Applications of Data Analytics, Machine Learning, Cybersecurity, and Blockchain in HEVs and EVs: Recent Trends

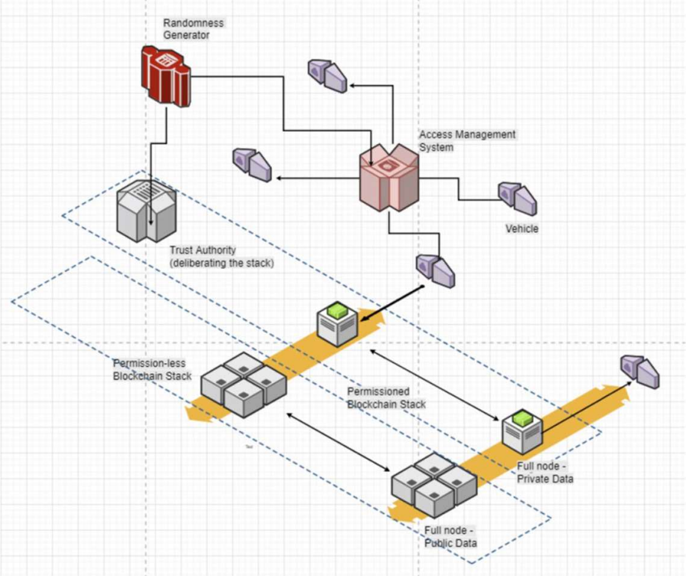
Hybrid and Electric Vehicles are being increasingly used for different mobility applications. For mass acceptance of EVs, it is important to not only to offer competitive Total Cost of Ownership (TCO) to the owners compared to conventionally powered vehicles but also to provide efficient Battery Management Systems and charging solutions. Complex algorithms are being developed using Machine Learning (ML) to optimize the power required to drive EVs based on real time State of Charge (SOC), State of Health (SOH), battery temperature and voltage parameters, environmental conditions and driving pattern.

Control strategies include rule-based approach for optimal usage of energy by setting the required threshold limits, Fuzzy logic using rule-based power controller approach by recognizing the driving pattern in a specific drive cycle, and probabilistic model based on power demand using dynamic programming to generalize the result in all driving conditions. Methods to estimate SOC parameter have evolved from Ampere hour counting method and Open circuit voltage method to advance methods such as Impedance and Internal resistance method, Electrochemical method, and Model based method.

Learning algorithms for efficient Battery Management System (BMS) include Artificial Neural Networks (ANN), Extreme Machine Learning (ELM), Genetic Algorithms (GA), and Fuzzy Logic. ANN uses Li-ion battery terminal voltage, discharge or charging current, and surrounding temperature as excitation to the system model and SOC value as output. The ELM technique is mostly used in estimating SOC mainly for online learning with the dual advantages of reduced error and faster computation time. The GA technique utilizes the algorithmic approach to generate randomly N chromosome based on the sensor data set available to learning and then initiates the process of biological evolution. This results in optimization of Li-ion battery model parameters, estimation of battery model parameters by using battery current and voltage and GA based back propagation (BP) neural network. The technique of Fuzzy Logic estimation utilizes a non-linear complex model and trains it appropriately. Though the technique has the ability to predict non-linear models it requires complex computations and large storage memory units and expensive processing units.

In order to protect the intra-vehicle and inter-vehicle communications among the connected devices, hardware security as well as software security must be taken into consideration while designing the system. Any security attack on the battery pack which plays a critical role in powering different modules and ECUs in EVs may result in surpassing the thermal runaway condition because of improper charging or discharging monitoring system. The cybersecurity threat to battery pack might be related to the application layer where attacks are generally in the form of SW attack (bug) or hardware attack (malfunction of control system) or network attack (compromise of CAN bus) or sensor attack (remote tampering of calibration settings). Anomaly detection algorithm using Machine Learning technique enables the system to learn from the experience and take decisions based on the input data. The most widely exploited cyber attacks are Denial of Service (DoS), Replay/man-in-middle attack, brute force attack for accessing the encrypted data, and forged traffic-based attack. The anomaly detection mechanisms identify anomalies based on the classifier such that a positive output indicates normal operation and negative output represents anomalous operation. Anomaly detection mechanisms include Support Vector Machine (SVM) which utilizes a generic method to fit the data points into a hyper-plane, Self-Organizing Map (SOM) algorithm based on Artificial Neural Networks (ANN), k-Nearest Neighbour (kNN) algorithm in which the prediction is done based on the geometrical framework using unsupervised learning, and Linkage based clustering algorithm which links up similar data into a cluster and based on the distance metric predicts the anomalous behaviour.

For Electric Vehicles (EVs), the blockchain technology offers a framework that is needed to provide a secure medium to communicate among the connected devices and ECUs. The blockchain system inherently provides a secure environment to exchange information in public domain without involving third-party intermediary to complete the exchange of information. In the proposed framework, a regulated access layer inside a permissioned blockchain is provided and data validation is provided in the permission less overlaying platform which enables the users to utilize the robustness of the blockchain algorithm by having control access to actual data transmission protocol as an outcome of permissioned blockchain and increase the transaction throughput and also without compromising the complexity of the method used for consensus between nodes in the network. This framework uses the open source proof-of-work consensus type to develop the data validation protocol. The data in the network is encrypted by the advance encryption algorithm in the private blockchain environment and transmitted by using access key which is generated and distributed to the node in the network. These hybrid implementations ensure that the data is safe from man-in-middle or distributed Denial of Service (DoS) attacks on the chain and also reduce the computational complexity. This framework provides hierarchical trust levels and also optimizes the transaction time as the transmitted data wait for all the nodes to solve cryptographic problem to reach consensus.


Randomness Generator
Access Management System
Vehicle
Trust Authority (deliberating the stack)
Permission-less Blockchain Stack
Permissioned Blockchain Stack
Full node - Private Data
Full node - Public Data

Reference: Mishra, V., Kodakkadan, A.R., Koduri, R., Nandyala, S. et al., “Wireless Charging for EV/HEV with Prescriptive Analytics,
Machine Learning, Cybersecurity and Blockchain Technology: Ongoing and Future Trends,” SAE Technical Paper 2019-01-0790, 2019, doi:10.4271/2019-01-0790.