Cyber Risk for Electrical Vehicle Infrastructure: Challenges and Possible solution against Cyber Intrusion

Vijaykumar K. Prajapati[1]
Assistant Professor
Electrical Engineering Department
L.D. College of Engineering, Ahmedabad

Vikas Ranjan[2]
Assistant Professor
Electrical Engineering Department
Haldia Institute of Technology, Haldia

Neeraj Singh[3]
Technical Lead
Automotive Department
HCL Tech, Bangalore

Abstract: The Electrical Vehicle Infrastructure consists of two-way communication, one from the grid side and the other is from the vehicle side. For two-way communication, it involves different intelligent sensors and electronic telemetry equipment for gathering and processing data. The presence of a large number of electronic equipment connected with the cyber layer for data transfer and monitoring makes the EVI a vulnerable system against cyber intrusion. This paper highlights the most common vulnerable points present in EVI and possible solutions to prevent intrusion. The main focus is on data security and customer information safety which can be used by intruders for some amiss planning. Using Gaussian Data Envelope Security the data confidentiality is increased and for reducing the data losses Fuzzy Logic Internet Protocol Protection (FLIPP) can play a vital role. Both methods are explained in detail for EVI security and safety.

Keywords: Electrical Vehicle Infrastructure (EVI), Gaussian Data Envelope Security (GDES), Cyber Intrusion, Fuzzy Logic Internet Protocol Protection (FLIPP)

I. INTRODUCTION

In the modern 21st century the demand for the electrical vehicle is increasing day by day to decrease the dependency on conventional fuel [1]. Also, the penetration of solar and wind energy converters need more electric storage devices which can easily available anytime during the excess generation for sudden storage purpose. For proper utilization of electric vehicles as sudden storage devices need a smart EVI throughout the grid [2, 3]. A smart EVI consists of a two-way communication network, smart and intelligent sensors, monitoring and control stations, interacting charging stations, global positioning network, wired/wireless connectivity to energy trading cloud for real-time pricing information, and many more [4].

Due to the presence of large sensors, communication devices in EVI and in the electrical vehicle increases the system vulnerability [5]. Engineers and researchers have shown significant interest in exploring the different aspects regarding the cyber-physical interaction

in terms of cyber safety [6, 7]. Most of the companies are working on a vehicle-to-grid concept to handle imbalance during peak load demand and peak energy generation. After integration of grid and vehicle, the second important aspect is the security of data communication during vehicle-to-grid interaction [8]. During cyber intrusion the attackers can target attack from the grid side or from the vehicle side which may lead to the following three attack scenario:

- False data intrusion
- Intrusion to gain access of vehicle monitoring and control system
- Intrusion to gain access in grid side systems

Much research literature addresses the problem specifying cybersecurity of smart grid but very few highlight security concern related to electric vehicle and grid integration [9-11]. The EV customers need a more fast and reliable security system to save their time, critical information, and personal safety [12]. So basically the interaction of electric vehicle and grid needs an Internet of Things platform which easily gets affected by Mirai malware [13]. The malware hits the IoT systems and uses to form a bot network which is used for Distributed Denial-of-Service attacks. Charging an electrical needs a secure payment getaway to enhance customer privacy and security. Last decade data shows that the many successful attacks were carried out on the payment gateway making customers bears the financial loss. So the EVI must have a private secure payment gateway with enhanced features like a one-time vehicle password or owner's driving license number to complete the financial transactions.

Although many new research work is going on to enhance the security and privacy of critical infrastructure but still more required for EVI. This paper contributes to EVI in two folds:

- Identifying the weak points in EVI
- GDES and fuzzy logic based approach for enhancing security of EVI

II. POSSIBLE INTRUSION IN CYBER-PHYSICAL EVI

The most common component, equipment, and sensors used for an electric vehicle are shown in figure 1 . The main electronic sensors installed in the almost all-electric vehicle are as follows:

- *AC/DC Converter sensors*: This is used to monitor the charging status of the vehicle from charging stations. This is the first sensor that comes into contact with the grid during the charging and discharging cycle of batteries.
- *Transmission sensors*: The transmission sensor monitors the transfer of mechanical power from the electrical motor to the driving axel connected to the wheel.
- *Electric motor sensor*: It is used for condition monitoring of electric motor against different faults which may affect the vehicle performance.
- *Engine monitoring sensors:* This kind of sensor is found in the hybrid electric vehicle where apart from electric motor transmission conventional transmission is also used.
- *Temperature sensors:* It's the most important sensor used to monitor the battery temperature and to provide real-time information regarding the cooling of drives attached to the traction battery pack.
- *Data Storage:* To store daily details in terms of usage and maintenance. Basically, it stores each and every detail of the vehicle during operations.

- *Wireless Communication:* To interact internally, with charging stations, and with the grid energy market, all-electric vehicles need wireless communication. Wireless communication provides flexibility and can be operated even during traveling.
- *Global Positioning System (GPS):* GPS is commonly used in all vehicles to locate the exact location of the vehicle during some emergency services also to locate the new track by the new driver. For an electric vehicle, it's very important to locate the next charging station during long drive routes.
- *Battery monitoring sensors:* The major part of an electric vehicle is a large traction battery pack for long hours' drive output. So proper monitoring is required for more efficient and economical output.

The most critical sensors which are given first priority to save from external and internal intrusion are shown in red colour in figure 1. The blue colour box indicates the list of sensors that comes second on the priority list and the rest are at the third number of the priority list. .

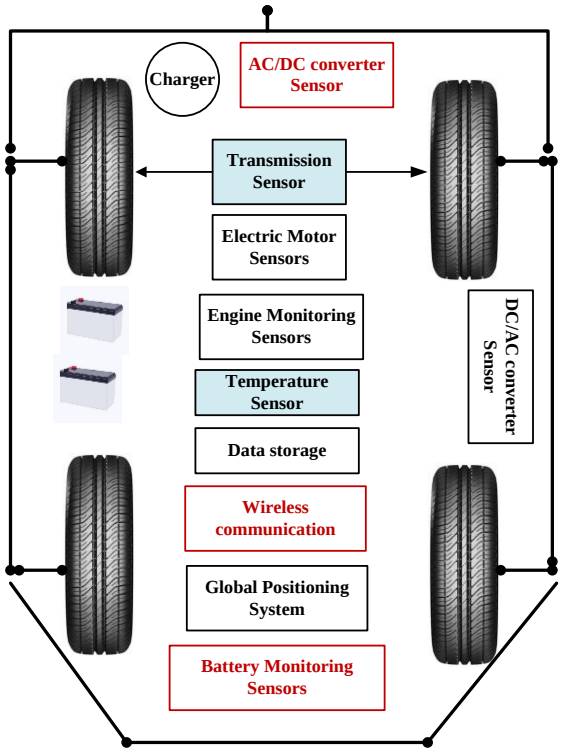

Figure 1. Main electric vehicle components

Similarly, the charging station consists of many sensors to interact with the vehicle and grid for economically feasible prices as shown in figure 2. The most critical points related to charging stations are communication link, grid interaction, customer data, and user interface.

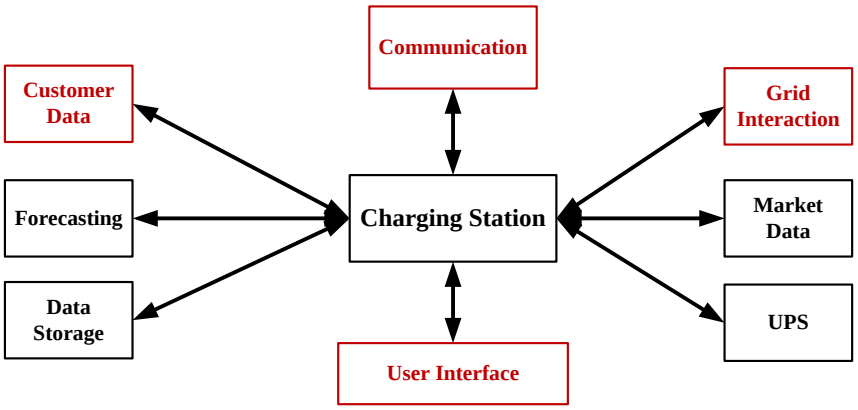

Figure 2. Charging station

So from the above discussions, three intrusion category is identified which can affect the operation of EVI are discussed below.

A. Intrusion from grid side

- *Using grid interaction stations*: This is the first weak point in EVI where the cyber intruders may try to get access to the EVI or electric vehicle from the grid side. Intrusion like stealth attack, false data injection, and many more can be used by the attackers to gain access of the charging station.

- *Using communication network*: The easiest way to penetrate any cyber network is to use a communication link. All possible attacks can be performed if the communication network is compromised.

- *Using user interface like Supervisory Control And Data Acquisition (SCADA)*: This is the most common link used by attackers in both grid-side intrusion and vehicle side intrusion. .

- *Using fake operator profile*: Making a duplicate platform similar to the grid operators so that the credentials of charging station operators can be obtained. Using those credentials the intrusion will become easier for the intruder.

B. Intrusion from vehicle side

- *Physical ports available in electric vehicle:* Nowadays every modern vehicle is equipped with Universal Serial BUS (USB) Port for data transfer in an electric vehicle. Usually, it is used to obtain regular data regarding battery status, traffic status, efficiency, and other important parameters. Using USB the intruders can target both the customer and the power grid. The USB attack is categorized into four different attacks which are software on the USB device, electrical attack, Reprogrammable Microcontroller USB Attacks, and reprogrammed USB peripherals. In all the four attack conditions the intruders get access to the main

control of the electrical vehicle and can find a possible path to enter the grid server using the charging station user interface unit.

- *Through wireless communication:* To interact with another electric vehicle, monitoring station, and emergency services every electric vehicle needs wireless communication. The most common attack in this category is the Denial of Service (DoS) attack. Using DoS the cyber attackers gain unauthorized access results in unreliable operation of the system. After DoS spoofing is the second most common attack used by intruders to gain unauthorized access to the system through phishing mail and message.

- *Through user interface at charging station*: For charging vehicles most of the time the customer will choose a charging station. The attackers may use the human-machine interface to get access and control of the vehicle and can use it to propagate the attack to the grid during the next charging/discharging session.

C. Intrusion against autonomous driving

- *Through traffic controller station:* To create mass destruction, the intruders can gain access to the traffic control station and then by getting access to traffic control of different areas which may lead to an accident.

- *Hacking radio stations:* For creating traffic jams and havoc in the city by providing wrong information through the hacked radio station. It may affect critical services like paramedical, firefighting, and police.

III. FEASIBLE SOLUTION AGAINST CYBER INTRUSION IN EVI

This section highlights two novel possible ways to secure the EVI from intruders. EVI provides various benefits to the grid, electric vehicle, and other companies involved in the booting electric vehicle concept. With the help of EVI grid operators can easily balance the power need during renewable energy variation using an electric vehicle as an energy storage device. Apart from charging optimization for electric vehicles, cybersecurity and customer protection is important issues. Two feasible protection schemes for the EVI against cyber intrusion are Gaussian Data Envelope Security (GDES) and Fuzzy Logic Internet Protocol Protection (FLIPP).

A. Gaussian Data Envelope Security (GDES)

EVI interacts with large data sets which need easy, fast, and secure availability during the operation periods. Figure 3 shows the GDES concept. The main data is protected by providing an envelope key and then mixing it with the Gaussian noise so that the data privacy is maintained [14]. The secure data is extracted from the mixed data using the end-user side key. .

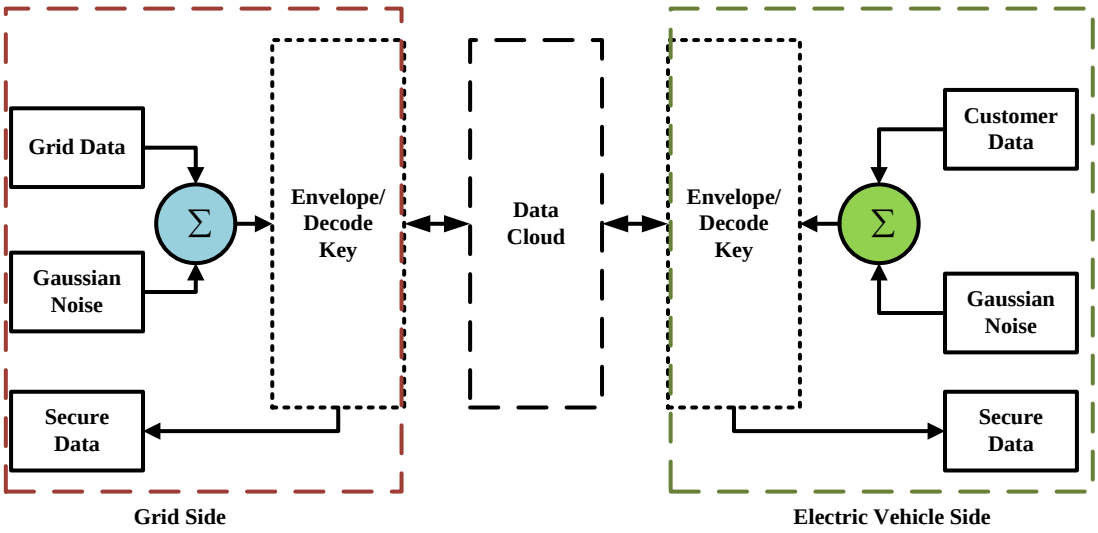

Figure 3. GDES

The Gaussian Mixture Model for GDES is expressed as:

$$g(d)=\sum_{i=1}^{k}\psi_i \mathrm{N}(d,\mu_i,\sigma_i) \tag{1}$$

Where, K is the Kth component, μ_i represent means and σ_i indicate variance of different component. ψ_i indicate the weight of the component with constraints as follows:

$$\sum_{i=1}^{k}\psi_i=1 \tag{2}$$

For the key envelope, any two processes can be followed as shown in figure 4. In A the key is mixed with data and a serial value is created, in B any arithmetic operation can be used.

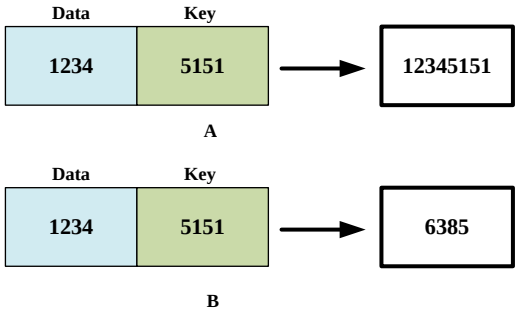

Figure 4. Key envelope

Using GDES the security of data is increased up to 99% and data losses reduces to 1% [15]. Also, GDES can act as a platform which helps different electric vehicle and charging station to interact with each other using the different personal key for more safety.

B. Fuzzy Logic Internet Protocol Protection (FLIPP)

This method is capable of protecting EVI against any intrusion and eliminating threats by blocking their internet protocol and altering the IP of other non-malicious systems [16-18]. In this method, each of the intelligent system connected with the internet is modelled like the graph at different level as shown in figure 5, where CS indicate n-number of charging station, M number of electric vehicle and Z number of the monitoring area. Level 1 consists of a monitoring area which use to monitor each activity of electric vehicle and charging station. Level 2 includes all charging stations and level 3 consists of the electric vehicle of a particular monitoring area. As each of these systems is equipped with the internet so it can act as a node of graph interacting with each other. Also, each of these systems has its own particular IP address. During cyber intrusion in any of the levels/systems, the other level IP will get an update with new IP status and will update regarding bad IP which should not be considered for communication.

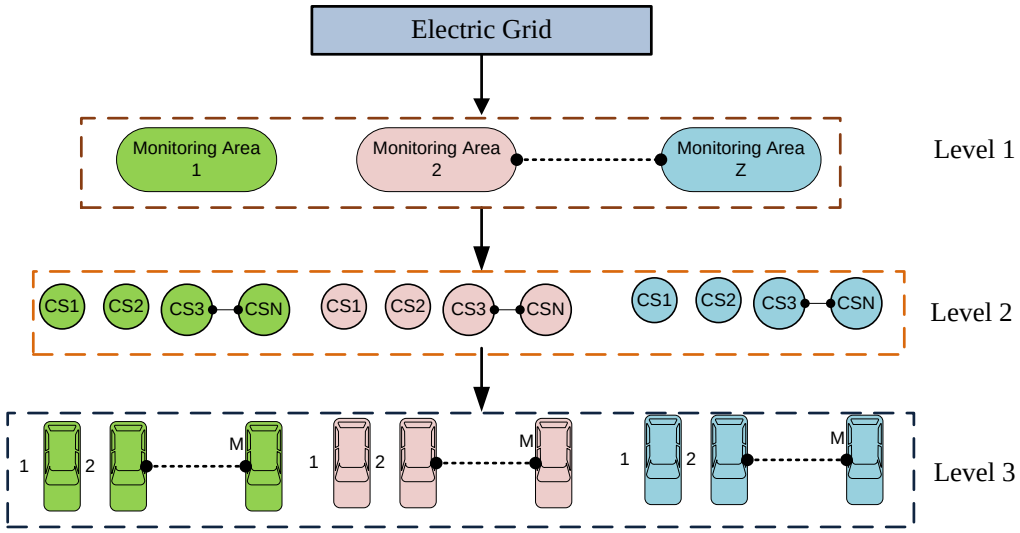

Figure 5. FLIPP approach

So the EVI can get its priority using FLIPP for each level against cyber intrusion. The priority using FLIPP is discussed in table 1. Using the priority parameters described in table 1, the fuzzy rules can be formed as highlighted in table 2. It can be extend and update according to the requirement.

Table 1. FLIPP priority parameter

Parameters	**To generate fuzzy rule 3 variation are chosen**		
Level 1	Low	Medium	High
	→		
Level 2	Low	Medium	High
	→		
Level 3	Low	Medium	High
	→		
Priority	Low	Medium	High
Arrow indicate large number of IP devices acting as node			

Table 2. FLIPP Rules

Sr. No	**IF**	**AND**	**AND**	**THEN**
	Level 1	**Level 2**	**Level 3**	**Priority**
1	Low	Low	Low	Low
2	Medium	Medium	Medium	Medium
3	High	High	High	High
4	Low	Medium	Medium	Low
5	Medium	High	High	High
6	High	Low	Low	Medium
7	Low	High	High	Medium
8	Medium	Low	Low	Low
9	High	Medium	Medium	High

IV. CONCLUSION

This paper unveils a novel GDES and FLIPP concept EVI grid data can be secure up to maximum limits making the system reliable and safe during the cyber intrusion. The attackers use weak points of EVI discussed in section II to design an attack to get access for maximum destruction in terms of physical or economic. Although there are many intrusion detection techniques available, the GDES and FLIPP can prove to be the best ones due to many advantages like flexible interaction nature, fast updates, and ease of implementation on a big platform like EVI. The goal of this paper is not only to identify the weak point but also to provide a futuristic solution that can be used by the researchers and companies involved in EVI to defend the privacy of customers and secure the EVI platform against any new cyber threats. Therefore, proper algorithms using the concept of GDES and FLIPP should be developed by the engineers and researchers' group.

REFERENCES

[1] R. R. Kumar and K. Alok, "Adoption of electric vehicle: A literature review and prospects for sustainability," *Journal of Cleaner Production*, vol. 253, p. 119911, 2020.

[2] U. H. Ramadhani, M. Shepero, J. Munkhammar, J. Widén, and N. Etherden, "Review of probabilistic load flow approaches for power distribution systems with photovoltaic generation and electric vehicle charging," *International Journal of Electrical Power & Energy Systems*, vol. 120, p. 106003, 2020.

[3] T. Chen, X.-P. Zhang, J. Wang, J. Li, C. Wu, M. Hu, *et al.*, "A review on electric vehicle charging infrastructure development in the uk," *Journal of Modern Power Systems and Clean Energy*, vol. 8, pp. 193-205, 2020.

[4] F. Teng, Z. Ding, Z. Hu, and P. Sarikprueck, "Technical Review on Advanced Approaches for Electric Vehicle Charging Demand Management, Part I: Applications in Electric Power Market and Renewable Energy Integration," *IEEE Transactions on Industry Applications*, vol. 56, pp. 5684-5694, 2020.

[5] 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.

[6] N. Bhusal, M. Gautam, and M. Benidris, "Cybersecurity of Electric Vehicle Smart Charging Management Systems," *arXiv preprint arXiv:2008.07511*, 2020.
[7] H. Cui, X. Dong, H. Deng, M. Dehghani, K. Alsubhi, and H. M. A. Aljahdali, "Cyber Attack Detection Process in Sensor of DC Micro-Grids Under Electric Vehicle based on Hilbert-Huang Transform and Deep Learning," *IEEE Sensors Journal*, 2020.
[8] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.
[9] A. C.-F. Chan and J. Zhou, "Cyber–physical device authentication for the smart grid electric vehicle ecosystem," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 1509-1517, 2014.
[10] Z. Guo, D. Shi, D. E. Quevedo, and L. Shi, "Secure state estimation against integrity attacks: A Gaussian mixture model approach," *IEEE Transactions on Signal Processing*, vol. 67, pp. 194-207, 2018.
[11] N. K. Singh and V. Mahajan, "Analysis and evaluation of cyber-attack impact on critical power system infrastructure," *Smart Science*, pp. 1-13, 2021.
[12] A. C.-F. Chan and J. Zhou, "A secure, intelligent electric vehicle ecosystem for safe integration with the smart grid," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, pp. 3367-3376, 2015.
[13] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, pp. 80-84, 2017.
[14] M. Shashanka, "A privacy preserving framework for Gaussian mixture models," in *2010 IEEE International Conference on Data Mining Workshops*, 2010, pp. 499-506.
[15] N. K. Singh and V. Mahajan, "End-User Privacy Protection Scheme from Cyber Intrusion in Smart Grid Advanced Metering Infrastructure," *International Journal of Critical Infrastructure Protection*, p. 100410, 2021.
[16] N. K. Singh and V. Mahajan, "Fuzzy logic for reducing data loss during cyber intrusion in smart grid wireless network," in *2019 IEEE Student Conference on Research and Development (SCOReD)*, 2019, pp. 192-197.
[17] N. Iyengar, A. Banerjee, and G. Ganapathy, "A fuzzy logic based defense mechanism against distributed denial of service attack in cloud computing environment," *International journal of communication networks and Information security*, vol. 6, p. 233, 2014.
[18] M. D. Alshehri and F. K. Hussain, "A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT)," *Computing*, vol. 101, pp. 791-818, 2019.