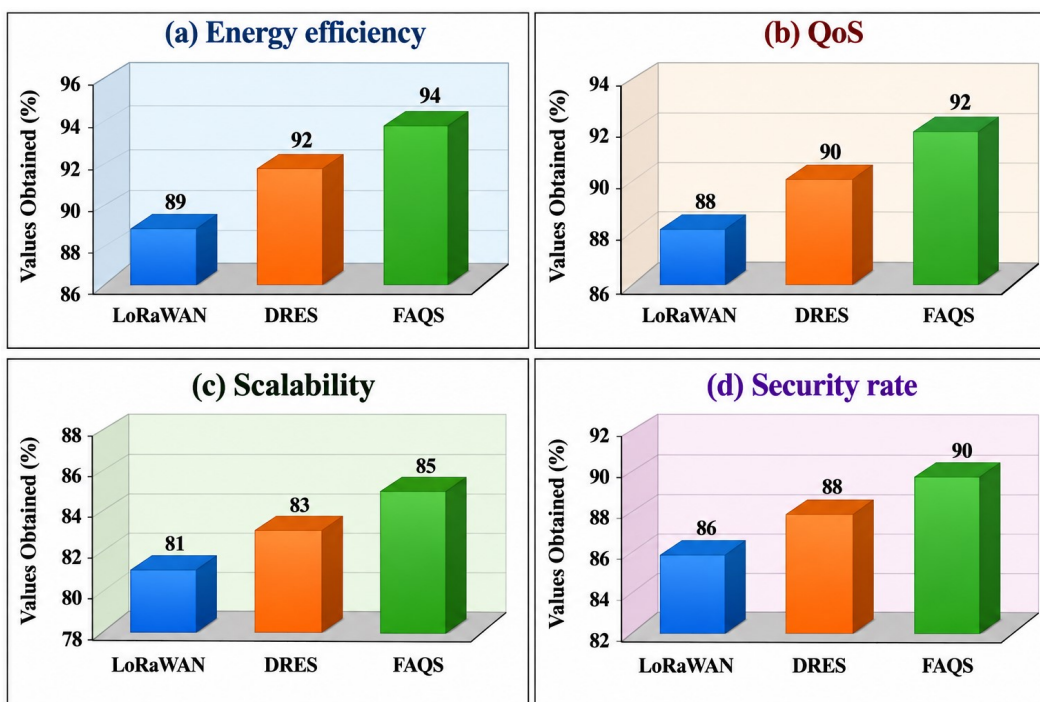


Figure 5. Performance Comparison for Different Numbers of Electric Vehicles.

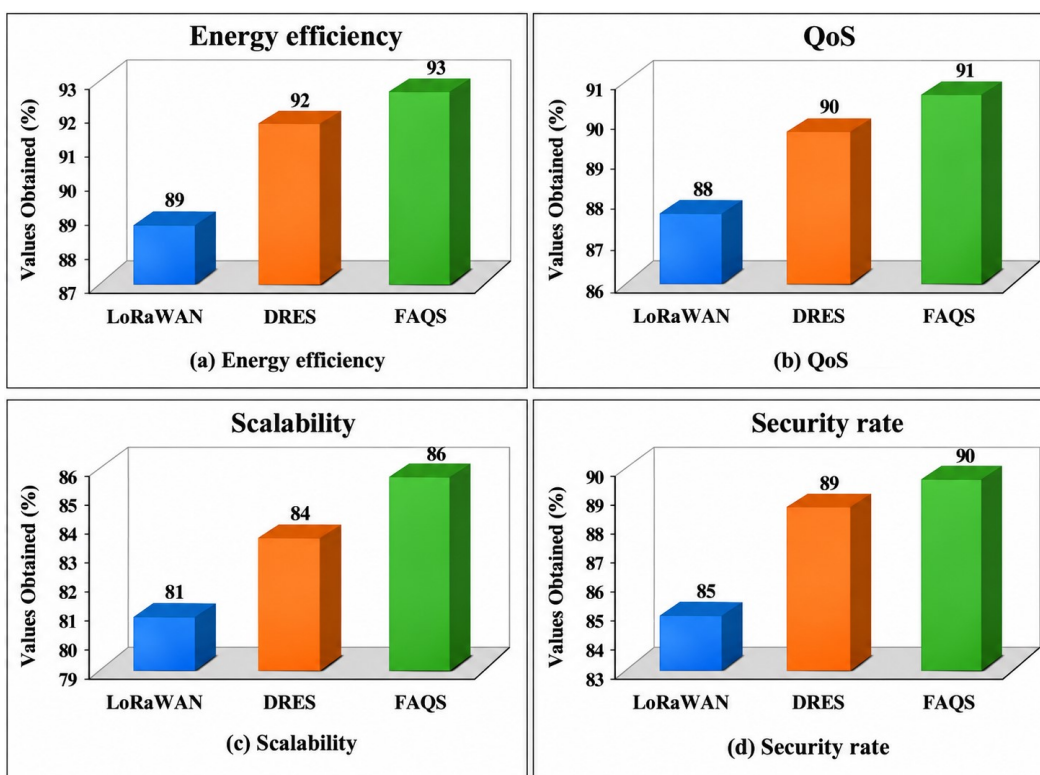


Figure 6. Performance Comparison for Different Numbers of Cloud Users.

4. CONCLUSION

This study developed an integrated cybersecurity framework for electric vehicle environments by combining the Fuzzy Adversarial Q-Stochastic (FAQS) model with blockchain technology in a smart cloud architecture. The FAQS mechanism supports the identification and monitoring of abnormal EV communication, while the blockchain layer provides secure and traceable management of charging, energy, and transaction information. A behavior-based EV classification mechanism was also considered to characterize charging patterns and support more effective charging management. The blockchain-enabled architecture further provides privacy protection, controlled access, authenticated communication, data integrity, and secure transaction processing through smart contracts. By distributing suitable computational operations to cloud resources, the framework can also reduce processing requirements at the user side while maintaining secure access to protected information. Experimental evaluation demonstrated that the proposed approach achieved 98.4% energy efficiency, 96.8% quality of service, 92.3% scalability, and 95.7% security rate, confirming its capability to support secure and scalable EV communication and charging services. Future research will focus on reducing the volume of training data required by the intelligent detection model while maintaining reliable classification performance. Further investigation will examine feature-selection techniques to identify the most informative cybersecurity attributes and reduce unnecessary computational complexity. The applicability of advanced deep-learning models to additional EV, smart-grid, and vehicular cybersecurity datasets will also be investigated. In addition, future work can evaluate the framework under larger-scale EV deployments, diverse attack scenarios, real-time charging environments, and practical blockchain networks to further assess its robustness, computational efficiency, and scalability.

REFERENCES:

- [1] M. Basnet and M. H. Ali, "Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning," *IET Generation, Transmission & Distribution*, vol. 15, no. 24, pp. 3435–3449, 2021, doi: 10.1049/gtd2.12275.
- [2] V. S. R. Kosuru and A. Kavasseri, "A smart battery management system for electric vehicles using deep learning-based sensor fault detection," *World Electric Vehicle Journal*, vol. 14, no. 4, p. 101, 2023, doi: 10.3390/wevj14040101.
- [3] N. Mohamed, M. Bajaj, S. K. Almazrouei, F. Jurado, A. Oubelaid, and S. Kamel, "Artificial intelligence (AI) and machine learning (ML)-based information security in electric vehicles: A review," in *Proc. 5th Global Power, Energy and Communication Conf. (GPECOM)*, 2023, pp. 108–113, doi: 10.1109/GPECOM58364.2023.10175817.
- [4] S. Hamdare, O. Kaiwartya, M. Aljaidi, M. Jugran, Y. Cao, S. Kumar, and J. Lloret, "Cybersecurity risk analysis of electric vehicles charging stations," *Sensors*, vol. 23, no. 15, p. 6716, 2023, doi: 10.3390/s23156716.
- [5] V. M. Macharia, V. K. Garg, and D. Kumar, "A review of electric vehicle technology: Architectures, battery technology and its management system, relevant standards, application of artificial intelligence, cyber security, and interoperability challenges," *IET Electrical Systems and Transportation*, vol. 13, no. 2, p. e12083, 2023.
- [6] F. M. Noori, A. Hafeez, H. Malik, M. Z. Uddin, and J. Torresen, "Source linking framework in vehicular networks for security of electric vehicles using machine learning," in *Proc. IEEE Vehicular Networking Conf. (VNC)*, 2023, pp. 207–214, doi: 10.1109/VNC57357.2023.10136272.
- [7] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, "Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability," *Energies*, vol. 16, no. 3, p. 1113, 2023, doi: 10.3390/en16031113.
- [8] X. Wei, C. Du, and J. Zhao, "A network security situation awareness model for electric vehicle shared charging pile system," *AIP Conference Proceedings*, vol. 2238, 2020.
- [9] B. N. Bhukya, S. M. Kuchibhatla, N. K. Bhagavatham, T. L. Narayana, M. R. Chunduru, and B. K. Madhavi, "Implementation of meta-heuristic and deep learning algorithms for power system cybersecurity," *Bulletin of Electrical Engineering and Informatics*, vol. 15, no. 1, pp. 648–656, Feb. 2026, doi: 10.11591/eei.v15i1.8569.
- [10] M. Dabbaghjamesh, A. Moeini, and A. Kavousi-Fard, "Reinforcement learning-based load forecasting of electric vehicle charging station using Q-learning technique," *IEEE*

- Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4229–4237, 2021.
- [11] B Naik B, Manam Ravindra, Simhadri Mallikarjuna Rao, Srikanth Kilaru, Madamanchi Brahmaiah, Bezawada Manasa, Muralidhar V “Cyberattack Prevention and Detection in Smart Power Systems Using Deep Learning” Journal of Theoretical and Applied Information Technology, May 2025. Vol.103. No.9, pp. 3934-3944.
- [12] J. Gan, S. Li, C. Wei, L. Deng, and X. Tang, “Intelligent learning algorithm and intelligent transportation-based energy management strategies for hybrid electric vehicles: A review,” IEEE Transactions on Intelligent Transportation Systems, 2023.
- [13] H. C. Lin, P. Wang, K. M. Chao, W. H. Lin, and J. H. Chen, “Using deep learning networks to identify cyber-attacks on intrusion detection for in-vehicle networks,” Electronics, vol. 11, no. 14, p. 2180, 2022, doi: 10.3390/electronics11142180.
- [14] B Naik Bhukya, V. Venkataiah, S. Mani.Kuchibhatla, S. Koteswari, R V S Lakshmi Kumari, and Yallapragada Ravi Raju, "Integrating the Internet of Things to Protect Electric Vehicle Control Systems from Cyber Attacks," IAENG International Journal of Applied Mathematics, vol. 54, no. 3, pp 433-440, 2024.
- [15] M. Basnet, Deep Learning-Powered Computational Intelligence for Cyber-Attacks Detection and Mitigation in 5G-Enabled Electric Vehicle Charging Station, Ph.D. dissertation, Univ. Memphis, Memphis, TN, USA, 2022.
- [16] M. ElKashlan, M. S. Elsayed, A. D. Jurcut, and M. Azer, “A machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs),” Electronics, vol. 12, no. 4, p. 1044, 2023, doi: 10.3390/electronics12041044.
- [17] M. Dabbaghjamanesh, A. Kavousi-Fard, and J. Zhang, “Stochastic modeling and integration of plug-in hybrid electric vehicles in reconfigurable microgrids with deep learning-based forecasting,” IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4394–4403, 2021.
- [18] P. Dixit and S. Silakari, “Deep learning algorithms for cybersecurity applications: A technological and status review,” Computer Science Review, vol. 39, Art. no. 100317, 2021.
- [19] L. Fu, T. Wang, M. Song, Y. Zhou, and S. Gao, “Electric vehicle charging scheduling control strategy for the large-scale scenario with non-cooperative game-based multi-agent reinforcement learning,” International Journal of Electrical Power & Energy Systems, vol. 153, Art. no. 109348, 2023.
- [20] B Naik Bhukya, Vutukuri Sarvani Duti Rekha, Venkata Krishnakanth Paruchuri, Ashok Kumar Kavuru and Kadiyala Sudhakar “Internet of Things for Effort Estimation and Controlling the State of an Electric Vehicle in a Cyber Attack Environment” Journal of Theoretical and Applied Information Technology, ISSN: 1817-3195, Vol. 101, No.10, pp. 4033 – 4040, May-2023.