Project Proposal

Area: Intrusion Detection in Cyber-Physical Systems

1. Title of the Proposal:

Enhancing Electric Vehicle Security: AI-Powered Detection and Prevention of Cyber Attacks

2. Name of PI and Co-PI and their affiliations:

Name of PI:

Dr. Amit Kumar
Assistant Professor,
Department of Electrical and Instrumentation Engineering [DEIE]
Thapar Institute of Engineering and Technology Patiala, Punjab India
Email ID: amit.kumar2@thapar.edu
Contact No.: 91-7978607568

Name of Co-PIs:

Co-PI 1: Dr. Ashima Anand
Assistant Professor
Department of Computer Science and Engineering [DCSE]
Thapar Institute of Engineering and Technology Patiala, Punjab India
Email ID: ashima.anand@thapar.edu
Contact No.: 91-7018111179

Co-PI 2: Dr. Prashant Singh Rana
Associate Professor
Department of Computer Science and Engineering [DCSE]
Thapar Institute of Engineering and Technology Patiala, Punjab India
Email ID: prashant.singh@thapar.edu
Contact No.: 91-9313889932

Co-PI 3: Dr. Mukesh Singh
Professor
Department of Electrical and Instrumentation Engineering [DEIE]
Thapar Institute of Engineering and Technology Patiala, Punjab India
Email ID: mukesh.singh@thapar.edu
Contact No.:91-9970633998

Industry Collaborator:

Silov Solutions Pvt. Ltd

TBIU, 2nd floor, Synergy Building, IIT Delhi, Hauz Khas New Delhi-110016

Email: silov.solutions@gmail.com

Contact no: 91-9810429715

3. Type of Proposal: 3 Years

4. Budget Total: INR 39.793 Lakhs

5. Proposal Detail (within 8 pages):

(i) Origin of the Problem

The rise of the Internet of Things (IoT) has opened the door to more intelligent and ultimately more efficient cyber-physical systems. A notable example is the incorporation of motor drives into computer networks for the control of industrial processes. Despite the evident benefits brought by IoT applications, power electronics systems are becoming increasingly susceptible to cyber-attacks. This vulnerability is particularly notable in power electronics systems utilized in IoT applications, such as Electric Vehicles (EVs) equipped with one or more electric drive systems (EDSs). Typically, the EDS is linked to the in-vehicle Controller Area Network (CAN). The connectivity level in connected cars exceeds that of traditional vehicles, creating a larger attack surface and enabling remote access for potential attackers [1]–[5].

The repercussions of cyber-attacks on a vehicle can extend beyond the targeted vehicle itself, as exemplified by the 2015 recall issued by Chrysler for 1.4 million vehicles due to the remote hacking and halting of a Jeep Cherokee on a highway [6]. Incidents have also been reported involving the hacking and disabling of electric car charging stations outside Moscow, where EV owners were unable to charge their vehicles, and station displays were manipulated for political messaging. Similarly, in the UK, certain chargers were compromised to display inappropriate content. In response, the UK is actively developing a new policy and technical framework to not only reduce energy bills for users but also enhance the overall cybersecurity of EV ecosystems [7]. The integration of IoT and connectivity in the in-vehicle network has brought cybersecurity concerns to every component of EVs, covering battery management, motor drives, braking, and steering. In a study [8] focused on the cybersecurity aspects of EV battery systems, an analytical framework for standards analysis and comparison is presented. This framework identifies key players in in-vehicle cybersecurity, assessing potential cyber threats to battery lifetime [9], [10]. Similarly, when examining the cybersecurity vulnerabilities of the inter-vehicle network in EVs, it is evident that cyber-attacks on electric drives can significantly impact motor current signatures, leading to performance degradation [11],[12]. Addressing the broader issue of cybersecurity in power electronic systems, a study [1] has highlighted the potential challenges associated with IoT-controlled power electronic systems. The authors advocate for hardware- and software-based intrusion detection, leveraging the physical layer as a preferred cybersecurity solution. Information security measures, such as secure hardware, communication techniques, firewalls, and secure software updates, are crucial for preventing malicious attacks [13]. Simultaneously, the emphasis on software-based intrusion detection is pronounced, aiming to design a reliable real-time monitoring system, especially for cyber-physical power systems [14]-[16]. Recognizing the cybersecurity challenges prevalent in the automotive industry, concerted efforts have been made to establish security standards. These include initiatives like the SAE J3061 [17], ISO 26262, and the committee draft of the "ISO-SAE Road Vehicles - Cybersecurity Engineering" standard [18]. Within academia, numerous research works have addressed the diverse threats, mitigation strategies, and potential countermeasures for vehicles in recent years [10], [11]. Furthermore, due to the limited research on the network and operating system security of EVs, the incidents reported in the literature above cannot be overlooked and may lead to more critical issues as more EVs become connected. In this proposal, this problem is regarded as a challenge, and an attempt will be made to provide a deployable solution.

(ii) Exact formulation of the problem in scientific terms

The integration of the IoT in power electronics systems, particularly EVs, presents significant cybersecurity challenges. The in-vehicle CAN exposes EVs to an expanded attack surface which includes current and torque sensors, position encoders, and PWM signals, allowing remote access for malicious entities. This extends cybersecurity concerns to critical components like battery management, motor drives, braking, and steering. Researchers have made efforts to develop AI-based cyber-attack detection systems for EVs. Despite this, several gaps still exist in the current solutions. The primary focus of existing research is on monitoring the CAN bus, disregarding the importance of comprehensive monitoring across multiple interfaces, including the Operating System and Network. Moreover, the restricted range of

datasets used for training and testing poses a significant lag, as they fail to accurately reflect the diverse real-world situations encountered by EVs. The use of standardized datasets is crucial in improving the resilience of ML models. Additionally, there is a lack of scalability and real-time implementation in current methods, which hinders their effectiveness in handling diverse real-world scenarios. Another challenge is adapting to dynamic environments, as existing approaches struggle to keep up with the constantly changing conditions. It is crucial to give utmost importance to researching all-inclusive cybersecurity solutions for EVs. Also, attention needs to be paid to the diversity of datasets, implementing ML-based anomaly detection, and conducting real-time analysis. It is necessary to carry out rigorous real-world testing to fortify resilience against constantly evolving cyber threats.

(iii) Significance of solving the problem in the current context

There are a few global organizations/ institutions that are dealing with the improvement of dependable, productive, and secure control for EVs. A few top-notch research in the domain of EV are outlined here:

- **National Renewable Energy Laboratory (NREL):** NREL has developed a co-simulation platform for conducting a cyber vulnerability analysis of EV charging infrastructure, assessing its interdependencies with communication and control systems [19].
- **Tesla:** Tesla a leading EV manufacturing company reported a case in March 2019, in which Tesla's autopilot system faced an attack by hackers from Tencent Keen Security Lab, resulting in the manipulation of the electric drive systems that power the vehicle There is a genuine concern that manufacturers could potentially insert Trojans or malware into controllers, leading to data integrity attacks. After, the incident Tesla's attention is more focused on the cyber security aspect in the OS of EVs [20].
- **Sandia National Laboratories, New Mexico (SNL):** Pacific Northwest National Laboratory, and Argonne National Laboratory have done cumulative exercises with SNL on cybersecurity for EV charging infrastructure and the report was framed based on their investigations. This research focuses on and emphasizes cyber security with charging systems [21].
- **Jio-BP:** Jio-BP, a leading provider of EV charging and battery swapping networks in India, recognizes the susceptibility of EV charging infrastructure to security incidents. They highlight the robustness of standard protocols, including the OCPP 1.6-J security update, addressing numerous vulnerabilities. Future enhancements are anticipated with the upcoming OCPP 2.0 release. Collaborating with car manufacturers such as Citroën India, Mahindra and Mahindra, and MG Motors, Jio-BP ensures top-tier security controls in their EV charging stations. The company emphasizes its proactive approach, partnering with cybersecurity experts and deploying advanced protection systems for effective detection and response to cyber threats [7].
- **CERT-In:** India's cybersecurity incident response team, has been alerted to vulnerabilities in EV charging station products and applications. They have issued alerts and recommendations to address the identified weaknesses, emphasizing the need for proactive cybersecurity measures in the early stages of India's EV ecosystem development, learning from cyber-attacks in more advanced ecosystems [7].

  Newcastle University, University of Strathclyde, and Alan Turing Institute have done joint exercises in finding effective solutions for designing secure EV charging infrastructure [22]. Only a few Indian institutions/Researchers have announced research related to cyberattacks on EVs which includes IIT Delhi, IIT Kanpur, IIT Bombay, etc., and so forth.

(iv) Specific objectives of the proposed work

1. Develop an AI-based intrusion detection system for EVs, focusing on rapid identification and prevention of cyber-attacks on critical components.
2. Conduct a comprehensive threat analysis to identify vulnerabilities in EV systems, with a specific emphasis on electric drive systems, charging infrastructure, and communication networks.
3. Integrate the AI-powered security solution into existing automotive cybersecurity

standards, fostering widespread adoption and ensuring alignment with industry best practices.

(v) Novelty of the proposed work

Proposing a cutting-edge approach to bolstering EV security, this project introduces an innovative solution through the integration of AI. By leveraging AI capabilities, the focus is on pioneering a robust system for the detection and prevention of cyber-attacks, specifically tailored to safeguard crucial EV components. This novel initiative aims to contribute to the evolving landscape of automotive cybersecurity by introducing advanced, proactive measures that go beyond conventional approaches, ensuring the resilience of EVs against emerging cyber threats. The major novelties of the project proposal are as follows:

a. **Identification of Attack Vectors and Dataset Generation:** Examination of different potential attack vectors in EVs, including CAN bus, Operating System, and Network. Collecting data from electronic components including sensors, controllers, and communication interfaces of the EV and encompassing a range of practical scenarios commonly faced by EVs, to fortify the adaptability of the model.
b. **Advanced ML Model Development and Testing:** Developing a sophisticated AI model that can identify anomalies tailored for cybersecurity in EVs, incorporating features like deep neural networks or ensemble methods. Also, systematically evaluate the effectiveness of the trained AI model by conducting real-world trials, guaranteeing practical application and resilience against emerging cyber dangers.
c. **Innovative Diagnosis and Prevention System Implementation:** Implementation of audible alerts, system isolation, and comprehensive resets on diagnosis of cyber-attack. Fortify security protocols such as CAN authentication, cryptography, hashing, and data hiding, to protect against any potential cyber threats.
d. **Focus on Real-Time Implementation and Deployment:** E-Cart developed under the E-MOBILITY Lab of TIET Patiala will be used for testing and deployment of the proposed solution interfaced with the CAN bus.

(vi) Methodology details

The typical Electric Drive Systems for any EV are shown in Fig.1. It also shows the locations that are vulnerable to cyberattacks.

Further, the proposed methodology based on data collection, data processing, and algorithmic methods is divided into sub-categories and their details are described below.

a. **Identification of Attack Vectors in Electronic Vehicles**

   There are five attack vectors which are given below.

   Inputs: Current sensor, Position encoders, speed/torque sensors, Reference torque, and reference current

   Output: PWM signals

b. **Detection and diagnosis of cyber attack**

   To conduct a comprehensive analysis, we propose utilizing the physics-based data features approach to thoroughly investigate cyber-attacks. These attacks can be classified into two distinct groups, based on how they affect signal waveforms. The first group exhibits clear and easily detectable effects such as ripples, impulses, or system instability. The second group, on the other hand, indirectly impacts the motor. This distinction is depicted in Fig.2, where the current id [A] is shown to vary under the different attack scenarios. Specifically, scenarios (I) and (II) represent the outcomes of the first and second attack types, respectively, and demonstrate their specific effects on the control system.

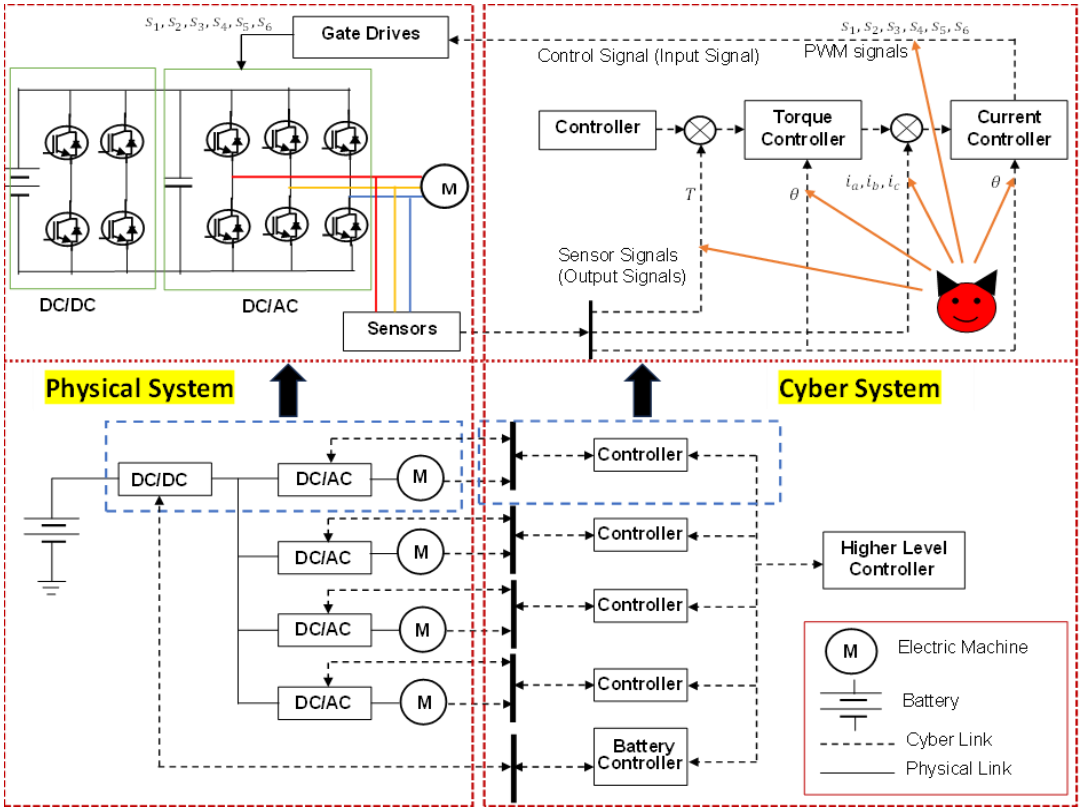


Fig.1: Layout of Cyber-Physical System for Electric Drive Systems

Before considering the AI model, data from electronic components including sensors, controllers, and communication interfaces of the EV will be collected. Once gathered, the collected data must then go through the process of preprocessing to guarantee seamless compatibility with the AI model. Further, deep learning or machine learning methods will be utilized to build an AI model that can identify anomalies, particularly trends that can point to a cyberattack. Our model will be trained on pre-processed datasets containing regular and irregular behavioral patterns to ensure maximum accuracy and efficacy. The overall procedure for the detection of a cyber-attack on an EV is shown in Fig.3.
Once the attack is detected, the following actions will be taken:

- Beep an alarm on detection of a cyber-attack on the EV.
- System isolation and reset the entire OS, network communication system, and CAN of the compromised EV.
- The human driver has the option to request car maintenance to improve detection and diagnosis capabilities.

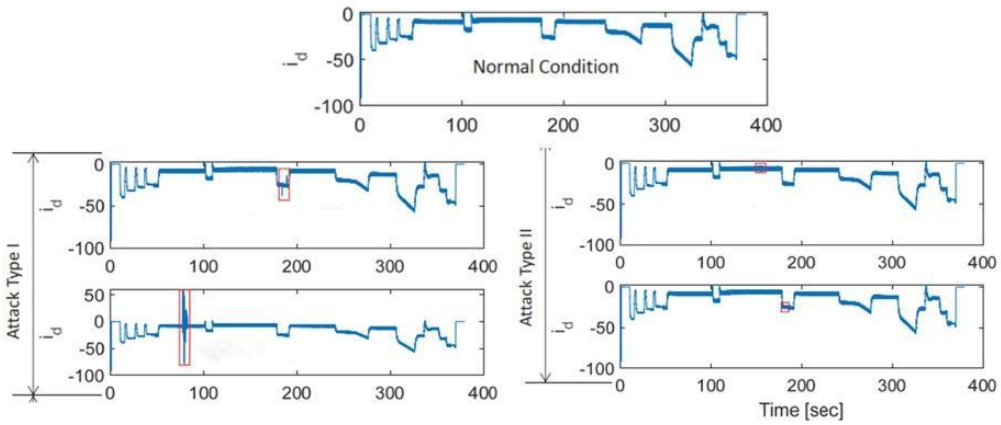


Fig.2: Attack scenarios (I) and (II) and their impact on current waveform [6].

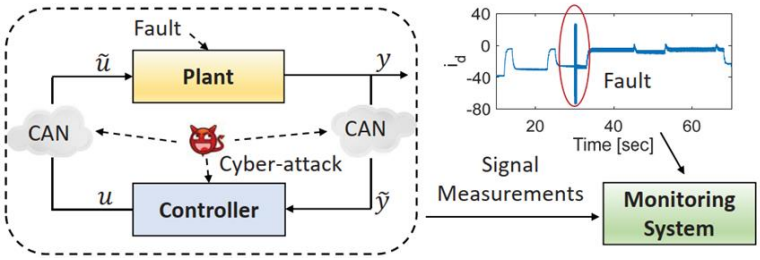


Fig.3: Cybersecurity breaches and tangible malfunctions in a control system [6]

c. Testing and deployment

In the final stage, the accuracy of the developed AI model for the detection of cyber-attacks will be validated across simulated, controlled, and real-world environments, ensuring scalability, adaptability, and robustness.

Further, a dual microprocessor system will be used to deploy the AI model for detection of the cyber-attack detection. It will allow the primary and secondary controllers to receive sensor feedback and issue commands to the system. Typically, the primary controller controls the system, while the secondary controller houses monitoring systems such as cyber-attack detection and diagnosis algorithms. In the event of a cyber-attack, the compromised signal is identified and diagnosed by the secondary controller, which then activates a robust control algorithm to safeguard the system.

(vii) Deliverables and outcomes

Deliverable 1: A dedicated AI module designed to detect and diagnose cyber-attacks on EVs, providing a comprehensive solution to enhance the cybersecurity of EV electronic systems.

Deliverable 2: An implementable module enabling continuous real-time monitoring of EVs, with the capability to prevent and mitigate cyber-attacks through proactive measures.

Deliverable 3: Other deliverables are:

- The findings, results, reports, novel techniques, and reputed research publications will be delivered as a tool for attack diagnosis and cyber-attack prevention in EV.
- The potential outcomes can be developed as Intellectual Property Rights (IPR) regarding international patents.
- Training/Workshop/Conference for increasing the benefit to a larger community.
- Undergraduate Projects, M.Tech. and Ph.D. thesis

(viii) Clear set of milestones

The work is planned in four phases ensuring the expected deliverables and objectives. The work plan details are provided below along with roles and responsibilities and they are abbreviated as Amit Kumar [AK], Ashima Anand [AA], Prashant Singh Rana [PSR], Mukesh Singh [MS] and industry collaborator Silov Solutions Pvt. Ltd [SS].

Work Package-1:

1.1 Data collection from EV [AA and MS]

In this work plan, we will collect the data of the defined target vectors from CAN of EV under different terrain running conditions through a data reader. We will also generate the data sets synthetically for cyber-attack conditions. All the data will be further segregated into normal, abnormal, and attack conditions.

1.2 Data preprocessing [AA and AK]

This work plan will involve collecting and organizing varied datasets while also cleaning, and normalizing the data. This will make the data adaptable to evolving environments, ensure consistency, and lay the foundation for resilient and accurate cybersecurity solutions for EV systems.

Work Package-2:

2.1 Generation of the AI model [PSR and AA]

The generation of an ML model will be pivotal for building robust anomaly detection systems. Following data preprocessing, in this work plan the features will be extracted to capture

relevant patterns and behaviors. The dataset will then be divided into training and testing sets, with a variety of ML techniques - such as deep neural networks and ensemble methods. By employing hyperparameter tuning and cross-validation methods, the performance of the model will be optimized.

2.2 Training and testing of the built AI model [AA and PSR]

In the following workplan, the AI model will be extensively trained and tested to enhance its ability to detect anomalies. Through the training phase, the model will gain an understanding of intricate patterns within preprocessed data from the CAN bus and fine-tune its parameters for optimal accuracy and versatility. Real-life situations, such as anomalies, and environmental factors, will be used to evaluate the model's durability and dependability in identifying potential cyber threats. The iterative training and testing process will pursue robust performance in diverse settings, thereby contributing to the development of an AI-based cybersecurity solution.

2.3 Design of diagnosis and prevention system [AA and PSR]

This work plan details the necessary steps for handling a cyber-attack on an EV and implementing measures to prevent such attacks. In the event of an attack, the EV system will trigger an audible alert, isolate the affected system, and perform a thorough reset of the operating system and communication network. Additionally, drivers have the option to request maintenance for further analysis. To protect against cyber-attacks, advanced security protocols will be implemented, including CAN authentication, cryptography, hashing, and data hiding.

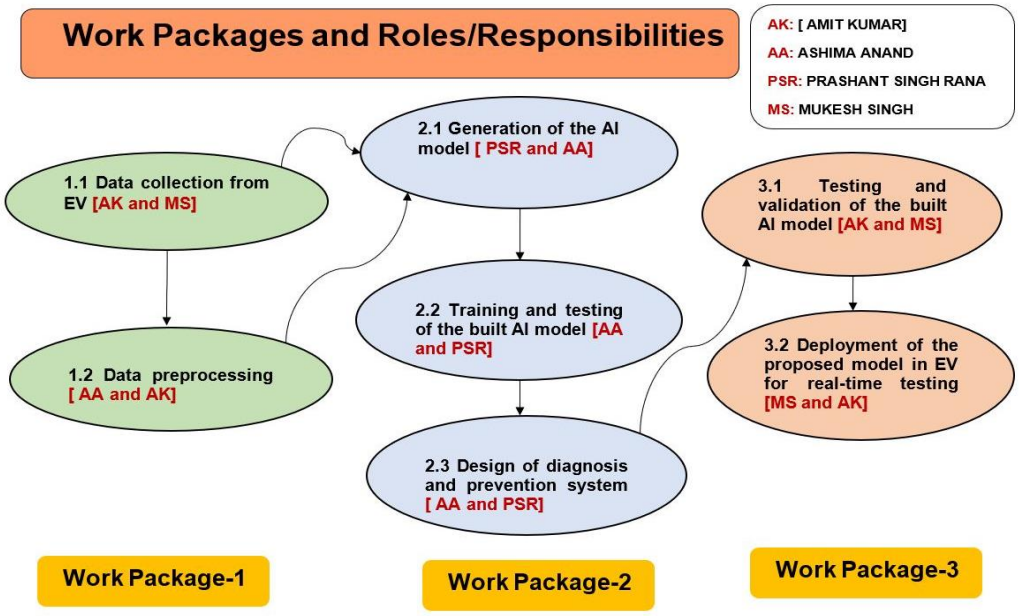
Work Package-3:

3.1 Testing and Validation of the built AI model [AK and MS]

This work plan of the proposal includes the testing and validation of the AI model for normal, abnormal, and cyber-attack conditions. The checking of the efficacy of the AI model will be carried out and fine-tuning of the parameter's adjustment will be done.

3.2 Deployment of the proposed model in EV for real-time testing [MS and AK]

This stage of the work package is the final stage in which the proposed module will be integrated into the EV system in the Vehicular Control Unit (VCU) for the final testing and it will be tested under different cyber-attacks created synthetically.



(ix) Timeline for achieving each milestone

The time schedule of activities giving milestones through bar diagram is provided below

Activity	1st Year				2nd Year				3rd Year			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Literature Survey												
Procurement of Equipments (sensors, data reader)												
Collection of data from EV under different conditions.												
Generation of AI model												
Training and Testing of the AI model												
Validation & comparative evaluation of different AI techniques												
Design of diagnosis and prevention system												
Deployment of the proposed AI solution to real EV in our campus												
Preparation of report and publication												

(x) Summary of past works of the PI and Co-PI

Dr. Amit Kumar (Principal Investigator) has been working in the domain of power electronics converter control, microgrid, and power system optimization for the last 10 years. He has worked as a Postdoctoral Research Associate at IIT Delhi on a research project titled "Developing and Prototyping of ICT Enabled Smart Charging Network Components (RP03638G)" sponsored by DST. He has published 19 SCI/SCIE-indexed journal research papers. He will be responsible for capturing data sets under various conditions and deploying of AI module in the EV.

Dr. Ashima Anand (Co-PI) interests include information security, data-hiding methods, digital image processing, and cryptography. She is an author of more than 30 publications in top international transactions and conferences. With an experience of more than 6 years in the security domain, she will be responsible for designing security-based solutions/architecture for the diagnosis and prevention of cyber-attacks in the EV.

Dr. Prashant Singh Rana (Co-PI) interest includes deep learning, machine learning, data analytics, visualization, etc. He is the Director and Co-Founder of MLTool Technologies Pvt Ltd. He has published more than 100 research articles in top international transactions and conferences. With an experience of more than two decades in the AI domain, he will be responsible for designing the architecture for the diagnosis and prevention of cyber-attacks in the EV.

Dr. Mukesh Singh (Co-PI) fields of interest include smart grid, vehicle to grid, EV battery management system, EV charging infrastructure and SoC and SoH estimation etc. With an experience of more than 15 years in the EV control. He will be responsible for designing the architecture for the diagnosis and prevention of cyber-attacks in the EV. He will contribute to the real data collection from EV, and offer expertise in understanding the impact of deployment at different strategic locations. He will ensure that the project stays on schedule and within budget.

(xi) Bibliographic references

[1] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things," IEEE Power Electronics Magazine, vol. 4, no. 4, pp. 37–43, Dec 2017.

[2] M. Levi, Y. Allouche, and A. Kontorovich, “Advanced analytics for connected car cybersecurity,” in 2018 IEEE 87th Vehicular Technology Conference (VTC Spring). IEEE, 2018, pp. 1–7.
[3] L. Guo, J. Ye, and L. Du, “Cyber-physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyber-attacks,” IEEE Transactions on Transportation Electrification, 2020.
[4] J. Liu, S. Zhang, W. Sun, and Y. Shi, “In-vehicle network attacks and countermeasures: Challenges and future directions,” IEEE Network, vol. 31, no. 5, pp. 50–58, 2017.
[5] S. Abbott-McCune and L. A. Shay, “Intrusion prevention system of automotive network can bus,” in 2016 IEEE International Carnahan Conference on Security Technology (ICCST). IEEE, 2016, pp. 1–8.
[6] L. Guo, J. Ye and B. Yang, "Cyberattack Detection for Electric Vehicles Using Physics-Guided Machine Learning," in *IEEE Transactions on Transportation Electrification*, vol. 7, no. 3, pp. 2010-2022, Sept. 2021
[7]https://theprint.in/tech/ev-charging-stations-prone-to-cyber-attacks-like-other-tech%20applications-govt-to-parliament/1454184/
[8] A. Khalid, A. Sundararajan, A. Hernandez, and A. I. Sarwat, “Facts approach to address cybersecurity issues in electric vehicle battery systems,” in 2019 IEEE Technology & Engineering Management Conference (TEMSCON). IEEE, 2019, pp. 1–6.
[9] S. Chakraborty, M. A. Al Faruque, W. Chang, D. Goswami, M. Wolf, and Q. Zhu, “Automotive cyber–physical systems: A tutorial introduction,” IEEE Design & Test, vol. 33, no. 4, pp. 92–108, 2016.
[10] R. Hull, “Nissan disables leaf electric car app after revelation that hackers can switch on the heater to drain the battery,” This is money, Feb, vol. 26, 2016.
[11] B. Yang, L. Guo, F. Li, J. Ye, and W.-Z. Song, “Vulnerability assessments of electric drive systems due to sensor data integrity attacks,” IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3301–3310, 2020.
[12] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, “Impact analysis of data integrity attacks on power electronics and electric drives,” in 2019 IEEE Transportation Electrification Conference and Expo (ITEC). IEEE, 2019, pp. 1–6.
[13] A. Weimerskirch and R. Gaynier, “An overview of automotive cybersecurity: Challenges and solution approaches.” in TrustED@ CCS, 2015, p. 53.
[14] J. Valenzuela, J. Wang, and N. Bissinger, “Real-time intrusion detection in power system operations,” IEEE Transactions on Power Systems, vol. 28, no. 2, pp. 1052–1062, 2012.
[15] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, “Detection of cyber-attacks against voltage control in distribution power grids with PVs,” IEEE Transactions on Smart Grid, vol. 7, no. 4, pp. 1824–1835, 2015.
[16] C. Schmittner and G. Macher, “Automotive cybersecurity standards relation and overview,” in International Conference on Computer Safety, Reliability, and Security. Springer, Cham, 2019, pp. 153–165.
[17] “Vehicle electrical system security committee: SAE J3061 cybersecurity guidebook for cyber-physical automotive systems,” SAE, Tech. Rep., 2016.
[18] “International organization for standardization: ISO 26262 road vehicles functional safety part 1–10. technical report, international organization for standardization,” ISO, Tech. Rep., 2011.
[19] https://www.nrel.gov/docs/fy21osti/75236.pdf
[20] T. K. S. Lab, “Experimental security research of tesla autopilot,” Tech. Rep., 2019.
[21] https://www.osti.gov/servlets/purl/1877784
[22]https://www-users.york.ac.uk/roberto.metere/preprints/Securing-the-Electric-Vehicle-Charging-Infrastructure.pdf

6. Yearly break up budget into categories – equipment, manpower, contingency, consumable, travel.

The estimated budget of the proposed project proposal entitled, "Enhancing Electric Vehicle Security: AI-Powered Detection and Prevention of Cyber Attacks" is Rs.39,79,272. The detailed break-up is given below.

Table 1 Detailed Break-up of Estimated Budget of the Proposed Project

Sl. No.	Particulars	Year wise break up (INR)			Total Cost (Rs Lakhs)
		1st year	2nd year	3rd year	
1	Equipment's				
	A. Sensor & Conditioning Circuits	50000.00	--	--	50000.00
	B. Controller board with connecting interfaces to interface other devices/sensors etc.	200000.00	--	--	200000.00
	C.High end computing devices (2 Nos.)	380000.00	--	--	380000.00
2	Temporary man power (JRF/SRF: 2 Nos)	810960.00	810960.00	915600.00	2537520.00
3	Consumables / Miscellaneous	50000.00	50000.00	50000.00	150000.00
4	Contingencies	50000.00	50000.00	50000.00	150000.00
5	Travel	50000.00	50000.00	50000.00	150000.00
6	Others (if any)	--	--	--	0.00
7	Institutional overheads (10%)	159096.00	96096.00	106560.00	361752.00
Grand Total		1750056.00	1057056.00	1172160.00	3979272.00

7. Budget justification

1. **Equipments:**

   A. Sensor & Conditioning Circuits: These are required for accessing the data and collecting the data from EVs.

   B. Controller board with connecting interfaces are required to embed the proposed AI based cyber security system in EV to interface other devices/sensors and VCU.

   C High end computing devices: For the development of AI based Cyber-attack detection and prevention system model, its training, testing and computation high end computing devices are required.

2. **Temporary Manpower:**

   First two years (JRF): Monthly Rs. 31000 + HRA @ 9% (Rs. 2790)= Rs. 33,790
   =Rs. 4,05,480 yearly

   Last one year (SRF): Monthly Rs. 35000 + HRA @ 9% (Rs. 3150)= Rs. 38150

= Rs. 4,57,800 yearly

Three-year budget for 1 Nos of person= Rs. 4,05,480 +Rs. 4,05,480 +Rs. 4,57,800

= Rs.12,68,760

Three Year manpower budget (2 Nos.): (Rs.12,68,760 x 2) = Rs. 25,37,520

3. **Consumables / Miscellaneous**
   To interface the hardware several other components like ICs and chips are required.

4. **Contingencies**
   It will be used for attending the conference, registration fee for the conference, dissemination of the output and results, and proper documentation printing etc.

5. **Travel**
   Traveling will be required to meet with experienced academic professionals and industry professionals to discuss the industry requirements.

6. **Institutional overheads (10%):**
   Institutional overheads are 10% as per the Department of Science and Technology Govt. of India per year of the sanctioned amount.