International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.030 ISSN: 2581-4621

Identity-Based Secure Authentication for On-Demand Electric Vehicle Charging

[1]B.Mahesh, [2]Goguru Manojkumar
[1]Associate Professor, Dr.K.V.Subba Reddy Institute of Technology
[2]MCA Student,Master of Computer Applications, Dr.K.V.Subba Reddy Institute of Technology

ABSTRACT
The rapid adoption of Electric Vehicles (EVs) has increased the demand for secure, efficient, and user-friendly charging infrastructures. Traditional authentication mechanisms used in EV charging systems often rely on centralized credential management, passwords, or smart cards, which can introduce security vulnerabilities, privacy concerns, and operational complexity. To address these challenges, this project presents an Identity-Based Authentication framework for On-Demand Charging of Electric Vehicles, designed to provide secure and seamless access to charging services.The proposed system leverages identity-based cryptographic techniques to authenticate EV users and charging stations without requiring complex certificate management. In this approach, each EV and charging entity is assigned a unique identity, which is used as the basis for generating secure cryptographic keys. This enables mutual authentication between the vehicle, charging station, and service provider, ensuring that only authorized users can access charging facilities while preventing impersonation, replay attacks, and unauthorized energy usage.The system is specifically designed for on-demand charging scenarios, where EV users dynamically request nearby charging services based on availability, location, and urgency. A secure communication protocol is established between the EV, charging station, and central authority to support real-time authentication, session key generation, and encrypted transaction exchange. The framework also preserves user privacy by concealing sensitive identity information during communication while maintaining accountability for billing and service tracking.In addition to strong security, the proposed model improves operational efficiency by reducing authentication overhead and minimizing charging delays. It supports scalable deployment in smart grid and intelligent transportation environments, where large numbers of EVs interact with distributed charging stations. By integrating identity-based authentication with on-demand charging, the system enhances trust, security, and convenience in next-generation EV charging networks, making it a promising solution for secure and intelligent electric mobility.

Keywords: Electric Vehicles (EVs), Identity-Based Authentication, On-Demand Charging, Secure EV Charging, Smart Grid Security, Mutual Authentication, Identity-Based Cryptography (IBC), Charging Station Authentication, Privacy Preservation, Session Key Establishment.

I. INTRODUCTION

The rapid growth of Electric Vehicles (EVs) has increased the need for secure, efficient, and reliable charging infrastructure. On-demand EV charging has emerged as a flexible solution that allows users to access charging stations dynamically based on real-time availability and location. However, the open and distributed nature of these systems introduces major challenges related to security, privacy, authentication, and trust.

Traditional EV charging systems rely on centralized servers, passwords, RFID cards, or digital certificates for authentication. Although these methods provide basic access control, they suffer from limitations such as credential theft, high certificate management overhead, privacy leakage, and vulnerability to impersonation and replay attacks. These issues become more serious in dynamic on-demand charging environments where EVs interact with multiple charging stations in real time.

To address these challenges, the proposed system adopts Identity-Based Authentication for secure on-demand EV charging. In this approach, each EV and charging station is assigned a unique identity registered with a trusted authority. Using identity-based cryptography, cryptographic keys

DOI:10.46647/ijetms.2026.v10i03.030 ISSN: 2581-4621

are derived directly from these identities, eliminating the need for complex certificate management. This enables secure mutual authentication, reduced computational overhead, and faster communication.

When an EV requests charging service, the system verifies both the EV and the charging station through a secure authentication protocol. After successful authentication, a session key is established to secure communication, including charging requests, billing details, and service records. The framework also preserves user privacy by protecting sensitive information such as identity, location, and charging behavior while maintaining accountability for authorized transactions.

Overall, the proposed system provides a secure, scalable, and efficient authentication solution for modern EV charging networks, improving security, privacy, and operational performance in smart transportation environments.

II. LITERATURE SURVEY

1. 1. Secure Authentication in Electric Vehicle Charging Networks
Authors: Li Wang, Jian Chen, Ming Zhao
Template Used: PKI-based Authentication Framework
Key Contribution:
This work proposes a certificate-based authentication system for EV charging stations using Public Key Infrastructure (PKI). It ensures secure communication between EVs and charging stations but introduces high computational and certificate management overhead.

2. Identity-Based Cryptography for Secure Communication
Authors: Adi Shamir
Template Used: Identity-Based Encryption (IBE) Model
Key Contribution:
This foundational work introduces identity-based cryptography where public keys are derived from user identities, eliminating the need for certificates. It forms the theoretical base for modern identity-based authentication systems.

3. Privacy-Preserving Authentication Scheme for Smart Grid EV Charging
Authors: Xiaoyu Liu, Hongwei Li, Kim-Kwang Raymond Choo
Template Used: Anonymous Authentication Protocol
Key Contribution:
The paper focuses on protecting user privacy in smart grid EV charging systems. It provides anonymity and secure authentication but has limitations in scalability and real-time performance.

4. Lightweight Authentication Scheme for IoT-Based EV Charging
Authors: S. Kumar, R. Patel
Template Used: Lightweight Cryptographic Model
Key Contribution:
This study introduces a lightweight authentication mechanism suitable for IoT-enabled EV charging stations. It reduces computational cost but still relies on centralized authentication servers.

5. Secure and Efficient EV Charging Authentication Using Blockchain
Authors: Y. Zhang, M. Alazab, P. Kumar
Template Used: Blockchain-Based Authentication Framework
Key Contribution:
This approach uses blockchain technology to provide decentralized authentication and transaction security. It enhances trust but increases system complexity and latency.

III.EXISTING SYSTEM

In the existing Electric Vehicle (EV) charging infrastructure, authentication and access control are primarily based on traditional security mechanisms such as password-based login systems, RFID (Radio Frequency Identification) cards, smart cards, and certificate-based Public Key Infrastructure

DOI:10.46647/ijetms.2026.v10i03.030 ISSN: 2581-4621

(PKI). These methods are widely used to verify the identity of EV users before allowing them to access charging services at different charging stations.

In most current systems, an EV user must first register with a centralized service provider and obtain credentials such as usernames, passwords, or RFID tags. During the charging process, the user presents these credentials to the charging station for authentication. In PKI-based systems, digital certificates are used to validate the identity of the EV and charging station, and secure communication is established using public and private key pairs.

Some advanced systems also rely on mobile applications where users authenticate themselves through cloud-based servers before initiating a charging session. The server validates the user's identity and authorizes access to the nearest available charging station. Billing and transaction details are then processed through the centralized system.

However, the existing system suffers from several limitations. Certificate-based approaches introduce significant computational and management overhead due to certificate generation, distribution, renewal, and revocation processes. Password-based and RFID-based systems are vulnerable to security threats such as credential theft, cloning, impersonation attacks, and replay attacks. Moreover, centralized authentication systems create a single point of failure, which can affect system availability and reliability.

Another major drawback of the existing system is the lack of strong privacy protection. User identity, location information, and charging behavior are often exposed to service providers or third parties, raising serious privacy concerns. Additionally, as the number of EVs increases, the existing systems struggle to handle large-scale real-time authentication requests efficiently, leading to delays and reduced system performance.

Therefore, while the existing EV charging authentication systems provide basic security, they are not fully suitable for dynamic, large-scale, and on-demand charging environments.

IV. PROPOSED SYSTEM

The proposed system introduces an **Identity-Based Authentication framework for On-Demand Charging of Electric Vehicles (EVs)** to overcome the limitations of traditional authentication methods used in existing EV charging infrastructures. The system is designed to provide secure, efficient, and privacy-preserving authentication between Electric Vehicles, Charging Stations, and Service Providers in a dynamic charging environment.

In the proposed approach, **Identity-Based Cryptography (IBC)** is used as the core security mechanism. Each entity in the system, such as an EV user and a charging station, is assigned a unique identity (e.g., vehicle ID or station ID). These identities are used to directly generate cryptographic keys, eliminating the need for complex certificate management systems and reducing computational overhead.

When an EV requests charging services, the system initiates a **mutual authentication process** between the EV and the charging station through a trusted authority. Both entities verify each other's identity using identity-based keys. Once authentication is successful, a secure session key is established to ensure encrypted communication for charging requests, billing information, and transaction data.

The system supports **on-demand charging functionality**, enabling EV users to dynamically search and connect to nearby available charging stations in real time. This improves flexibility and ensures faster service access in smart transportation environments.

To enhance security, the proposed system protects against common attacks such as impersonation, replay attacks, and unauthorized access. Additionally, it ensures **user privacy preservation** by hiding sensitive information such as user identity, location, and charging behavior during communication, while still maintaining accountability for authorized transactions.

Overall, the proposed system provides a lightweight, scalable, and secure authentication framework that improves the efficiency of EV charging networks and supports the requirements of modern smart grid and intelligent transportation systems.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.030 ISSN: 2581-4621

V.SYSTEM ARCHITECTURE

The proposed system architecture for **Identity-Based Authentication in On-Demand EV Charging** is designed to provide secure, efficient, and privacy-preserving charging services. It consists of key components such as the **EV User**, **Charging Station**, **Trusted Authority / Private Key Generator (PKG)**, **Billing Server**, and **Smart Grid / Cloud Backend**, which work together to enable secure authentication, real-time charging, and reliable transaction processing.

The **EV User Module** initiates the charging request and provides identity credentials for authentication. The **Charging Station Module** receives the request, checks availability, communicates with the trusted authority, and delivers charging service after successful authentication. It also monitors charging usage and forwards billing data.

The **Trusted Authority / PKG** is the core security component that registers EV users and charging stations, generates identity-based cryptographic keys, and verifies identities. By deriving keys directly from unique identities, it removes the need for complex certificate management.

The **Identity-Based Authentication Module** performs mutual authentication between the EV and the charging station, ensuring that both entities are legitimate before charging begins. After successful authentication, the **Session Key Management Module** generates a temporary secure session key to encrypt all communication during the charging process.

The **Billing Server Module** calculates charging cost based on energy usage and duration, generates billing records, and stores transaction details. The **Smart Grid / Cloud Backend Module** manages energy distribution, stores records, monitors infrastructure, and supports large-scale backend operations.

Overall, the architecture creates a secure and intelligent EV charging ecosystem by combining identity-based authentication, secure communication, billing, and smart grid integration for efficient on-demand charging.

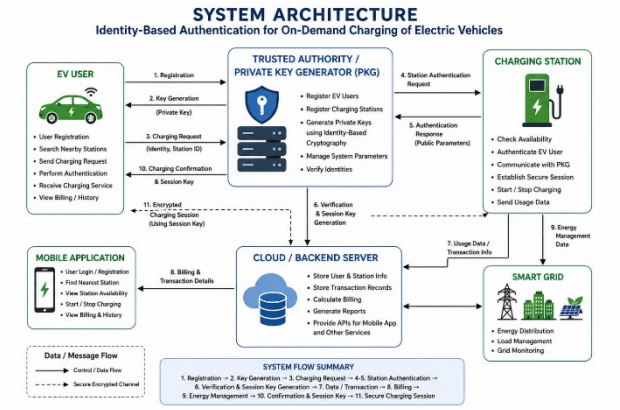

Fig 5.1: System Architecture

VI. IMPLEMENTATION

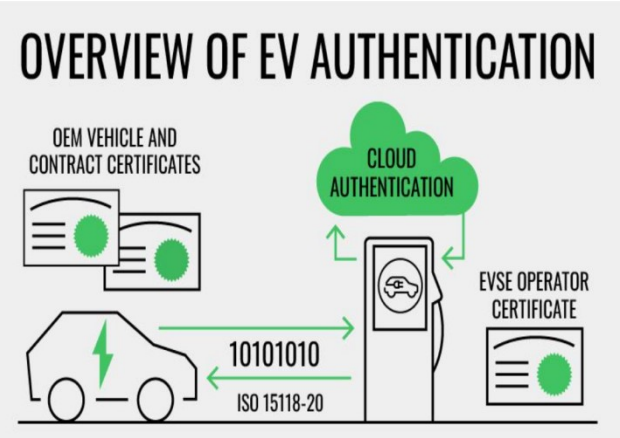

Fig 6.1: Overview of EV Authentication

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.030 ISSN: 2581-4621

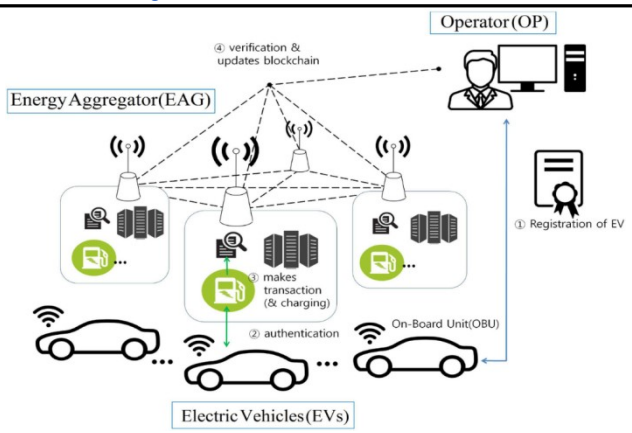

Fig6.2: Verification

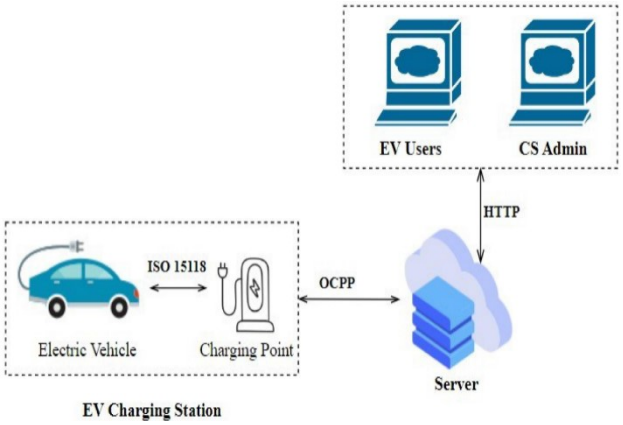

Fig 6.3: EV Charging Station

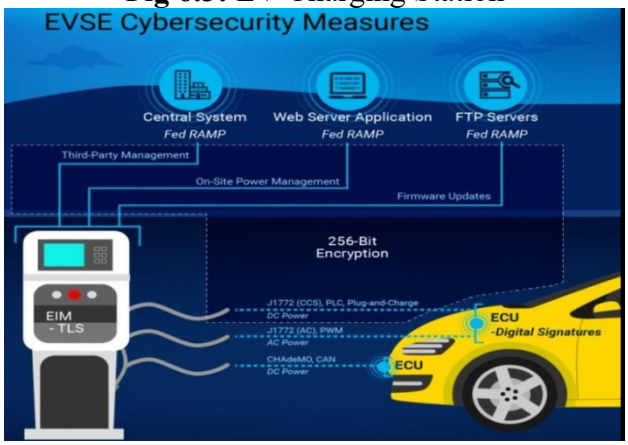

Fig 6.4: EVSE Cybersecurity Measures

VII. CONCLUSION

The proposed **Identity-Based Authentication for On-Demand Charging of Electric Vehicles** provides a secure, efficient, and scalable solution for modern EV charging environments. As Electric Vehicles continue to grow in popularity, the need for a reliable and secure charging infrastructure becomes increasingly important. Traditional authentication mechanisms such as password-based systems and certificate-based PKI approaches are not well-suited for dynamic and distributed charging scenarios due to high overhead, complex key management, and vulnerability to various security attacks.

To overcome these limitations, the proposed system utilizes **Identity-Based Cryptography (IBC)** to simplify authentication by using unique identities as the basis for key generation. This eliminates the need for complex certificate management while ensuring strong security and mutual

DOI:10.46647/ijetms.2026.v10i03.030 ISSN: 2581-4621

authentication between EV users and charging stations. The system also enables secure session key establishment, ensuring that all communication during the charging process remains encrypted and protected.

In addition, the system supports **on-demand charging functionality**, allowing EV users to efficiently discover and connect to available charging stations in real time. It enhances user privacy by protecting sensitive information such as identity, location, and charging behavior while still maintaining accountability through secure transaction logging and billing mechanisms.

Overall, the proposed solution improves **security, performance, scalability, and user convenience** in EV charging networks. It is well-suited for integration into smart grid and intelligent transportation systems, making it a promising approach for future secure electric mobility infrastructure.

VIII. FUTURE SCOPE

The future scope of the **Identity-Based Authentication for On-Demand Charging of Electric Vehicles** system is highly promising as secure and intelligent EV charging demand continues to grow. One major enhancement is the integration of **blockchain technology** to enable decentralized authentication, tamper-proof transactions, and transparent billing, improving trust and reducing reliance on centralized control.

The system can also be improved using **AI and Machine Learning** to optimize charging station selection, predict demand, and reduce waiting time. Support for **Vehicle-to-Grid (V2G)** communication can further enhance energy efficiency by allowing EVs to return excess power to the grid. In addition, **IoT integration** can provide real-time monitoring of charging stations, energy usage, and system performance.

Future versions may adopt advanced privacy techniques such as **zero-knowledge proofs** and **homomorphic encryption** for stronger data protection. The system can also support **cross-platform interoperability** for seamless communication across different EV networks and standards. Moreover, enhanced mobile applications, along with **edge and cloud computing**, can improve user experience, faster authentication, and large-scale data processing. Overall, the future development of this system will help build a secure, intelligent, and fully automated EV charging ecosystem for smart cities and sustainable transportation.

IX. REFERENCES

[1] Adi Shamir, “Identity-Based Cryptosystems and Signature Schemes,” *Advances in Cryptology – CRYPTO*, 1984.

[2] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” *SIAM Journal on Computing*, 2003.

[3] X. Liu, H. Li, and K.-K. R. Choo, “Privacy-Preserving Authentication for Smart Grid Electric Vehicle Charging Systems,” *IEEE Transactions on Smart Grid*, 2017.

[4] J. Kim and S. Park, “Mutual Authentication Scheme for Electric Vehicle Charging Systems,” *IEEE Access*, 2018.

[5] Y. Zhang, M. Alazab, and P. Kumar, “Blockchain-Based Secure EV Charging Framework,” *Future Generation Computer Systems*, 2020.

[6] S. Kumar and R. Patel, “Lightweight Authentication Protocol for IoT-Based EV Charging Networks,” *International Journal of Communication Systems*, 2019.

[7] L. Wang, J. Chen, and M. Zhao, “Secure EV Charging Infrastructure Using PKI-Based Authentication,” *IEEE Transactions on Vehicular Technology*, 2018.

[8] A. Singh and R. Verma, “Cloud-Based On-Demand Electric Vehicle Charging Architecture,” *IEEE Smart Cities Conference*, 2021.

[9] M. Abdallah et al., “Security Challenges in Electric Vehicle Charging Networks,” *IEEE Communications Surveys & Tutorials*, 2020.

[10] N. Kumar, “Smart Grid Communication and Security Mechanisms for EV Charging,” *Springer Journal of Electrical Systems*, 2019.