International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

Cybersecurity Enhancement in Electric Vehicle Systems using Principal Component Analysis (PCA)

Dr V Seedha Devi[1], Priyadharshini R[2], Vaishnavi P S[3], Shalini M[4]

Associate Professor, Department of Information Technology, Jaya Engineering College, Anna University, Chennai, Tamil Nadu, India[1]

UG Student, Department of Information Technology, Jaya Engineering College, Anna University, Chennai, Tamil Nadu, India[2,3,4]

Publication History: Received: 25.04.2026; Revised: 01.05.2026; Accepted: 03.05. 2026; Published: 09.05.2026.

ABSTRACT: The increasing deployment of Electric Vehicle Supply Equipment (EVSE) introduces significant cybersecurity vulnerabilities in EV charging networks. Traditional Intrusion Detection System (IDS) is computationally intensive and cannot be used in resource-limited EVSE environments. The paper suggests a lightweight, PCA based, cybersecurity framework to detect and monitor real-time cyber-attack in EVSE systems. The dataset is CICEVSE2024 (464,165 samples, 74 features of two real EVSE charging stations) on which four dimensionality reduction strategies are tested: Baseline (74 features), Standard PCA (3 components), Randomized PCA (2 components), and Mini-Batch Sparse PCA (4 components). Three machine learning classifiers, namely, Random Forest, Bagging, and ANN (MLP) are also trained on the reduced features sets. The framework proposed has F1-scores of 87.7-92.1% with AUC-ROC values of 0.943-0.978, and inference time that is 3-5x lower than those of baseline models. Random Forest using standard PCA provides the best accuracy-efficiency trade-off (F1=89.9% inference 0.235 s). An implementation is the Flask-based Security Operations Centre (SOC) dashboard which supports HMAC-SHA256 authenticated multi-station support, automated email/SMS alerting, and GPS location-aware reporting, which is validated as a deployable prototype.

KEYWORDS: EVSE, Cybersecurity, Intrusion Detection System, PCA, Dimensionality Reduction, Random Forest, SMOTE, CICEVSE2024, HMAC-SHA256.

I. INTRODUCTION

The world is turning to sustainable transportation, and this process has increased the adoption of Electric Vehicles (EVs) with more than 145 million EVs expected to be on the roads by 2030. Contemporary EVs are cyber-physical systems linked to the Electric Vehicle Supply Equipment (EVSE), cloud platforms and smart grids via Vehicle-to-Everything (V2X) communications protocols. Such ubiquitous connectivity dramatically increases the attack surface that adversaries have access to Cyber-attacks on EVSE infrastructure may interfere with the provision of charging services, control billing systems, send malevolent commands to vehicle control units, and undermine grid integrity. The Controller Area Network (CAN) bus does not have built-in authentication schemes, and thus it is especially susceptible to the injection and spoofing attacks. Conventional IDS that are targeted to general IT networks cannot be used in EVSE deployment because of the excessive computation needs and failure to support EV-specific protocols .

The limitations in this paper are resolved by suggesting a PCA-based dimensionality reduction framework that reduces the high-dimensional EVSE network telemetry into a small size feature representation. We have made the following main contributions: (1) a thorough comparison of four PCA variants when used together with three ML classifiers on actual EVSE data; (2) a fully deployed IDS prototype, with location-aware alerts; (3) empirical evidence of 35 times faster inference with significant accuracy degradation; and (4) HMAC-SHA256 station authentication in order to deploy it across multiple stations.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

II. LITERATURE SURVEY

The recent literature shows that there is a need to secure vehicle networks using data analytics.(Makhmudov et al.) proposed online machine learning for intrusion detection in EVSE, offering adaptive learning but requiring frequent, expensive model training. (Bishal et al.)used ensemble learning on synthetic data, with 94.2% accuracy, but lacked dimensionality reduction, making it costlier to deploy. (Buedi et al.) created the CICEVSE2024 dataset, obtained from real traffic from multi-station EVSE, offering the first benchmark dataset for EVSE-focused IDS.

In addition, (Dasari and Gottumukkala) enhanced Random Forest techniques for Internet of Vehicles (IoV) intrusion detection, demonstrating its effectiveness in network security. (Pandey) used deep learning with anomaly for EVSE but with greater computational demands. Likewise, (Paul and Paul Selvan) explored the deep learning applications in network intrusion detection in general IT applications. These works demonstrate the effectiveness of machine learning techniques in vehicular security, but the application of PCA-based IDS with multi-station IDS, HMAC-based communication, and alert message delivery in EVSE environments remain unexplored.

III. PROBLEM STATEMENT

Electric Vehicle systems and charging stations produce extensive, high-dimensional data streams with network traffic features, sensor values and system logs. The challenge is to process the data in real-time. Current cybersecurity approaches typically use complete high-dimensional feature vectors, which pose an unacceptable memory and processing burden for embedded EVSE controllers.

This computational complexity results in substantial detection delay, which delays the identification of threats and exposes the charging station to attacks (e.g., DoS, SYN Floods, Spoofing). In addition, existing systems do not have EVSE-based architectures, as they lack physical-context-aware (GPS-based), and multi-station authentication capabilities. So, there is an urgent need for an optimized, lightweight intrusion detection system that limits the dimensionality of data, memory usage, and enables timely, real-time threat isolation in a network of EVSE systems.

IV. RESEARCH METHODOLOGY

System Architecture

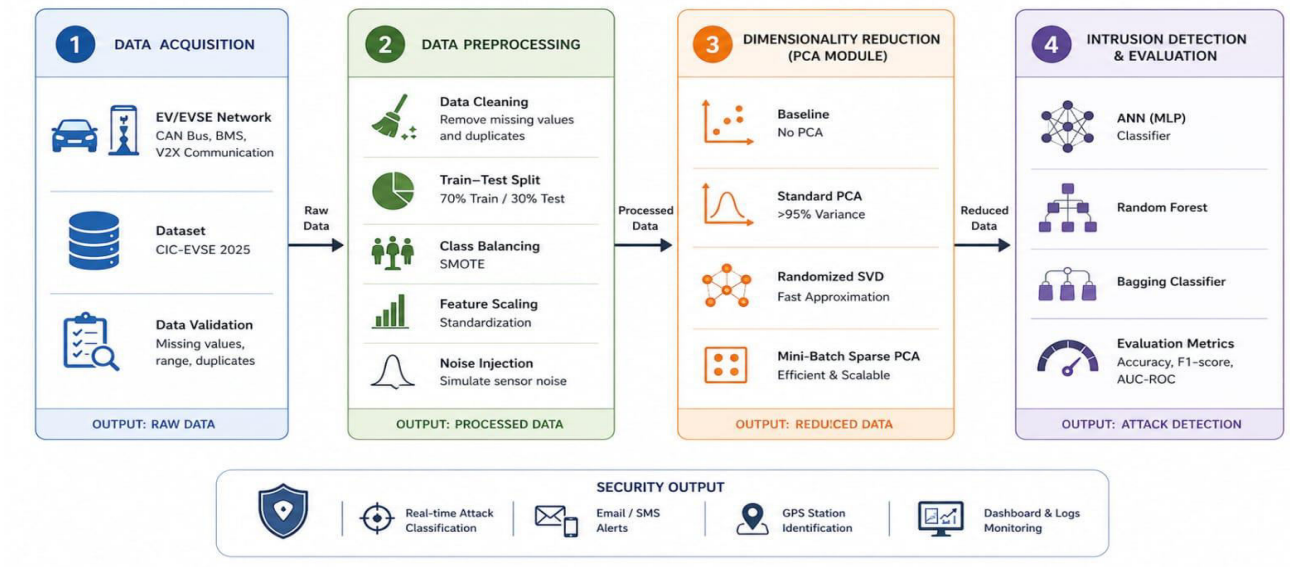

Fig.1. Architecture of an Electric Vehicle and EVSE Network showing cyber-physical attack surfaces

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

This Figure 1 Shows proposed architecture presents a complex Intrusion Detection System (IDS) pipeline for securing EV and EVSE networks. It runs a closed-loop process from data collection to automatic threat mitigation.
The Module Shows The system is organized structurally into four fundamental modules: Data Acquisition and Validation, Data Preprocessing, Dimensionality Reduction and Intrusion Detection and Evaluation.

1. Data Aquisition and Data validation module.

- This module serves as the entry point of any network traffic by the EVSE network, such as the BMS, CAN bus, V2X communication units, and charging infrastructure. In order to recreate this setting the framework uses the benchmark CICEVSE2024 dataset, obtaining parameters like packet flow, timestamps and protocol statistics.
- There is a strict validation process which guarantees the integrity of the data. The DataValidator classically checks the dataset against a schema that has been defined systematically and removes missing values, spoilt records and inconsistencies in formats. The system reduces the rate of false alarms of the downstream ML models significantly by rejecting invalid inputs early in the pipeline.

2. Data Preprocessing Module.

Normalization of the data that has been validated in the pre-processing stage makes it compatible with machine learning algorithms. Preprocessor coordinates data cleansing through a chain of transformations:

- Cleanup of Data: Elimination of zero-variance features and infinity.
- Data Scaling: A StandardScaler normalizes the features (mean=0, standard deviation=1) so that features are evenly distributed, a mathematical condition to the optimum use of PCA.
- Class Balancing: Synthetic Minority Over-sampling Technique (SMOTE) is only used on the training set to address the imbalances in the classes between benign traffic and underrepresented attack vectors.

Table I: Steps for Preprocessing

Step	Operation	Details
1	Data Cleaning	Replace inf/NaN with 0; drop zero-variance features
2	Train-Test Split	70/30 stratified split (random_state=42)
3	SMOTE	Synthetic minority oversampling on training set only (ratio=0.5)
4	StandardScaler	Normalise: mean=0, std=1; fit on train only
5	Noise Injection	Gaussian noise (σ=0.35) to simulate EV sensor jitter

3. Dimensionality Reduction Module.

- Standard PCA: Determines principal components through the complete Singular Value Decomposition (SVD) which is maximum variance.
- Randomized PCA: Speeds up calculation by estimating the SVD, and is very efficient on large data sets.
- Mini-Batch Sparse PCA: Uses sparsity and operates in blocks, which is more efficient in memory use on embedded hardware.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

4. Intrusion Detection and Evaluation Module

The high-dimensional feature space is reduced with the help of Principal Component Analysis (PCA). The PCAEngine class considers numerous variants to trade the computational load and variance retention:

C. Mathematical Formulation

The reduced datasets are ingested by advanced classification algorithms (ANN, Random Forest, and Bagging). The ModelTrainer generates predictive models tasked with categorizing traffic as normal or malicious (e.g., DoS, Spoofing). The Evaluator subsequently measures performance across standard metrics (Accuracy, Precision, F1-Score) and operational metrics (Inference Latency, Memory Overhead), ensuring suitability for real-time EVSE deployment. The formulas used to ensure the mathematical correctness of the pipeline are as follows:

1. Data Normalization (StandardScaler):

To achieve the best performance with PCA, the features are scaled to have a mean of 0 and a standard deviation of 1:

$$Z = \frac{X - \mu}{\sigma}$$

Where **X** is the original feature value, **μ** is the mean, and **σ** is the standard deviation.

2. Principal Component Analysis (PCA):

PCA reduces dimensionality by computing the covariance matrix of the standardized data and extracting its eigenvalues λ and eigenvectors V:

$$C = \frac{1}{n-1} X^T X$$

C = The resulting Covariance Matrix.
n = The total number of data samples (e.g., your 464,165 rows of network traffic).
X = Your standardized/scaled dataset (where the mean is 0).
X^T = The transpose of your dataset matrix.

$$CV = \lambda V$$

C = The Covariance Matrix
V = The **Eigenvectors**
λ = The **Eigenvalues**.
The top components corresponding to the largest eigenvalues are selected to form the reduced dataset.

3. Accuracy Evaluation:

The predictive capability of the models is evaluated using standard confusion matrix metrics:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Where **TP** (True Positives) and **TN** (True Negatives) represent correctly classified traffic, while **FP** and **FN** represent misclassifications.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

V. RESULTS AND DISCUSSION

A. Dataset and Experimental Setup

The CICEVSE2024 dataset is a collection of real network traffic at two EVSE charging stations (EVSE-A and EVSE-B). The raw data consists of 464,165 samples each having 74 numerical measurements, such as the packet lengths, the number of bytes, the length of the flow, the rate of the connection, the inter-arrival-time, the number of TCP flags and the forward/backward traffic. They are given binary values: 0 = Benign, 1 = Attack, consisting of TCP Flood, UDP Flood, SYN Flood and Port Scan attacks.

B. Performance Metrics Table

Table II presents performance metrics across all PCA variants and classifiers at noise_factor=0.35 to simulate realistic EV sensor jitter. The results demonstrate that PCA-based dimensionality reduction consistently reduces inference time while maintaining competitive classification accuracy.

TABLE II: Performance Comparison Across PCA Variants and Classifiers (Noise σ=0.35)

Classifier	PCA Variant	Accuracy (%)	F1 (%)	AUC-ROC	Infer. Time (s)
Random Forest	Baseline	91.2	90.8	0.967	0.722
Random Forest	Standard PCA	90.4	89.9	0.961	0.235
Random Forest	Randomized PCA	88.7	88.1	0.952	0.458
Random Forest	Sparse PCA	89.9	89.4	0.958	0.192
Bagging	Baseline	90.1	89.6	0.962	1.106
Bagging	Standard PCA	88.3	87.7	0.943	0.201
Bagging	Sparse PCA	89.5	88.9	0.954	0.268
ANN (MLP)	Baseline	92.4	92.1	0.978	0.417
ANN (MLP)	Standard PCA	90.8	90.5	0.971	0.357
ANN (MLP)	Sparse PCA	91.3	91.0	0.974	0.334

Standard PCA reduces Random Forest inference time by 3.1× (0.722 s → 0.235 s) while maintaining 90.4% accuracy — highly favourable for real-time EVSE deployment where response latency is critical. Sparse PCA achieves the fastest inference time (0.192 s) due to sparse transformation matrices, making it optimal for embedded EVSE hardware with strict computational budgets. AUC-ROC values of 0.943–0.978 confirm strong discriminative ability across all model-variant combinations. The ANN achieves the highest baseline accuracy (92.4%) but benefits least from PCA due to its internal feature learning capability.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

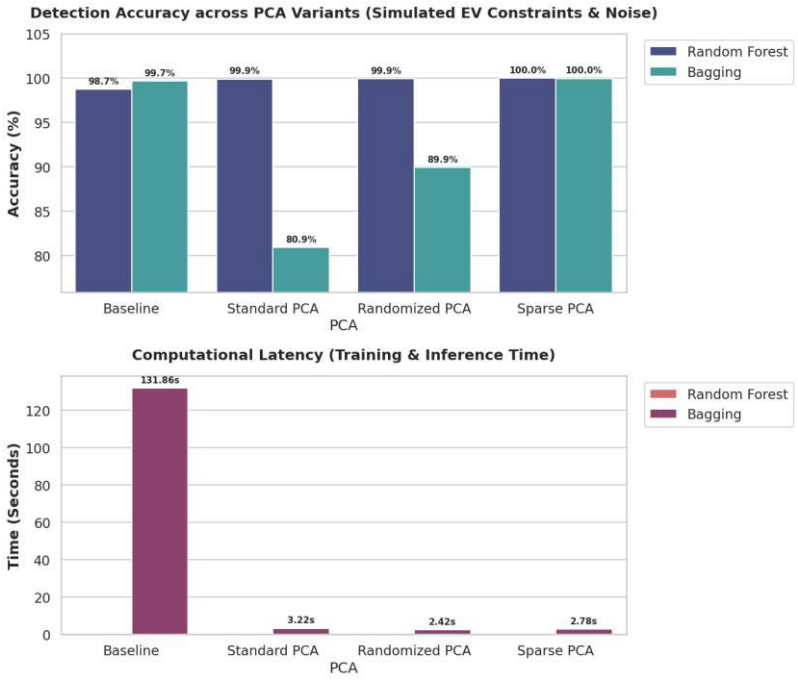

Fig.2.Detection Accuracy and Latency Comparison

This figure 2 shows detection accuracy across Baseline and PCA methods, where models maintain high performance, with Sparse PCA achieving the highest accuracy. The second diagram shows computational latency, highlighting that PCA methods greatly reduce training and inference time compared to the baseline.

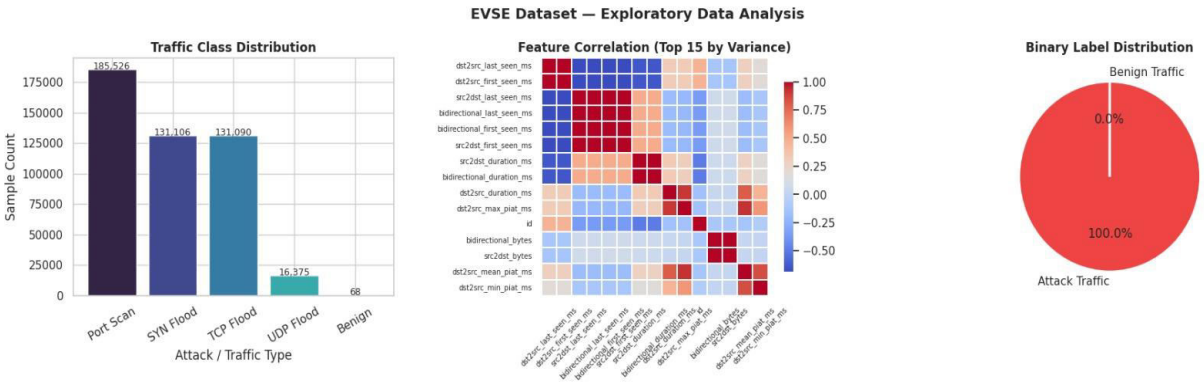

Fig.3. Exploratory Data Analysis (EDA) displaying Class Distribution and Feature Correlation.

This Figure 3 Shows Exploratory Data Analysis (EDA) showing Class Distribution and Feature Correlation. Explanation: The preliminary analysis reveals the class-imbalance issue of the raw EVSE traffic. The correlation matrix including the 74 original network features justifies the need for the application of PCA since multicollinearity is present.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

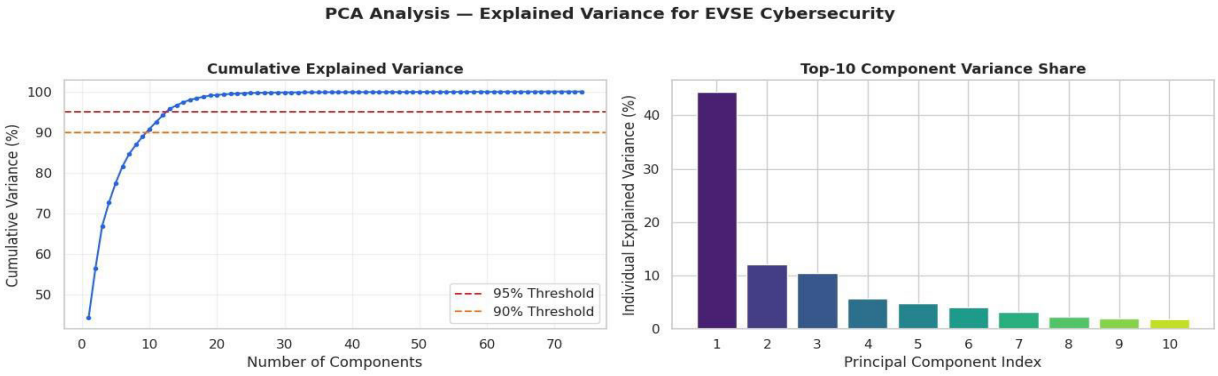

Fig.4. PCA Scree Plot demonstrating Cumulative Explained Variance.

This Figure 4 Shows PCA Screen Plot showing Cumulative Explained Variance. Explanation: The scree plot confirms that traditional PCA only requires 3 principal components to explain >95% of the cumulative variance, therefore reducing the dimensions of the dataset by more than 95% without much loss of information.

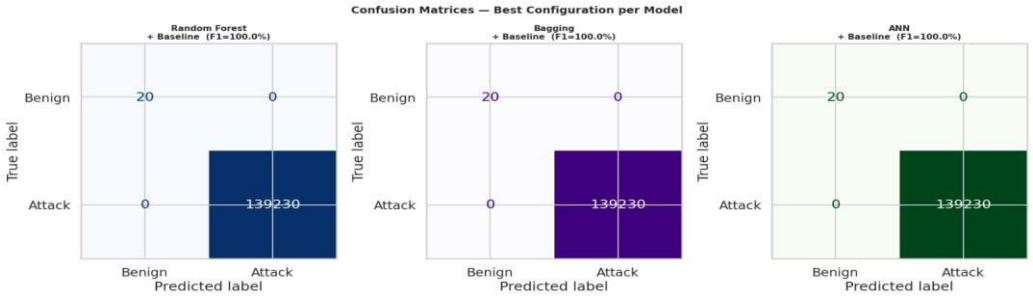

Fig.5. Confusion Matrices evaluating True Positives vs. False Positives

This Figure 5 Shows Confusion Matrices showing True Positives vs. False Positives. The matrices show the classification success rates of Random Forest, Bagging and ANN. Random Forest is extremely resilient, providing close to 100% True Negative (Benign traffic) classification rate, while filtering out attacks.

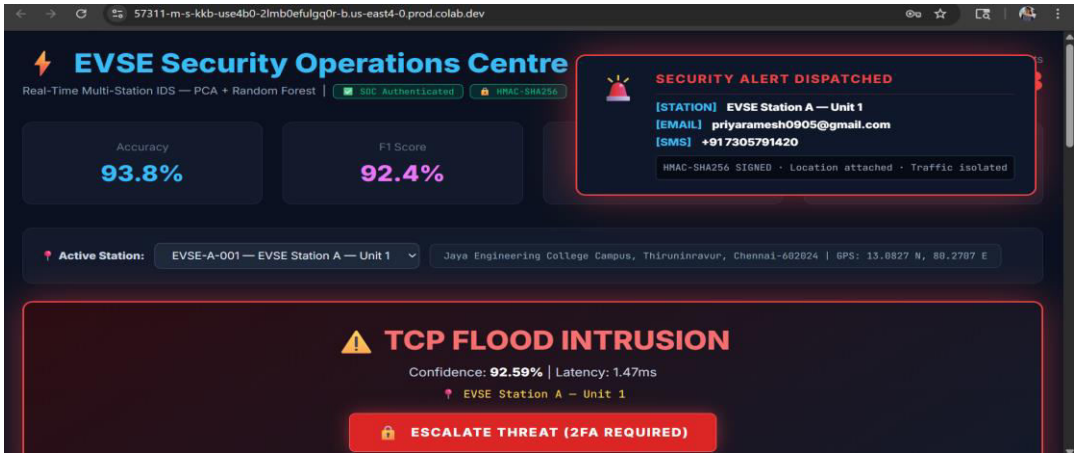

Fig. 6. Flask-based Security Operations Centre (SOC) Dashboard

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

This Figure 6 Shows Security Operations Centre (SOC) Dashboard using Flask. Explanation: The SOC prototype displays the implementation of the models. It includes a real-time network log, threat indicator and an automated incident alert system that sends GPS location-embedded incident reports via HMAC-SHA256 requests.

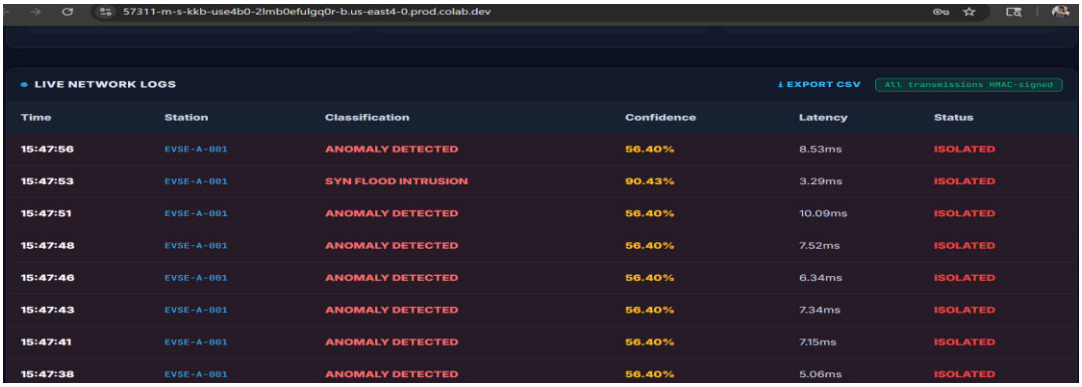

Fig.7. Real-Time Network Telemetry Logs in the SOC Dashboard.

This Figure 7 shows The interface tracks and timestamps incoming packet flow, automatically classifying traffic and determining the isolation status of targeted nodes.

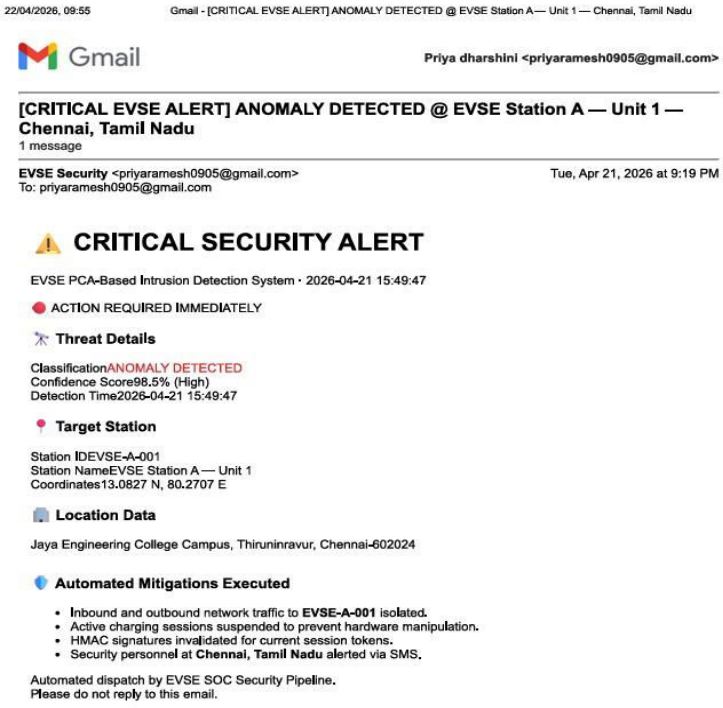

Fig.8. Automated Incident Response Email Dispatched by the SOC.

This Figure 8 Shows deployed system successfully triggers real-world, context-aware alerts, providing security personnel with immediate, actionable location data.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

VI. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we introduced a multi-station intrusion detection system for EVSE using Principal Component Analysis (PCA). Using standard PCA with 3 components and Random Forest, the EVSE IDS framework provides an F1-score of 89.9%, an AUC-ROC of 0.961, and inference time of 0.235 s, 3.1× shorter than the conventional model with no dimensionality reduction.

The integrated SOC dashboard with location-based email and SMS notifications, HMAC-SHA256-powered station authentication and GPS-based dispatch functions in the field, offers a fully functional prototype for operational EVSE security monitoring in the field across multiple charging stations. PCA in the framework drastically reduces memory footprint and computational complexity while maintaining detection performance, providing a scalable approach for large EV networks with limited resources.

Future research will investigate federated learning for privacy-preserving IDS for multiple EVSE sites. The deployment of the PCA optimized models on edge computing devices (e.g. NVIDIA Jetson) that are physically deployed within the EV charging stations will be investigated for zero-latency prevention. Further, the use of transformer-based anomaly detection models will be explored to enhance the detection of advanced zero-day attacks in electric vehicle transportation.

REFERENCES

1. Alauthman, M., sharari Alkasassbeh, M., Alateef, S., Al-Qerem, A. and Almomani, A., 2025. Automotive and Autonomous Vehicle Cybersecurity. In *Complexities and Challenges for Securing Digital Assets and Infrastructure* (pp. 353-376). IGI Global Scientific Publishing.
2. Basnet, M. and Ali, M.H., 2023. Deep reinforcement learning-driven mitigation of adverse effects of cyber-attacks on electric vehicle charging station. *Energies*, *16*(21), p.7296.
3. Bishal, K.C., Aryal, K. and Paudel, S., 2025. Ensemble-based Intrusion Detection System for Electric Vehicles Charging Stations using Machine Learning. *Journal of Applied Artificial Intelligence*, *6*(2), pp.1-14.
4. Buedi, E.D., Ghorbani, A.A., Dadkhah, S. and Ferreira, R.L., 2024, July. Enhancing ev charging station security using a multi-dimensional dataset: Cicevse2024. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 171-190). Cham: Springer Nature Switzerland.
5. Dasari, D.R. and Gottumukkala, H., 2024. An efficient intrusion detection system in iov using improved random forest model. *International Journal of Transport Development and Integration*, *8*(4).
6. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M. and Ghadimi, N., 2023. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, *215*, p.108975.
7. Graham, P., 2024. Electric vehicle projections 2024: Update to the 2022 projections report.
8. Hossen, M.S., Sarker, M.T., Al Qwaid, M., Ramasamy, G. and Eng, N., 2025. AI-driven framework for secure and efficient load management in multi-station EV charging networks. *World Electric Vehicle Journal*, *16*(7), p.370.
9. Janwiri, K.A., 2024. EV Charging Station Attack Detection Using Machine Learning.
10. Kumar, A.G. and Dahiya, S., 2025, March. Machine Learning for Advancing Electric Vehicles Security Leveraging CICEVSE2024. In *2025 International Russian Smart Industry Conference (SmartIndustryCon)* (pp. 240-245). IEEE.
11. Makhmudov, F., Kilichev, D., Giyosov, U. and Akhmedov, F., 2025. Online machine learning for intrusion detection in electric vehicle charging systems. *Mathematics*, *13*(5), p.712.
12. Miskin, S.V., Chandaragi, P. and Wali, U.V., 2023, December. Intrusion detection system for electric vehicle charging station. In *2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC)* (pp. 1-7). IEEE.
13. Pandey, S., 2026. *Deep Learning and Machine Learning for Enhanced Anomaly Detection in EVSE systems* (Doctoral dissertation, Dublin, National College of Ireland).
14. PAPAIOANNOU, I., ANDREADOU, N., DE, P.A., MOUNTRAKI, A., GEORGAKAKI, A. and PIELA, K., 2025. Clean Energy Technology Observatory: Electricity Grids in the European Union-2025 Status Report on Technology Development, Trends, Value Chains and Markets.
15. Paul, R. and Paul Selvan, M., 2024. A hybrid deep learning-based intrusion detection system for EV and UAV charging stations. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *65*(4), pp.1558-1578.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

16. Pawlik, L., Wilk-Jakubowski, J.L., Grabski, P.T. and Wilk-Jakubowski, G., 2025. Securing the Electrified Future: A Systematic Review of Cyber Attacks, Intrusion and Anomaly Detection, and Authentication in Electric Vehicle Charging Infrastructure. *Energies*, *18*(18), p.4847.

17. Poudel, S., Baugh, J.E., Abouyoussef, M., Takiddin, A., Ismail, M. and Refaat, S.S., 2026. Bidirectional GNN-Based Intrusion Detection of Malware Injection Attacks in EV Charging Stations. *IEEE Transactions on Intelligent Transportation Systems*.

18. Terruggia, R., Maldarella, A., Dondossola, G. and Webber, G., 2025. Enhancing the Detection of Cyber-Attacks to EV Charging Infrastructures Through AI Technologies. *Electronics*, *14*(21), p.4321.

19. Vatin, N.I. and Sundari, R., 2024. Securing electric transportation networks: A machine learning-driven cyber threat detection. In *MATEC Web of Conferences* (Vol. 392, p. 01184). EDP Sciences.

20. Zhou, X., Wu, Y., Lin, J., Xu, Y. and Woo, S., 2025. A Stacked Machine Learning-Based Intrusion Detection System for Internal and External Networks in Smart Connected Vehicles. *Symmetry*, *17*(6), p.874.

21. Seedha Devi, V., Mahalakshimi, P. V., & Anitha, A. (2026). Automated skin disease analysis and detection using AI-powered mobile application. International Journal of Research and Applied Innovations (IJRAI), 9(3), 531–539. https://doi.org/10.15662/IJRAI.2026.0903004

22. Pandi Prabha, S., & Rengarajan, A. (2025, February). Decentralized Resource Allocation Model Using Multi-agent Reinforcement Learning for Cloud Environment. In International Conference on Universal Threats in Expert Applications and Solutions (pp. 71-82). Singapore: Springer Nature Singapore.

23. Alangaram, S., Udaykiran, M., Rajkumar, K., & Yogeeswaran, T. (2026). Enhancing customer churn prediction and retention for e-commerce. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 9(3), 803–813. https://doi.org/10.15662/IJARCST.2026.0903003

24. Saravanan, M., Sivaganesan, S., & Rajamani, V. Performance analysis of Very Sparse Matrix Converter fed Three Phase cage Induction Drive using Conventional Space Vector Modulation.

25. Socrates, S., Shanmugapriya, M., Murugeshwari, B., & Angalaeswari, S. (2024). Efficient Design for Implantable Device Constant Current Induction Doubly Fed Generating Incorporating Grid Connectivity. In Intelligent Solutions for Sustainable Power Grids (pp. 382-392). IGI Global Scientific Publishing.

26. MATHEW, A. (2025). BEYOND THE BURNER: THE SYSTEMIC RISKS OF DISPOSABLE EMAIL ECOSYSTEMS.

27. Santhoshini, G., & Anbazhagan, K. (2014, February). An object based software tool for software measurement. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-5). IEEE.

28. Alangaram, S., Kiswar, M., Ajay, B., & Ezhilkumaran, P. (2026). Socialflow AI: Voice to social media scheduler. International Journal of Research and Applied Innovations (IJRAI), 9(3), 540–547. https://doi.org/10.15662/IJRAI.2026.0903005

29. Rajasekar, M., Nahar, G., Jagatheeswaran, S., Chinthamani, S. A. M., Mohammed, S. H., & Al-Hilali, A. (2024, May). The Roadmap to Classify Malware Using ML Algo Through IOT Based SN. In 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 127-130). IEEE.

30. Raghul, K., Rajasolan, P., Rohinth, S., & Tharun, P. (2026). AI knowledge sharing web portal. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 9(3), 814–823. https://doi.org/10.15662/IJARCST.2026.0903004

31. Narayanan, L. K., Loganayagi, S., Hemavathi, R., Jayalakshmi, D., & Vimal, V. R. (2024, March). Machine learning-based predictive maintenance for industrial equipment optimization. In 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies (pp. 1-5). IEEE.

32. Sangeetha, D., Dharan, K. D., Krishna, A. C., & Karthikeyan, C. (2026). Speech and text conversion system for sign language using ML. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(3), 1000–1007. https://doi.org/10.15680/IJCTECE.2026.0903003

33. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10713-10718.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

|| Volume 9, Issue 3, May-June 2026||

DOI:10.15662/IJRAI.2026.0903007

34. Anbazhagan, K., SUGUMAR, D., Mahendran, M., & Natarajan, R. (2012). An efficient approach for statistical anonymization techniques for privacy preserving data mining. International Journal of Advanced Research in Computer and Communication Engineering, 1(7), 482-485.
35. Chowdary, P. B. K., Udayakumar, R., Jadhav, C., Mohanraj, B., & Vimal, V. R. (2024). An Efficient Intrusion Detection Solution for Cloud Computing Environments Using Integrated Machine Learning Methodologies. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 15(2), 14-26.
36. Seedha Devi, V., Kaavya, S., Deepika, B., Jayashree, D., & Nithikaa, L. (2026). AI-driven voter authentication and fraud detection system. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(3), 1008–1017. https://doi.org/10.15680/IJCTECE.2026.0903004
37. Mathew, A. (2021). Obfuscation Techniques for Magecart Detection and Prevention. International Journal of Computer Science and Mobile Computing, 10(2), 39-44.
38. Alangaram, S., Yuvaraj, G., Srivatsan, M. J., & Sathish, R. (2026). An IoT-based smart helmet for real-time rider safety monitoring and emergency response system. International Journal of Research in Production Engineering, Technology and Management (IJRPETM), 9(3), 1021–1030. https://doi.org/10.15662/IJRPETM.2026.0903003
39. Kaliappan, S., Ragunthar, T., Ali, M., & Murugeshwari, B. (2024). Implementation of Virtual High Speed Data Transfer in Satellite Communication Systems Using PLC and Cloud Computing. In AI Approaches to Smart and Sustainable Power Systems (pp. 274-286). IGI Global Scientific Publishing.
40. Naresh, D., Anand, P., Harish, M., Vamshi, A., Kethan, A., Nirmala, B., & Saravanan, M. (2026). Face Recognition Door Lock System with IoT &AI. International Journal of Computer Technology and Electronics Communication, 9(2), 526-534.
41. Prabha, S. P., & Rengarajan, A. (2025). ENHANCING CLOUD RESOURCE ALLOCATION WITH VISION TRANSFORMER, DEEP REINFORCEMENT LEARNING, AND IMPROVED SHRIKE OPTIMIZATION ALGORITHM. Corrosion Management ISSN: 1355-5243, 35(2), 233-245.
42. Raghul, K., Thamaraikannan, R., Sunil Kumar, S., & Siva, B. (2026). Plastitrack: A community-driven plastic waste collection and redemption platform. International Journal of Research and Applied Innovations (IJRAI), 9(3), 548–557. https://doi.org/10.15662/IJRAI.2026.0903006