Journal of Theoretical and Applied Information Technology
30th November 2025. Vol.103. No.22
© Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A HYBRID CYBERSECURITY FRAMEWORK FOR SMART EV CLOUD SYSTEMS USING FUZZY LOGIC, MACHINE LEARNING, AND BLOCKCHAIN

PANTHANGI VENKATESWARA RAO[1], SK. MD. SHAREEF[2], DEEPIKA VODNALA[3], SIRISHA NARKEDAMILLI[4], ASHISH B. JIRAPURE[5], P. LAKSHMI PRASANNA[6], P. S. SUBHASHINI PEDALANKA[7]

[1]Department of Computer Science and Engineering (Cys, DS) and (AI & DS),

Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India

[2]Department of EEE, Narasaraopeta Engineering College, Narasaraopeta, Andhra Pradesh, India

[3]Department of CSE (CS), CVR College of Engineering, Vasthunagar, Ibrahimpatnam, Telangana, India

[4]Department of EEE, Aditya University, Surampalem, Andhra Pradesh, India

[5]Department of Industrial IoT, Priyadarshini College of Engineering (PCE), Nagpur, Maharashtra, Inia

[6]Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

[7]Department of ECE, R.V.R. & J.C.College of Engineering, Chowdavaram, Guntur, Andhra Pradesh, India

E-mail: [1]venkateswararao_panthangi@vnrvjiet.in, [2]skmseee@gmail.com, [3]deepuvodnala19@gmail.com,
[4]sirishanarkeda@gmail.com, [5]ashish.jirapure@pcenagpur.edu.in, [6]lakshmiprasannap87@gmail.com,
[7]pssubhashini.pedalanka@gmail.com

ABSTRACT

The increasing need for communication within and between electric vehicles can create serious challenges for infrastructure. This paper focuses on protecting electric cars from cyberattacks by introducing a secure and intelligent framework. We propose a new cybersecurity method that combines blockchain technology with smart cloud computing and fuzzy machine learning, specifically designed for electric vehicle systems. To handle data from vehicles, the model uses a cloud system integrated with the smart grid, while the fuzzy adversarial Q-stochastic (FAQS) model detects and analyzes suspicious activities. Data is protected through encryption and decryption, based on role-based access control, which ensures only authorized users can access information according to their responsibilities. The proposed system was tested using different cybersecurity datasets and evaluated on performance measures such as security rate, error (RMSE), quality of service (QoS), scalability, and energy efficiency.

Keywords: *Electric Vehicle, Smart Cloud Computing, Cyber Security Analysis, Fuzzy Machine Learning, Blockchain Model*

1. INTRODUCTION

Electric vehicle supplies equipment (EVSE) is being strategically and extensively implemented, which is putting a lot of pressure on customers and other stakeholders to work together and share data. Electric grid infrastructures—utility, generation, transmission, distribution, sensors, protection, and relays—as well as intelligent transportation system (ITS)/vehicle to everything (V2X) infrastructures—including roadside sensors, connected automated vehicles (CAVs), and electric vehicles (EVs)—are the primary topics of discussion among the various stakeholders. Financial institutions, like credit card companies, are involved in transaction management [1]. Because there aren't yet fully formed, trustworthy settings and clear rules for appropriate interoperability, there's a continuing conflict of interest about how much administrative privilege is necessary to coordinate these quirky parties to and from EVSE. Electric vehicle charging stations have been included into an increasing number of smart city projects. Rapid and extensive installation of charging stations for electric vehicles is a priority for a number of nations [2]. Thanks to developments in Internet of Things technology, these new charging stations include ingenious features that simplify life and provide EVCS operators more control. Because it is an IoT device, the EVCS cannot be disconnected from the network. In order to give our clients comprehensive services, we have done this. Unfortunately, this opens the door for several cyberattacks that might target the entire EVCS ecosystem. Except for EVCSs, impact can happen anywhere. The electrical grid and its end users are both included in this. The electric vehicle charging station (EVCS), the power grid, and the final consumers make up the triad of the EVCS ecosystem. These EVCS ecosystem components are susceptible to a wide range of Internet of Things (IoT) hacks [3]. The rapid development of infrastructure is crucial if the EVCS sector is to have sustained growth. This highlights the importance of establishing a network of reliable electric vehicle charging stations. An IoT network powers the rich data collected from electric vehicle charging stations. This frees up development time for more user-friendly features, such remote monitoring and user accounting. One helpful feature is the option to remotely plan EV charging based on the cheaper nighttime power cost. An important problem with Internet of Things cybersecurity is the difficulty in differentiating between legitimate and malicious communication that flows via an IoT device. The smart grid's electric vehicle charging ecosystem is its beating heart. This cyber-physical system is complex, with many interdependent parts, including software, hardware, and communication protocols. Power for electric vehicles is supplied by the grid through EVCS. The EVCS is an autonomous system that can run its own firmware and is ready to connect to the internet. Users are able to set up and manage charge sessions, track their consumption data, and be directed to accessible EVCS using a cloud server that manages public EVCS. Charging management methods can be communicated with by users of public EVCSs through the Internet. Users may usually schedule charging sessions, change the charging rate, begin and end charging, and check on the status of their electric vehicles using these services. The availability and connectivity of electrical infrastructure is crucial for charging electric vehicles [4]. Since EVCS are connected to the grid and get their electrical needs met from it, they pose a significant risk to the reliability and safety of the power supply. All data transmitted between user applications, EVs, and EVCS is encrypted to guarantee the reliability and security of the ecosystem. There is a difference in the protocols that are advocated for enabling cybersecurity by equipment vendors, national governments, and EVCS operators. The absence of protocol standardization leads to discrepancies, which in turn cause serious cybersecurity risks. In a nutshell, anomaly identification is the difficulty of finding dataset patterns that don't follow expected patterns of behavior [5]. Many diverse areas of study have contributed to the body of knowledge about anomaly detection. In the context of the CAN bus protocol, anomaly detection refers to the practice of monitoring the communication traffic between ECUs and using ML approaches to identify any odd activity. More and more, ML techniques are attracting the attention of cybersecurity specialists these days [6].

The overarching goal of this study is to shed fresh insight on cyber security evaluations. This approach uses smart cloud computing based on blockchain technology and fuzzy machine learning; it is based on electric vehicle technology. Here, the smart grid integrated cloud computing architecture is used to transmit and monitor data from electric automobiles. On the other hand, FAQS is used to evaluate behaviors that could be considered dangerous. According to role-based access control rules, people are given access permissions according to their duties, which determines whether they can encrypt or decrypt data. Whether or whether the users have authorization doesn't matter; this is still done. To determine the energy efficiency, scalability, quality of service, root mean square error (RMSE), and security rate of various cyber security data sets, we conduct experimental investigations.

2. RELATED WORKS

Data provisioning security has been the subject of extensive testing and research, which has revealed storage and access techniques; nonetheless, there are still certain vulnerabilities that can affect the cloud ecosystem, such as data leakage. Methods for ensuring the safety of sensitive information stored in the cloud informed the selection of several articles for this section of the study. Author [7] suggests outsourcing data security with trustworthy decryption and attribute protection of privacy to guarantee cloud computing on the mobile network.

Prior to the decryption step, two anonymous strategies were demonstrated. An efficient method of decryption known as match-then-decrypt with a matching phase, CiphertextPolicy with Attribute-Based Encryption (CP-ABE) is the first. Secure distributed massive data storage using sophisticated cryptographic algorithms has been investigated in work [8]. Cloud operators circumvented the issue of cloud data storage by acquiring sensitive user data. When protecting against assaults in the cloud, the proposed solution drastically cuts down on computation time. The downside of data retrieval is that it increases the availability of data. In order to facilitate massive data cloud computing on mobile devices while protecting user privacy, the author [9] presented algorithms for encrypting data. To classify and encrypt sensitive information under a certain time constraint, we used a dynamic data encryption method (D2ES). To ensure maximum privacy protection within the given execution time, a selective encryption approach was employed. We tested D2ES's performance to make sure the privacy improvement was real. Prior work has succeeded in classifying data for use in cloud computing with security features [10]. The data must be strengthened, improved, and made more secure. An operational module is used to evaluate prototypes and classify simulations, putting the method into action. We could test the suggested method's accuracy using just a little dataset. The author suggested [11] that an intrusion detection system (IDS) integrate a deep neural network (DNN). In order to train the parameters of the DNN, feature vectors based on probability are collected from the CAN bus communications. Statistical features of each class are utilized to distinguish between valid communication and attacks in a particular CAN transport packet. Recent work has offered anomaly detection that does not require expert parameter setting and can detect both known and unknown sorts of faults [12]. In order to build an ensemble classifier that can identify both multivariate and univariate anomalies, two-class and one-class classifiers are combined. The author [13] suggested a Hidden Markov model (HMM), a stochastic model with Markov characteristics, to detect outliers in real-world data acquired from a moving vehicle. Like Markov's processes, HMMs operate on the fundamental premise that the vehicle's motion is a series of interdependent events.

A clock-based intrusion detection system (CIDS) was built using an architecture for ECU fingerprinting proposed in study [14]. The use of "a tiny timing error known as clock skew," a feature of all digital systems, is one way that has been suggested for clock-based fingerprinting [15]. Findings from the study [16] proposed using DL in conjunction with a blockchain-based EV fault detection system to identify a variety of vehicle faults, such as temperature, low tire pressure, and battery concerns. Additionally, in order to carry out dependable and extremely scalable data transfers for EV defect detection, a fault tree analysis (FTA) is integrated into [17]. The study's proposed method for diagnosing voltage issues was shown utilizing a real-world electric vehicle (EV) equipped with a multiple-cell battery system [18]. This study found that voltage curves analysed after the typical data collection and processing times from the Operation Service and Management Centre for Electric Vehicles (OSMC-EV) were able to identify overvoltage issues with Li-ion battery cells. A system for identifying dead batteries by means of deep learning models was presented in the article [19]. A huge dataset for electric vehicle batteries, including clean charging data from hundreds of vehicles, is made available by this study. We examined the interclass correlation coefficient (ICC) approach for defect detection in this work [20]. We recorded any voltage decreases that were not on trend and used operational and EV management center data to calculate ICC values.

3. MODEL OF THE SYSTEM

Data is processed and stored in data centers around the world by cloud service providers. Several fog and cloud data centers are part of the cloud-fog operational environment that has been suggested. Figure 1 shows the three-layer approach that has been proposed. The concept is structured as follows: end-user layer (where SG applications are executed), fog node layer (in the middle), and cloud layer (at the top), which contains data centers and services offered by service providers.

3.1 Blockchain model for electric vehicle system

Using blockchain technology, users may reliably store and create data without relying on a third party or even the other party in a transaction. A trusting connection is essential for all parties participating in the EV charging infrastructure. We have proposed a smart contract-based digital wallet for payments on electric vehicles. This method reduces the amount of time that humans are required to charge electric vehicles. Using a private blockchain software developed on a hyper ledger, our proposed method instantly transfers value between each other. "Prosumers" are those who not only consume energy, but also produce it. Through a decentralized system of peer-to-peer trading, prosumers can offer surplus energy to charging stations. Prosumers often generate their own electricity using solar panels. Our proposed solution is based on the blockchain since it guarantees trustworthy transactions for prosumers, charging station owners, and electric vehicle owners. It provides a smart contract ecosystem where users can have trust in the system. The agreed-upon rate will be deducted from wallets automatically

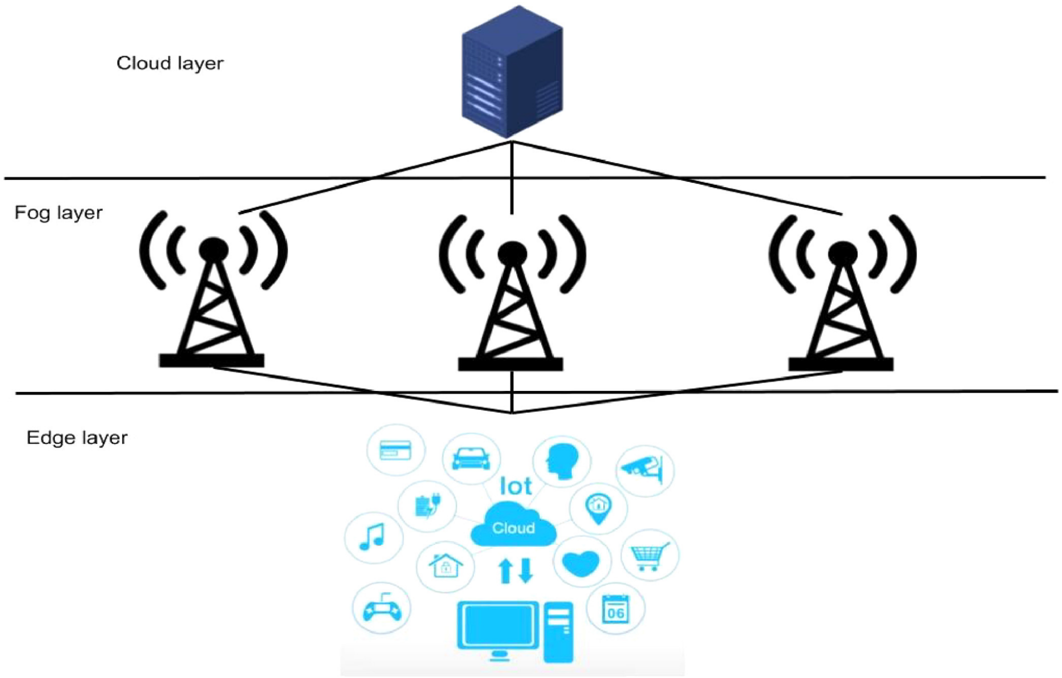


Figure 1: Electric vehicle architecture based on a smart cloud network.

Every block on the blockchain, which records transactions, must first be validated by other nodes in the network using a predefined consensus procedure. Figure 2 shows a schematic representation of a charging situation along with an electric vehicle data integration scenario. Each charging station has its own controller, load switch, meter, and blockchain-authenticated data storage for distinct nodes. Electric vehicle applications extend the functionality of vehicles beyond what is included into the vehicle itself. With the help of the app, drivers can find the nearest charging station. The charge history can also be viewed through their applications. Processing on the blockchain starts when a transaction is initiated by any peer or node in the network. Following this, a block is formed by combining all of the transactions. The consensus algorithm verifies that block. Once a block has passed verification, it is added to an immutable ledger where every transaction is timestamped and cannot be altered by any third party.

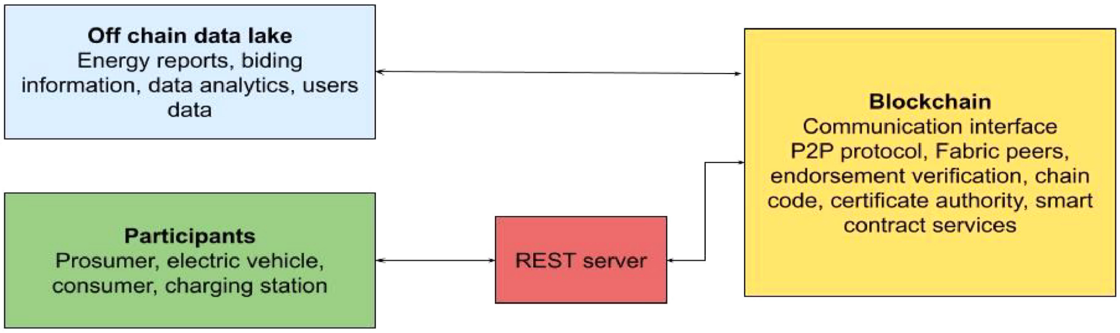

Off chain data lake
Energy reports, biding information, data analytics, users data
Blockchain
Communication interface P2P protocol, Fabric peers, endorsement verification, chain code, certificate authority, smart contract services
Participants
Prosumer, electric vehicle, consumer, charging station
REST server

Figure 2: Block diagram of the blockchain method that has been proposed.

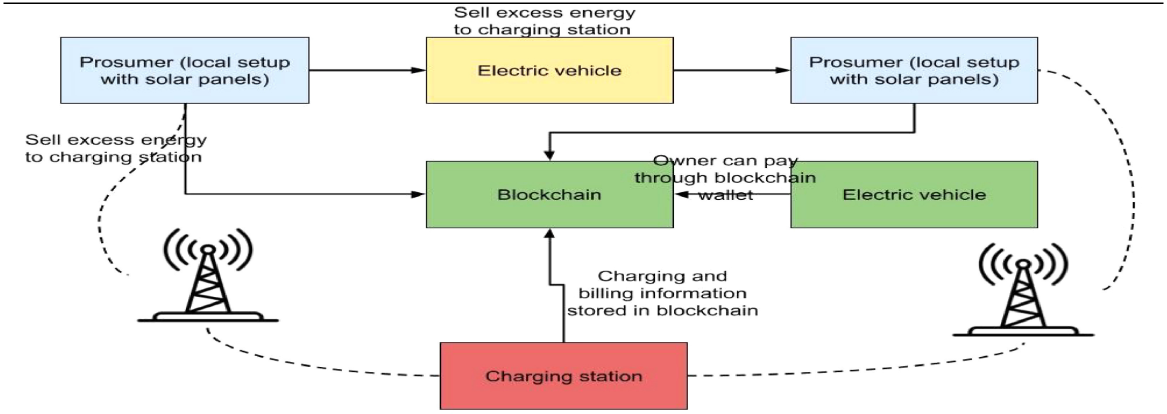

Sell excess energy to charging station
Prosumer (local setup with solar panels)
Electric vehicle
Prosumer (local setup with solar panels)
Sell excess energy to charging station
Blockchain
Owner can pay through blockchain wallet
Electric vehicle
Charging and billing information stored in blockchain
Charging station

Figure 3: Energy trading and charging system approach.

Owners or users of electric vehicles are the first. The consumer ranks third, followed by the operator of the charging station. An account on the blockchain network must be created by every participant. One set of private keys will be distributed to each user by the membership service provider. Additionally, information pertaining to EVs will be entered into the blockchain. Figure 3 shows the proposed system model. Power lines are depicted by a dotted line, whereas flow lines are portrayed by linked arrows. Electric vehicle owners can act as prosumers if they have a renewable energy system installed on their property. In addition to charging their own electric vehicle, they can also sell it to other stations. The use of smart contracts allows for the potential storage of all billing and payment data on the blockchain. Smart contracts allow users to connect with those who desire more energy at a predetermined price, which could lead to people selling more energy than they need. It is possible to store the data recorded by smart metres, which pertain to energy usage, on a blockchain. Users are able to communicate autonomously with the Hyperledger fabric-based system through blockchain technology. Charging stations can save all billing and charging data on the blockchain, which can then be confirmed by everyone. Digital wallets can also be used by owners of electric automobiles. Payment will be automatically deducted from their wallet by the smart contract according to the amount and charge time.

4. RESULTS AND DISCUSSION

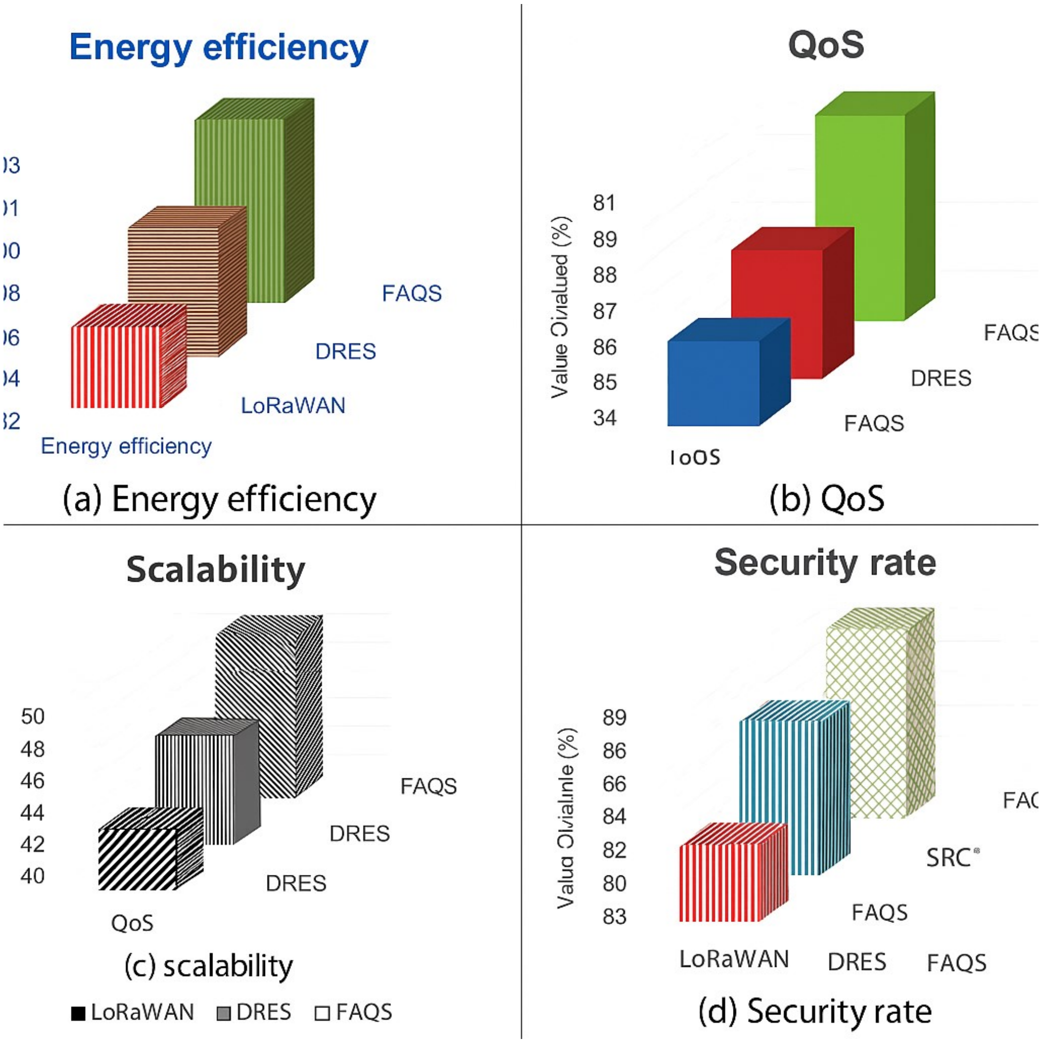
Since this research is focusing on vehicle intercommunication, an area where denial-of-service (DoS) attacks are prevalent, it is able to provide an evaluation of these attacks. Programmers attempt to block legitimate users (drivers) from accessing the service in a denial-of-service attack. Considering that cars are mobile phones, denial-of-service attacks pose a significant threat in vehicles, as they have the potential to cause serious accidents. One example of a denial-of-service (DoS) attack on a car is the ability to suddenly shift the steering wheel to the left or right, turn off the engine, or unlock the door. Based on analysis of recorded CAN traffic during a typical 10-minute driving season, the proposed irregularity identification technique has identified a few notable frequencies for each message outline with a given ID.

Several network simulation parameters using data from analyses of smart grids and cloud computing. The number of smart grid nodes, electric vehicles, and cloud users are examined in this network case study in relation to energy efficiency, quality of service, scalability, and security rate. For the binary classification results, we employed 285,000 flows, with 73,000/212,000 representing the labels for malicious and lawful traffic, respectively, to evaluate the algorithm's performance. Using the hardware specifications of the experimental setup, we first determined the time required to build the model. The figures should be viewed as a point of reference, as all the experiments were conducted on the same hardware, although the actual time may vary depending on the model.

You can see the suggested and existing techniques compared in figure 6, which is based on the number of smart grids. Presented below is a method DRES achieved energy efficiency of 91%, QoS of 89%, scalability of 83%, and security rate of 88%; current LoRaWAN had energy efficiency of 89%, QoS of 88%, scalability of 81%, and security rate of 89%. This is how the simulation parameters are set up. Given that in the strategy space of game group EVs and EVp, p11 + p10 + p01 + p00 = 1, we may say that the probabilities of each technique, pij = qij = 0.25, are equal. Assume that there are typically two vehicles in the game, that the parameter for the Poisson distribution is set to 0.8, and that the likelihood of two EVs connecting is quite high under typical conditions. Revenue parameters esell = 6, ereceive = 4, and erupload = 5 were defined, whereas energy consumption parameters ebuy = 6, echadischa = 3, and ecupload = 2 were set.

A comparison based on the number of EVs is shown in Fig. 5 above. A comparison of the current state of LoRaWAN, DRES, and the proposed technique reveals that the former is 95% efficient, the latter 93%, the former 86%, and the latter 91% in terms of QoS, scalability, and security rate, respectively.

Figure 6 shows a comparison based on the overall number of users of the cloud. An impressive 98% energy efficiency, 96% quality of service, 91% scalability, and 95% security rate are all features of the proposed strategy. Currently, LoRaWAN technology boasts a 93% energy efficiency, 92% quality of service, 85% scalability, and 91% security rate. The energy efficiency, quality of service, scalability, and security of DRES technology are all 95%. As shown in the equations that follow, we calculate the return capability of the EVs choice technique x11 and the EVp determination approach y11 independently; the rest are comparative. From the chart above, it is clear that the addition is smallest for system x00 when EVs choose it, the largest for determination technique x11, and somewhat larger for choice methodology x10 than the advantage of determination procedure x01. So, according to our incentive configuration, if the car wants to earn more money, it needs to commit more power and transfer more data. Plus, as the number of gaming cars increases, the income will level out at a reasonable value.



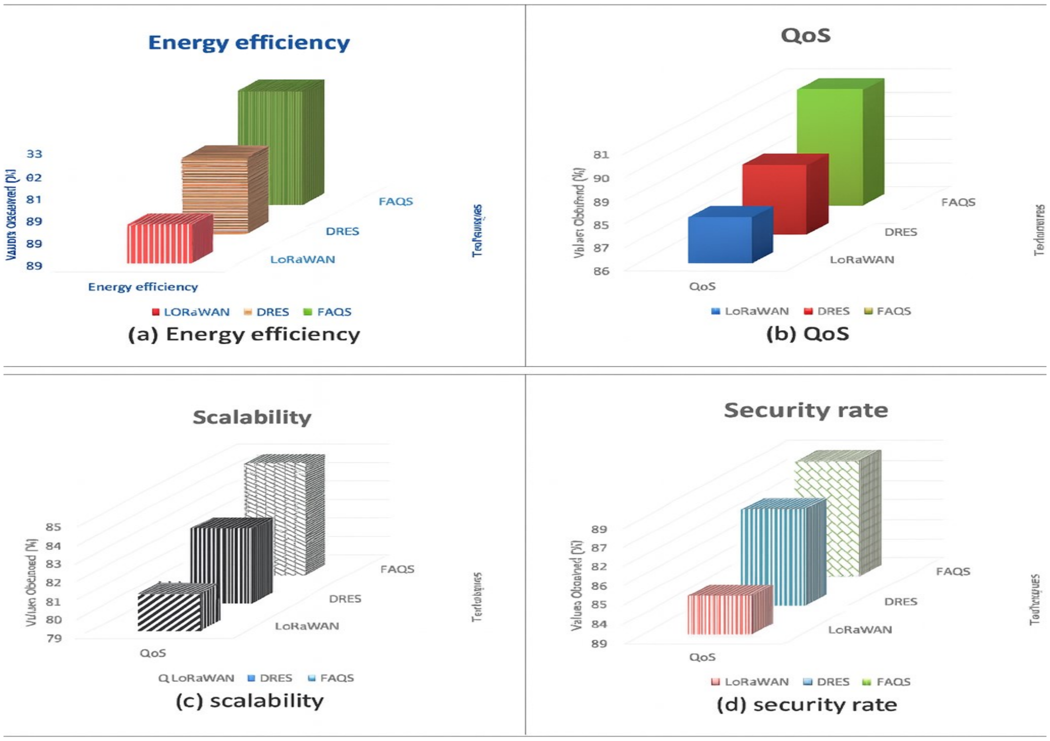
(a) Energy efficiency

(b) QoS

(c) scalability

(d) Security rate

Figure 4: Analyzed comparatively according to smart grid count.



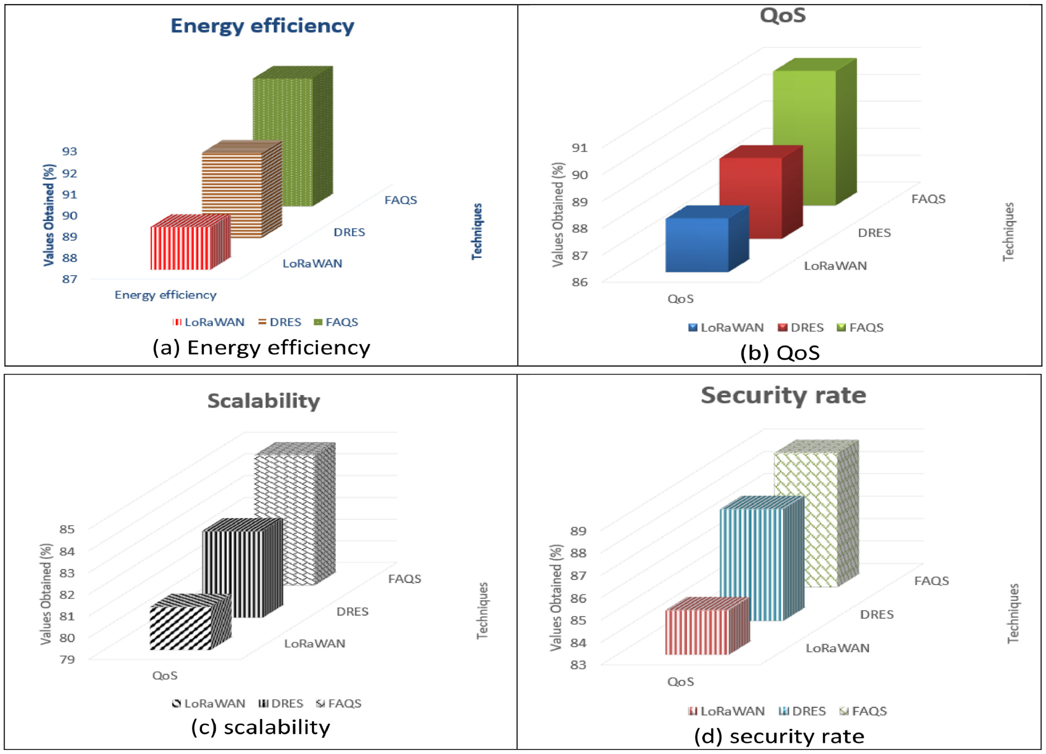
(a) Energy efficiency

(b) QoS

(c) scalability

(d) security rate

Figure 5: comparing results according to EV count.



(a) Energy efficiency

(b) QoS

(c) scalability

(d) security rate

Figure 6: A comparison based on the amount of people using the cloud.

Electric vehicle payments might be easier to handle using blockchain technology. A more streamlined system for EV charging stations is provided, and the directory is kept up to date. The reach anxiety problem is a big roadblock to EV acceptability. A lot of individuals are afraid that during long hikes, their batteries would fail. This is because assuming that the charger will be readily available in every location is an unrealistic expectation. Without a suitable and publicly available framework, potential customers are hesitant to transition to EVs. In any case, blockchain technology addresses numerous issues; these include reputational, technological, and interoperability issues with older systems. Adding to the list of challenges are issues with administrative and cryptographic money, and there is no assurance that EVs will be widely utilized in the future. Integrating blockchain technology with energy infrastructure has the potential to improve electric vehicle charging infrastructure as well. Despite the blockchain framework's inherent security, assaults can nevertheless originate via the interconnection networks that link it to other digital or physical frameworks. No matter how simple it is, a single-user framework's behavior is more natural. More EV users using different administrations will allow for a more effective prioritization computation. The system's complexity and strength may expand as the number of users competes with each other. Thirdly, the EVSE administration claims that meeting its own financial demands requires maintaining a high level of EVSE usage. Customers of electric vehicles should limit the amount of time and money they spend charging their vehicles, taking into account their own financial circumstances, because as the number of electric vehicle clients in the system grows, EVSE will become a competitive asset. This leads to even more systemic advancements and adjustments brought about by local EVSE and EV optimization.

5. CONCLUSION

This study presents a new approach to finding and monitoring smart cloud electric vehicle anomalies using the fuzzy adversarial Q-stochastic model (FAQS) and the blockchain model. We introduced an EV driver grading system that takes charging behaviors into account in order to categorize drivers and guide their charging habits. No monetary incentives are required to make this approach work. We also proposed EVcoin, a blockchain-based incentive that provides an implicit monetary advantage, to supplement the existing directing capacity. After that, we had to show how our encrypted cloud storage solution was beneficial in several ways, such as how it could store a secret message up to a specific size along with the decryption key. The proposed method incorporates the standard model's security safeguards while adding several useful features, such as privacy, enforceability, coarse-grained access control, unidentifiable authentication, and public conformity. By delegating expensive tasks to a cloud attendant, we may be able to reduce the running expenses of the decryption technique without compromising role privacy. Both the security and scalability of the suggested method are very excellent, at 95% and 91%, respectively. Not only that, it's quite efficient with energy (98%). Next, research should focus on finding the minimum amount of data needed for training that yet yields a reliable level of accuracy. The impacts of feature selection should be the subject of future research, alongside the investigation of new methodological approaches to deep learning model construction.

REFERENCES:

[1] Basnet M, Ali MH. Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning. IET Generation, Transmission Distribution 2021;15(24):3435–49.

[2] Kosuru VSR, Kavasseri A. A smart battery management system for electric vehicles using deep learning-based sensor fault detection. World Electric Vehicle J. 2023;14(4):101.

[3] Mohamed N, Bajaj M, Almazrouei SK, Jurado F, Oubelaid A, Kamel S. Artificial Intelligence (AI) and Machine Learning (ML)-based information security in electric vehicles: a review. In: 2023 5th Global Power, Energy and Communication Conference (GPECOM). IEEE; 2023. p. 108–13.

[4] Hamdare, S.; Kaiwartya, O.; Aljaidi, M.; Jugran, M.; Cao, Y.; Kumar, S.; Mahmud, M.; Brown, D.; Lloret, J. Cybersecurity Risk Analysis of Electric Vehicles Charging Stations. Sensors 2023, 23, 6716. https://doi.org/10.3390/s23156716

[5] Baddu 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, pp433-440, 2024

[6] Noori FM, Hafeez A, Malik H, Uddin MZ, Torresen J. Source Link-ing Framework in Vehicu-

lar Networks for Security of Electric Vehi-cles using Machine Learning. In: 2023 IEEE Vehicular Networking Conference (VNC). IEEE; 2023. p. 207–14.

[7] Muhammad Z, Anwar Z, Saleem B, Shahid J. Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability. Energies (Basel) 2023;16(3):1113.

[8] Wei X, Du C, Zhao J. A network security situation awareness model for electric vehicle shared charging pile system. In: AIP Conference Proceedings. 2238. AIP Publishing; 2020.

[9] Basnet M, Ali MH. Multi-Agent Deep Reinforcement Learning-Driven Mitigation of Adverse Effects of Cyber-Attacks on Electric Vehicle Charging Station. arXiv preprint 2022. arXiv:2207.07041.

[10] Dabbaghjamanesh M, Moeini A, Kavousi-Fard A. Reinforcement learning-based load forecasting of electric vehicle charging station us-ing Q-learning technique. IEEE Trans Industr Inform 2020;17(6):4229–37.

[11] Baddu 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.

[12] Gan J, Li S, Wei C, Deng L, Tang X. Intelligent Learning Algorithm and Intelligent Transportation-Based Energy Management Strategies for Hybrid Electric Vehicles: A Review. IEEE Trans. Intelligent Transp. Syst. 2023.

[13] Lin HC, Wang P, Chao KM, Lin WH, Chen JH. Using deep learning networks to identify cyber-attacks on intrusion detection for in-vehicle networks. Electronics (Basel) 2022;11(14):2180.

[14] Avatefipour O, Al-Sumaiti AS, El-Sherbeeny AM, Awwad EM, Elmeligy MA, Mohamed MA, Malik H. An intelligent secured framework for cyberattack detection in electric vehicles' can bus using machine learning, 7. IEEE Access; 2019. p. 127580–92.

[15] Basnet, M. (2022). Deep Learning-Powered Computational Intelli-gence for Cyber-Attacks Detection and Mitigation in 5G-Enabled Electric Vehicle Charging Station (Doctoral dissertation, The Univer-sity of Memphis).

[16] ElKashlan M, Elsayed MS, Jurcut AD, Azer M. A machine learning-based intrusion detection system for IOT electric vehicle charging stations (EVCSs), 12. Electronics; 2023. p. 1044.

[17] Baddu Naik B, M Ravindra, Simhadri Mallikarjuna Rao, Srikanth K, M Brahmaiah, 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.

[18] Dixit P, Silakari S. Deep learning algorithms for cybersecurity applica-tions: A technological and status review. Comput Sci Rev 2021; 39:100317.

[19] Bala Saibabu Bommidi, Baddu Naik Bhukya, Swarupa Rani Bondalapati, Hemanth Sai Madupu, "Congestion Management in Power Transmission Lines with Advanced Control Using Innovative Algorithm," WSEAS Transactions on Power Systems, vol. 17, pp. 354-363, November 2022.

[20] Vasanthkumar P, Revathi AR, Devi GR, Kavitha RJ, Muniappan A, Karthikeyan C. Improved wild horse optimizer with deep learning en-abled battery management system for internet of things based hybrid electric vehicles. Sustain. Energy Technol. Assessments 2022; 52:102281.