Next-Generation Edge-AI Architectures for Secure EV Charging Infrastructure

[1*]Priyanka Kar, [2]Pabitra Kumar Nayak, [3]Prashanta Kumar Nayak, [4]Subrat Kumar Mohanty, [5]Sasmita Nayak

[1]Department of Electrical Engineering, Silicon University, Bhubaneswar, Odisha, India*
[2]Electrical Engineering, Synergy School of Engineering, Dhenkanal, Odisha, India
[3]Electronics and Telecommunication Engineering, Synergy Institute of Engineering and Technology, Dhenkanal, Odisha, India
[4]Electronics and Communication Engineering, Templecity Institute of Technology and Engineering, Bhubaneswar, Odisha, India
[5]Mechanical Engineering, Government College of Engineering, Kalahandi, Bhawanipatna, Odisha, India

Abstract: The growth in the use of electric vehicles (EVs) has led to a massive increase in the demand for infrastructure needed for the charging infrastructure, thus putting an immense amount of pressure on the stability of the grid, cybersecurity and efficiency. In this work, we propose a novel Edge AI architecture for threat and security in the EV charging infrastructure powered by integrating the distributed intelligence, application of real-time anomaly detection and adaptive load optimisation. The proposed system employs artificial intelligence models that are based on fuzzy logic and run at the edge of the network, in the monitoring of the grid conditions, the health of the EVs and cyber threats. Secure coordination between EV's, charging stations and central servers is put in place for increased system reliability, congestion and infrastructure resilience.

Motivation: Weaknesses in the grid control structures and cybersecurity frameworks have been exposed by the increase in the number of EV charging stations. Uncoordinated charging loads have the potential to destabilise power distribution networks and pose to create complex danger due to cyberattacks and data breaches. Current centralised solutions have latency and scalability issues, which emphasise the need for a decentralised and intelligent framework that can make decisions at the edge level 2 (in real-time) regimes. This paper is motivated by the need to ensure safe, efficient and scalable EV charging operations and protect grid stability and the safety of the critical energy infrastructure.

Novelty: The novelty in this study is to combine Edge AI intelligence with a fuzzy logic-based decision mechanism for the security of EV charging infrastructure. As opposed to typical architectures that are developed on the premise of cloud dependency, the proposed architecture shifts computational intelligence to the charging stations to achieve the specific purpose of ensuring low-latency anomaly detection and adaptive load balancing. The framework provides the unique combination of a grid stress analysis, EV battery health monitoring and cyber security threat analysis as a single decision module. This multidimensional and edge-centric design helps to increase the system resilience and improve the scalability, and allow to correct coordination of the involved components (EV, grid and communication networks).

Findings: Simulation and analytical exams indicate that the proposed Edge-AI architecture has a very positive impact on improving the reliability of charging operations and security of the charging infrastructure. The system can identify the abnormal charging behaviour and counter the cyber threats, and also dynamically adjust the charging loads to prevent grid overloading. Results show a reduction in response time, increased efficiency in load distribution and better security than unauthorised access. The integrated decision framework provides a higher degree of integration of operational stability as opposed to the traditional centralised systems, and this justifies the effectiveness of implementing distributed approaches using Edge AI to change the performance of the EV charging infrastructure and enhance cybersecurity resilience.

Keywords: *Edge-AI Architecture, Secure EV Charging, Smart Grid Security, Fuzzy Logic Controller, Cyber-Physical Systems, Load Optimization*

1. Introduction

The electrification of the world has witnessed a very rapid growth in the installation of EV charging infrastructure at an unprecedented level. Governments and utilities are all adding more charging networks in response to increased levels of EV adoption and the resultant reduction of carbon emissions [1]. However, the growth of the density in charging stations imposes critical technical challenges such as instability of the grid, peak load fluctuations and voltage deviations in smart grid environments [2-3]. Uncoordinated charging behaviour can cause overload of the transformer due to the operation cost inflation and reliability of energy distribution [4].

Beyond considerations of the grid, modern EV charging infrastructure systems are extremely connected through the use of cloud platforms, communications systems, and authentication systems. This integration calls for advanced and united methods prolonging operational might and provocative cybersecurity safety, and sustainable and scalable EV recharge network deployments in cybersecurity. While connectivity increases the level of monitoring and control, it also makes the infrastructure more vulnerable to cybersecurity threats such as spoofing, denial-of-service attacks and unauthorised access [5 - 6]. Compromised charging networks could be used to interfere with charging system-related services, as well as to manipulate billing data and possibly even to destabilise power systems. Therefore, the secure and intelligent charging operations have become a research priority [7].

There are recent innovations in edge computing and artificial intelligence (AI) that potentially provide the solution. Edge-AI powers processing at the point (where the battery is charging) - there is a latency problem and relying extensively on centralised cloud systems is a pose [8]. Distributed intelligence supports the detection of anomalies in real-time, adaptation of loads and optimisation of energy consumption [9]. In addition, fuzzy-logic inspired AI models have proved to be effective for handling uncertainty and multi-parameter decision-making, for cyber - physical energy systems [10].

To solve these issues, in this paper, a next-generation Edge-AI architecture for EV charging infrastructure is proposed to tackle these security challenges. By combining the distributed intelligence, cybersecurity monitoring, and intelligent load control, the proposed system has the following important contributions:

- Enables real-time anomaly detection and secure authentication at the edge to mitigate cyber threats promptly.
- Optimises charging load distribution to prevent grid congestion and voltage instability.
- Integrates EV battery health monitoring to ensure safe and efficient charging operations.
- Reduces response latency through decentralised Edge-AI decision-making.
- Enhances coordination between EVs, charging stations, and central energy servers.
- Improves infrastructure resilience by combining grid, vehicle, and cybersecurity analytics within a unified framework.

This includes an integrated approach strengthening the operational efficiency and advanced cyber security resilience, and sustainable and scalable deployment of secure EV charging networks.

2. Literature Survey

The rapid development of the EV infrastructure for charging has undergone extensive research, in particular in the areas of smart grid integration, cybersecurity and smart energy management. Numerous studies have been carried out regarding optimal ways of charging scheduling in order to reduce the peak demand and improve the stability of the grid [11-12]. These works focused on the coordinated charging strategies and demand response mechanisms to minimise voltage and stress fluctuations of the transformer of the distribution networks.

The development of smart grids has resulted in the use of AI and machine learning techniques in order to better optimise energy utilisation and perform predictive load management [13, 14]. AI-based predictive models, which permit the answering of a question, static load balancing and real-time adjustment of charging rate according to the conditions present on the grid. Besides, fuzzy logic-based control systems also proved successful in addressing energy demand and uncertainties in the environment [15], which offers flexible decision making mechanisms capable of addressing complex cyber-physical energy systems.

Edge computing, as a new paradigm for decentralised energy management, is interesting. Researchers [16-17] have proposed the usefulness of using the intelligence of computation at the edge of the network to minimise the time of latency and increase the reaction times for smart infrastructure applications. In application areas of EV charging, the edge architectures help in localised detection of anomalies and adaptive power allocation without excessive dependence upon the centralised servers in the cloud.

The specific example of the field of cybersecurity in EV charging systems has also been explored in detail. Secure communication protocols and authentication frameworks have been proposed to overcome unauthorised access to the charging transactions [18]. However, a number of vulnerabilities such as man- in-the-middle and denial of service attacks still pose a challenge to distributed charging ecosystems [19]. Recent research made the argument for integration of artificial intelligence (AI) driven intrusion detection systems for cyber resilience in smart grid infrastructure [20].

Despite such advancements, currently, research is often based on either optimisation of the grid, cybersecurity or battery management; each individually. A detailed Edge-AI architecture that simultaneously receives grid stress analysis, monitors the health of electric vehicles (EV) and detects cybersecurity threats in the mutually integrated decision-making framework is limited. This research, therefore, aims to reduce that gap by proposing a more intelligent, secure and distributed charging system architecture for the next generation EV charging systems.

The rest of this paper is organised as follows: Section III presents the objectives of the proposed framework; Section IV details the system architecture and Edge- AI modules; Section V discusses the simulation results and analytical evaluation; finally, Section VI concludes this paper by presenting future research directions.

3. Problem Statement and Research Objectives

The boom in EV charging infrastructure creates huge challenges in aspects of grid instability, cybersecurity vulnerabilities and inefficient load management. Existing centralised systems often have issues like high latency, low scalability, and fragmented grid, vehicle and security parameters monitoring. The lack of an integrated and real timeline decision framework puts communities at a high risk of overload, unsafe charging conditions and cyber attacks. Therefore, a secure, intelligent, and distributed Edge - AI - based architecture is needed to provide reliable and resilient EV charging operations.

The main goal of this research is to design and implement a secure, intelligent and scalable Edge-AI architecture for next-generation EV charging infrastructure. Specific objectives are stated below:

1. To create a decentralised architecture where the artificial intelligence capabilities are embedded at the EV-charging stations to enable low-latency decision-making capabilities while also reducing the reliance on the centralised cloud systems.
2. To have in place the adaptive load management mechanisms to monitor the voltage deviation, power demand and stress in the grid in real time and prevent congestion, overloading of the transformer and peak demand instability
3. To integrate the intelligent authentication verification and anomaly detection modules that identify cyber threats such as spoofing, unauthorised access and denial of service attacks in the charging infrastructure.
4. To incorporate a battery state of charge (SoC) and temperature monitoring mechanism that would ensure safe charging operations without overheating or damaging the battery, or which may cause dangerous conditions.
5. To establish a fuzzy logic-inspired decision model with a combination of grid conditions, e-vehicle health status and cybersecurity parameters for secure authorisation and prioritisation of charging.

6. To develop an end-to-end framework to improve system reliability, support massive charging station deployment, and improve the resiliency of the EV charge network to operational and cyber-physical system disruptions.

4. Proposed work

The architecture of the proposed system is given in Fig. 1. The integrated Edge-AI EV charging framework is a visualisation of the communication between the EV module, edge charging station, central energy server and the utility grid interface. The emphasis of the architecture is towards secure communication, distributed intelligence and real-time decision coordination.

The proposed architecture combines the distributed Edge-AI intelligence in EV-charging infrastructure for ensuring secure, adaptive, and efficient infrastructure operations. The system is comprised of four major components: EV Module, Edge Charging Station Module, Central Energy Management Server and Utility Grid & Operator Interface. Real-time monitoring of the grid parameters, the health of the EV battery, and cybersecurity conditions is done at the edge. A Mamdani fuzzy logistic model-based intelligence (AI) engine uses multi-parameter inputs to authorise charge sessions, optimise load distribution and control cyber-attackers and keep the grid stable.

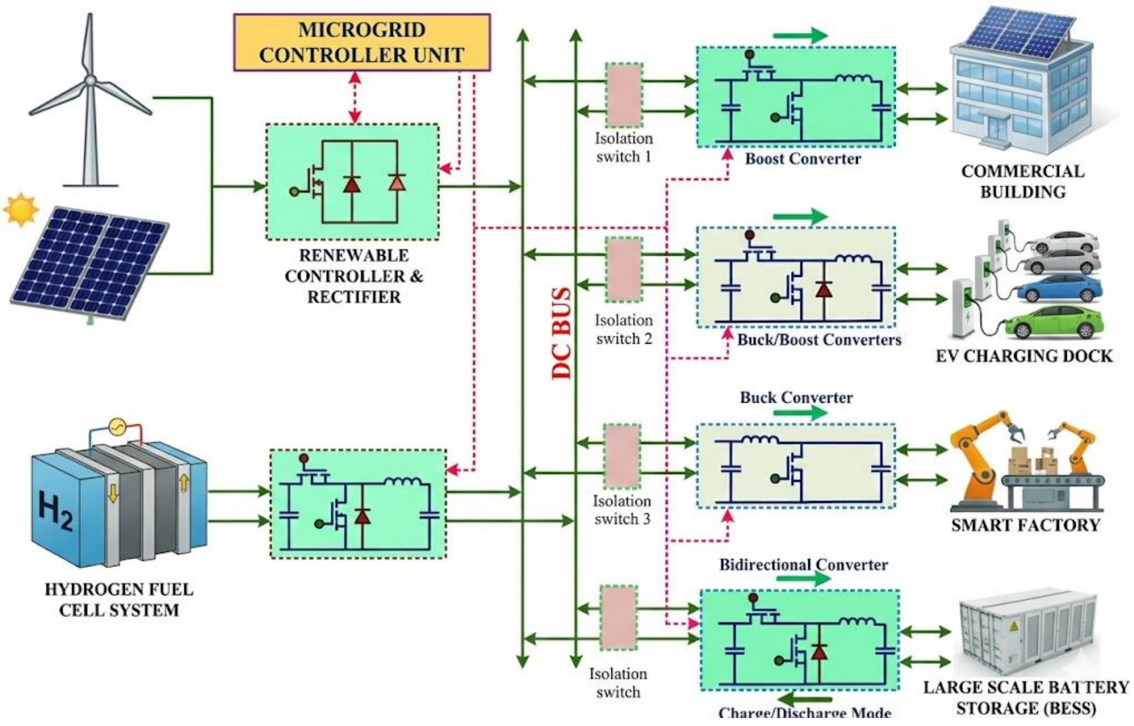


Fig. 1 Architecture of the Proposed Edge-AI EV Charging System

4.1 Selection of Sensors and Edge Hardware

The ***Edge Charging Unit (ECU)*** serves as the central intelligence layer of the proposed EV that incorporates sensing, integrated processing, secure communication, and an Edge-AI decision module together in each of the charging stations. It constantly monitors grid parameters, EV apartment batteries, and cybersecurity parameters, analyses them locally, and communicates the results to the central energy management system as needed. The architecture of the Edge Charging Unit (ECU) is shown in Fig.2.

1. Grid Monitoring Sensors

To ensure stability of the grid and avoid entering overload conditions, the ECU takes control of important parameters of electricity:

- **Voltage Fluctuation Sensor:** Detects variations from nominal voltage levels caused by load spikes or grid disturbances." On sensing any abnormality in the voltage drops or rising values, ECU dynamically adjusts the charging rates to prevent infrastructure damage to the grid.
- **Current Sensor:** Tests for the actual time charging demand check and the total current demand. This allows adaptive load balancing, peak-demand management and prevention of transformer or component overheating.

2. EV Health Monitoring

For safe and efficient charging, the ECU monitors the batteries that are essential parameters:

- **Battery State of Charge (SoC):** Keeps track of the amount of battery remaining and optimises charging priority so as not to overcharge.
- **Battery Temperature Sensor:** This provides detection of the risk of overheating due to charging. If unsafe temperatures are found, the charging power is applied less or suspended in order to avoid thermal hazards.

3. Cybersecurity Monitoring

To ensure police work in protecting connected charging infrastructure, ECU includes:

- **Authentication Token Integrity Monitor:** Grants access to the session to authenticate the user, avoiding unauthorised access and spoofing attacks on the user.
- **Network Latency Monitor:** Keep track of abnormal delays of communications, which can be transferred to cyber threats such as denial-of-service attacks.

By combining these modules, the ECU creates a safe, intelligent and adaptive control framework which keeps the grid stable, the EV operation is safe and cyber-physical resilience is increased.

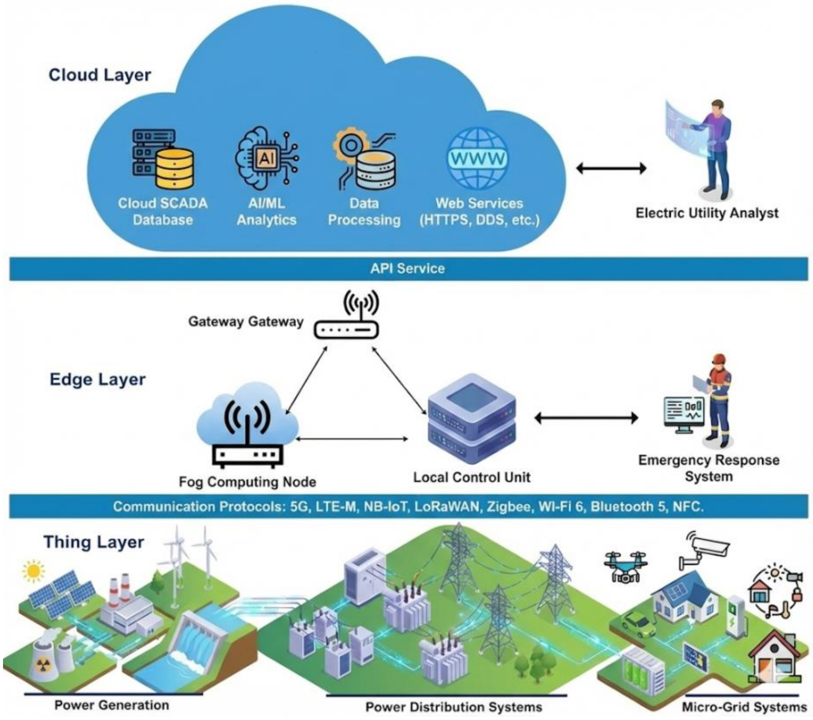


Fig.2 Edge Charging Unit (ECU) Hardware Architecture

4.2 Edge-AI Decision Support System

A Mamdani fuzzy logic-based AI engine is embedded inside the Edge Charging Unit (ECU) to enable real-time intelligent decision-making at each charging station. It is designed to handle the uncertainty and multi-parameter interactions of the EV charging environment using structured rule-based inference. The three basic modules of the engine are:

1. Grid Stability Module

This module analyses the voltage deviation and load variation to measure the levels of grid stress. Based on predefined membership functions and fuzzy rule sets, it classifies the grid conditions and adapts the charging power accordingly in order to guarantee that the grid is not overloaded, that the voltage is not unstable and that the transformer is not stressed.

2. EV Health Module

In other words, it evaluates the battery state of charge or SoC and temperature to determine the safety of the charging. The fuzzy rule base determines the abnormal conditions of the battery and controls or interrupts the charging process of the battery to prevent overheating and battery deterioration.

3. Cyber Threat Detection Module

This module keeps track of the integrity of authentication and network latency for possible cyber attacks. If the anomalies are detected, the charging sessions could be limited, or they could be shifted to secure operational modes.

Fuzzy Inference Process

The Mamdani engine performs:

- **Fuzzification** of sensor inputs,
- **Rule evaluation** using predefined decision rules, and
- **Defuzzification** to generate precise charging control actions.

This structured process ensures secure, adaptive, and stable EV charging operations at the edge.

4.3 *Membership Functions and AI Rules*

4.3.1 *Grid Stability Module*

The Grid Stability Module analyses electrical situations at the charging point with an aim to find the stress exerted in the distribution network as a result of electric vehicle (EV) charging operations.

Inputs:

- **Voltage Deviation (Low, Medium, High):**
- defective by the amount at which the measured voltage deviates from its nominal value, i.e. possible cause of instability due to a sudden spike on the scheme or from upgrips of the upstream grid.
- **Load Variation (Low, Medium, High):**
- shows the fluctuation of charging demand and current draw of the station, which is representative of dynamic changes in the level of power consumption.

Output:

- **Grid Stress Level (Low, Moderate, High):**
- Indicates the general effects of deviation and load variation voltages, overall stability of the network, and adaptation charging control decisions to avoid group overload or voltage collapse. Script Well-being.

Fig.3 (a), (b), and (c) show the membership functions (MF) of input and output parameter i.e. Voltage Deviation, Load Variation and Grid Stress Level, respectively.

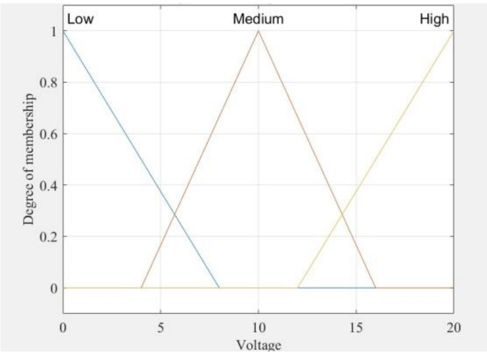


Fig. 3(a) MF of Voltage Deviation

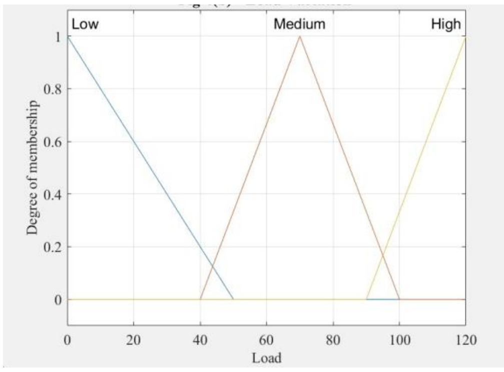


Fig. 3(b) MF of Load Variation

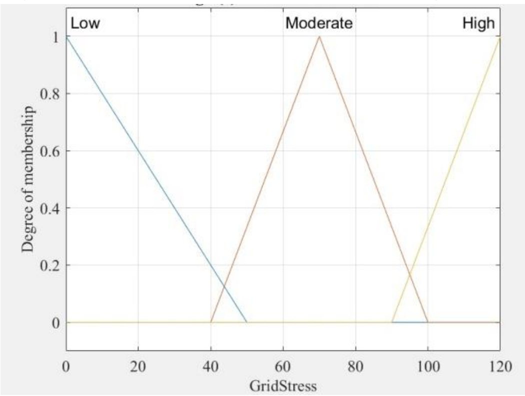


Fig. 3(c) MF of Grid Stress Level

Table 1 shows the fuzzy rule base for the Grid Stability Module, which establishes the connection between deviation of the voltage and load variation in order to determine the overall grid stress level. These rules are based on how to make a decision in the field of adaptive charging control operations, and maintain the voltage stability and avoid overloading the infrastructure.

Table 1: Fuzzy Rules for Grid Stability Module

Voltage Deviation	**Load Variation**	**Grid Stress Level**
Low	Low	Low
Low	Medium	Low
Low	High	Moderate
Medium	Low	Low
Medium	Medium	Moderate
Medium	High	High
High	Low	Moderate
High	Medium	High
High	High	High

Fuzzy Rules used in Table 1

Inputs: Voltage Deviation (Low, Medium, High)
Inputs: Load Variation (Low, Medium, High)
Output: Grid Stress (Low, Moderate, High)

1. IF Voltage is **Low** AND Load is **Low** THEN Grid Stress is **Low**
2. IF Voltage is **Low** AND Load is **Medium** THEN Grid Stress is **Moderate**
3. IF Voltage is **Low** AND Load is **High** THEN Grid Stress is **High**
4. IF Voltage is **Medium** AND Load is **Low** THEN Grid Stress is **Moderate**
5. IF Voltage is **Medium** AND Load is **Medium** THEN Grid Stress is **Moderate**
6. IF Voltage is **Medium** AND Load is **High** THEN Grid Stress is **High**
7. IF Voltage is **High** AND Load is **Low** THEN Grid Stress is **Moderate**

8. IF Voltage is **High** AND Load is **Medium** THEN Grid Stress is **High**
9. IF Voltage is **High** AND Load is **High** THEN Grid Stress is **High**

4.3.2 *EV Health Monitoring Module*

The EV Health Monitoring Module checks the battery-related parameters to ensure the safe, efficient and reliable charging operations.

Inputs:

- **Battery Temperature (Low, Medium, High):**
  Characterises the thermal condition of the EV battery when it is being charged; elevated temperatures possibly pose decent overheating dangers or unsanitary charging conditions.
- **State of Charge (Low, Medium, High):**
  shows the actual amount of energy in the battery, still remaining, and it is therefore favourable for determining charging priority as well as for preventing overcharging or deep discharge stress.

Output:

- **EV Health Risk (Low, Moderate, High):**
  represents a comprehensive measure of the safety and working status of the battery under different conditions (temperature and charging level) to ensure the control of the corresponding charging rate or the protective shutdown.

Fig. 4(a) shows the membership function of the Battery Temperature (Low, Medium, High), Fig. 4(b) shows the membership function of the State of Charge level, and Fig. 4(c) shows the membership function of the EV Health Risk, which is used for the safety regulation of charging.

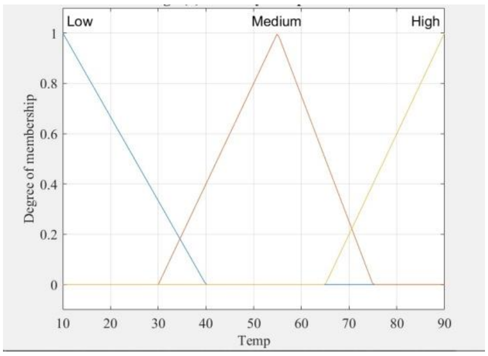


Fig 4. (a) MF of Battery Temperature

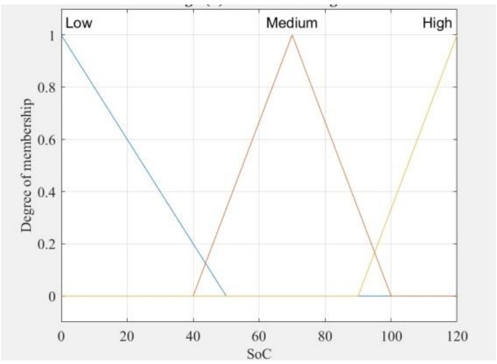


Fig 4. (b) MF of SoC

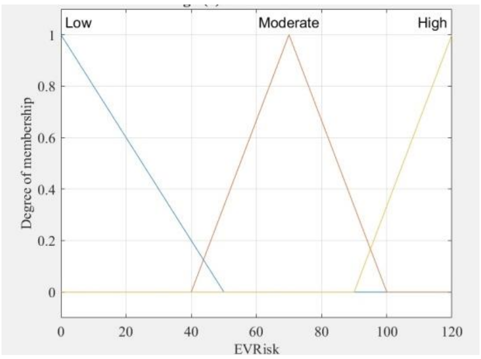


Fig 4. (c) MF of EV Health Risk

Table 2 defines the fuzzy rule base for the EV Health Monitoring Module, establishing the relationship between battery temperature and state of charge to determine the overall EV health risk level, enabling safe charging control and prevention of thermal or operational hazards.

Table 2: Fuzzy Fuzzy Rules for EV Health Module

Battery Temp	SoC	EV Health Risk
Low	High	Low
Low	Medium	Low
Low	Low	Moderate
Medium	High	Low
Medium	Medium	Moderate
Medium	Low	High
High	High	Moderate
High	Medium	High
High	Low	High

Fuzzy Rules used in Table 2

Inputs: Battery Temperature (Low, Medium, High)
Inputs: State of Charge (Low, Medium, High)
Output: EV Health Risk (Low, Moderate, High)

1. IF Temperature is **Low** AND SoC is **Low** THEN Risk is **Low**
2. IF Temperature is **Low** AND SoC is **Medium** THEN Risk is **Moderate**
3. IF Temperature is **Low** AND SoC is **High** THEN Risk is **High**
4. IF Temperature is **Medium** AND SoC is **Low** THEN Risk is **Moderate**
5. IF Temperature is **Medium** AND SoC is **Medium** THEN Risk is **Moderate**
6. IF Temperature is **Medium** AND SoC is **High** THEN Risk is **High**
7. IF Temperature is **High** AND SoC is **Low** THEN Risk is **High**
8. IF Temperature is **High** AND SoC is **Medium** THEN Risk is **High**
9. IF Temperature is **High** AND SoC is **High** THEN Risk is **High**

4.3.3 *Cybersecurity Monitoring Module*

The Cyber Threat Detection Module analyses parameters such as communication and authentication in order to guarantee safe and trustworthy EV charging operations.

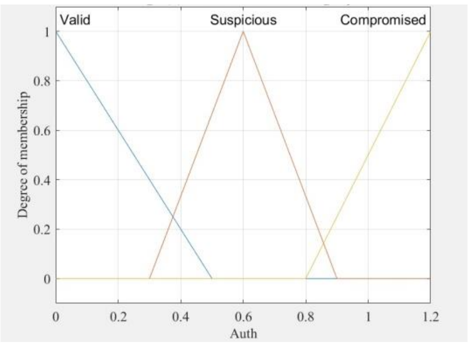
Inputs:

- **Authentication Integrity (Valid, Suspicious, Compromised):**
- Charge-relevant authentication integrity and validity (valid = Good), charging - Compromised Authentication can refer to charged authorization. (Compromised Auth) could go down to Suspicious Auth. Charge has valid, suspicious, and compromised authentication functions inɯɲɰɯɕovdesks.de, which is the relevant network of the client and server.
- **Network Latency (Low, Medium, High):**
- Measures communication delay between the EV, the charging station, and the central server. Unusually high latency may indicate network congestion or DoS cyberattacks.

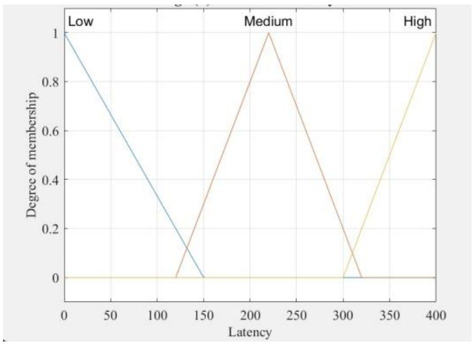
Output:

- **Cyber Threat Level (Low, Moderate, High):**
- Refers to the level of security threat of the charging session overall and therefore determines the protection measures to be taken, such as monitoring the session, restricting it, or terminating it.

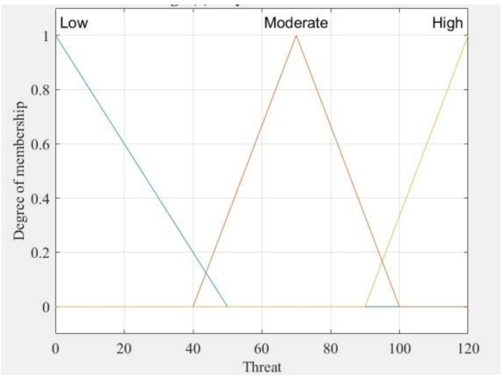
Fig. 5(a) presents the membership function of Authentication Integrity, Fig. 5(b) represents the membership function for Network Latency levels, and Fig. 5(c) represents the membership function for Cyber Threat Level, which is utilised for deciding control for secure charging.



(Fig. 5(a) MF of Authentication Integrity)



(Fig. 5(b) MF of Network Latency)



(Fig. 5(c) MF of Cyber Threat Level)

Table 3 gives the fuzzy rule base for the Cyber Threat Detection Module. The relation between the integrity of authentication and the latency of the network is required to identify the overall level of cyber threat. This can help to validate the sessions securely and protect from any unauthorised or malicious charging activities.

Table 3: Fuzzy Rules for Cybersecurity Module

Auth Integrity	Latency	Cyber Threat Level
Valid	Low	Low
Valid	Medium	Low
Valid	High	Moderate
Suspicious	Low	Moderate
Suspicious	Medium	Moderate
Suspicious	High	High
Compromised	Low	High
Compromised	Medium	High
Compromised	High	High

Fuzzy Rules used in Table 3

Inputs: Authentication Integrity (Valid, Suspicious, Compromised)
Inputs: Network Latency (Low, Medium, High)
Output: Cyber Threat Level (Low, Moderate, High)

1. IF Authentication is **Valid** AND Latency is **Low** THEN Threat is **Low**
2. IF Authentication is **Valid** AND Latency is **Medium** THEN Threat is **Moderate**
3. IF Authentication is **Valid** AND Latency is **High** THEN Threat is **High**
4. IF Authentication is **Suspicious** AND Latency is **Low** THEN Threat is **Moderate**
5. IF Authentication is **Suspicious** AND Latency is **Medium** THEN Threat is **Moderate**
6. IF Authentication is **Suspicious** AND Latency is **High** THEN Threat is **High**
7. IF Authentication is **Compromised** AND Latency is **Low** THEN Threat is **High**
8. IF Authentication is **Compromised** AND Latency is **Medium** THEN Threat is **High**
9. IF Authentication is **Compromised** AND Latency is **High** THEN Threat is **High**

4.3.4 *Secure Charging Decision Module*

The Secure Charging Decision Module takes inputs from all the previous modules and decides whether to either continue charging, delay or prohibit it.

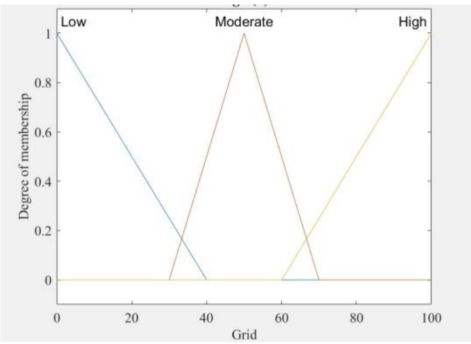
Inputs:

- **Grid Stress Level:**
- That represents the current load situation of the distribution network and thereby ensures that the charging decisions will not affect the stability of the grid.
- **EV Health Risk:**
- Indicates the safety status of the battery connected to the vehicle, avoiding unsafe charging under thermal/operational stress.
- **Cyber Threat Level:**
- Reflects the security condition of the charging session, to provide the security of such activity from unauthorised access or malicious activity.

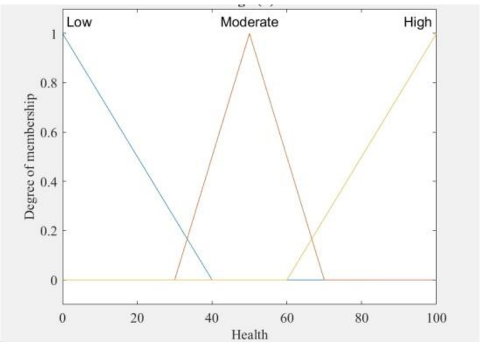
Output:

- **Charging Permission & Priority Index (Allow, Delay, Block):**
- Determines whether charging is permitted immediately, postponed due to risk factors, or blocked to protect infrastructure and user safety.

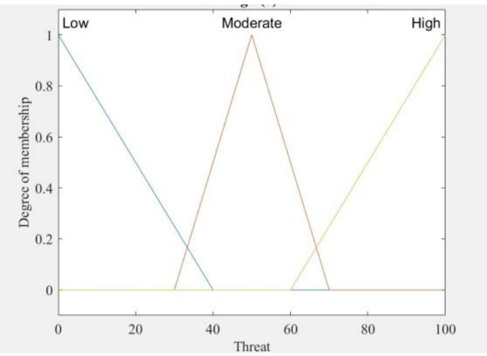
Fig. 6(a) represents the membership function for Grid Stress Level, Fig. 6(b) the EV Health Risk, Fig. 6(c) shows Cyber Threat Level and Fig. 6(d) the Charging Permission & Priority Index used for final decision making.



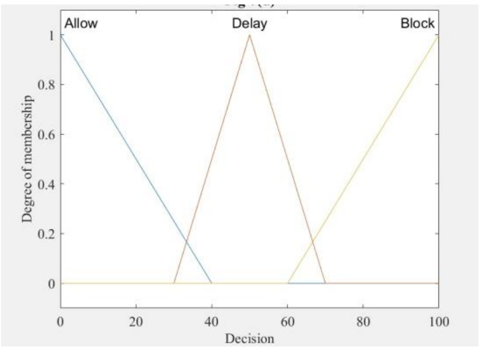
(Fig. 6(a) MF of Grid Stress)



(Fig. 6(b) MF of EV Health)



(Fig. 6(c) MF of Cyber Threat)



(Fig. 6(d) MF of Charging Decision Index)

Table 4 presents the integrated fuzzy rule base for the Secure Charging Decision Module, which includes a combination of grid stress level, EV health risk, and cyber threat level for identifying the final result or charging permission and priority index for safe and secure operation.

Table 4: Fuzzy Rules for Secure Charging Decision Module

Grid Stress	EV Health Risk	Cyber Threat	Charging Decision
Low	Low	Low	Allow
Low	Moderate	Low	Allow
Low	High	Low	Delay
Moderate	Low	Low	Allow
Moderate	Moderate	Moderate	Delay
Moderate	High	Low	Delay
High	Low	Low	Delay
High	Moderate	Moderate	Delay
High	Any	High	Block
Any	Any	High	Block

Fuzzy Rules used in Table 4

Inputs: Grid Stress (Low, Moderate, High)
Inputs: EV Health Risk (Low, Moderate, High)
Inputs: Cyber Threat Level (Low, Moderate, High)
Output: Charging Decision (Allow, Delay, Block)

Case 1: All Conditions Low

1. IF Grid Low AND Health Low AND Threat Low THEN Allow

Case 2: Any Single Moderate Risk

2. IF Grid Moderate AND Health Low AND Threat Low THEN Delay
3. IF Grid Low AND Health Moderate AND Threat Low THEN Delay
4. IF Grid Low AND Health Low AND Threat Moderate THEN Delay

Case 3: Any High Threat

5. IF Threat High AND Grid Low AND Health Low THEN Block
6. IF Threat High AND Grid Moderate AND Health Low THEN Block
7. IF Threat High AND Grid High AND Health Low THEN Block
8. IF Threat High AND Health Moderate THEN Block
9. IF Threat High AND Health High THEN Block

Case 4: High Grid Stress

10. IF Grid High AND Health Low AND Threat Low THEN Delay
11. IF Grid High AND Health Moderate THEN Block
12. IF Grid High AND Health High THEN Block

Case 5: High EV Health Risk

13. IF Health High AND Threat Low AND Grid Low THEN Delay
14. IF Health High AND Threat Moderate THEN Block
15. IF Health High AND Grid Moderate THEN Block

Case 6: Multiple Moderate Risks

16. IF Grid Moderate AND Health Moderate AND Threat Low THEN Delay
17. IF Grid Moderate AND Threat Moderate THEN Block
18. IF Health Moderate AND Threat Moderate THEN Block

Case 7: All Moderate

19. IF Grid Moderate AND Health Moderate AND Threat Moderate THEN Block

Case 8: All High

20. IF Grid High AND Health High AND Threat High THEN Block

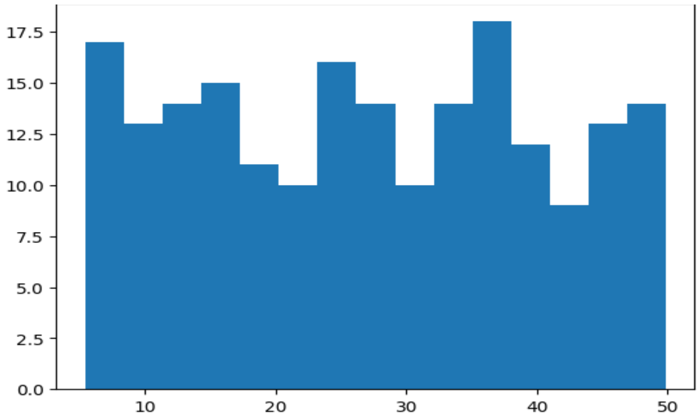
Remaining Combinations (Safe Bias Control)

21–27. Any combination where two or more inputs are High → Block

The final module guarantees that charging will only be authorised under safe grid conditions, acceptable EV health and secure communication integrity, which will enable a strong and intelligent charging infrastructure that is secure.

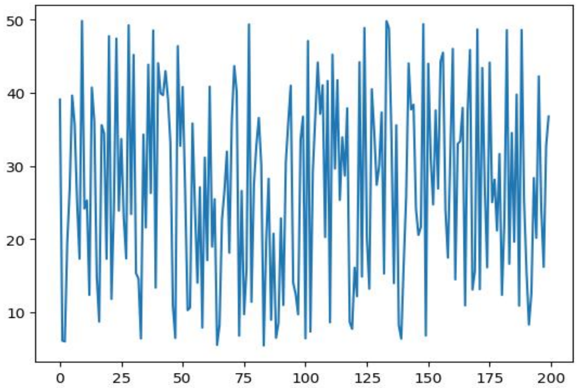
5. Result and Analysis

Fig. 7(a) shows the statistical distribution of charging loads for several EV charging sessions. The histogram has frequency variation within delimited power ranges (kW). The major part of charging sessions is located in the moderate load band, pointing to a balance of demand under Nell management Edge-ai scheduling. High load occurrences are limited because of adaptive load optimisation and therefore demonstrate improved peak load management and reduced grid stress.



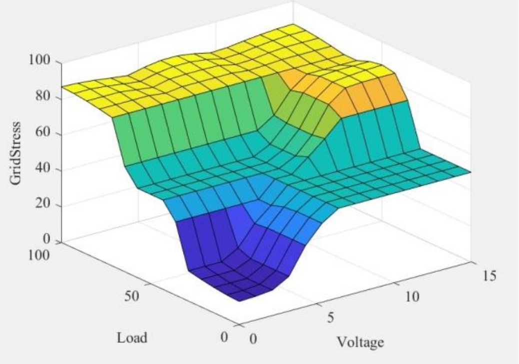
(Fig. 7 (a) Histogram of Charging Load Distribution)

Time Series Variation of Charging Load Fig. 7(b) shows the time series variation of charging load. Sudden spikes are an indicator of anomalous behaviour like unauthorised access attempts or abnormal demand. The Edge-AI system detects anomalies to be intervened on. Results confirm the value of real-time monitoring that allows for rapid mitigation of unstable charging patterns.

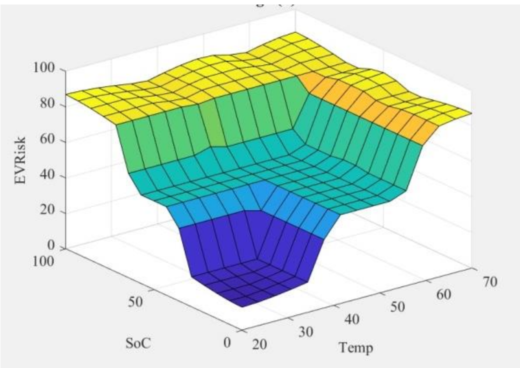


(Fig.7 (b) Variation of Charging Load and Anomaly Occurrence)

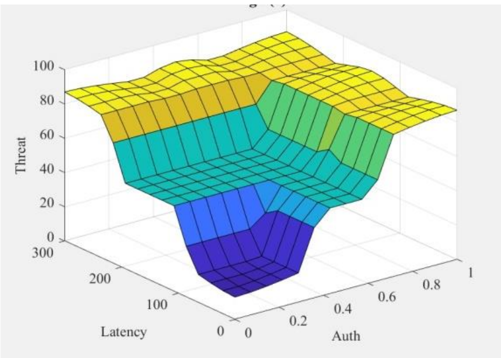
The surface plot of Grid Stability is shown in Fig. 8(a), the surface of the EV Health evaluation is shown in Fig. 8(b), the surface of Cybersecurity Threat is shown in Fig. 8(c), and lastly, the surface of Charging Decision Index is shown in Fig. 8(d), obtained through the fuzzy inference method.



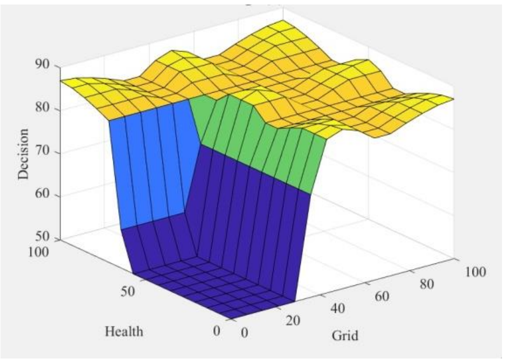
(Fig. 8(a) Surface Plot of Grid Stability)



(Fig. 8(b) Surface Plot of EV Health)

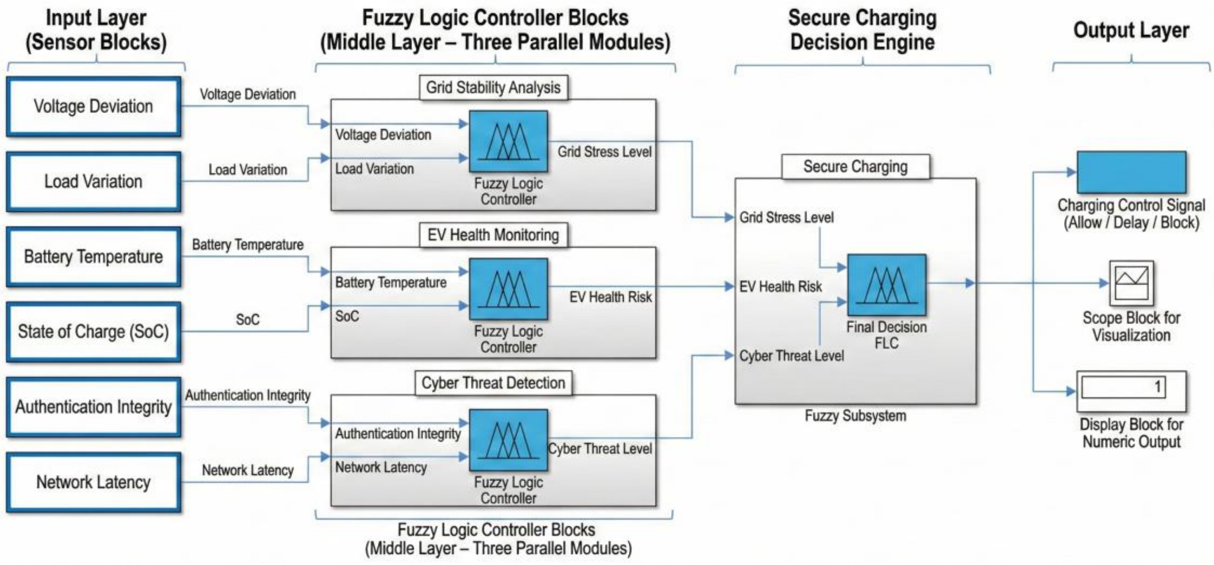


(Fig. 8(c) Surface Plot of Cybersecurity Threat)



(Fig. 8(d) Surface Plot of Charging Decision Index)

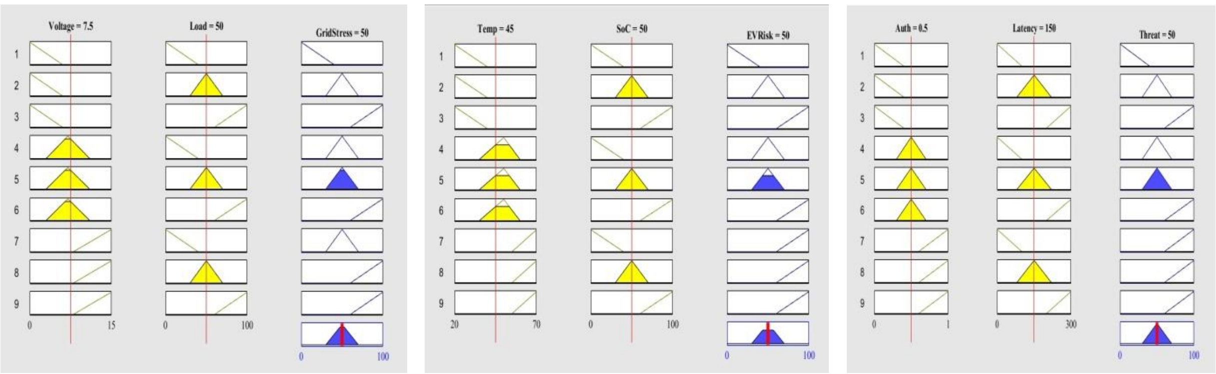
Surface plots: the surface plot is a representation of a three-dimensional fuzzy inferential relationship between inputs and outputs. The stability surface of the grids indicates that increasing voltage deviation and intensity will cause more stress. The EV health surface shows the risk at high temperature levels with low SoC. Cybersecurity surface plots provide evidence of increasing threat levels under compromised authentication and high latency. The final decision surface combines all parameters to create the secure authorisation of charging. The Simulink model of the proposed Edge-AI model is shown in Fig.9.



(Fig.9 Simulink/Edge-AI Simulation Model Representation)

5.1 Rule Viewer Analysis

The Fuzzy inference transparent representation provided by the Rule Viewer shows active rules, activation level of membership, and the aggregate output. This helps in understanding the effect of the combination of the inputs on the final decisions and also helps in verifying the logical consistency of the rule base of the fuzzy system. The Rule Viewer outputs of the three main fuzzy logic modules are shown in Figure 10. In Fig. 10(a), in the case of medium voltage deviation and High load variation, the Grid Stability Module concludes on the basis of this situation that the level of grid stress is around 78 %, which is considered to signal an overload risk situation and requires charging regulation. In Fig. 10(b), when the battery temperature is High and the State of Charge (SoC) is Low, the EV Health Module calculated the health risk value close to 85%, indicating unsafe charging conditions. In Fig. 10(c), when the authentication status is Suspicious, and the network latency is High, the Cyber Threat detection Module represents the threat level approaching 82 %, which implies a possible security compromise.



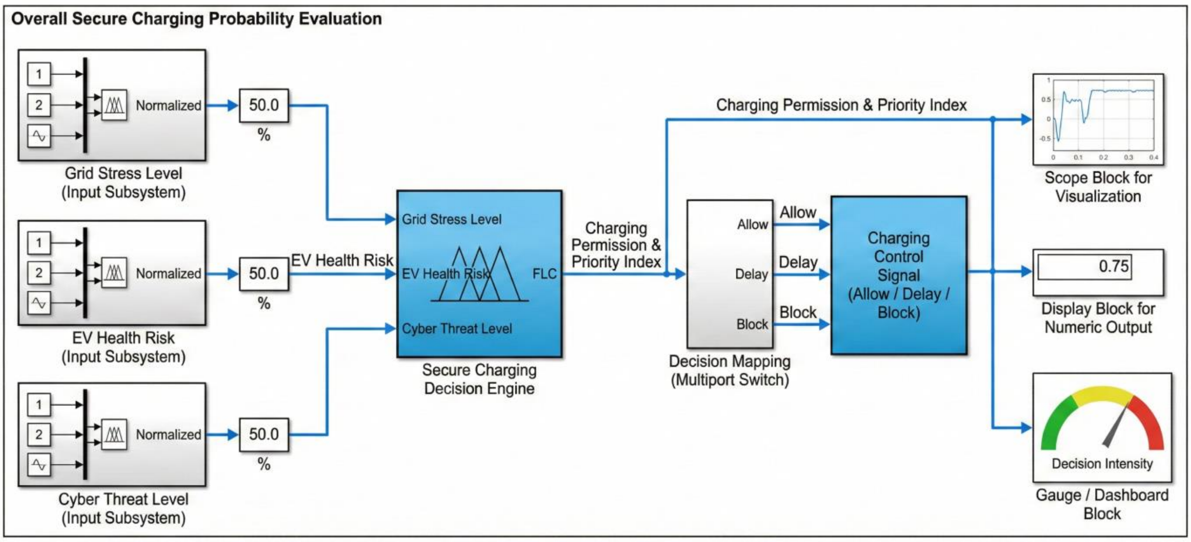
(Fig.10. (a) Rule Viewer of Grid Stability)

(Fig.10. (b) Rule Viewer of EV Health)

(Fig.10. (c) Rule Viewer of Cyber Threat)

(Fig.10 Rule Viewer outputs of the three main fuzzy logic modules)

5.2 Overall Secure Charging Impact



(Fig.11 Overall Secure Charging Probability Index)

Fig. 11 shows the overall secure charging decision model, in which grid stress level, EV health risk and cyber threat level are combined using the Mamdani fuzzy inference engine to generate the final charging permission and priority index.

6. Future Scope and Conclusion

The Edge Artificial Intelligence architecture proposed in our paper can potentially be further developed in future research work, involving the integration of real-time renewable energy (solar, wind) in EV charging optimization frameworks. Advanced models using deep learning could be used instead of rule-based fuzzy computing for predictive anomaly detection and adaptive energy forecast. Blockchain-based secure transaction mechanisms could help further improve authentication and billing transparency. In addition, large-scale field deployment and hardware-in-the-loop validation may help to strengthen the robustness of the system. The combination of the vehicle-to-grid (V2G) capabilities and federated learning methodologies may provide superior distributed intelligence, scalability and resilience in the next generation of secure electric vehicle (EV) charging infrastructures.

This paper describes the design of a safe and distributed Edge AI architecture targeted towards the future evolution of EV charging systems. By combining the monitoring of grid stability, testing the health of EV batteries and the identification of threats from cybersecurity in a fuzzy inference system, the real-life resilience of the system is fundamentally improved. The proposed methodology aims to reduce the strain on the grid by means of adaptive load management, countering cyber threats in real-time and supplementing the charging efficiency of the energy grids through smart authorisation controls. An edge-first design can ensure low latency, scalability and strong infrastructural security. Consequently, architecture helps to create solid foundations for safe and smart energy management in a collaborative EV ecosystem in the current picture.

References:

[1] Al-Dahabreh, N., Sayed, M. A., Sarieddine, K., Elhattab, M., Khabbaz, M. J., Atallah, R. F., & Assi, C. (2023). A data-driven framework for improving public EV charging infrastructure: Modeling and forecasting. *IEEE Transactions on Intelligent Transportation Systems*, *25*(6), 5935-5948.doi: https://doi.org/10.1109/TITS.2023.3337324

[2] Sultan, V., Aryal, A., Chang, H., & Kral, J. (2022). Integration of EVs into the smart grid: A systematic literature review. *Energy Informatics*, *5*(1), 65.doi: 10.1186/s42162-022-00251-2

[3] Koundinya, N. S., Vignesh, S., Narayanan, K., Sharma, G., & Senjyu, T. (2020, November). Voltage stability analysis of distribution systems in the presence of electric vehicle charging stations with uncoordinated charging scheme. In *2020 International Conference on Smart Grids and Energy Systems (SGES)* (pp. 303-308). IEEE.doi: https://doi.org/10.1109/SGES51519.2020.00060

[4] Muthukaruppan, V., Baran, M., Lu, N., Rehm, P. J., Miller, E., & Makdad, M. (2022, April). Overloading analysis of distribution transformers using smart meter data. In *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1-5). IEEE.doi: https://doi.org/10.1109/ISGT50606.2022.9817534

[5] Skarga-Bandurova, I., Kotsiuba, I., & Biloborodova, T. (2022, December). Cyber security of electric vehicle charging infrastructure: Open issues and recommendations. In *2022 IEEE International Conference on Big Data (Big Data)* (pp. 3099-3106). IEEE.doi: https://doi.org/10.1109/BigData55660.2022.10020644

[6] Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEe Access*, *9*, 29775-29818.doi: https://doi.org/10.1109/ACCESS.2021.3058403

[7] Ismail, M., & Ahmed, R. (2024). A comprehensive review of cloud-based lithium-ion battery management systems for electric vehicle applications. *IEEE Access*, *12*, 116259-116273.doi: https://doi.org/10.1109/ACCESS.2024.3446880

[8] Younis, A., Maheshwari, S., & Pompili, D. (2024). Energy-latency computation offloading and approximate computing in mobile-edge computing networks. *IEEE Transactions on Network and Service Management*, *21*(3), 3401-3415.doi: https://doi.org/10.1109/TNSM.2024.3360850

[9] Kumar, A., Alaraj, M., Rizwan, M., & Nangia, U. (2021). Novel AI based energy management system for smart grid with RES integration. *IEEE Access*, *9*, 162530-162542.doi: https://doi.org/10.1109/ACCESS.2021.3131502

[10] Queiroz, J., Leitão, P., & Oliveira, E. (2022). A fuzzy logic recommendation system to support the design of cloud-edge data analysis in cyber-physical systems. *IEEE Open Journal of the Industrial Electronics Society*, *3*, 174-187.doi: https://doi.org/10.1109/OJIES.2022.3152725

[11] Liu, J., Lin, G., Huang, S., Zhou, Y., Li, Y., & Rehtanz, C. (2020). Optimal EV charging scheduling by considering the limited number of chargers. *IEEE Transactions on Transportation Electrification*, *7*(3), 1112-1122.doi: https://doi.org/10.1109/TTE.2020.3033995

[12] Vardakas, J. S., Zorba, N., & Verikoukis, C. V. (2014). A survey on demand response programs in smart grids: Pricing methods and optimization algorithms. *IEEE Communications Surveys & Tutorials*, *17*(1), 152-178.doi: https://doi.org/10.1109/COMST.2014.2341586

[13] Eseye, A. T., Lehtonen, M., Tukia, T., Uimonen, S., & Millar, R. J. (2019). Machine learning based integrated feature selection approach for improved electricity demand forecasting in decentralized energy systems. *IEEE Access*, *7*, 91463-91475.doi: https://doi.org/10.1109/ACCESS.2019.2924685

[14] Torkamani, M. M., Khodabakhshi-Javinani, N., & Valizadeh, S. (2025, December). An AI-Driven Integrated Framework for EV Charging: Demand Forecasting, Load Balancing, SoC Estimation, and Cybersecurity. In *2025 15th Smart Grid Conference (SGC)* (pp. 1-7). IEEE.doi: https://doi.org/10.1109/SGC69320.2025.11372419

[15] Acun, F., & Çunkaş, M. (2023). Low-cost fuzzy logic-controlled home energy management system. *Journal of Electrical Systems and Information Technology*, *10*(1), 31.doi: 10.1186/s43067-023-00100-6

[16] Khan, L. U., Yaqoob, I., Tran, N. H., Kazmi, S. A., Dang, T. N., & Hong, C. S. (2020). Edge-computing-enabled smart cities: A comprehensive survey. *IEEE Internet of Things journal*, *7*(10), 10200-10232. doi: https://doi.org/10.1109/JIOT.2020.2987070

[17] Strasser, T., Andren, F., Kathan, J., Cecati, C., Buccella, C., Siano, P., ... & Mařík, V. (2014). A review of architectures and concepts for intelligence in future electric energy systems. *IEEE Transactions on Industrial Electronics*, *62*(4), 2424-2438.doi: https://doi.org/10.1109/TIE.2014.2361486

[18] Kwon, D., Son, S., Park, K., Das, A. K., & Park, Y. (2024). Design of blockchain-based multi-domain authentication protocol for secure EV charging services in V2G environments. *IEEE Transactions on Intelligent Transportation Systems*, *25*(12), 21783-21795. doi: https://doi.org/10.1109/TITS.2024.3472013

[19] Kurt, M. N., Ogundijo, O., Li, C., & Wang, X. (2018). Online cyber-attack detection in smart grid: A reinforcement learning approach. *IEEE Transactions on Smart Grid*, *10*(5), 5174-5185.doi: https://doi.org/10.1109/TSG.2018.2878570

[20] Andronikidis, G., Eleftheriadis, C., Batzos, Z., Kyranou, K., Maropoulos, N., Sargsyan, G., ... & Sarigiannidis, P. (2024, September). Ai-driven anomaly and intrusion detection in energy systems: Current trends and future direction. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 777-782). IEEE.doi: https://doi.org/10.1109/CSR61664.2024.10679380