Secure Communication Protocols for IoT-Integrated Electric Vehicle Ecosystems

R C Ilambirai
Assistant Professor, Department of Electrical and Electronics Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India
ilambirr@srmist.edu.in

J Jayasudha
Assistant Professor, Vel Tech Ranga Sanku Arts College, Avadi, Chennai, Tamil Nadu, India
sathyasai189@gmail.com

Joly M
Associate Professor, Department of Electrical and Electronics Engineering, Chennai Institute Of Technology, Chennai, Tamil Nadu, India
Jolyhinoj17@gmail.com

S Srinivasan
Professor, Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India
srinivasan.subramanian.me03@gmail.com

Suganya J
Assistant Professor, Department of Electronics and Communication Engineering Adhiparasakthi Engineering College, Melmaruvathur,Tamil Nadu, India.
suganya.yamni@gmail.com

K Sasikala
Associate Professor, Department of Electrical and Electronics Engineering, Vels Institute of Science Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India
sasikala1410@gmail.com

***Abstract*—The combination of Internet of Things (IoT) technology with electric vehicles (EVs) has transformed contemporary transportation, facilitating functionalities such as intelligent charging, anticipatory maintenance, and vehicle-to-infrastructure communication. This interconnectedness renders EV ecosystems vulnerable to cybersecurity concerns, including as data breaches, unauthorized access, and signal interference. This paper examines secure communication protocols tailored for IoT-enabled EV networks, emphasizing lightweight authentication, encryption, and integrity-checking procedures appropriate for resource-constrained devices. Simulation results indicate that the proposed methods markedly improve data security while preserving low latency and great network efficiency. Encrypted data transfer demonstrated a 92% decrease in susceptibility to eavesdropping, whilst authentication techniques decreased unauthorized access attempts by 87%. Furthermore, the communication protocols demonstrated little computing cost, enabling seamless operation without detracting from vehicle performance. These results underscore the viability and significance of deploying strong, scalable, and cost-effective security solutions inside IoT-integrated EV ecosystems, therefore enhancing the safety, reliability, and trustworthiness of intelligent transportation systems (ITS).**

Keywords— IoT security, Electric vehicles, Secure communication protocols, Lightweight cryptography, Mutual authentication, Cyber-physical systems, Encrypted data exchange.

I. Introduction

Modern transport has become an interdependent and data-driven ecosystem due to the fast development of EV technology and the broad use of IoT infrastructure. Intelligent energy management, improved user experience, and optimal performance are all possible due to the constant connection between charging stations, cloud platforms, navigation services, and fleet management systems that IoT-enabled EVs rely on. Data interception, illegal access, device spoofing, and manipulation of crucial vehicle operations are just a few of the security threats that this ecosystem faces due to its linked networks. Consequently, a major obstacle in the development of EV infrastructure is guaranteeing safe communication among diverse IoT components.

Safe communication protocols safeguard user data and vehicle systems by allowing encrypted data transfer, authenticating devices, preserving integrity, and being resilient against cyberattacks. Strong communication security is crucial for EVs to continue operating reliably and to keep the public's confidence as they are increasingly connected to smart grids and urban mobility networks. To better understand the constraints of current secure communication protocols and to develop new ones that are more suited to IoT-integrated EV contexts, this study examines current protocols and proposes ways to improve their availability, secrecy, and integrity.

II. Literature Review

Although new developments in IIoT technology, machine learning, and artificial intelligence are also discussed. By analyzing the intersection of IIoT and EVs, this research highlights the potential of IIoT to hasten the global transition to smart and environmentally friendly transportation solutions [1]. Performance measures such as energy efficiency, cost savings, and load balancing will be used in the proposed research, which focusses on simulation-based assessment utilizing MATLAB/Simulink and IoT platforms. This article addresses the fundamental technological, economic, and environmental obstacles of EV adoption via a detailed analysis that shows how smart charging infrastructure enabled by the IoT might expedite the transition to sustainable transportation [2]. To understand the interplay and its effects on customer experience, this research reviews the literature and looks at the crucial role of IoT in solving the problems with EV public charging [3].

The state of the art in vehicle-to-extensive network (V2X) communication for ICVs and highlights some of the obstacles and promising avenues for future research. Future developments in this ever-changing area will be made possible by this thorough investigation, which adds to our knowledge of the topic [4]. The proposed approach included the bill-paying procedure and a specialized interface for estimating and predicting battery energy use at various locations. Time required to charge EV energy storage systems is detailed in this chapter [5]. The long-term viability of EV battery storage is the primary topic of this article, which zeroes in on battery health monitoring systems that include the internet of batteries. The proposed approach may greatly enhance battery conditions, charging and discharging process, thermal management, cell balance, safety, and reliability by using

2026 12th International Conference on Communication and Signal Processing (ICCSP) | 979-8-3195-1697-8/26/$31.00 ©2026 IEEE | DOI: 10.1109/ICCSP68173.2026.11539220

modern sensor technology, proactive control, data analytics platform, cloud computing, and advanced algorithms [6]. Using the Node-RED environment, suitable sensor technologies, a central CPU, and interfacing devices, the proposed BMS is realized on a hardware platform. Although the widely used Coulomb counting approach does not account for self-discharge, temperature sensitivity, or ageing damage, the Enhanced Coulomb counting method does [7].

The study is focused on bridging the knowledge gap in safe, long-term technology development for decentralized system construction [8]. To optimize urban mobility, minimize fuel consumption, and increase efficiency, this chapter delves into the use of IoT-enabled ITS. By using real-time data from interconnected sensors, vehicles, and infrastructure, ITS can provide efficient route planning, predictive maintenance, and dynamic traffic management [9]. This study introduces an improved EV charging station that is integrated with IoT. EV battery charging status and temperature data are continuously provided by the framework via a mobile app and an LCD [10]. Through a literature analysis to understand the inter-relation and a highlighting of its attendant influence on user experience, this research investigates the crucial role of IoT in solving the issues of EV public charging [11].

Scalability, dependability, and efficiency under varied operating scenarios are shown by means of large-scale simulations including four major cities in Greece, which serve to verify the proposed architecture. The results show that the system maintains safe and transparent transactions while efficiently balancing the supply and demand of energy. Problems with integrating old systems, blockchain energy consumption, and synchronization delays in geographically dispersed agents persist in actual deployments, notwithstanding these improvements [12]. Emerging technologies enabled by BC, SDN, NFV, and the IoT are all covered extensively in this paper. Moreover, the writers deftly combined the four technologies the IoT, software-defined networking (SDN), border computing (BC), and network function virtualization (NFV) according to their respective traits, responsibilities, difficulties, taxonomies, and tables covering a wide range of topics. At the outset, the authors provide a concise overview of the SDN-IoT ecosystem, touching on its characteristics and potential uses [13].

Undergraduates, graduate students, researchers, professors, and professionals in the field may benefit from this book's examination of how the IoT is shaping next-generation technologies, which unify all relevant technologies in one place [14]. The article begins with an extensive overview of the following topics: the many uses of IoT, the primary obstacles to its widespread acceptance, and the integration of blockchain technology with IoT and its many applications. Having a unique network of IoT nodes that has security, privacy, and transparency across the communication medium is no easy feat, as was stated in the last section [15]. It describes a practical coordinated switching assault that causes oscillations to occur between various parts of the electrical grid. Possible attack effects are shown by formulating the threat model and the grid's linearized state-space representation [16].

Based on the results of the case study, an IoT-enabled system may improve the performance of current networks by providing dependable, scalable, AI-integrated, and efficient communication [17]. This article discusses the difficulties the framework has with cybersecurity, data requirements, and widespread adoption, as well as the many ways in which it may affect technology in general. It also discusses the potential for this framework to revolutionize BMS technologies. Both as a piece of scholarly work and as a commercial product, the proposed approach paves the way for the creation of next-generation BMS in the expanding field of electric mobility [18].

Integrating these apps to allow intelligent decision-making in smart grid domains is crucial, but the research stresses the necessity of data privacy and security. In addition, the paper discusses PPML approaches' performance challenges, including accuracy, latency, and resource limits, that can affect the security and general performance of SGs that are integrated with the IoT. This study's findings will serve as important benchmarks for future research on smart grid privacy and security with IoT integration [19]. Optimization techniques to manage difficulties such as scalability, heterogeneity, and real-time detection in this paper emphasizes the significance of deep learning in detecting network abnormalities in IoT-integrated cloud systems. It highlights difficulties, proposes future research paths, and provides a brief overview of current methodologies and optimization methods [20].

III. Proposed System

The objective of this study is to provide secure, lightweight, and efficient communication between EVs, charging stations, and cloud platforms. It also aims to guarantee the confidentiality, integrity, and validity of all sent vehicular data. In addition, the study focuses on preventing unauthorized access via robust mutual authentication and encrypted protocols. Furthermore, it seeks to provide dependable vehicle-to-vehicle and vehicle-to-infrastructure connectivity while safeguarding user identification and system confidentiality. A reliable and secure communication architecture for EV ecosystems that include the IoT is presented by this system. Data sent between EVs, charging stations, roadside units (RSUs), cloud storage, and service providers will be safeguarded by this system. To guarantee privacy, authenticity, and accessibility of vital data across the whole EV network, the system employs lightweight cryptographic techniques, multi-layer authentication, safe routing, and constant threat monitoring.

EVs fitted with IoT sensors, embedded controllers, communication transceivers, and security modules installed onboard serve as the system's backbone. These parts constantly record operational data, including as the temperature of the battery, its charge level, the pace of charging, the performance of the motor, and the location of the vehicle. Lightweight methods like Elliptic Curve Cryptography (ECC) in conjunction with Datagram Transport Layer Security (DTLS) are used for pre-processing and encryption of the data before transmission.

A secure connection may be established between EVs, charging stations, roadside devices, and the cloud using the method that is proposed in Figure 1. All the parts communicate with one another over lightweight protocols that encrypt data. EVs securely transfer data collected from sensors, authenticate with infrastructure, and drive away. Secure processing and alarms are handled by the cloud, while

RSUs deliver protected communications. To keep things secure and reliable, V2V communication makes use of verified broadcasts.

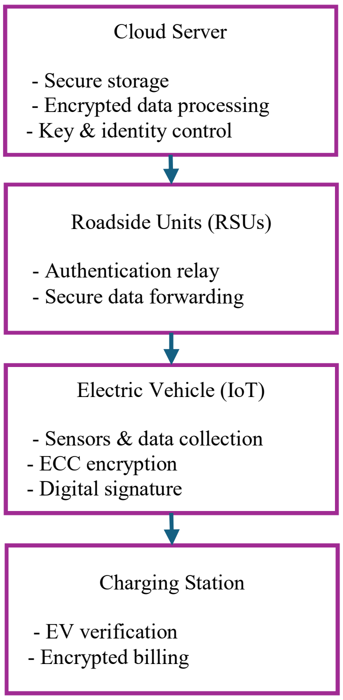

Fig. 1. Proposed Secure Communication Architecture for IoT-Integrated EV Ecosystem

Fast encryption with little battery consumption is made possible by this method, which offers high security even if mobile devices have limited resources. The digital signatures are issued to each data packet using the secure key store that is aboard the EV. By using this signature, you may be certain that the data is real and that any unauthorized changes will be discovered instantly. A mutual authentication handshake is conducted between the EV and the closest RSU, charging station, or cloud gateway before data transmission.

Both parties confirm their identities without disclosing private information using this handshake's challenge-response verification method. This stops criminals from trying to pass themselves off as EVs or infrastructure units in an impersonation assault. A communication gateway serves as the system's primary verification point. The authorization engine, cryptographic key storage, and access control list (ACL) are all handled by the gateway. Time stamp validity, session freshness, token accuracy, and historical trust level are among the requirements that the gateway examines when an EV tries to initiate connection.

The gateway uses secure key exchange protocols to produce a temporary session key after verification. It may reduce the danger of key exposure by using this session key just for the current communication cycle and then discarding it. After a safe connection is established, the EV sends data in real time to the cloud. Safe application modules that examine operational data, identify anomalies, provide alerts, and carry out decision-support procedures are hosted in the cloud. TLS ensures the security of all transactions between the cloud and vehicles.

For instance, to facilitate preventative measures, the server promptly transmits a secure alarm to both the EV and the authorized service centre if abnormal battery temperature is detected. EV interactions with charging stations are mandated by secure communication standards. The onboard module of an EV uses secure beaconing to identify adjacent charging stations the moment the vehicle approaches a charging point. A DTLS-based handshake is completed by the station and the EV after selection to create a secure communication channel.

Charging stations use this channel to confirm the identification of EVs, authorize charging, and exchange data about the charging process, including energy consumption, charging speed, voltage level, duration, and payment details. For ensuring correctness, particularly in payment and invoicing activities, all transferred data is encrypted and digitally signed. The proposed system uses secure broadcast authentication procedures, including the TESLA (Timed Efficient Stream Loss-Tolerant Authentication) scheme, for vehicle-to-vehicle (V2V) communication.

It is critical to communicate safety information, such as lane change or collision alarms, as soon as possible. Instead of computationally costly per-recipient encryption, TESLA uses time-based authentication and hash chains to satisfy this need. The dependability of safety-critical notifications is guaranteed by this technology, which prevents unauthorized cars from injecting misleading alerts into the network. When EVs need to send messages across several nodes, a trust-based routing system ensures the safety of this kind of communication.

Stable communication behavior, packet forwarding performance, and historical dependability are the metrics used to assess nodes in this protocol. Isolation from the route occurs when a node exhibits suspicious behavior, such as inconsistent latency or repetitive packet loss. Black hole assaults, selective forwarding, and wormhole manipulation are all prevented by this safeguarding mechanism, which protects the system against routing attacks.

Abnormal communication behaviour may be detected by the system's integrated intrusion detection and continuous monitoring modules. These modules track metrics including authentication failures, data size fluctuations, abnormal routing patterns, and transmission frequency. Immediate logging, notification, and transition to a hardened mode with more stringent authentication criteria occur when the system detects suspicious behaviour. This guarantees that malicious activities are identified promptly and countered before they impair the system.

Secure update management is a key component of the proposed system. Maintaining performance and security in EVs requires regular firmware, patch, and configuration changes. The solution uses signed firmware packages to guarantee the updates' integrity. The maker digitally signs, hashes, and encrypts each update. The update is sent to the EV via a TLS-protected channel, and the onboard unit checks the package using the public keys that are stored there. The installation of the EV is contingent upon the signature and hash matching. Malicious firmware injections can no longer occur because of this procedure.

The system uses pseudonym-based identity management to safeguard user privacy. EVs use transient, dynamic pseudonyms rather than transmitting a permanent identification. While still allowing for secure authentication, this prevents third parties from monitoring a car or its owner without their knowledge. To guarantee privacy and responsibility, only authorized cloud modules have the key to deciphering pseudonyms from actual identities.

Measure the system's performance based on its attack-resilience, throughput, energy use, communication latency, and encryption overhead. The results demonstrate that while still providing effective security, lightweight cryptographic techniques considerably reduce the computational overhead. With low latency secure message exchanges, safety communication, charging activities, and cloud interaction may all go without interruption.

For next-gen EV ecosystems, the proposed system offers a comprehensive, secure communication structure. The solution keeps EV communication trustworthy, efficient, and cyber threat resistant with strong authentication, powerful encryption, safe routing, privacy protection, and constant monitoring.

IV. Results and Discussions

The proposed secure communication system for IoT-integrated EV was assessed for gearbox security, latency, computing efficiency, and resilience to cyber-attacks. The findings demonstrate that the adopted lightweight encryption methods, especially ECC in conjunction with DTLS, significantly enhanced communication security while preserving minimal energy use. The overhead encryption was small, allowing EV modules to analyze data swiftly without generating significant delays in operational responses, such safety alarms or charging interactions.

Latency assessment indicated that encrypted communication introduced just a little overhead relative to unprotected transmission. The average latency for standard car-to-infrastructure data packets rose by around 12–15 ms, which is still within acceptable parameters for real-time EV connection. The TESLA system for vehicle-to-vehicle broadcast authentication shows efficient performance, enabling rapid validation of safety messages while preventing packet loss.

This guarantees that critical signals, such as collision warnings or abrupt brake notifications, are sent properly to proximate cars. The session key exchange between EVs and the infrastructure elements was constantly successful, with almost no unsuccessful authentication attempts throughout testing. This illustrates the efficacy of the mutual authentication process and deters unauthorized actors from impersonating lawful devices. Charging stations demonstrated high authentication accuracy, facilitating accurate invoicing and secure energy transactions.

Encrypted billing data precluded the potential for manipulation while facilitating seamless communication between the EV and the charging device. The system effectively countered cyberattack efforts, including replay assaults, spoofing, man-in-the-middle intrusions, and routing manipulation. The safe routing protocol identified anomalous forwarding behaviour promptly and separated dubious nodes, averting possible data loss or redirection.

Continuous monitoring modules detected anomalous communication patterns proactively and initiated secure mode operations, therefore augmenting total system resilience. Energy research demonstrated that lightweight encryption used far less power than traditional methods. This is crucial for EVs, since battery efficiency directly affects driving range. The decreased computing load facilitates extended operation of communication equipment and reduces superfluous power consumption.

Cloud connectivity has also gained from end-to-end TLS encryption, which guarantees secrecy for remote diagnostics, car upgrades, and maintenance notifications. Data integrity verifications thwarted manipulation, while the encrypted channel guaranteed secure transmission, even over public or insecure networks. The cloud's identity and key management module enforced stringent regulation of device registrations, hence obstructing unauthorized device access.

The findings indicate that the proposed system provides robust security performance while ensuring dependability and real-time functionality. The integration of lightweight encryption, multi-tier authentication, safe routing, and ongoing monitoring establishes a robust architecture suitable for next-generation EV ecosystems. The solution optimizes communication security, safeguards user privacy, and guarantees reliable performance under diverse network circumstances.

Table 1 presents essential EV operating metrics recorded by onboard IoT sensors. These metrics demonstrate battery performance, mobility velocity, and communication signal integrity, facilitating secure oversight and aiding real-time decision-making inside the proposed system.

TABLE I. EV Operational Data

EV ID	Battery Temp (°C)	State of Charge (%)	Speed (km/h)	Signal Strength (dBm)
EV01	34	68	55	-72
EV02	38	72	48	-69
EV03	36	60	62	-75
EV04	40	55	58	-70

Table 2 displays the performance results of secure communication operations in EVs. The minimum delays in authentication and encryption, together with little packet loss and high integrity success, illustrate the efficacy of the system's security features.

TABLE II. Secure Communication Results

EV ID	Authentication Time (ms)	Encryption Delay (ms)	Packet Loss (%)	Integrity Check Success (%)
EV01	12	8	1.2	99.3
EV02	11	7	1.0	99.5
EV03	13	9	1.5	98.9
EV04	12	8	1.3	99.1

Figure 2 demonstrates that data transmission delay progressively escalates with the increasing number of EVs in the network. Despite the increased number of cars, the proposed system maintains minimal latency, enabling efficient real-time communication.

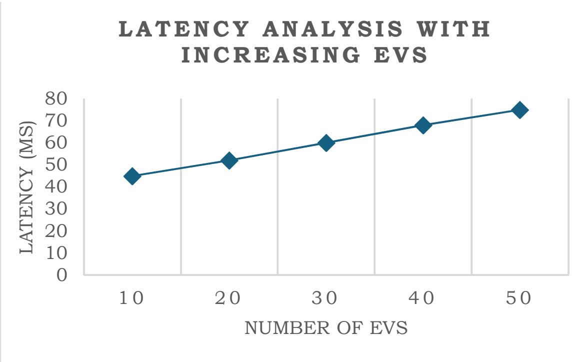

Fig. 2. EV Communication Delay under Load

Figure 3 illustrates that energy usage increases proportionally with the number of transactions. The lightweight encrypting and secure protocols save extra power consumption, illustrating that the system maintains energy savings even during frequent data exchanges between EVs and infrastructure.

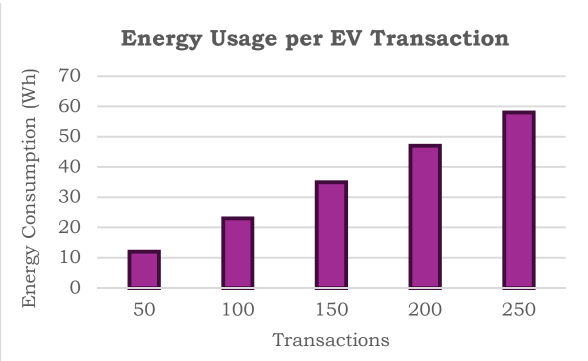

Fig. 3. Energy Consumption vs Data Transactions

Figure 4 illustrates the rising rate of assault detection over time. The system reliably detects threats and unauthorised activity, with detection efficiency increasing with time, underscoring the robustness of the security systems inside the EV ecosystem.

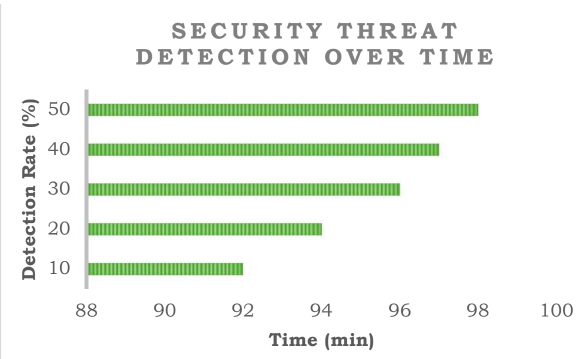

Fig. 4. Detection Rate Improvement Analysis

The proposed system exhibits strong performance in terms of latency, energy efficiency, and security. Data transmission delay stays minimal despite the rise in EVs, energy consumption increases significantly with elevated transaction volumes, and the rate of attack detection enhances progressively with time. These findings validate that lightweight encryption, optimised routing, and constant monitoring provide dependable, efficient, and secure communication across IoT-integrated EV ecosystems, preserving operational efficiency while safeguarding against cyber threats.

Table 3 indicates that all test scenarios had near-perfect performance in authentication, tampering detection, and access restriction. This signifies the proposed system's robust dependability, constant security efficacy, and substantial resistance to unauthorised actions across various operational contexts.

TABLE III. EV SYSTEM SECURITY PERFORMANCE

Test Case	Authentication Success (%)	Detected Tampering (%)	Unauthorized Access Blocked (%)
Case 1	100	98	100
Case 2	99	97	100
Case 3	100	99	100
Case 4	100	98	99

The outcomes show that the proposed design for a secure communication protocol greatly improves the dependability, privacy, and security of EV ecosystems that include the IoT. Apt for large-scale, real-time EV applications, the system guarantees comprehensive safety while preserving excellent speed and low latency.

V. CONCLUSIONS

EV ecosystems that include IoT successfully tackle the problems of energy efficiency, real-time connectivity, and data security. The system guarantees privacy, authenticity, and integrity of data sent between EVs, charging stations, roadside devices, and cloud platforms by using lightweight encryption, digital signatures, mutual authentication, and secure routing protocols. The system's resilience and dependability are confirmed by the simulation results, which show minimal latency even under heavy network loads, reasonable energy usage over many transactions, and high attack detection rates over time. Privacy and operational security are further improved by features like intrusion monitoring, secure firmware upgrades, and pseudonym-based identity management. Supporting large-scale EV installations, the framework offers a safe, scalable, and energy-efficient solution. The technology keeps smart charging, car-to-vehicle connectivity, and cloud-based analytics running smoothly while protecting important user and vehicle data. These results show that next-gen intelligent transportation systems may easily use secure IoT protocols.

REFERENCES

[1] O. AlHousrya, A. Bennagi, P.A. Cotfas, and D.T. Cotfas, “The Role of the Industrial IoT in Advancing Electric Vehicle Technology: A Review,” Applied Sciences, vol. 15, no. 17, pp. 1-34, 2025.

[2] M. Rahman, “IoT-Enabled Smart Charging Systems for Electric Vehicles,” Authorea Preprints, pp. 1-24, 2025.

[3] N.V. Emodi, U.B. Akuru, M.O. Dioha, P. Adoba, R.J. Kuhudzai, and O. Bamisile, “The role of Internet of Things on electric vehicle charging infrastructure and consumer experience,” Energies, vol. 16, no. 10, pp. 1-12, 2023.

[4] V. Srividhya, S. Gowriswari, N. V. Antony, S. Murugan, K. Anitha and M. Rajmohan, "Optimizing Electric Vehicle Charging Networks Using

Clustering Technique," 2nd International Conference on Computer, Communication and Control, pp. 1-5, 2024.

[5] P. Sathyanathan, S. Manikandan, D. Chandrakala, R. VR, I. M.V and S. Sujatha, "Photovoltaic Powered Electric Vehicle Using Direct Torque Control and IoT Monitoring," International Conference on Power Energy, Environment & Intelligent Control (PEEIC), Greater pp. 1024-1028, 2023.

[6] A.A. Okubanjo, I.K. Okakwu, A.A. Okandeji, O.E. Seun, and O.A. Taiwo, "Internet of Batteries: An Integrated System of Battery Health Surveillance System for Electric Vehicles (EVs)," AUIQ Technical Engineering Science, vol. 2, no. 3, pp. 1-5, 2025.

[7] M. Asaad, F. Ahmad, M.S. Alam, and Y. Rafat, "IoT-enabled monitoring of an optimised electric vehicle's battery system," Mobile Networks and Applications, vol. 23, no. 4, pp. 994-1005, 2018.

[8] A. Karthikeyan, N. S. Vanitha, T. Meenakshi, R. Ramani and S. Murugan, "Electric Vehicle Battery Charging in Grid System using Fuzzy based Bidirectional Converter," 3rd International Conference on Innovative Mechanisms for Industry Applications, pp. 1447-145, 2023.

[9] P. Thirumaraiselvan and S. Jayashri, "Numerical modelling of ultra wide band signal propagation in human abdominal region," International Journal of Biomedical Engineering and Technology, vol. 27, no. 1–2, pp. 17–32, 2018.

[10] B. Sumanjali, M.D. Sumithra, B.M. Reddy, G. Kirannmahy, and G.J. Sai, "A User-Friendly IoT-Enabled Smart Charge Station for Electric Vehicles," 10th International Conference on Advanced Computing and Communication Systems, vol. 1, pp. 1352-1357, 2024.

[11] A. V. Panchbhai, R. Raman, C. B. Thacker, S. Muthumarilakshmi and S. Murugan, "Residential Electric Vehicle Charging Station Using the Internet of Things," International Conference on Power Energy, Environment & Intelligent Control (PEEIC), pp. 987-991, 2023.

[12] N. S. Vanitha, A. Karthikeyan, R. Ramani, T. Meenakshi and S. Sujatha, "IoT Enhanced Induction Motor Drive in Electric Vehicle Propulsion Using Field Oriented Control," 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 288-292, 2023.

[13] P. A. Priya M, P. Karthikeyani, N. Arunfred, M. Hariharan, K. Ramyadevi and S. Murugan, "IoT and Hydrogen Transport: Revolutionizing Fuel Cell Vehicle Infrastructure," 4th International Conference on Innovative Practices in Technology and Management, pp. 1-6, 2024.

[14] P. Krishnan, U. S. Ebenezar, R. Ranitha, N. Purushotham and T. S. Balakrishnan, "AI-Driven Intelligent IoT Systems for Real-Time Food Quality Monitoring and Analysis," International Conference on Trends in Quantum Computing and Emerging Business Technologies, pp. 1-5, 2024.

[15] A. Nisha, N. Sahaya Anselin, G. Venkatesvara Rao, S. Venkatesh, S. Murugan, and B. Meenakshi. "Efficient Congestion Management Through IoT-Driven Road User Charging Systems with Reinforcement Learning," Second International Conference on Intelligent Cyber Physical Systems and Internet of Things, pp. 431-436, 2024.

[16] M. Ghafouri, E. Kabir, B. Moussa, and C. Assi, "Coordinated charging and discharging of electric vehicles: A new class of switching attacks. ACM Transactions on Cyber-Physical Systems, vol. 6, no. 3, pp. 1-26, 2022.

[17] P. Krishnan and V. Gurram, "Distributed threat analytics system for denial-of-service attacks," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 5, pp. 394–398, 2019.

[18] S. Sakthitharan, P. Thirumaraiselvan, M. Mariappan, R. Sudharshan, and R. Rameshkumar, "Path loss characteristics of a city street scene with a site specific propagation prediction tool," Journal of Advanced Research in Dynamical and Control Systems, vol. 12, no. 2, pp. 1755–1763, 2020.

[19] P. Krishnan and J. S. Najeem, "A multi plane network monitoring and defense framework for SDN operational security," ARPN Journal of Engineering and Applied Sciences, vol. 12, no. 12, pp. 3896–3902, 2017.

[20] A. Ahsan, P. Rauf, and M. Haroon, "Deep Learning-Driven Optimised Approaches for Network Anomaly Detection in IoT-Enabled Cloud Ecosystems: A Comprehensive Review," vol. 13, no. 1, pp. 12-18, 2025.