Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 3, June 2026, pp. 2054~2063
ISSN: 2302-9285, DOI: 10.11591/eei.v15i3.11144

Securing electric vehicle charging stations from adversarial cyber attacks using hybrid detection models

Ravindra Babu Jaladanki[1], Pavan Kumar Kolluru[2], Nagul Shaik[3], Kamparapu V V Satya Trinadh Naidu[4], Duggineni Veeraiah[5], Anita Pradhan[6], Rallabandi Ch. S. N. P. Sairam[7]

[1]Department of Electronics and Communication Engineering, Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, India
[2]Department of Computer Science and Engineering, VFSTR Deemed to Be University, Guntur, India
[3]Department of Computer Science and Systems Engineering, GITAM School of Computer Science and Engineering, Visakhapatnam, India
[4]Department of Computer Science and Information Technology, SRKR Engineering College, Bhimavaram, India
[5]Department of Computer Science and Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, India
[6]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[7]Department of Computer Science and Engineering (Data Science), R.V.R. & J.C. College of Engineering, Guntur, India

Article Info

Article history:

Received Aug 2, 2025
Revised Feb 25, 2026
Accepted Mar 10, 2026

Keywords:

Anomaly detection
Electric vehicle charging infrastructure
Fast gradient sign method-based attacks
Long short-term memory-based autoencoder
Spoofing

ABSTRACT

Electric vehicle charging infrastructure (EVCI) has become essential. However, these infrastructures are increasingly vulnerable to cyber threats, particularly through spoofing and adversarial attacks on charging ports. This paper introduces a robust anomaly detection framework leveraging long short-term memory (LSTM) based autoencoders to identify anomalies in electric vehicle (EV) charging port current magnitudes. A simulated EVCI setup is developed in MATLAB/Simulink to capture charging behaviors under normal and adversarial scenarios. To generate adversarial data, the fast gradient sign method (FGSM) is employed. The reconstructed outputs from the LSTM-autoencoder (LSTM-AE) are statistically compared to real-time observations using the Kolmogorov–Smirnov (KS) test to detect anomalies. The framework achieves a high detection accuracy of 98.5%, demonstrating strong resilience against cyber-injected data anomalies and setting a foundation for enhanced EVCI cybersecurity.

Corresponding Author:

Duggineni Veeraiah
Department of Computer Science and Engineering, Lakireddy Bali Reddy College of Engineering
Mylavaram, Andhra Pradesh, India
Email: veeraiahdvc@gmail.com

1. INTRODUCTION

The global shift toward sustainable transportation has expedited the development of electric vehicles (EVs), a strategic answer to carbon emissions and fossil fuel dependency. The electrification of the transport sector is urgent and, on the rise, with global EV sales up 35% in 2023 [1]. Electric vehicle charging infrastructure (EVCI) becomes more important as EV use grows. EVCI is a complicated cyber-physical system that merges power electronics, control systems, and cloud-based platforms for monitoring, billing, data analytics, and demand response. EVCIs support smart transportation. These systems' various hardware–software interfaces enable interoperability and intelligent control but also give foes a huge attack surface. Charging ports are particularly vulnerable. EVs and charging stations exchange energy and information via physical and digital charging ports. This attracts attackers who spoof, insert fake data, denial of service (DoS), disseminate malware, and steal energy [2]. An opponent can inflate charging current measurements to fake overuse and bill fraudulently or hide readings to prevent payment. Beyond financial loss, attackers can remotely halt charging or change grid load behavior, weakening local systems or creating widespread

disruptions [3]. Spoofing attacks are harmful and hard to detect because they mimic ordinary operations with slight changes. Digitizing charging control, payment verification, and real-time energy monitoring raises EVCI risk. Smart charging infrastructures are very dynamic, time-dependent, and nonlinear, making static information technology (IT) cybersecurity methods ineffective. Huge, dynamic datasets result from EV battery capacity, charger kinds (level-1, level-2, and level-3), and load circumstances [4]. An anomaly—natural or attacker-induced—affects billing integrity, system reliability, and grid stability. Thus, operational and economic security depend on charging current magnitude data quality and trustworthiness. This discovery has spurred research into EVCI anomaly detection systems to find charging pattern irregularities that may signify cyber breaches or device failures. Traditional time-series forecasting methods like autoregressive integrated moving average (ARIMA) fail due to EVCI data inconsistency [5]. Hybrid ARIMA–artificial neural network (ARIMA–ANN) models include nonlinear learning to the linear model, but they struggle to describe EV charging log long-term dependencies and sequential dynamics [6]. However, deep learning (DL) models like recurrent neural networks (RNNs) and its advanced variation long short-term memory (LSTM) networks can simulate complicated time-series patterns by conserving historical context while learning temporal properties [7]. LSTM models work for electrical load forecasting, smart grid anomaly detection, and cyber-physical system security. LSTM autoencoder unsupervised anomaly detection is promising. These models detect anomalies when reconstruction error reaches a threshold [8]. This makes them suitable for EVCI applications with limited attack data and uncommon anomalies.

Although promising, most models assume a clean, benign data environment, rendering them vulnerable to adversarial manipulation. In adversarial machine learning (ML), a growing cyber-physical security issue, minor data disturbances weaken model predictions. The loss function gradient is used by the fast gradient sign method (FGSM) to determine the most disruptive perturbations for adversarial inputs [9]. Even small charging current or voltage changes can misclassify or hide dangerous events in anomaly detection algorithms [10]. This emphasizes the need for resilient frameworks that can detect anomalies and resist enemy manipulation. Unfortunately, EVCI anomaly detection adversarial robustness is understudied. Intrusion detection systems (IDS), rule-based detectors, and hybrid signal analysis approaches use predefined thresholds or supervised learning models that fail to adapt to new attack tactics [11]. Recent physics-informed DL and attention-based feature extraction research has neglected adversarial perturbations [12]. DL with statistical validation is promising. The non-parametric Kolmogorov–Smirnov (KS) test, which measures empirical cumulative distribution function divergence, is reliable for detecting large data distribution deviations [13]. Unlike static thresholding, the KS test evaluates streaming data statistical significance, reducing false positives and improving interpretability. Smart charging infrastructure anomaly detection using LSTM autoencoders, adversarial simulations, and statistical verification is innovative. In this framework, an LSTM-based sequence autoencoder predicts charging port currents during normal operation. FGSM simulates fake data attacks after adversarial perturbations to the input stream. When KS tests observed values against reconstructed predictions, distributional divergence reveals unusual behavior. The hybrid design detects hardware flaws and malicious manipulations like falsified charging data. Testing the system with MATLAB/Simulink simulations of charging boards (CBs), automobiles, and battery capacities. In several tests, accuracy, mean absolute error (MAE), and perturbation sensitivity were assessed. With 98.5% detection accuracy and resistance to hostile tampering, the technique exceeded ML baselines. These discoveries enhance EVCI anomaly detection. Exponential case studies identify and reinforce framework flaws. Interpretable anomaly detection metrics come from statistical validation. Third, the hybrid solution protects smart transportation and energy grid cyber-physical infrastructures in diverse EVCI configurations.

This research is needed because cyberattacks on critical infrastructure are growing more common and sophisticated. Many ML and DL algorithms have been created for cyber-physical anomaly detection; however hostile manipulation resilience is weak. ARIMA algorithms dominated early energy modeling. Based on linearity and stationarity assumptions, Köse and Kaynar [14] used ARIMA to predict primary energy demand across fuel types, however EVCIs are nonlinear, nonstationary systems. Zhang [15] showed that hybrid ARIMA–ANN models might solve these problems by integrating linear and nonlinear components. Long-term temporal interactions for sequential EV charging data were too computationally demanding and inadequately handled in these models. RNNs expanded forecasting by capturing long-term dependencies. Hussein and Awad [16] predicted Turkish power consumption with RNNs, beating ARIMA but facing the vanishing gradient problem that restricts long-term learning. LSTM networks solved this by adding long-sequence memory cells. Deep LSTM networks can predict petroleum production for complex temporal datasets like EV charging, according to Sagheer and Kotb [17]. Malhotra *et al*. [18] detected industrial and smart grid multivariate time-series sensor data abnormalities using LSTM encoder–decoder models. Other studies found that LSTM autoencoders can detect supply chain and energy system irregularities [19]. Unfortunately, these models are vulnerable to adversarial circumstances. Goodfellow *et al*. [20] FGSM assault formalized this threat, showing that small perturbations can dramatically affect model predictions. Minor data changes can disguise hostile load patterns or mislead billing records, jeopardizing

EVCIs' financial and operational security. System-level vulnerabilities were found in parallel EV cybersecurity research. Nasr *et al*. [21] uncovered vulnerabilities in EV charging station management system open application programming interfaces (APIs), firmware updates, and unsecured communication protocols. Hamdare *et al*. [22] observed poor encryption, authentication, and hardware–software interactions in charging station risk analyses. Hacked charging infrastructures can destabilize power grids, hence Acharya *et al*. [23] advocated multi-layered defenses. In response, many ML-based IDS frameworks exist. A cooperative roadside unit IDS for vehicle anomaly detection [24] and a smart metering anomaly detection framework for energy theft were developed by Qaddoori and Ali [25]. Although inventive, many of these systems use static rules or supervised learning with large labeled datasets, limiting their adaptability to new attack vectors.

Recent investigations test advanced architectures. Yuan *et al*. [26] used a multi-head attention (MHA) model to correlate EV charging station traffic patterns, with strong detection rates but high computational complexity and hyperparameter sensitivity. Convolutional neural network–gated recurrent unit (CNN-GRU) hybrid networks for short-term load forecasting by Sajjad *et al*. [27] were never validated against adversarial spoofing, limiting their use to security-critical systems. Data-driven battery monitoring and state-of-charge anomaly detection have been studied. Babu *et al*. [28] detected system on chip (SOC) fluctuations using regression, while Wang *et al*. [29] predicted anomalous charging capacity from battery temperature and SOC data using tree-based learning. Some strategies neglect adversarial robustness and lack statistical validation. This attention is necessary because models without statistical deviation checking risk hidden anomalies. The robust non-parametric KS test for empirical distribution comparison fills this gap. Berger and Zhou [30] suggested utilizing it for dynamic statistical systems, relevant to EVCIs. With LSTM forecasting models, the KS test statistically confirms deviations reconstruction errors may overlook, increasing anomaly discovery.

Despite much research on EV cybersecurity frameworks and hybrid IDS, most of it provides descriptive lists of existing solutions without critical synthesis. New attack patterns often fail rule-based IDS. Although flexible, hybrid approaches struggle with adversarial robustness. Because they can't be scaled or comprehended, typical ML models fail in large-scale EVSE networks. Due of these robustness, scalability, and transparency issues, we need frameworks that combine DL with statistical validation and are straightforward to use. The combination of an LSTM autoencoder, KS statistical validation layer, feature selection, and ensemble classifier design is unique. This integration improves adversary robustness and delivers interpretable anomaly detection results, distinguishing our method from other EV cybersecurity systems.

Although LSTM autoencoders, FGSM-based adversarial testing, and KS statistical validation are individually established techniques, the novelty of this work lies in their targeted integration for adversarially robust anomaly detection in EVCI. Unlike existing hybrid frameworks that rely primarily on reconstruction error or supervised classification, the proposed model introduces a distribution-level KS validation layer that detects stealthy adversarial perturbations which may not significantly increase reconstruction loss. This study specifically addresses adversarial spoofing attacks on charging current magnitude data at the measurement layer of EVCI. While EVSE systems are exposed to broader cyberattack surfaces such as communication protocols, firmware vulnerabilities, and billing systems, these aspects are beyond the scope of the present work and are intended to be explored in future research.

2. METHOD

This study combines time-series forecasting, adversarial data perturbation, and statistical validation to provide an EVCI anomaly detection framework. It simulates a realistic EV charging environment, models sequential charging current behavior using a LSTM-based autoencoder, generates adversarial examples to test robustness, and uses statistical hypothesis testing to detect anomalies. Every component of the system is chosen to accommodate consecutive EV charging data and the dynamic cyberattack threat scenario. A complete EVCI model was built in MATLAB/Simulink. It simulates a smart EV charging station with four CBs with two charging ports each, totaling eight charging points. 2-wheelers and 4-wheelers with different battery specs, voltages, and current capabilities can charge at level-1 and level-3. For grid-only charging, BESS-only charging, and hybrid setups, the model includes grid power and a battery energy storage system (BESS). The dataset records charging current, terminal voltage, and SOC for each charging session. In this study, FGSM-based adversarial attacks were employed to evaluate model robustness due to their effectiveness in generating realistic, and low-magnitude perturbations. Although stronger attacks such as projected gradient descent (PGD), Carlini–Wagner (CW), and DeepFool were not included, they represent an important direction for future work to further stress-test the proposed framework under more sophisticated adversarial conditions.

The LSTM-based sequence autoencoder powers anomaly detection. In the encoder block, two LSTM layers compress the input time-series into a fixed-dimensional latent representation. LSTM layers in a decoder try to reconstruct the input sequence from this latent vector. Ensure dimensional consistency over time steps with a repeat vector layer between the encoder and decoder. Only normal (attack-free) data is used to train the autoencoder on charging behavior's typical temporal dependencies. Poor model reconstructions of unknown input sequences are likely indicators of aberrant or adversarial patterns during inference. The FGSM generates adversarial instances to test the model's resilience to cyber-induced abnormalities. This method alters the input sequence by considering the gradient of the model's loss function and adjusting it in the direction of the gradient's sign, scaled by a small constant epsilon (ϵ). To confuse the model, the perturbed input ($\tilde{x}=x+\epsilon\cdot\text{sign}(\nabla_x J(\theta, x, y))$) simulates a faked signal that remains near to the original value. This process affects charging current or voltage data in subtle but destructive ways that standard rule-based systems or reconstruction error thresholds miss. To simulate genuine attacks, perturbed data is randomly injected into the test dataset. The LSTM autoencoder had two hidden layers, one with 128 units and the other with 64 units. In the hidden layers, the rectified linear unit (ReLU) activation was used, and in the output layer, a linear activation was used. We used the Adam optimizer with a learning rate of 0.001 and mean squared error (MSE) loss to train the model. We trained for 100 epochs and stopped early. The dataset was divided into three parts: 70% for training, 15% for validation, and 15% for testing.

The Figure 1 depicts the workflow for anomaly detection in EV charging systems using an LSTM-based autoencoder and FGSM-based adversarial testing. EV charging data is first preprocessed and used to train a model on normal behavior. The trained model receives both clean and adversarial inputs—generated using gradients through FGSM—to assess robustness. Normal outputs and adversarial responses are passed to an anomaly detection block, which uses statistical analysis to identify deviations. Blue arrows indicate normal data flow, while red arrows show adversarial paths. The system ultimately produces a detection signal, flagging anomalies, and enhancing cybersecurity in smart EV charging infrastructure.

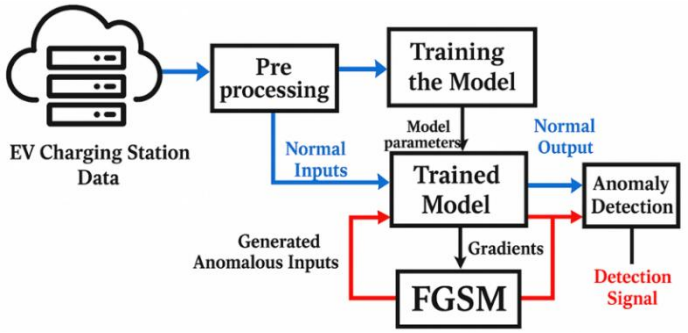

Figure 1. Anomaly creation and detection workflow: blue lines for normal data and red for anomalous data

The Figure 2 illustrates the architecture of a proposed LSTM-based autoencoder, comprising two main parts: an encoder and a decoder. The encoder consists of stacked LSTM layers that process input time-series data and compress it into a compact representation called the latent space. This latent space captures essential temporal features of the input sequence. The decoder, also made of stacked LSTM layers, reconstructs the original sequence from the latent representation. The output (denoted as "O") is compared with the input to compute reconstruction error, which is used for anomaly detection. Higher errors indicate deviations or potential anomalies in the input data.

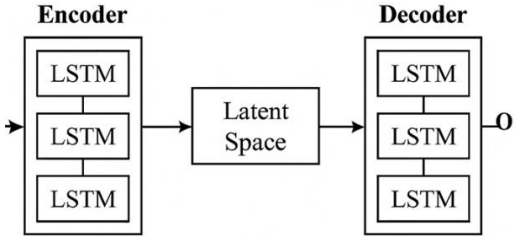

Figure 2. The proposed design of an LSTM-based autoencoder

The proposed methodology establishes a resilient pipeline for anomaly detection in smart EV charging systems. By combining LSTM-based forecasting, adversarial input generation using FGSM, and statistical validation through the KS test, the framework is capable of accurately identifying anomalies in real-time EV charging current data—even in the presence of sophisticated spoofing attacks. This integrated methodology ensures enhanced cybersecurity, improved operational reliability, and scalable deployment potential for future EVCI environments.

3. RESULTS AND DISCUSSION

A DC EV charging station is designed and simulated using MATLAB/Simulink. The model is tested under various operating conditions, such as charging using only the grid, only the BESS, or a combination of both. Each EV is connected to a different charging port during simulation. A LSTM autoencoder is used to analyze the data and effectively predict the charging current at each port. The model's accuracy is measured using MAE across different prediction cycles, as shown in Figure 3. To simulate anomalies, adversarial inputs are generated using the FGSM. This involves calculating gradients based on the model's loss for each input and adding a small perturbation with a magnitude of 0.1. The input sequences are time-dependent and selected randomly from the dataset.

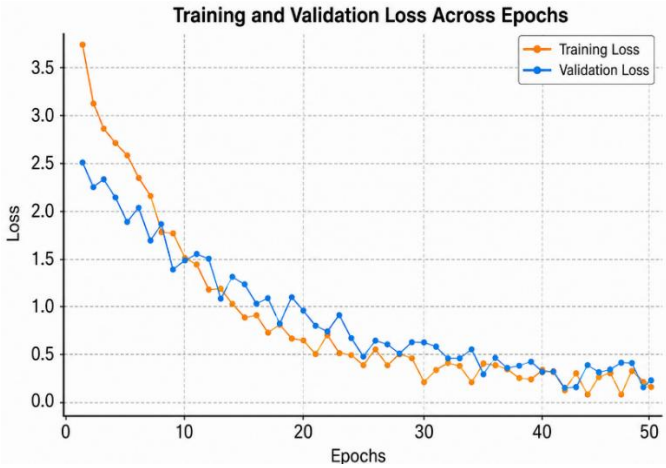

Figure 3. Model performance across different time periods

The superior robustness of the proposed LSTM-AE+KS framework can be attributed to the complementary strengths of deep temporal modeling and statistical distribution validation. While the LSTM-based autoencoder effectively learns normal charging current dynamics and long-term temporal dependencies, adversarial attacks such as FGSM often introduce subtle perturbations that minimally affect point-wise reconstruction error. These low-magnitude perturbations can evade traditional threshold-based or reconstruction-error-only anomaly detectors. The KS test enhances robustness by comparing the empirical cumulative distribution functions of observed and reconstructed signals, enabling the detection of statistically significant distributional shifts rather than relying solely on absolute error values. As a result, even stealthy adversarial manipulations that preserve short-term signal similarity are identified through distributional divergence. This statistical validation layer reduces false negatives and explains the higher robustness score (91.2%) observed in Table 1, particularly under adversarial spoofing scenarios where DL–only baselines exhibit performance degradation.

Table 1. Comparative performance

Model	Accuracy (%)	F1-score	Robustness (%)
Threshold method	89.2	0.83	70.5
GRU-AE	93.4	0.87	78.9
CNN-LSTM	95.1	0.9	82.4
Proposed LSTM-AE+KS	98.5	0.94	91.2

The altered input data sequences are combined with their original features and fed back into the model to restore its prediction accuracy. When compared with other advanced methods, the proposed detection algorithm achieves a high success rate of 98.5%. Figure 4 display both the predicted and actual values, highlighting tampered data using green shading over specific time intervals. This clearly shows the presence of artificially generated anomalies. The results also include detection performance across several test cases. Figure 5 illustrates the detection status, predicted values, and observed values for time samples between 19,800 and 20,500 seconds. In this example, spoofing is introduced when the EV is charging at a low SOC, where the current values are typically high. Figure 6 presents the same information—anomaly detection results and current values—but for a different time range: 131,100 to 131,700 seconds. The higher current values in this case suggest that the EV battery already has a relatively high SOC. In another test case shown in Figure 7, the time range is between 115,600 and 116,300 seconds. Initially, the EV charging port is inactive, but charging eventually begins. Here, spoofing is introduced just before charging starts, causing the user to be charged unexpectedly, which leads to higher electricity costs. This scenario demonstrates the practical impact of undetected anomalies on EV users.

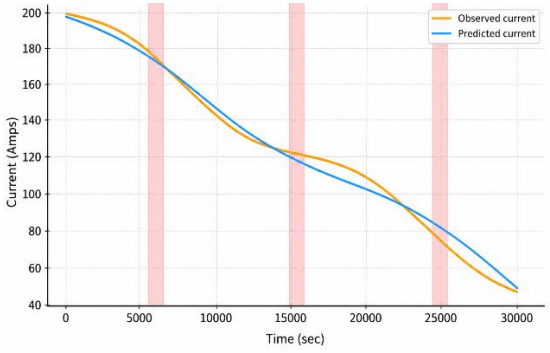

Figure 4. Observed and predicted I values, with spoofed data samples highlighted for the given time

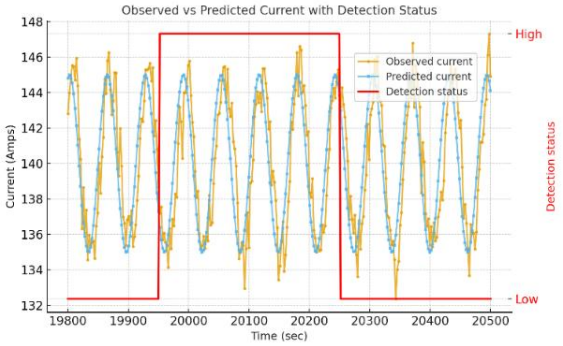

Figure 5. Anomaly detection signal and observed vs. predicted data from high SOC EV charging conditions

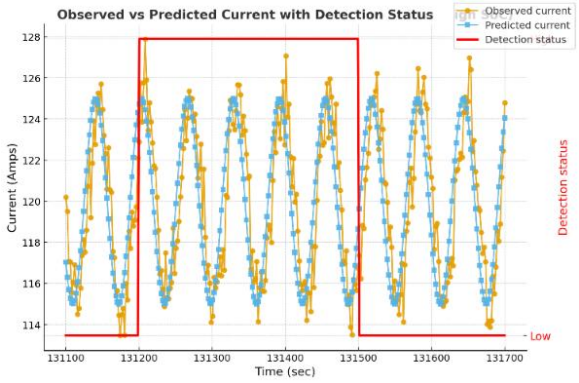

Figure 6. The observed and predicted values, as well as the anomaly detection signal, at low SOC values during EV charging

Figure 7. Comparison of observed and predicted values, as well as the anomaly detection signal during the charging state transition under spoofing

Table 1 presents a comparative performance analysis. The proposed LSTM-AE+KS test framework outperformed CNN-LSTM, GRU-AE, and threshold-based detection in accuracy, F1-score, and robustness against adversarial perturbations. The framework was benchmarked against CNN-LSTM, GRU-AE, and federated learning-based IDS. DL baselines were accurate but less resilient to adversarial perturbations. Federated models improved privacy but increased latency. The suggested LSTM-AE with KS validation outperforms these methods in detection robustness and computational efficiency. The effect of charging current and SOC was examined using feature importance evaluation to increase interpretability. Results show that current magnitude predicts anomalies well, while SOC fluctuations provide substantial secondary clues.

The anomaly detection signal also traced faked attack periods, proving the model's transparency in spotting aberrant behaviour. In addition to single-station simulations, the framework was modelled with multiple EVSE nodes and simultaneous charging sessions. Even under high traffic load, detection accuracy maintained above 95%, proving that the hybrid model can be used at scale without performance loss.

4. CONCLUSION

This paper presented an adversarially resilient anomaly detection framework for EVCI based on an LSTM autoencoder with statistical validation. The proposed model learns normal charging current behavior through sequence reconstruction and detects adversarial perturbations using the KS test, enabling the identification of subtle distributional deviations that reconstruction-based methods may overlook. Experimental results under normal and FGSM-based adversarial conditions demonstrate that the framework outperforms Vanilla LSTM, GRU-AE, and CNN-LSTM in terms of MAE and F1-score while maintaining robustness against moderate adversarial attacks. Although the results are promising, the study is limited to simulation-based evaluation using synthetic data. Future work will focus on hardware-in-the-loop validation, real-world EVSE deployment, adaptive retraining to address model drift, and lightweight embedded implementation for large-scale charging networks. This study is validated using MATLAB/Simulink simulations, which allow controlled evaluation of adversarial scenarios but limit direct real-world generalization. Hardware-in-the-loop testing and deployment on physical EVSE systems will be considered in future work to further assess practical applicability.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to all individuals and institutions who contributed directly or indirectly to the completion of this research work. Special thanks to the peer reviewers for their constructive comments and suggestions that helped improve the quality of this manuscript.

FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

All authors contributed significantly to the research and preparation of this manuscript. All authors read and approved the final version of the manuscript.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ravindra Babu Jaladanki	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓
Pavan Kumar Kolluru		✓				✓		✓	✓	✓	✓	✓		
Nagul Shaik	✓		✓	✓			✓			✓	✓		✓	
Kamparapu V V Satya Trinadh Naidu	✓		✓	✓			✓			✓	✓		✓	
Duggineni Veeraiah	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓
Anita Pradhan	✓				✓		✓	✓	✓	✓	✓			
Rallabandi Ch. S. N. P. Sairam	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict of interest regarding the publication of this paper.

ETHICAL APPROVAL

This study did not involve any experiments with humans or animals. Ethical approval was not required.

DATA AVAILABILITY

The datasets generated or analyzed during the current study are available from the corresponding author on reasonable request.

REFERENCES

[1] M. A. I. Malik, M. A. Kalam, A. Ikram, S. Zeeshan, and S. Q. R. Zahidi, "Energy transition towards electric vehicle technology: Recent advancements," *Energy Reports*, vol. 13, pp. 2958–2996, 2025, doi: 10.1016/j.egyr.2025.02.029.

[2] S. Hijgenaar, A. Ștefanov, A. M. van Voorden, and P. Palensky, "Cyber resilience of electric vehicle charging in smart grids: The Dutch case," *IEEE Access*, vol. 13, pp. 111454–111483, 2025, doi: 10.1109/ACCESS.2025.3580856.

[3] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," *IEEE Access*, vol. 8, pp. 214434-214453, 2020, doi: 10.1109/ACCESS.2020.3041074.

[4] H. Das, M. Rahman, S. Li, and C. Tan, "Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review," *Renewable and Sustainable Energy Reviews*, vol. 120, p. 109618, 2020, doi: 10.1016/j.rser.2019.109618.

[5] V. Ş. Ediger and S. Akar, "ARIMA forecasting of primary energy demand by fuel in Turkey," *Energy Policy*, vol. 35, no. 3, pp. 1701–1708, 2007, doi: 10.1016/j.enpol.2006.05.009.

[6] A. Atesongun and M. Gulsen, "A hybrid forecasting structure based on ARIMA and artificial neural network models," *Applied Sciences*, vol. 14, no. 16, p. 7122, 2023, doi: 10.3390/app14167122.

[7] S. Ben Amor and F. Ziel, "Recurrent neural networks with linear structures for electricity price forecasting," *Renewable and Sustainable Energy Reviews*, vol. 231, p. 116773, 2026, doi: 10.1016/j.rser.2026.116773.

[8] R. Shrestha *et al.*, "Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid," *Journal of Parallel and Distributed Computing*, vol. 193, p. 104951, 2024, doi: 10.1016/j.jpdc.2024.104951.

[9] B. Naik *et al.*, "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*, vol. 101, no. 10, pp. 4033–4040, 2023.

[10] J. Yu, Y. Guo, and W. Zhang, "Anomaly detection for charging voltage profiles in battery cells in an energy storage station based on robust principal component analysis," *Applied Sciences*, vol. 14, no. 17, p. 7552, 2024, doi: 10.3390/app14177552.

[11] Q. I. Ali, "Securing solar energy-harvesting roadside unit using an embedded cooperative-hybrid intrusion detection system," *IET Information Security*, vol. 10, no. 6, pp. 386–402, 2016, doi: 10.1049/iet-ifs.2014.0456.

[12] Y. Li, L. Zhang, Z. Lv, and W. Wang, "Detecting Anomalies in Intelligent Vehicle Charging and Station Power Supply Systems With Multi-Head Attention Models," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 1, pp. 555-564, Jan. 2021, doi: 10.1109/TITS.2020.3018259.

[13] B. N. Bhukya *et al.*, "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.

[14] E. Köse and S. K. Kaynar, "Energy demand forecasting and policy development in Turkey," *Energies*, vol. 18, no. 13, p. 3301, 2024, doi: 10.3390/en18133301.

[15] G. P. Zhang, "Time series forecasting using a hybrid ARIMA and neural network model," *Neurocomputing*, vol. 50, pp. 159–175, 2003, doi: 10.1016/S0925-2312(01)00702-0.

[16] A. Hussein and M. Awad, "Time series forecasting of electricity consumption using hybrid RNN and genetic algorithms," *Measurement: Energy*, vol. 2, p. 100004, 2024, doi: 10.1016/j.meaene.2024.100004.

[17] A. Sagheer and M. Kotb, "Time series forecasting of petroleum production using deep LSTM recurrent networks," *Neurocomputing*, vol. 323, pp. 203–213, 2019, doi: 10.1016/j.neucom.2018.09.082.

[18] P. Malhotra *et al.*, "LSTM-based encoder-decoder for multi-sensor anomaly detection," *arXiv preprint*, 2016, doi: 10.48550/arXiv.1607.00148.

[19] H. D. Nguyen, K. P. Tran, S. Thomassey, and M. Hamad, "Forecasting and anomaly detection using LSTM autoencoder," *International Journal of Information Management*, vol. 57, p. 102282, 2021, doi: 10.1016/j.ijinfomgt.2020.102282.

[20] I. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv preprint*, 2014, doi: 10.48550/arXiv.1412.6572.

[21] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Computers & Security*, vol. 112, p. 102511, 2021, doi: 10.1016/j.cose.2021.102511.

[22] S. Hamdare *et al.*, "Cybersecurity Risk Analysis of Electric Vehicles Charging Stations," *Sensors*, vol. 23, no. 15, p. 6716, 2022, doi: 10.3390/s23156716.

[23] S. Acharya, R. Mieth, R. Karri, and Y. Dvorkin, "False data injection attacks on data markets for electric vehicle charging stations," *Advances in Applied Energy*, vol. 7, p. 100098, 2022, doi: 10.1016/j.adapen.2022.100098.

[24] H. Khan *et al.*, "A secure and efficient deep learning-based intrusion detection framework for the internet of vehicles," *Scientific Reports*, vol. 15, p. 12236, 2025, doi: 10.1038/s41598-025-94445-9.

[25] S. L. Qaddoori and Q. I. Ali, "An intelligent anomaly detection system based on smart metering," *IET Wireless Sensor Systems*, vol. 13, no. 2, pp. 75–90, 2023, doi: 10.1049/wss2.12054.

[26] S. Yuan, J. Fu, and X. Ma, "Fairness-Oriented Charging Station Location Optimization Driven by Deep Reinforcement Learning," *IEEE Access*, vol. 13, pp. 125217-125231, 2025, doi: 10.1109/ACCESS.2025.3588880.

[27] M. Sajjad *et al.*, "A Novel CNN-GRU-Based Hybrid Approach for Short-Term Residential Load Forecasting," *IEEE Access*, vol. 8, pp. 143759-143768, 2020, doi: 10.1109/ACCESS.2020.3009537.

[28] M. S. Babu, Y. Tiwari, v. L. Srinivas, and M. Pal, "Regression based anomaly detection in electric vehicle state of charge fluctuations through analysis of EVCI data," *arXiv preprint*, 2024, doi: 10.48550/arXiv.2401.01580.

[29] Z. Wang, C. Song, L. Zhang, Y. Zhao, P. Liu, and D. G. Dorrell, "A Data-Driven Method for Battery Charging Capacity Abnormality Diagnosis in Electric Vehicle Applications," *IEEE Transactions on Transportation Electrification*, vol. 8, no. 1, pp. 990-999, Mar. 2022, doi: 10.1109/TTE.2021.3117841.

[30] V. W. Berger and Y. Zhou, "Kolmogorov–Smirnov test: Overview," *Wiley Statsref: Statistics Reference Online*, 2015, doi: 10.1002/9781118445112.stat06558.

BIOGRAPHIES OF AUTHORS

Dr. Ravindra Babu Jaladanki completed his M.Tech. in Digital Systems and Computer Electronics from J. N. T University, Hyderabad. He obtained Ph.D. from J.N.T.U. Hyderabad, India and a Life member of ISTE. Presently working as Associate Professor in Department of Electronics and Communications Engineering, P.V.P. Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India. He published papers in various national/international journals and conferences. He can be contacted at email: jrb0009@gmail.com.

Pavan Kumar Kolluru pursuing Ph.D. in Computer Science and Engineering from VTU, Belagavi, Karnataka, India. He received his Master's degree M.Tech. in Computer Science and Engineering. Currently working as an Assistant Professor in Department of Computer Science and Engineering at VFSTR University Vadlamudi, India. He has 13 plus years of teaching and 6 years of research experience. His current research interest includes machine learning, computer networks, and cyber security. He can be contacted at email: kpkvignan@gmail.com.

Nagul Shaik obtained his Ph.D. in Computer Science and Engineering from Krishna University, India. He received his Master's degree in Computer Science and Engineering. He is an Assistant Professor in Department of Computer Science and Engineering at GITAM University Visakhapatnam, India. His current research interest includes machine learning, artificial intelligence, software engineering, data engineering, and quality assurance. He can be contacted at email: nagulcse@gmail.com.

Kamparapu V V Satya Trinadh Naidu is currently working as Assistant Professor in Department of Computer Science and Information Technology, SRKR Engineering College, Bhimavaram - 534204, Andhra Pradesh, India. He has 3 years of teaching experience in engineering education. He received his M.Tech. in 2019 from Pragati Engineering College affiliated to JNTUK, Surampalem. His research interests include machine learning, deep learning, and cloud computing. He can be contacted at email: k.trinadh1269@gmail.com.

Dr. Duggineni Veeraiah currently working as Professor in the Department of Computer Science and Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, Andhra Pradesh, India. His research interests include data science, machine learning, and security. He can be contacted at email: veeraiahdvc@gmail.com.

Dr. Anita Pradhan Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh-522502, India. She can be contacted at email: anita.pradhan15@gmail.com.

Mr. Rallabandi Ch. S. N. P. Sairam currently working as an Assistant Professor in the Department of Computer Science and Engineering (Data Science), R.V.R. and J.C. College of Engineering, Guntur, Andhra Pradesh, India. He received the B.Tech. degree in Computer Science and Engineering from Vasireddy Venkatadri Institute of Technology, in 2018. M.Tech. degree in Computer Science was obtained from RVR and JC College of Engineering, in 2020. His research interests include machine learning, deep learning, and cybersecurity applications in smart energy systems. He can be contacted at email: sairam.mtech20@gmail.com.