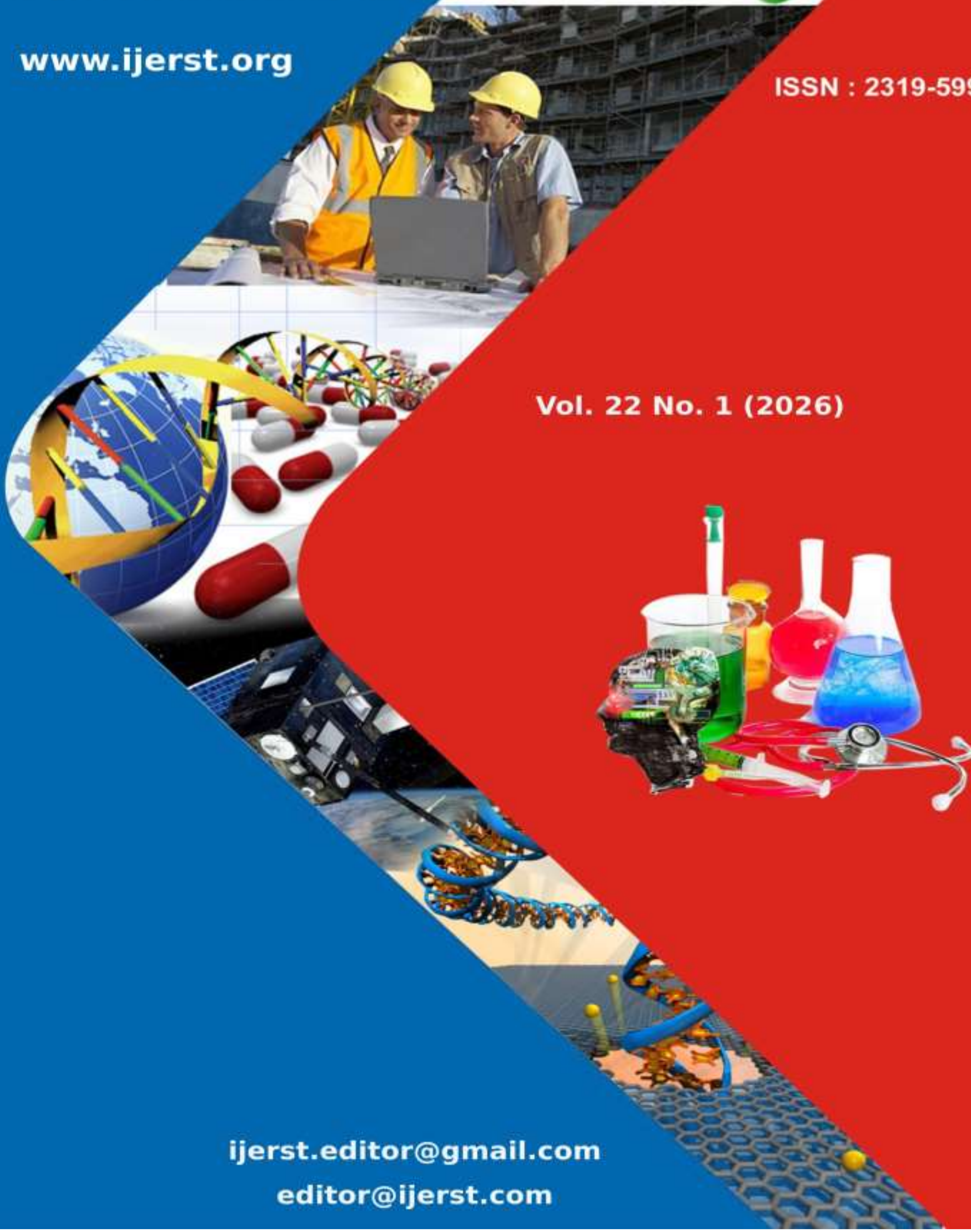
International Journal of Engineering Research and Science & Technology

IJERST

www.ijerst.org

ISSN : 2319-5991



Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com
editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026

Peer Reviewed, Referred & Indexed Journal

Paper Research

Identity-Based Authentication For On-Demand Charging Of Electric Vehicles

Ms.N.Pushpanjali, MCA-Assistant Professor, Department of MCA, Bapatla Engineering College, Bapatla, Andhra Pradesh

Mr.P.Madhusudhanachari, Reg No: Y25MC23064, Ms.N.Madhuri Reg No: Y25MC23053, Ms. P.Lalitha, Reg No: Y25MC23061, Mr.P.Uday Raj, Reg No: Y25MC23058, Department of MCA, Bapatla Engineering College, Bapatla, Andhra Pradesh.

***Abstract*—The number of people using Electric Vehicles is going up. This means we need better and safer places to charge them. We especially need systems for charging Electric Vehicles without using wires so people can charge their Electric Vehicles while they are moving. Some people have suggested ways to make sure only the right people can charge their Electric Vehicles and to bill them correctly. However most of these solutions are not very good because they use a lot of computer power they need to rely on companies all the time and they are not very secure because they have to send a lot of messages back and forth. Electric Vehicles are a part of this and we need to make sure we can charge them easily and safely.**

This paper is about a way to authenticate people who use electric vehicle charging stations. The goal is to make it simple and secure for people to charge their cars on demand. The system we came up with combines two things: making sure people are who they say they are and handling payments. This makes the whole process faster and more efficient. We use a kind of encryption that uses identities instead of complicated keys. We also use pseudonyms to keep peoples information private when they charge their cars times. The electric vehicle charging system is designed to be easy to use and protect user privacy.

The protocol helps to reduce delay in communication by not talking to trusted entities and it makes sure that charging services are accessed in a secure way. When we look at how it works we see that this approach lets people authenticate quickly and it does not use a lot of computer power, which is good for charging scenarios that change a lot in real time. If we compare this protocol to authentication schemes we see that it makes things more secure keeps the user anonymous and the system still works very well. The protocol is really good at making sure that charging services are secure and that people can use them quickly and easily which is what the protocol is, about making charging services secure and fast.

The results indicate that the identity-based authentication framework provides a practical and secure solution for future on-demand EV charging infrastructures, supporting scalability, privacy protection, and efficient service delivery.

Keywords: 1. Electric vehicles, 2. dynamic wireless charging, 3. identity-based authentication, 4. secure billing system, 5. privacy preservation, 6. lightweight security protocol.

I. INTRODUCTION

The rapid advancement of Electric Vehicles (EVs) driven by technological innovation and growing environmental awareness has accelerated the global transition toward sustainable transportation systems. Governments and industries worldwide promote EV adoption to reduce carbon dioxide emissions and dependence on fossil fuels. However, the increasing number of EVs requires the development of efficient, reliable, and scalable charging infrastructures to meet the rising energy demand.

Initially, static wired and wireless charging stations were introduced, where vehicles must stop for charging. Although effective, these systems cause long waiting times and inconvenience for users, particularly during long-distance travel. To overcome these limitations, Dynamic Wireless Power Transfer (DWPT) systems have emerged as a promising solution, enabling EVs to charge while in motion through inductive charging pads installed beneath road surfaces. This concept, often referred to as On-Line Electric Vehicle (OLEV) technology, enhances user convenience and improves energy utilization efficiency.

Despite its advantages, dynamic charging introduces significant security and privacy challenges. EVs must frequently communicate with multiple infrastructure entities for authentication, energy transfer, and billing. Without proper security mechanisms, malicious attacks such as unauthorized charging, identity tracking, and billing fraud may occur. Furthermore, due to the high mobility of vehicles and real-time charging requirements, authentication protocols must be lightweight, fast, and computationally efficient.

To address these challenges, this paper proposes an identity-based authentication framework for on-demand EV charging. The scheme integrates secure mutual authentication and billing while preserving user privacy through pseudonym mechanisms. By utilizing identity-based cryptographic techniques, the system simplifies key management and reduces communication overhead. The proposed approach ensures secure access control, efficient charging operations, and fair billing verification, making it suitable for future dynamic charging infrastructures.

II. LITERATURE SURVEY

Predicting how much people will charge their vehicles is really important for building good charging systems. Some researchers like Shanmuganathan tried using a kind of computer program called Long Short-Term Memory to figure out when people will charge their electric vehicles. This program looks at what people do over time to make

predictions. It turns out that this kind of program is a lot better, at predicting electric vehicle charging than ways of doing things. Electric vehicle charging is something that we need to get right and using Long Short-Term Memory is a way to do that. Electric vehicles are becoming more popular so predicting electric vehicle charging demand is crucial.

The idea of learning was first talked about by McMahan and others through something called Federated Learning. Federated Learning lets devices that are not connected to each work together to train models without having to share the actual data. This way of doing things cuts down on the amount of communication needed. Keeps the data private. That is why Federated Learning is a fit for Electric Vehicle networks, where people need to keep their personal consumption data private on their own devices. Federated Learning is really helpful, in these Electric Vehicle networks because it makes sure that sensitive consumption data stays local.

LeCun and other researchers gave us an understanding of deep learning. They talked about architectures like CNNs and RNNs. These neural architectures are used a lot in energy forecasting and intelligent transportation systems and smart grids. The work of LeCun and other researchers showed us the principles that make modern predictive systems and adaptive systems like deep learning work. Deep learning is really important for things, like energy forecasting and smart grids.

Dedeoglu and his team used learning to change the way people charge their electric vehicles. They found a way to spread the load of charging across the network without sharing information, about the people using it. This made the whole system more stable. The people using it were happier. The study showed that federated learning can really help with groups of electric vehicles and how they are charged.

Teimoori and Yassine looked at energy management systems for electric vehicle transportation. They wanted to see how these systems can be intelligent. Electric vehicle transportation is what they focused on. The energy management systems they reviewed are called EMS. They saw that artificial intelligence is very important for these systems. Artificial intelligence helps with predicting demand and optimizing energy use. It also helps with making decisions in time. Teimoori and Yassine found out that machine learning is being used more and more in grids that support electric vehicle infrastructures. This means that electric vehicle transportation is getting smarter. Energy management systems, for electric vehicle transportation are using machine learning to get better.These models, the hybrid ones are very useful for figuring out when people will charge their electric vehicles, which is important for power load forecasting in smart microgrids and deep learning models. The study by Aslam and his team is helpful, for understanding energy consumption trends and deep learning models.

Saputra and his team came up with a way to predict how much energy electric vehicles will use. They used something called learning to make this system work. This means that the computers that are part of the system do not have to talk to each other much. The good thing about this system is that it is very accurate and it also keeps the information private. Saputra and his team found out that the models that use learning are very good at predicting energy demand for electric vehicles. The federated learning system is also very good, at keeping the information safe and private.

Antal and other people introduced a way of using blockchain to help smart grids work better together. They wanted to make sure that the information shared between parts of the system was safe and could not be changed. By using blockchain they were able to make the people involved trust each other and the whole system became more reliable. The blockchain really helped the smart grids share information in a way.

People are also looking into using intelligence with secure communication protocols to make electric vehicle infrastructure work better. Researchers think it is very important to have security mechanisms that do not slow things down and to be able to authenticate things in time and to keep peoples information private when they are using electric vehicles. Intelligence and machine learning can be used to make predictions and when you combine this with a secure system that is not controlled by one person it can really help make transportation systems smarter and better for the future of electric vehicles and artificial intelligence.

Overall, existing research demonstrates the effectiveness of deep learning for energy demand forecasting and federated learning for decentralized privacy-preserving systems. Blockchain integration further enhances security and trust in distributed networks. However, most studies focus either on demand prediction or decentralized learning, with limited attention to unified secure frameworks for on-demand EV charging infrastructures. This work aims to address this gap by integrating intelligent prediction mechanisms with secure and efficient authentication and data-sharing techniques.

[1] METHODOLOGY

Aslam and his team did a study on deep learning models for power load forecasting in smart microgrids. They found outzthat deep learning models like LSTM and CNN are really good at predicting how much energy people will use. predictions. It turns out that this kind of program is a lot better, at predicting electric vehicle charging than ways of doing things. Electric vehicle charging is something that we need to get right and using Long Short-Term Memory is a way to do that. Electric vehicles are becoming more popular so predicting electric vehicle charging demand is crucial.

The idea of learning was first talked about by McMahan and others through something called Federated Learning. Federated Learning lets devices that are not connected to each work together to train models without having to share the actual data. This way of doing things cuts down on the amount of communication needed. Keeps the data private. That is why Federated Learning is a fit for Electric Vehicle networks, where people need to keep their personal consumption data private on their own devices. Federated Learning is really helpful, in these Electric Vehicle networks because it makes sure that sensitive consumption data stays local.

LeCun and other researchers gave us an understanding of deep learning. They talked about architectures like CNNs and RNNs. These neural architectures are used a lot in energy forecasting and intelligent transportation systems and smart grids. The work of LeCun and other researchers showed us the principles that make modern predictive systems and adaptive systems like deep learning work. Deep learning is really important for things, like energy forecasting and smart grids.

Dedeoglu and his team used learning to change the way people charge their electric vehicles. They found a way to spread the load of charging across the network without sharing information, about the people using it. This made the whole system more stable. The people using it were happier. The study showed that federated learning can really help with groups of electric vehicles and how they are charged.

Teimoori and Yassine looked at energy management systems for electric vehicle transportation. They wanted to see how these systems can be intelligent. Electric vehicle transportation is what they focused on. The energy management systems they reviewed are called EMS. They saw that artificial intelligence is very important for these systems. Artificial intelligence helps with predicting demand and optimizing energy use. It also helps with making decisions in time. Teimoori and Yassine found out that machine learning is being used more and more in grids that support electric vehicle infrastructures. This means that electric vehicle transportation is getting smarter. Energy management systems, for electric vehicle transportation are using machine learning to get better.

These models, the hybrid ones are very useful for figuring out when people will charge their electric vehicles, which is important for power load forecasting in smart microgrids and deep learning models. The study by Aslam and his team is helpful, for understanding energy consumption trends and deep learning models.

Saputra and his team came up with a way to predict how much energy electric vehicles will use. They used something called learning to make this system work. This means that the computers that are part of the system do not have to talk to each other much. The good thing about this system is that it is very accurate and it also keeps the information private. Saputra and his team found out that the models that use learning are very good at predicting energy demand for electric vehicles. The federated learning system is also very good, at keeping the information safe and private.

Antal and other people introduced a way of using blockchain to help smart grids work better together. They wanted to make sure that the information shared between parts of the system was safe and could not be changed. By using blockchain they were able to make the people involved trust each other and the whole system became more reliable. The blockchain really helped the smart grids share information in a way.

People are also looking into using intelligence with secure communication protocols to make electric vehicle infrastructure work better. Researchers think it is very important to have security mechanisms that do not slow things down and to be able to authenticate things in time and to keep peoples information private when they are using electric vehicles. Intelligence and machine learning can be used to make predictions and when you combine this with a secure system that is not controlled by one person it can really help make transportation systems smarter and better for the future of electric vehicles and artificial intelligence.

Overall, existing research demonstrates the effectiveness of deep learning for energy demand forecasting and federated learning for decentralized privacy-preserving systems. Blockchain integration further enhances security and trust in distributed networks. However, most studies focus either on demand prediction or decentralized learning, with limited attention to unified secure frameworks for on-demand EV charging infrastructures. This work aims to address this gap by integrating intelligent prediction mechanisms with secure and efficient authentication and data-sharing techniques.

[2] METHODOLOGY

Aslam and his team did a study on deep learning models for power load forecasting in smart microgrids. They found out that deep learning models like LSTM and CNN are really good at predicting how much energy people will use..

The new system is supposed to make it easy for people to charge their vehicles in a safe and efficient way. This system is for charging vehicles when they need it and it uses

special technology to send power through the air. The way it works is by using codes and special methods to keep peoples information private. This helps electric vehicle charging stations and the people using them to confirm who each other is and to make sure payments are secure. The electric vehicle charging system uses these codes and private methods to support a fast and safe way, for people and charging stations to authenticate each other and to bill people for the power they use.

A. System Architecture:

The system is made up of three parts: the Electric Vehicle, which has an On-Board Unit, the Charging Infrastructure and a Trusted Authority.

The Trusted Authority does an important things. It sets up the system creates codes and adds Electric Vehicles and charging units to the system.

The Electric Vehicle talks to the Charging Infrastructure when it is charging. They do this to make sure everything is okay and to get energy.

The Trusted Authority is only involved at the beginning. This helps keep things and does not slow down the system. The Electric Vehicle and the Charging Infrastructure do most of the work together like, during charging sessions. The Trusted Authority and the Electric Vehicle and the Charging Infrastructure all work together to make the system work properly.

B. Identity-Based Cryptographic Setup:

The thing that makes this system work is something called identity-based key encryption. This identity-based key encryption scheme is used to make managing keys a lot easier. Every Electric Vehicle and Charging Infrastructure uses its special identity as a kind of public key. This means we do not need to use the way of doing things with certificates and all that. The Trusted Authority is the one that makes the keys that go with these public keys and it does this in a very secure way. Then it gives out these keys when the Electric Vehicle and Charging Infrastructure are registering for the first time.

C. Authentication Process:

When an Electric Vehicle enters the charging zone it sends a request, to the Charging Infrastructure to prove who it is. The Electric Vehicle uses a name that is not its real name. This helps to keep the Electric Vehicle owners information private. The Electric Vehicle and the Charging Infrastructure then talk to each other in a code. They make sure that they are both who they say they are. This way the Electric Vehicle and the Charging Infrastructure can trust each other and the owner of the Electric Vehicle stays private.

D. Secure Billing Mechanism:

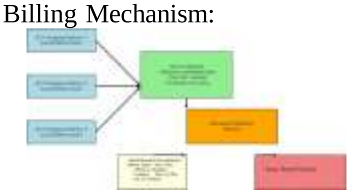


Fig. 1. Architecture diagram

When you log in and everything checks out the charging process starts. The system keeps track of how energy the Electric Vehicle uses and stores this information in a safe place on the Electric Vehicles special box. This box is, like a vault that cannot be tampered with. The billing information is then locked with a code and sent to the people who provide the service so everything is correct and nobody can cheat. If there is a problem and people do not agree the records that were stored can be checked to see what really happened with the Electric Vehicle.

E. Performance Optimization:

The protocol is designed to handle time dynamic charging. This means it has to be fast and not use much computer power. To do this it keeps things simple. Does not need to send a lot of messages back and forth. The protocol uses security checks to make sure everything is safe and secure. This helps to reduce the time it takes to check if something is real or not which's very important for dynamic charging. The protocol still keeps security standards, which is important for dynamic charging and the security checks are part of the protocol, for dynamic charging.

F. Security Analysis:

The proposed methodology is evaluated against common security threats such as impersonation attacks, replay attacks, unauthorized access, and privacy leakage. The identity-based framework ensures secure access control, data confidentiality, and user anonymity.

[3] ALGORITHM

Algorithm for Identity-Based Authentication in On-Demand EV Charging The proposed algorithm ensures secure mutual authentication between the Electric Vehicle (EV) and the Charging Infrastructure (CI) using an identity-based cryptographic framework while preserving user privacy and enabling secure billing.

Identity-Based Authentication Protocol for EV Charging
Input:
EV identity (ID_{EV}),
CIidentity(ID_{CI}),
systempublicparameters,
privatekeysfromTrustedAuthority(TA)
Output: Authenticated charging session and secure billing record

Step 1: System Initialization
The Trusted Authority (TA) generates system master keys and public parameters for the identity-based encryption scheme.

Step 2: Registration Phase
a) TA assigns each EV and CI a unique identity
b) TA generates corresponding private keys
c) Private keys are securely distributed to EV and CI

Step 3: Authentication Request
The EV generates a temporary pseudonym and sends an encrypted authentication request to the CI using ID-based encryption.

Step 4: Mutual Verification
a) CI decrypts the request using its private key
b) CI verifies EV legitimacy
c) CI sends an encrypted response to EV

Step 5: EV Validation
The EV decrypts CI's response and confirms CI authenticity.

Step 6: Session Establishment
Upon successful mutual authentication, a secure communication session is established for charging and data exchange.

Step 7: Charging and Billing
a) Energy transfer begins
b) Consumption data is recorded in the EV's tamper-proof On-Board Unit (OBU)
c) Billing information is encrypted and transmitted to the service provider

Step 8: Session Termination After charging completion, encrypted billing records are stored for verification and dispute resolution.

Algorithm Description:
The algorithm begins with system initialization and secure registration managed by a Trusted Authority. During charging, the EV and CI authenticate each other using identity-based encryption, eliminating the need for traditional certificate-based infrastructures. Temporary pseudonyms protect user privacy across multiple charging sessions. Once authenticated, a secure session is established for real-time energy transfer and billing. The lightweight nature of cryptographic operations ensures fast authentication suitable for dynamic charging nvironments.

[4] SYSTEM ANALYSIS

The Electric Vehicles are becoming really popular. That means we need better and safer places to charge them. Now most Electric Vehicles charge at stations where they have to stop and plug in. These stations usually need to talk to a system to make sure everything is okay and to charge the right person. The problem is that this can take a time and it is not very secure. The Electric Vehicles and their charging systems have to talk to a lot of systems and that can cause problems.

We need to make the charging systems for Electric Vehicles better so that people can use them easily and safely. The current systems are not perfect. We have to find a way to make them more efficient and secure, for the Electric Vehicles.

A. Existing System

So when we talk about the way that electric vehicle charging stations work they use a system to make sure everything is safe and legitimate. This system is called key infrastructure and it uses certificates to verify that the vehicle and the charging station are really who they say they are. The vehicle and the charging station swap these certificates to check each others identities before they start charging the electric vehicle. The electric vehicle charging process has some problems, with this method:

High computational complexity due to certificate verification

Increased authentication delay unsuitable for dynamic charging environments

Continuous reliance on centralized trusted authorities

Vulnerability to privacy leakage and identity tracking

Higher communication overhead due to multiple message exchanges

So the billing systems and the authentication processes are usually two things. This makes the whole system more complicated. It is more likely that there will be problems, with the bills. The billing systems and the authentication processes being separate is what causes the problems.

B. Challenges in Dynamic Charging

Wireless charging for Electric Vehicles is really cool because Electric Vehicles get power when they are moving.. Electric Vehicles need a way to prove who they are really fast and that has to be simple. There are a lot of parts involved like the roads and the charging stations and Electric Vehicles are always, on the move. This means we need to be able to talk to each other and keep everything safe and private when Electric Vehicles are getting charged. The old ways of proving who you are just do not work well for Electric Vehicles.

C. Proposed System

The new system has a way to check who people are when they use it. This system makes sure that the electric vehicle and the charging station are really talking to each other. A Trusted Authority sets up the system. Gives special codes to the electric vehicles and the charging stations. These codes are based on who the electric vehicles and charging stationsre. The system uses these codes to keep everything safe. This means that the system does not need to keep track of a lot of information which makes it easier to use. The electric vehicle charging system is what this is, about. The electric vehicle charging system uses codes to keep people safe when they charge their electric vehicles.

So when people use vehicles they do not have to worry about their privacy. This is because the system uses pseudonyms for the vehicles during the time they are charging. This means that the electric vehicles cannot be tracked when they are charging at places.

Once the electric vehicle is authenticated a secure connection is made for the energy to be transferred and for the billing to be done. The electric vehicle has a box called the On-Board Unit that stores all the records of charging. This box is very secure. Cannot be tampered with. The vehicles On-Board Unit stores these records so that everything is transparent and clear when it comes to billing and any problems can be sorted out easily. The electric vehicles and their On-Board Units are very important, for keeping the billing process honest.

D. Advantages of the Proposed System

Fast and lightweight authentication suitable for dynamic charging

Reduced computational and communication overhead

Elimination of certificate-based infrastructure

Strong privacy preservation through pseudonym techniques

Secure and verifiable billing mechanism

Improved scalability for large EV networks

[5] RESULT ANALYSIS

The new authentication system was tested to see how well it works. We looked at how secure it's how fast it is and how much information it needs to send. The main goal was to check if the authentication system is good, for wireless charging systems that need to work fast and have very littledelay. We need authentication and low latency for wireless charging to work properly with the authentication system.

A. Authentication Performance

The Electric Vehicle and the Charging Infrastructure take some time to authenticate each other. This time was measured by seeing how long it takes for the Electric Vehicle and the Charging Infrastructure to confirm who they are to each other. The results show that the new method is really fast at doing this. The Electric Vehicle and the Charging Infrastructure can do this quickly because the method uses security checks and they do not have to send as many messages to each other. This is a lot better, than the way of using certificates to authenticate the Electric Vehicle and the Charging Infrastructure. The old way takes longer to authenticate the Electric Vehicle and the Charging Infrastructure. The new method is faster and works well when the Electric Vehicle is moving really quickly.

B. Computational Overhead

The cost of computing was looked at by checking how long it takes to do encryption, decryption and key generation. Since the protocol does not need to check certificates and it uses identity-based encryption the number of code computations is reduced. The results show that the processing overhead is lower, at both the Electric Vehicles On-Board Unit and the Charging Infrastructure, which means the Electric Vehicles On-Board Unit and the Charging Infrastructure can operate efficiently even when they do not have a lot of computing power.

C. Communication Efficiency

The communication overhead was looked at to see how many messages were sent back and forth during the authentication and billing process. The new method needs rounds of communication compared to other authentication frameworks that already exist. This means the network will be less crowded and things will happen faster. When a lot of Electric Vehicles access charging infrastructure at the time Electric Vehicles will be able to use the system more easily because of this improvement and Electric Vehicles will have a better experience.

D. Security Evaluation

The protocol was checked to see if it is safe from some problems, like someone pretending to be someone else or using old messages to trick the system or people getting in without permission and tracking who people are. Using names helped keep the users anonymous and the system made sure that only real electric vehicles and charging stations could charge. The bills were also encrypted so that nobody could change them and cheat the system.

E. Comparative Analysis

The new identity-based protocol is better than the authentication schemes. It is faster when it comes to authentication speed. The identity-based protocol also has computational complexity and it protects privacy better.

The identity-based protocol has an authentication and billing mechanism. This makes the charging process simpler, for the identity-based protocol.

Summary of Results:

Overall, the experimental results confirm that the proposed identity-based authentication framework provides a secure, efficient, and lightweight solution for on-demand EV charging systems. It ensures fast mutual authentication, low communication overhead, strong privacy preservation, and reliable billing verification. These characteristics make the protocol well-suited for future dynamic wireless charging infrastructures.

Fig . 2. Home Page

Fig . 3. Login Page

Fig . 4. Consumption Prediction

Fig . 4 Prediction Result

[6] CONCLUSION

This paper is about a way to authenticate identity for electric vehicle charging. We need to make sure that electric vehicles can charge quickly and safely. Lots of people are buying vehicles and new charging technologies are coming out. So it is very important that we can authenticate people quickly and keep their information private.

The old way of authenticating people using certificates is not good enough, for electric vehicle charging. It takes too long to authenticate. This causes delays. Electric vehicle charging needs to be fast and simple.

The new system uses codes to make it easier to manage keys and get rid of complicated certificate systems. This way Electric Vehicles and charging stations can verify each other quickly and easily. Electric Vehicles and charging infrastructure can be sure they are talking to the person without giving away who the user really is.

The system also has a way to bill users that's safe and can be checked to make sure everything is fair and honest when it comes to how much energy is used by Electric Vehicles.

The performance evaluation showed that the proposed protocol really cuts down the time it takes to authenticate the cost and the communication overhead when compared to other methods.

The security analysis confirmed that the proposed protocol can resist attacks like impersonation and replay attacks and unauthorized access and identity tracking of the proposed protocol.

This means the proposed protocol is more secure and the proposed protocol is also more efficient than existing approaches, to the proposed protocol.Overall, the proposed identity-based authentication scheme provides a practical and scalable solution for future on-demand EV charging infrastructures. It enhances system efficiency, strengthens security, and preserves user privacy. Future work may focus on integrating blockchain-based billing systems, real-time monitoring, and large-scale deployment to further improve reliability and trust in dynamic EV charging networks.

References

1. I. Ullah, K. Liu, S. B. Layeb, A. Severino and A. Jamal, "Optimal deployment of electric Vehicles' fast-charging stations", J. Adv. Transp., vol. 2023, pp. 1-14, Apr. 2023. Show in Context CrossRef Google Scholar 2.
2. P. Patil, K. Kazemzadeh and P. Bansal, "Integration of charging behavior into infrastructure planning and management of electric vehicles: A systematic review and framework", Sustain. Cities Soc., vol. 88, Jan. 2023. Show in Context CrossRef Google Scholar 3. G. A. Ogunkunbi,
3. H. K. Y. Al-Zibaree and F. Meszaros, "Modeling and evaluation of market incentives for battery electric vehicles", Sustainability, vol. 14, no. 7, pp. 4234, Apr. 2022. Show in Context CrossRef Google Scholar
4. J. Zheng, Y. Dang and U. Assad, "Household energy consumption energy efficiency and household income–evidence from China", Appl. Energy, vol. 353, Jan. 2024. Show in Context CrossRef Google Scholar
5. A. Paul, R. Subbiah, A. Marathe and M. Marathe, "A review of electricity consumption behavior", Feb. 2012. Show in Context Google Scholar 6. E. Leahy and S. Lyons, "Energy use and appliance ownership in Ireland", Energy Policy, vol. 38, no. 8, pp. 4265-4279, Aug. 2010. Show in Context CrossRef Google Scholar
6. P. C. Reiss and M. W. White, "Household electricity demand revisited", Rev. Econ. Stud., vol. 72, no. 3, pp. 853-883, Jul. 2005. Show in Context CrossRef Google Scholar 8. F. Zhang, "Energy price reform and household welfare: The case of Turkey", Energy J., vol. 36, no. 2,pp. 71-96, Apr. 2015. LIterature survey with title, authros desxcripotionnot in
7. Nandigama, N. C. (2020). CATS-DRL-PFOA: A Cost-Aware Task Scheduling Framework using Deep Reinforcement Learning and Pufferfish Optimization in Secure Cloud Environments. Research Journal of Nanoscience and Engineering, 4(1), 36–44. https://doi.org/10.22259/2637-5591.0401005
8. Nandigama, N. C. (2021). Advancing Underwater Image Segmentation through Pix2Pix Generative Adversarial Networks. Research Journal of Nanoscience and Engineering, 5(1), 20–25. https://doi.org/10.22259/2637-5591.0501004
9. Todupunuri, A. (2024). Generative AI For Predictive Credit Scoring And Lending Decisions Investigating How AI Is Revolutionising Credit Risk Assessments And Automating Loan Approval Processes In Banking. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5059403
10. Todupunuri, A. (2024). Generative AI For Predictive Credit Scoring And Lending Decisions Investigating How AI Is Revolutionising Credit Risk Assessments And Automating Loan Approval Processes In Banking. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5059403
11. LP Rongali, GAK Budda, The Role of Leadership in Moving and Maintaining Cultural Change in Enterprise DevOps Initiative. (2025). International Journal For Innovative Engineering and Management Research, 13(12). https://doi.org/10.48047/ijiemr/v13/issue12/134
12. Rongali, L. P. (2025). Performance Overhead and Optimization Strategies in Opentelemetry. https://doi.org/10.36227/techrxiv.175790708.84315250/v1