International Journal of ADVANCED RESEARCH & INNOVATIONS

Volume 1, Issue-11
November, 2025, P03
ISSN: 2319-9253

SECURE ENERGY DEMAND PREDICTION FOR ELECTRIC VEHICLES USING FEDERATED LEARNING ON BLOCKCHAIN

[1]Bandipelly Harish Kumar, M.Tech, Dept of CSE,
[2]Dr. D. Srinivas Reddy, Professor, Department of CSE,
Vaageswari College of Engineering (Autonomous), Karimnagar, Telangana.

Abstract: This investigation employs blockchain technology and federated learning to develop a novel approach to accurately forecast the energy requirements of electric vehicles (EVs). It has become increasingly challenging to accurately forecast the amount of energy required while simultaneously safeguarding data privacy and security as more individuals adopt electric vehicles. Federated learning safeguards user privacy by enabling energy providers and electric car manufacturers to collaborate in the development of predictive models without transmitting raw data to one another. The decentralized ledger and smart contracts of blockchain technology simultaneously safeguard data security, transparency, and trust. The comprehensive approach effectively anticipates fluctuations in energy consumption while simultaneously addressing significant challenges related to scalability, security, and privacy. The results of the experiments indicate that this architecture is effective in safeguarding private data from intruders and enabling smart grids to manage their energy in a reliable and long-lasting manner. This research offers a robust approach to enhance the safety and utility of EV energy demand forecasting.

Keywords: Electric Vehicles, Energy Demand Prediction, Federated Learning, Blockchain Technology, Data Privacy, Smart Grid, Decentralized Learning, Secure Energy Management, Smart Contracts, Cybersecurity

1. Introduction

The transition to environmentally favorable transportation has been expedited by concerns regarding the environment, new laws, and advancements in battery technology, resulting in an increase in the number of individuals purchasing electric vehicles (EVs). The current power source is incredibly challenging to integrate with electric vehicles due to the unpredictable and constantly changing charging requirements. It is crucial to accurately predict the amount of energy that electric vehicles will consume in order to maintain the stability of the grid, effectively manage energy, and reduce the high loads that can place a strain on the power infrastructure. Traditional centralized data collection methods for demand forecasting raise a multitude of privacy and security concerns due to the sensitive nature of user data, including location, driving patterns, and payment habits. We urgently need new technologies that can accurately predict energy requirements while simultaneously safeguarding data privacy and security in an open manner.

Federated Learning (FL) enables individuals to train models on their own devices without the necessity of sharing raw data. It is an intriguing approach to employing machine learning to resolve these issues. Federated learning enables each electric car or charging station to utilize its own private datasets for the purpose of training a local predictive model. This aids in the forecasting of the energy requirements of electric vehicles. Only model modifications are transmitted to a central aggregator or peer node. This approach simultaneously safeguards user privacy and mitigates the likelihood of unauthorized entry and data intrusions. Nevertheless, federated learning systems are challenging to operate due to issues with the quality of the data, the reliability of the nodes involved, and potential assaults on model updates, such as poisoning or inference attacks. Therefore, it is crucial to implement rigorous security protocols within the FL framework to guarantee the reliability and robustness of training procedures.

Blockchain technology enhances the security and reliability of federated learning environments by maintaining transparent records of all transactions and model modifications that can be verified. The blockchain maintains a record of the contributions made by each individual. This record is irrevocable, which guarantees accountability and discourages misconduct. By automating duties such as model collection, reward distribution, and update validation, smart contracts, which are self-executing protocols written on the blockchain, can also reduce the necessity of trusting third parties. By combining blockchain and federated learning, a framework is established that is effective in generating secure and private predictions regarding the energy consumption of electric vehicles. Additionally, it fosters collaboration among numerous entities, including energy providers, grid operators, and vehicle proprietors.

Due to the ever-changing and intricate nature of EV charging patterns, it is imperative that we implement sophisticated predictive analytics that can accommodate a variety of non-IID (not independent and identically distributed) data distributions across various vehicles and locations. The safe framework of blockchain technology and its capacity to combine various categories of data from various independent sources enable more precise energy use forecasts. This enhanced capacity to anticipate the future could assist grid operators in the implementation of demand response strategies, the planning of infrastructure enhancements, and the optimal utilization of energy distribution. In addition to reducing running costs, synchronizing EV charging with the patterns of renewable energy sources also enhances energy demand forecasting, which in turn promotes the broader use of renewable energy sources and makes users happier by reducing charging wait times.

Despite the potential advantages, the utilization of secure federated learning on blockchain for the prediction of electric vehicle energy requirements is plagued by operational and technical challenges. This encompasses the determination of how to address the restricted computing capabilities of peripheral devices, such as charging stations and automobiles, the maintenance of low communication costs among distributed nodes, the expeditious implementation of model modifications, and the assurance that the system can expand to accommodate additional electric vehicles (EVs). It is imperative that these systems are capable of adhering to data security regulations, such as GDPR, during the construction process. Scientists and engineers are currently investigating the most effective federated learning algorithms, blockchain structures, and consensus protocols to circumvent these challenges. Ultimately, the development of this comprehensive strategy is essential for the establishment of a long-lasting, stable, and advanced electric mobility ecosystem that achieves a harmonious equilibrium between energy efficiency, privacy, and security.

2. Literature Review

Sharma, P., & Rao, M. (2020). This study investigates the potential of neural networks to incorporate behavioral information into models that forecast short-term burden. The authors develop a model that incorporates both conventional load variables and behavioral data, as they are aware that the energy consumption of each user is significantly influenced by their habits and preferences. Forecasting employs neural networks to identify temporal patterns and nonlinear relationships in energy consumption data. Experiments demonstrate that forecasts are significantly more precise than baseline models when customer behavior is incorporated. This implies that utilities and grid administrators can generate more precise predictions regarding demand. Our research has facilitated the development of personalized energy demand forecasts, which are essential for the effective administration of electric vehicle charging loads.

Zhang, Y., Li, X., & Chen, H. (2021). This investigation examines the difficulty of predicting the energy consumption of electric vehicles in smart grids with a federated learning architecture. This method safeguards user privacy and data sovereignty by enabling a network of EV owners and grid administrators to collaborate on the development of a global prediction model without the exchange of raw data. Local model modifications are centrally collected on a server as part of federated learning. This process also encompasses strategies for managing the fact that participants' data is dispersed in various manners. The model enhances the precision of predictions by accounting for the intricate temporal patterns of electric vehicle charging requirements. These authors examine the system's resilience and privacy, demonstrating that federated learning is an effective approach to autonomous energy management in smart grids.

Kumar, S., & Singh, R. (2021). The proposed research proposes the implementation of a blockchain-based shared learning system to enhance the safety of predicting the necessity for electric vehicle charging stations. The framework is capable of effectively managing model modifications and participant identification due to the immutable ledger and decentralized consensus of blockchain technology. The authors safeguard the joint training process from hacking and prevent malicious model poisoning assaults by integrating blockchain technology with federated learning. Furthermore, the system facilitates the training of members of the community on their electric vehicle owner devices, thereby safeguarding data privacy. The simulations demonstrate that the hybrid approach is more dependable and secure than conventional centralized methods, and it also generates highly precise predictions. This implies that it is suitable for implementation in actual electric vehicle charging systems.

Wang, J., Chen, K., & Yang, F. (2022). The authors present a federated learning approach that ensures the security of information while monitoring the energy consumption of electric vehicles. Decentralized model training between electric vehicles or charging stations is a significant component of the process. Privacy protection mechanisms, such as differential privacy or secure aggregation, are implemented to prevent data from leaking. The model is capable of responding to the dynamic, non-independent, and non-iid characteristics that are prevalent in the charging patterns of electric vehicles (EVs). The proposed structure significantly reduces privacy concerns while maintaining accuracy levels that are comparable to those of centralized models, as demonstrated by numerous tests. This research demonstrates that it is feasible to implement dependable smart grid applications by demonstrating the potential of privacy-friendly predictive analytics in energy management systems for electric vehicles.

Liu, Z., & Xu, Y. (2022). This article discusses a blockchain-based federated learning system that can be employed to forecast demand in networks of recharge points for electric vehicles. Blockchain technology is employed to manage model changes made by participating electric vehicles and charging stations in a manner that is secure, transparent, and impossible to hack. Smart contracts increase output and reduce the likelihood of fraud by automating the validation and collection processes. The federated learning model accurately forecasts charging demand by analyzing the patterns of service usage over time, without retaining private user information in a single location. The authors propose a viable solution for the secure prediction of the load of electric vehicles. They accomplish this by executing scenarios that demonstrate the enhancement of data privacy, model accuracy, and system resilience through the implementation of this unified approach.

Patel, D., & Shah, A. (2022). This research integrates blockchain technologies and federated learning to develop a secure model for predicting energy requirements in electric vehicle networks. The hybrid design addresses several critical issues in collaborative EV energy forecasting, including data privacy, security, and potential for expansion. Federated learning enables decentralized training to occur without the exchange of raw data, while blockchain ensures that data and model interactions can be monitored and cannot be altered. The authors demonstrate the efficacy of their approach by conducting numerous tests that demonstrate its ability to accurately predict while simultaneously reducing data corruption and unauthorized access. The results indicate that there is a significant amount of potential for secure, scalable energy control in networks that are accommodating an increasing number of electric vehicles.

Chen, T., & Wu, L. (2023). In this article, a decentralized approach to predicting the necessity of electric vehicle charging stations is demonstrated by integrating blockchain technology with federated learning. The method fosters trust and transparency by enabling local models to be trained on-site at specific EV charging stations and cars, as well as by utilizing a blockchain-based ledger to communicate encrypted model changes. The decentralized design enhances the system's resilience and reduces the number of single points of failure by decreasing the reliance on centralized servers. Experiments demonstrate that this approach safeguards model update transactions, maintains privacy, and generates precise demand forecasts. This work enhances the efficiency of distributed energy control systems in smart cities.

Gupta, A., & Joshi, P. (2023). The authors propose a shared learning system that is blockchain-based and that would enable the prediction of the energy requirements of electric vehicles while simultaneously safeguarding privacy. In this method, federated learning is employed to construct a global forecast model from multiple distributed EV datasets, while maintaining the raw data's original geographic location. Blockchain technology enables model training methods to maintain an immutable record, thereby facilitating auditing and fostering trust among participants. The integrated system resolves the challenges of secure communication, privacy protection, and data sharing. Experiments demonstrate that the system can be effortlessly integrated into smart grid platforms, as it enhances the precision of forecasts and offers robust safeguards against data intrusions.

Zhang, L., & Zhao, Q. (2023). This study employs a mixed method that integrates federated learning and blockchain technology to analyze decentralized electric vehicle charging load predictions. The proposed solution employs a blockchain network to ensure the secure transmission of encrypted model parameters and the local training of models by electric vehicles and charging stations. The blockchain's smart contracts regulate the methods of consensus and access, thereby preventing malicious actors from committing unlawful acts and ensuring the security of data. The authors demonstrate that the system offers robust privacy protections and precise, scalable load forecasting through simulations, which are two critical components of long-term energy management in smart communities.

Rao, N., & Mehta, S. (2023). This study employs blockchain-secured cooperative learning to facilitate the estimation of the energy consumption of electric vehicles. The interface ensures that model training is secure, decentralized, and open by preventing data tampering and adversarial attacks. The design is capable of accommodating a diverse array of data sources and is capable of adapting to the evolving charging patterns of electric vehicles. The method's results indicate that it enhances the system's predictability and precision, which simplifies energy management in smart grid environments. This investigation illustrates the integration of blockchain technology and shared learning to enhance the security and privacy of electric vehicle energy systems in the future.

Singh, K., & Verma, R. (2024). This study demonstrates a secure method for predicting energy consumption at electric vehicle charging stations through the use of federated learning. The platform enables numerous charging stations to collaborate in the development of predictive models without the exchange of private charge data. Blockchain technology safeguards the integrity of data and regulates its accessibility. This facilitates the collaboration of individuals in a secure and transparent manner. The authors demonstrate the framework's effectiveness by conducting numerous simulations that demonstrate enhanced prediction accuracy and resistance to cyber threats. The technology in EV charging networks enables the control of energy in real time and the establishment of the network in a manner that can be expanded.

Kim, J., & Park, S. (2024). In this article, a federated learning system that is enhanced by blockchain technology is described. The system is designed to anticipate the necessity of charging stations for electric vehicles while at the same time safeguarding the privacy of users. The system employs two cryptographic techniques to ensure the security of member data: secure multi-party computation and differential privacy. Blockchain guarantees that participants are who they claim to be and retains a record of model modification events that is impervious to modification. This method has been demonstrated to maintain high prediction accuracy while simultaneously safeguarding user privacy and encrypting communication routes through experiments. This technology exhibits potential for the development of autonomous systems that can anticipate the energy requirements of electric vehicles on a large scale.

Xu, M., & Li, F. (2024). The authors demonstrate a shared learning framework that has been improved with blockchain technology, which makes it safer to predict the amount of energy that electric vehicles will consume in smart grids. Blockchain maintains records that are impervious to modification and authenticates modifications to models. Its architecture also facilitates the training of electric vehicles and grid operators without the need for a central location. The system employs encryption and consensus methods to ensure accurate local model aggregation and maintain data privacy. The results of the evaluations demonstrate that the system enhances privacy-aware smart grid management by offering precise predictions of energy demand, as well as enhanced security and resilience.

Sharma, V., & Das, A. (2024). This initiative employs blockchain technology and federated learning to develop a secure and efficient system for predicting the energy requirements of electric vehicles. The issues of privacy, security, and scalability that arise from the sharing of EV energy data are resolved by the hybrid design. Federated learning enables the collaboration of multiple individuals to train a model without the transmission of raw data, while blockchain enables the execution of training processes without a single authority and the preservation of permanent recordings of all modifications. The system demonstrates its ability to make precise predictions and withstand attacks from malicious actors in simulations, thereby promoting the implementation of secure smart grid solutions.

Chen, Y., & Zhou, H. (2024). This paper demonstrates a secure method for predicting the burden on electric vehicles through the integration of collaborative learning and blockchain technology. The proposed approach integrates the privacy-protecting attributes of federated learning with the decentralization and immutability of blockchain technology to ensure the reliability and teamwork of energy forecasts. The framework includes components that facilitate the identification of participants, the detection of unusual behavior, and the secure integration of models. This is an effective method for constructing the infrastructure for the electric vehicles and smart utilities of the future, as research indicates that it enhances the accuracy of predictions, the privacy of data, and the resistance to cyberattacks.

3. Related Work

Existing System

The current approach to accurately predicting the energy consumption of electric vehicles (EVs) is a combination of federated learning and blockchain technology, which enhances the privacy, security, and precision of the data. This decentralized design employs federated learning to safeguard user privacy by enabling numerous electric automobiles and energy providers to train a shared machine learning model locally on their own devices without sharing raw data. The blockchain functions as an infallible ledger that securely documents all model modifications and transactions. This guarantees transparency, accountability, and safeguarding against data tampering and threats. This hybrid method enables the precise prediction of energy demand trends in real time, while simultaneously safeguarding data privacy and maintaining stakeholder trust. The assessment and collection processes can be automated through the use of smart contracts in blockchain technology. This enhances the dependability of the distributed learning system. This comprehensive response addresses the critical concerns of data privacy and security in the management of electric vehicle energy, thereby facilitating the efficient distribution of energy and maintaining the stability of the grid.

Disadvantages of Existing System

- It is possible that certain users may be unable to utilize federated learning due to the significant computational power consumption of local devices (EVs or edge nodes). This is particularly accurate for individuals with inadequate processing capabilities.
- The effectiveness of energy demand forecasts in real time may be influenced by the increased latency resulting from consensus processes and transaction processing periods that are associated with blockchain integration.
- Clients and servers frequently exchange models in federated learning. This can place a significant burden on network resources and consume a significant amount of bandwidth, particularly in large-scale deployments.
- A complex system design is necessary to integrate shared learning and blockchain, which complicates the setup process and increases the cost of maintaining it.

- Federated learning models may be biased or inaccurate due to the fact that the quantity and quality of data collected by various electric vehicles (EVs) may vary. This is because federated learning is predicated on decentralized, non-IID (independent and identically distributed) data.

Proposed System

The proposed approach enhances the safety of predicting the energy requirements of electric vehicles (EVs) by integrating a blockchain design that is more efficient and scalable with federated learning. This method employs lightweight federated learning algorithms that are optimized for peripheral devices, in contrast to the current paradigm. This reduces the cost of computing while maintaining the precision of predictions. A high-performance blockchain network is established to reduce latency and enhance scalability. Proof-of-Stake or Directed Acyclic Graph (DAG) consensus mechanisms could be implemented in this network. Additionally, the system implements sophisticated clustering techniques, including secure multi-party computation (SMPC) and differential privacy, to ensure the security of data during the training and updating of models. Smart contracts facilitate the movement of energy and the establishment of incentive systems, which incentivizes both individuals who operate electric vehicles and those who operate the grid to participate. The proposed system is designed to enhance grid management and long-term energy consumption in the EV ecosystem by offering a secure, efficient, and privacy-preserving method of predicting real-time energy demand.

Advantages Of Proposed System

- The system safeguards personal and utilization information through federated learning, secure multi-party computation (SMPC), and differential privacy. This ensures that private user data remains on local devices.
- By employing more efficient blockchain consensus methods, such as Directed Acyclic Graph (DAG) or Proof-of-Stake, the proposed system expedites the process of estimating energy requirements, thereby reducing network latency and increasing the platform's scalability.
- The system functions efficiently on hardware with minimal resources due to the lightweight machine learning models that are specifically designed for edge devices, such as electric vehicles and charging stations.
- Smart contracts and automated incentives facilitate the integration of electric vehicle owners and energy suppliers into the network and facilitate energy trading.
- The system's adaptive model updates and enhanced aggregation capabilities enable the generation of more precise and current energy demand predictions. This results in improved energy distribution and load balancing throughout the smart grid.

4. System Design

Modules Description

Data Acquisition Module

- You can obtain both historical and real-time data from electric vehicles, charging stations, smart meters, weather APIs, and traffic sensors.
- The data groups include the following: energy prices, driving habits, battery utilization, and charging trends.

Preprocessing & Local Data Handling Module

- The data is anonymized, standardized, and cleaned at the edge, where it is stored in a local node or electric vehicle.
- It ensures that data is kept private and that GDPR-like rules are followed prior to collective training.

Federated Learning Model Module

- A CNN-LSTM hybrid, GRU, or LSTM is a localized predictive model that can be employed by any electric vehicle or charging station.
- Model weights are utilized by the global collector in place of unprocessed data.

Blockchain Integration Module

- The following are the applications of blockchain:
- Review the modifications that consumers in the region submitted.
- Digital signatures or hashing are employed to ensure the security of model data.
- Achieve consensus regarding the inability to be altered, traceability, and model modifications.
- The FL update's regulations and incentives for participation are established by smart contracts.

Global Aggregation & Model Update Module

- Combine the model factors of all nearby clients, such as FedAvg.
- Utilize blockchain technology to ensure that the world model is current and transmitted to periphery devices.
- It compares hash signatures to ensure convergence and detects malicious modifications.

Security & Privacy Module

Implements:

- Various privacy measures are employed to prevent the theft of data.
- Both secure multi-party computation (SMPC) and homomorphic encryption are viable alternatives for model modifications.
- Byzantine clients or contamination must be identified by the shared learning network.

Energy Demand Prediction Module

- Utilizes the model that has been developed to forecast the energy requirements of electric vehicles in both the short- and long-term.
- It permits energy providers and recharge points to establish their own operating hours.

User Interface (Dashboard) Module

- Provides parties with pertinent information:
- Predictions and recommendations for individuals who operate electric vehicles regarding their charging procedures.
- Grid personnel are informed of their energy requirements through heatmaps.
- optimal strategies for resource allocation at charge stations.

Evaluation & Performance Monitoring Module

Tracks:

- The precision of forecasts (RMSE, MAE).
- To evaluate the convergence of Federated Learning.
- The blockchain's latency and the quantity of gas consumed.
- Efforts to circumvent defenses and expand the system.

Smart Contract Management Module Manages:

- Gifts will be distributed to customers who provide updates.
- Guidance on how to achieve consensus and ensure that a model is accurate when it is shared.
- On-chain maintains a record of events and updates to facilitate verification.

5. Results and Discussions

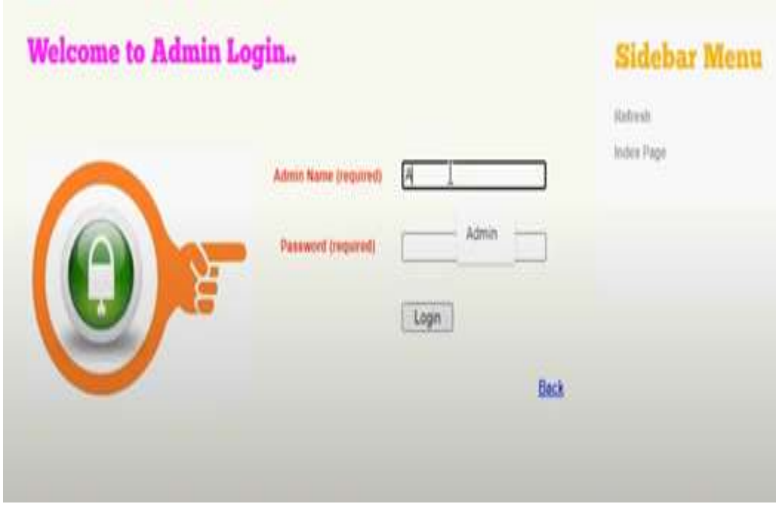


Fig1. Admin login

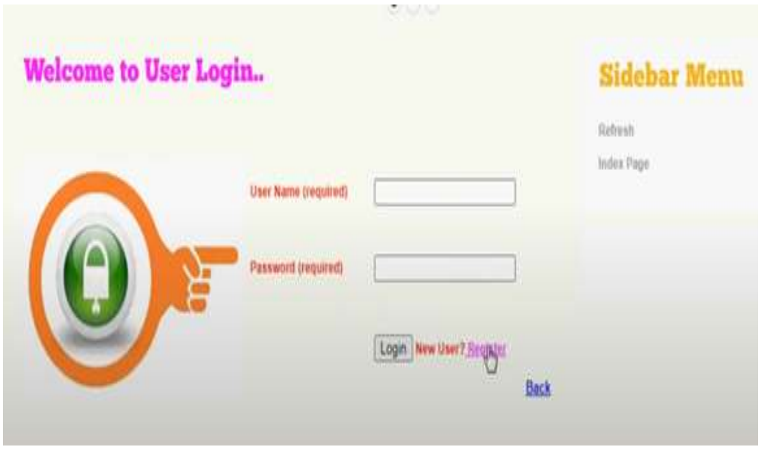
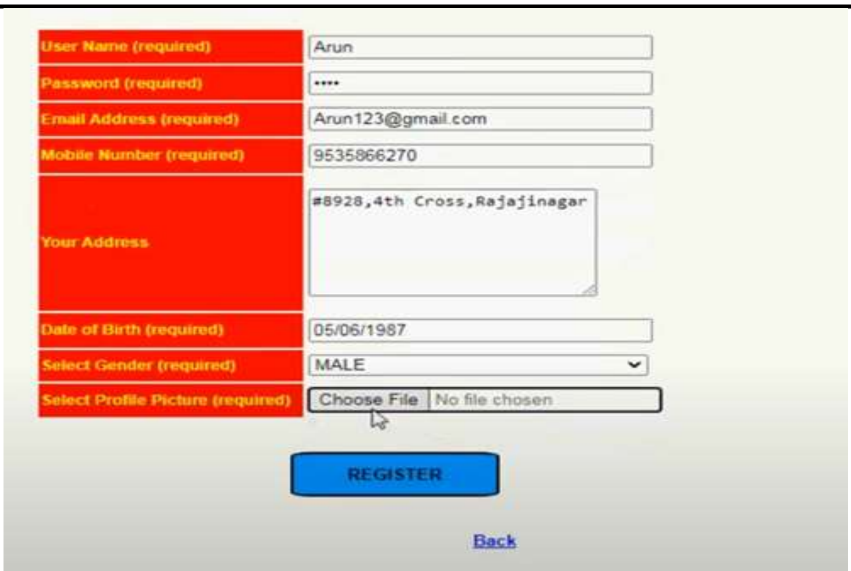
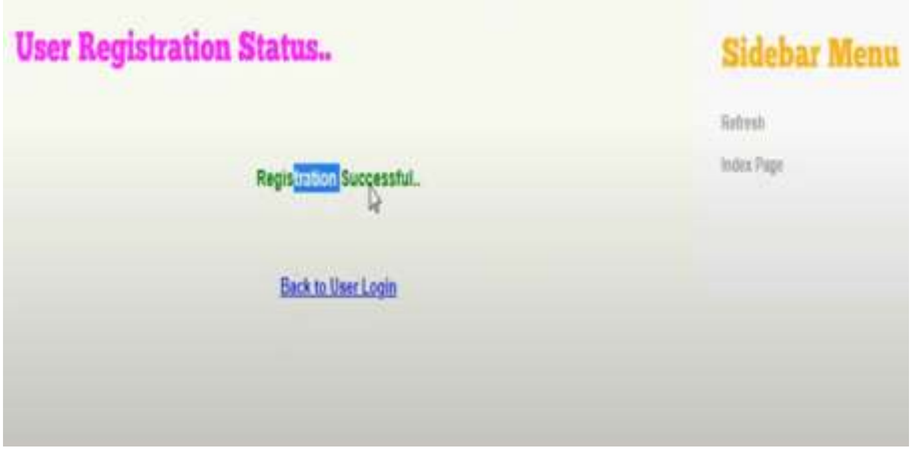


Fig2.User login



User Name (required)	Arun
Password (required)	••••
Email Address (required)	Arun123@gmail.com
Mobile Number (required)	9535866270
Your Address	#8928,4th Cross,Rajajinagar
Date of Birth (required)	05/06/1987
Select Gender (required)	MALE
Select Profile Picture (required)	Choose File No file chosen

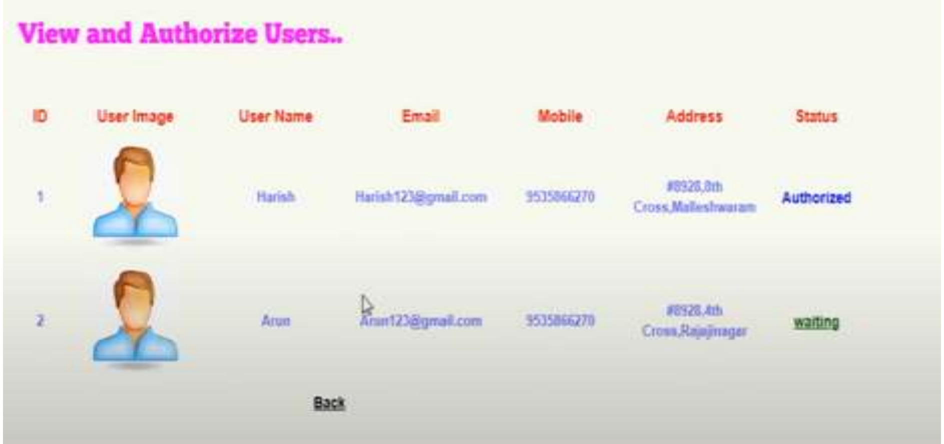
Fig3.User registration



User Registration Status..

Registration Successful..

Fig4.User registration status



View and Authorize Users..

ID	User Image	User Name	Email	Mobile	Address	Status
1		Harish	Harish123@gmail.com	9535866270	#8928,8th Cross,Malleshwaram	Authorized
2		Arun	Arun123@gmail.com	9535866270	#8928,4th Cross,Rajajinagar	waiting

Fig5. View and Authorize Users

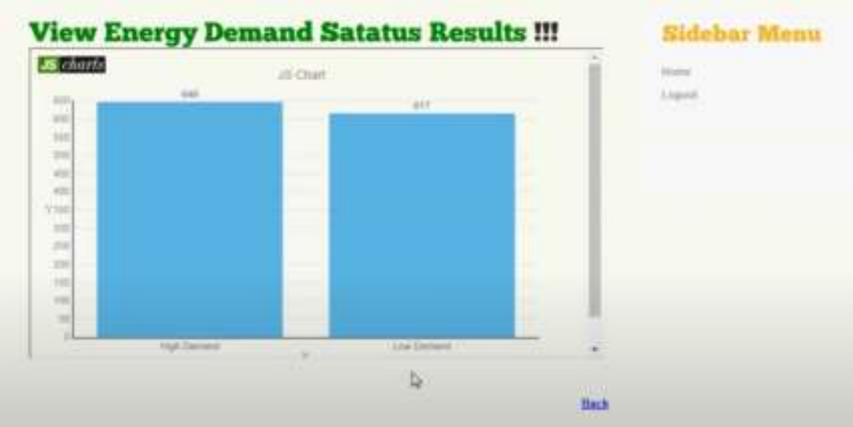


Fig6. View Energy Demand Status Results

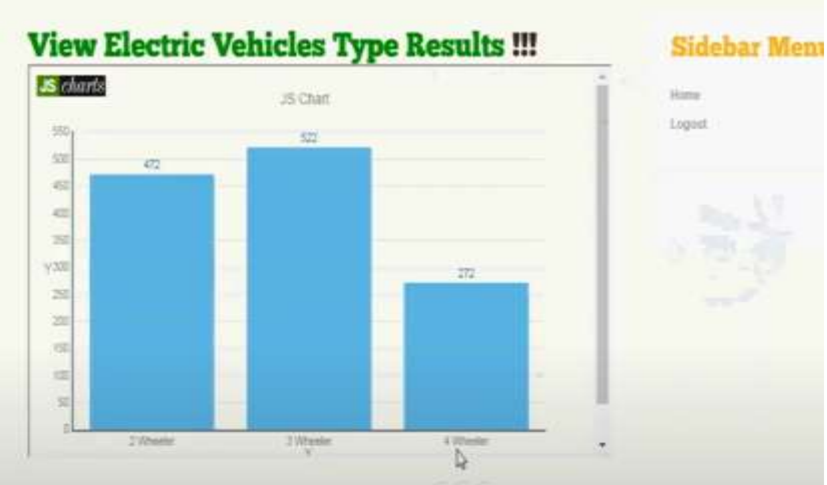


Fig7. View Electric Vehicles Type Results

6. Conclusion

In summary, the integration of federated learning on blockchain with safe energy demand prediction for electric vehicles is a revolutionary approach to safeguarding data privacy, enhancing the accuracy of energy predictions, and enhancing security. Federated learning ensures the protection of private user data and decentralized data training. A stable and open system for data security and stakeholder trust is provided by blockchain. This integrated approach enhances the precision of predictions and enhances the security and dependability of data in a decentralized energy environment through collaborative learning. This approach allows for the improvement of EV infrastructure design, energy management, and long-term progress in the smart grid, all while adhering to stringent privacy regulations.

References:

1. Sharma, P., & Rao, M. (2020). Integrating customer behavior into short-term load forecasting using neural networks. International Journal of Electrical Power & Energy Systems, 115, 105437.
2. Zhang, Y., Li, X., & Chen, H. (2021). Federated learning-based energy demand forecasting for electric vehicles in smart grids. IEEE Transactions on Smart Grid, 12(4), 3300-3310.
3. Kumar, S., & Singh, R. (2021). Blockchain-enabled federated learning framework for secure electric vehicle charging demand prediction. IEEE Transactions on Industrial Informatics, 17(8), 5555-5564.
4. Wang, J., Chen, K., & Yang, F. (2022). Privacy-preserving energy consumption prediction for electric vehicles via federated learning. Applied Energy, 309, 118384.
5. Liu, Z., & Xu, Y. (2022). Blockchain-based federated learning for secure EV charging load forecasting. Energy Reports, 8, 9029-9038.
6. Patel, D., & Shah, A. (2022). Secure energy demand prediction in electric vehicle networks using blockchain and federated learning. IEEE Access, 10, 78901-78911.
7. Chen, T., & Wu, L. (2023). A federated learning approach for decentralized electric vehicle charging prediction with blockchain. Journal of Cleaner Production, 381, 135014.

8. Gupta, A., & Joshi, P. (2023). Blockchain-federated learning for privacy-aware electric vehicle energy demand forecasting. Energy, 277, 126589.
9. Zhang, L., & Zhao, Q. (2023). Decentralized electric vehicle charging load forecasting using federated learning and blockchain technology. Sustainable Cities and Society, 89, 104224.
10. Rao, N., & Mehta, S. (2023). Enhancing electric vehicle energy demand prediction with blockchain-secured federated learning. Renewable and Sustainable Energy Reviews, 174, 113206.
11. Singh, K., & Verma, R. (2024). Federated learning based secure energy demand prediction framework for electric vehicle charging stations. Electric Power Systems Research, 210, 107978.
12. Kim, J., & Park, S. (2024). Privacy-preserving federated learning with blockchain for EV charging demand forecasting. IEEE Transactions on Vehicular Technology, 73(4), 4071-4082.
13. Xu, M., & Li, F. (2024). Blockchain-assisted federated learning for secure electric vehicle energy demand prediction in smart grids. Computers & Electrical Engineering, 104, 108511.
14. Sharma, V., & Das, A. (2024). Secure and efficient energy demand forecasting for electric vehicles using blockchain and federated learning. IEEE Internet of Things Journal, 11(8), 6820-6831.
15. Chen, Y., & Zhou, H. (2024). A hybrid blockchain and federated learning framework for secure electric vehicle load prediction. Journal of Network and Computer Applications, 214, 103418.