



Enhancing Electric Vehicle Security and Privacy through Decentralized Identity Management

ABDULLAH AYDEGER, EECS, Florida Institute of Technology, Melbourne, Florida, USA

ENGİN ZEYDAN and JOSEP MANGUES-BAFALLUY, Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain

SUAYB S. ARSLAN, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA and Bogazici University, Istanbul, Türkiye

YEKTA TURK, ASELSAN AS, Ankara, Türkiye

In the next decade, Electric Vehicles (EVs) are expected to contribute to reducing climate change and transforming road mobility significantly. However, the security and privacy of EV charging systems pose considerable challenges that need to be addressed. This article introduces a novel approach by integrating blockchain-based Self-Sovereign Identity (SSI) to enhance the security and privacy of EV charging systems. By leveraging the decentralized and immutable nature of blockchain, the proposed SSI framework can ensure secure and private data exchanges between EVs, charging stations, and backend systems. This three-way integration addresses the vulnerabilities identified in existing EV charging methods, such as conductive, inductive, and battery swapping and complies with cybersecurity regulations like UNECE R155. This article provides a comprehensive analysis, practical case study, and evaluation of the security and privacy enhancements achieved through the proposed SSI framework, offering valuable insights for industry professionals and researchers. We have conducted extensive end-to-end testing to evaluate the performance of our blockchain-based SSI framework in the EV charging ecosystem, focusing on identity verification, credential management, and service orchestration. The results show that the system enables fast wallet creation, efficient metadata retrieval, and low-latency service deployment, ensuring seamless identity management and service orchestration.

CCS Concepts: • **Security and privacy** → *Authentication; Access control; Privacy-preserving protocols; Authorization;*

Additional Key Words and Phrases: Electric Vehicle, Charging Methods, Security, Blockchain, Self-Sovereign Identity

ACM Reference format:

Abdullah Aydeger, Engin Zeydan, Josep Manges-Bafalluy, Suayb S. Arslan, and Yekta Turk. 2025. Enhancing Electric Vehicle Security and Privacy through Decentralized Identity Management. *Digit. Threat. Res. Pract.* 6, 3, Article 11 (September 2025), 20 pages.

<https://doi.org/10.1145/3743151>

This work was partially funded by “ERDF A way of making Europe” project under grant PID2021-126431OB-I00 and Spanish Ministry of Economy and Competitiveness (MINECO)—Program UNICO I+D funded by MCIN/AEI/ 10.13039/501100011033 (grants TSI-063000-2021-54 and -55) and Generalitat de Catalunya grant 2021 SGR 00770.

Authors’ Contact Information: Abdullah Aydeger (corresponding author), EECS, Florida Institute of Technology, Melbourne, Florida, USA; e-mail: aaydeger@fit.edu; Engin Zeydan, Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain; e-mail: ezeidan@cttc.es; Josep Manges-Bafalluy, Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain; e-mail: jmanges@cttc.es; Suayb S. Arslan, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA and Bogazici University, Istanbul, Türkiye; e-mail: sarslan@mit.edu; Yekta Turk, ASELSAN AS, Ankara, Türkiye; e-mail: yektaturk@aselsan.com.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM 2576-5337/2025/9-ART11

<https://doi.org/10.1145/3743151>

1 Introduction

Electric Vehicles (EVs) are rapidly changing road mobility, and they play a crucial role in reducing greenhouse gas emissions and meeting global decarbonization targets. With many countries planning to phase out the production of new gasoline and diesel vehicles over the next decade, the use of EVs is expected to increase significantly and transform the urban environment and daily commuting patterns. Central to this transition is the EV charging ecosystem, which includes **Electric Vehicle Charging Station (EVCS)** and power grids. While the proliferation of EVs brings significant environmental benefits, it also poses new challenges in terms of the security and privacy of the charging infrastructure. EV charging systems involve complex interactions between vehicles, **Charging Stations (CSs)**, and backend systems that often require the exchange of sensitive data such as payment information, user credentials, and location data. These interactions are vulnerable to various cyber threats, including unauthorized access, data tampering, and information disclosure. Therefore, EVCSs require robust security and privacy mechanisms to protect the charging infrastructure and user data. There has been recent interest in securing EVCSs. However, existing research highlights vulnerabilities in various EV charging methods, but there is a lack of a comprehensive solution to address these issues. This article introduces blockchain-based **Self-Sovereign Identity (SSI)** as a novel approach to improve the security and privacy of EV charging systems. Blockchain technology offers a decentralized and immutable ledger that provides a robust foundation for secure data management. SSI builds on this technology by enabling people to create, manage, and share their digital identities securely and privately without relying on centralized authorities. By leveraging the decentralized and immutable nature of the blockchain, SSI can provide a secure and private data exchange that ensures compliance with regulations such as UNECE R155 [1]. The security and privacy of EVCSs have been the subject of increasing research interest in recent years [2, 3]. Numerous studies have focused on identifying and mitigating vulnerabilities in various EV charging methods, including conductive, inductive, and battery-swapping systems [4].

1.1 Security Challenges in EV Charging Systems

Many works highlight the importance of securing the EV charging ecosystem due to its complexity and the sensitive nature of the data involved [5]. The authors in [6] analyzed potential attacks on EV **Charging Station Management Systems (CSMSs)**, such as firmware and billing manipulation, and proposed mitigations, including endpoint authentication, to address information disclosure issues. The article in [7] provided a comprehensive review of the global EV market with a focus on cybersecurity needs, emphasizing the necessity for techniques to prevent the loss or tampering of charging signals through side-channel assaults. In [8], authors recommended a platform to bring together emerging key players for the EVCSs manufacturers and aggregators in order to work on the security issues, agree on requirements, develop capabilities, and liaise with international activities. Moreover, they claim that such a platform could bring the mobility and energy industries together to support the design of a **Public Key Infrastructure (PKI)** platform. Deep learning approaches have been proposed and shown effective for some of the security issues of EVCSs, specifically charge manipulation attacks [9]. Authors in [10] developed a framework for Internet-scale discovery and security analysis of EV charging management systems. In [11], researchers analyze the deployment security of EVCSs and highlight operator-induced vulnerabilities which may cause the ecosystem to be exposed to remote intrusions. Privacy concerns have also been a key research focus. The authors in [12] provided an in-depth analysis of privacy preservation in the EV charging ecosystem, suggesting standardized methodologies for privacy analysis and common naming conventions. Efficient privacy-preserving authentication mechanisms based on elliptic curve cryptography to fulfill re-authentication requirements are proposed in [13].

1.2 EV Charging Communication Protocol Security

Another important concern in securing EV charging systems is the communication protocols used for the interaction between the backend and the CS. As one of the frontiers in the field, authors in [14] developed a protocol for vehicular *ad hoc* network, which later was utilized for the deployment of a secure EV charging system using **Open Charge Point Protocol (OCPP)** [15]. The authors in [16] discussed various backend communication

protocols of the EVCSs and presented their security benefits against each other. The authors in [17] describe potential problems involved in the communication protocols, specifically within the Dutch EVCSs. The paper in [18] examined the security challenges associated with the OCPP, identifying potential security threats and proposing solutions to enhance the security of OCPP-based smart charging scenarios. Similarly, the paper in [19] discussed attacks on OCPP that could lead to energy theft or fraud. In addition to the EVCSs and protocols involved in the process, there have been some works focusing on the security of the mobile applications that interact with the EVCSs [20]. The researchers [21] by developing a framework that is designed to optimize charging price, manage load balancing, and provide security across multiple CS by leveraging the OCPP.

1.3 Blockchain for EV Charging Security and Privacy

The integration of blockchain technology into various domains has shown promising results in enhancing security and privacy, and several works have explored blockchain's role in securing EV charging infrastructures. For instance, authors in [22] proposed blockchain-based EV charging with dynamic tariff decisions for privacy preservation. In [23], similar approach of blockchain-based solutions was used for energy trading schemes for EVs. Meanwhile in [24], intelligent CS selection for EVs is proposed via the blockchain-based framework. Furthermore, in [25], researchers investigated blockchain-based ideas as networking strategy for dynamic wireless charging of EVs. Wang et al. proposed a blockchain-based decentralized energy trading system for **Vehicle-to-Vehicle (V2V)** networks to ensure transaction integrity and prevent energy fraud [26]. Similarly, Khan et al. introduced a secure EV charging scheme that utilizes smart contracts for automated billing and fraud prevention, though it does not address identity management or decentralized authentication [27]. The authors in [28] presented a framework to employ blockchain for enhanced smart grid security. Blockchain's decentralized and immutable nature makes it a suitable candidate for securing the EV charging ecosystem. Studies by [29] proposed intelligent privacy preservation schemes for EV charging infrastructures using local differential privacy techniques. The article in [30] presents a lightweight non-interactive secure charging model that uses blockchain for decentralized trust management between EVs and CSs. Their model focuses on the security of transactions and the execution of smart contracts. The paper in [31] developed a privacy-preserving EV charging system that uses blockchain and fog computing to protect the privacy of charging data. However, their model focuses primarily on the confidentiality of energy transactions, ignoring **End-to-End (E2E)** identity management, real-time authorization and compliance with ISO 15118 and UNECE R155. A two-layer optimization model for EV charging and discharging trading using a consortium blockchain to optimize energy pricing and distributed charging coordination is proposed in [32]. In [33], a new privacy-preserving consensus mechanism for an EV charging scheme has been proposed. As one of the recent manuscript, [34] explored blockchain applications for secure EV charging and energy management for sustainability purposes. While blockchain improves transaction integrity and decentralized security, previous work lacks a structured approach to decentralized identity management in EV charging systems. Most existing studies focus on secure payments and fraud detection rather than addressing the challenges of identity verification and authorization—a limitation that our work addresses by integrating SSI-based authentication mechanisms.

1.4 SSI in EV Charging Systems

SSI has emerged as a promising solution for privacy-preserving identity management in smart city and mobility sectors. Richter et al. discussed that the inherent characteristics of SSI simplify the establishment of trust in service processes but also influence the overall design of the service system, such as EV Charging Systems [35]. An authentication scheme based on SSI has also been proposed and presented for V2V communications recently [36]. Stockburger et al. examined SSI's role in decentralized identity management for smart cities (more specifically public transformation), demonstrating its effectiveness in reducing reliance on central authorities [37]. Similarly, Zeydan et al. proposed an SSI-based mobility framework for secure vehicle access control, enhancing user privacy while eliminating third-party identity providers [38]. However, these previous approaches focus on general

identity management and do not specifically address EV charging ecosystems or energy transactions. However, utilizing SSI has been shown as a favorable solution for the security issues within the EV ecosystem in other previous works such as [39, 40]. The experimental results of SSI integration of the EV charging scheme have also demonstrated its great potential to improve the security of the EVCS [40]. Blockchain-based SSI offers individuals control over their digital identities without relying on centralized authorities [41]. This approach aligns with the principles of decentralized trust and privacy preservation. Despite advances in securing EV charging systems, the integration of blockchain-based SSIs into the EV ecosystem is a novel approach that has not yet been extensively explored. At the same time, a comprehensive integration of blockchain-based SSI with EVCS security—that ensures compliance with standards such as ISO 15118 and UNECE R155 has also not yet been explored in depth.

1.5 Contributions of This Work

Blockchain technology has been recognized for its potential to enhance security across various domains, including IoT and automotive industries. SSI, based on the blockchain-based identity management system, allows individuals to own and control their digital identities. Integrating SSI with EV charging systems can address existing vulnerabilities and provide a robust framework for secure data management. The integration of blockchain-based SSI into EV charging systems can enhance security and privacy in several ways. First, blockchain-based SSI ensures that only authenticated and authorized users can initiate charging sessions, thereby preventing unauthorized access or use. Second, personal and billing information can be encrypted and securely stored on a blockchain network, safeguarding against potential data breaches. Third, all transactions are recorded on the blockchain, ensuring transparency and preventing tampering or fraud. This article aims to bridge this gap by proposing a comprehensive framework that leverages SSI to enhance the security and privacy of EV charging methods, including conductive or inductive charging and battery swapping. We evaluate the security and privacy benefits of SSI and map these improvements to the requirements of cybersecurity regulations such as UNECE R155. Our simulation results show that while traditional **Vehicle-to-Grid (V2G)** authentication systems such as [39] can achieve low latency for EV authentication (28.0 ms) and processing at the CS (45.95 ms), our system has more comprehensive identity networking operations, including credential management and metadata validation, and therefore requires a longer time for identity verification (5 seconds) and presentation (11 seconds). In addition, our system includes Kubernetes-based service orchestration (40 ms) and OpenDaylight configuration (100 ms), which are missing in the V2G scheme. This makes our approach more suitable for comprehensive EV charging security.

The rest of the article is organized as follows. Section 2 presents EV charging ecosystem, security threats, application of STRIDE threat model, and enhanced security with blockchain-based SSI. Section 3 presents the design architecture of the blockchain-based SSI framework. Section 4 presents the integration aspects of blockchain-based SSI with various EV charging methods. Section 5 demonstrates experimental setup and results. Finally, Section 6 provides the conclusions and future work of the article.

2 EV Charging Ecosystem and Security Model

The EV charging ecosystem comprises EVs, EVCS, and power grids with multiple interconnected components, each playing a crucial role in energy transfer, identity verification, and transaction security. Each component is susceptible to various cyber attacks, including spoofing, tampering, and information disclosure. The STRIDE threat model helps identify and categorize these threats, providing a comprehensive understanding of the security landscape. Common vulnerabilities in the EV charging ecosystem include weak authentication mechanisms, unencrypted communication channels, and insecure backend systems. This section provides a structured analysis of (i) key components of the EV charging ecosystem, (ii) security threats affecting charging infrastructure, (iii) STRIDE-based threat modeling, and (iv) integration of blockchain-based SSI as a mitigation strategy.

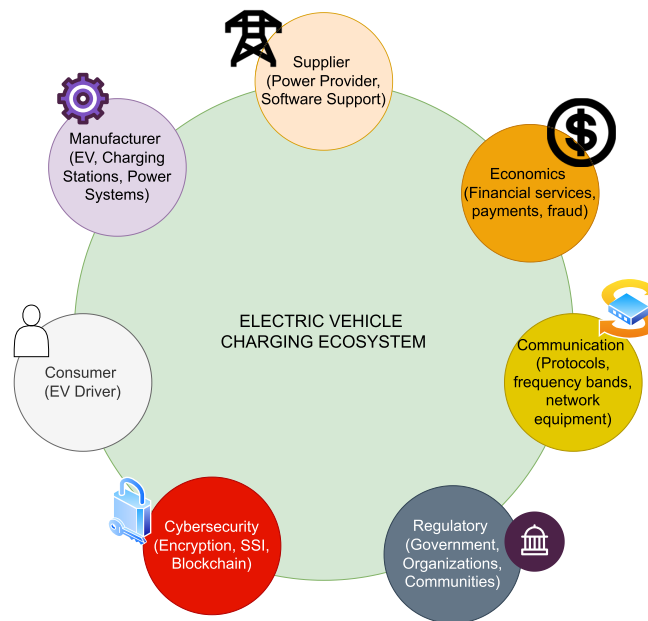


Fig. 1. Components of EVCS ecosystem.

2.1 EV Charging Ecosystem, Components, and SSI

The EV charging ecosystem consists of the following primary components: (i) *EVs*: These are the end users of the charging infrastructure. EVs require secure and reliable methods to charge their batteries while protecting sensitive data such as user identity, payment information, and location data. EVs can easily be equipped with SSI-compatible software for identity management and secure communication. (ii) *EVCS*: These stations serve as the access points for EVs to connect to the electric grid. EVCS can be installed in various locations, including homes, workplaces, and public areas. They are equipped with different types of chargers, such as conductive (**Alternating Current (AC)** and **Direct Current (DC)**) and inductive (static and dynamic) chargers. EVCS can be enhanced with blockchain nodes to facilitate secure data exchange and transaction recording. (iii) *Blockchain Network*: A decentralized network that stores encrypted identities and transaction records, ensuring immutability and transparency. For our environment, they keep track of the EV, power, payment, and location details. (iv) *SSI Framework*: Includes identity creation, verification, and management processes, leveraging blockchain technology. (v) *Backend Systems*: Comprising the **Energy Management System (EMS)** and CSMS, integrated with blockchain for secure operations. (vi) *Power Grid*: This is the network that delivers electricity from producers to consumers. The power grid must be resilient and secure to handle the additional load from EV charging and prevent disruptions.

Additionally, various communication protocols and standards are used to facilitate data exchange between the EV, EVCS, and backend systems. Common protocols include the OCPP (to communicate from CSMS and the physical EVCS) and the open smart charging protocol (to communicate between the management system of a power grid and the CSMS) [4]. The parties involved as contributors or users within the EVCS have been presented in Figure 1. For the BCN-based SSI, all of the parties that are part of the EVCS should have been considered and agreed on the setup and configurations.

In today's digital world, identities are scattered across various platforms and services and the identity data are managed by centralized entities raising concerns about privacy and control. SSI offers a new approach, empowering individuals to own and control their digital identities. The key concepts in SSI are as follows: (i) SSI

puts users in control where what information to share and with whom is decided by users. Unlike traditional systems where companies manage your data, the keys to digital identity are held by users [42]. (ii) The identity is represented by digital credentials issued by trusted parties (e.g., universities, banks). These credentials are cryptographically verifiable, ensuring their authenticity and integrity [43]. (iii) These act as unique identifiers for your SSI. Unlike usernames tied to specific platforms, **Decentralized Identifiers (DIDs)** are independent and remain under your control. (iv) These secure apps store **Verifiable Credentials (VCs)** and allow users to share them selectively with **Service Providers (SPs)** or individuals who need to verify their identity. The main benefits of SSI are (i) enhanced privacy as you control what information you share, reducing unnecessary data collection by third parties; (ii) improved security as the VCs and strong cryptography minimize the risk of data breaches and identity theft, (iii) greater empowerment since the SSI allows you to easily switch SPs without having to re-establish your identity each time, and (iv) reduced friction due to faster and more streamlined identity verification processes across different platforms.

The current main application and use cases of SSI are in healthcare, telecommunication, education, financial services, transportation, and border control domain [44]. It can also empower individuals with greater control and privacy, paving the way for a more secure and user-centric digital future for the EV Charging security problems [39]. However, there are some challenges in adapting SSI with blockchain in the EV Charging schemes since SSI is still an emerging technology, and widespread adoption requires collaboration between various stakeholders. In addition to that, standardization is needed to ensure seamless interaction between different SSI systems.

2.2 Security Threats in the EV Charging Ecosystem (STRIDE Threat Model)

The complexity of the EV charging ecosystem poses numerous security threats that can jeopardize the security, privacy, and reliability of the system. Common security threats include unauthorized access, where unauthorized entities gain access to EVCS or backend systems and manipulate charging sessions, steal personal data, or disrupt operations. Data tampering is another major threat, as attackers can alter data during transmission between EVs, EVCS, and backend systems, leading to incorrect billing, energy theft or system malfunctions. Information disclosure involves the interception and disclosure of sensitive information such as user identity, payment details, and location data during data exchange. **Denial of Service (DoS)** attacks can occur when attackers overload EVCS or backend systems, making them unavailable to legitimate users and interrupting the charging process. In addition, malware and intruders pose a serious risk, as malware can be introduced into the EVCS or backend systems, resulting in data breaches, unauthorized access, and system failures.

The STRIDE threat model provides a structured approach to identifying and categorizing security threats in the EV charging ecosystem [45]. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, DoS, and Elevation of Privilege. Each component of the EV charging ecosystem is analyzed using the STRIDE model to identify potential vulnerabilities and their impacts [46]. Spoofing involves attackers impersonating legitimate entities to gain unauthorized access to the EVCS or backend systems. For example, a common spoofing attack is the use of stolen credentials to initiate a charging session. Tampering refers to the unauthorized modification of data or components within the EV charging ecosystem. An example of tampering is the modification of the firmware in EVCS in order to circumvent security measures. Repudiation is the denial of an action or transaction by an entity, making it difficult to trace and verify activities. An example of repudiation is when a user denies having initiated a charging session or made a payment. Disclosure of information is the unauthorized exposure of sensitive information. For example, intercepting communication between EVs and EVCS to steal personal data is an information disclosure attack. DoS is the disruption of services by overloading the system with excessive requests. Flooding EVCS with illegitimate requests to prevent legitimate charging sessions is a typical DoS attack. Privilege escalation involves the unauthorized acquisition of higher access rights by exploiting vulnerabilities. An example of this is the exploitation of software vulnerabilities in the CSMS to gain administrative rights.

Table 1. Application of Blockchain-Based SSI against Security Threats in EV Charging Systems, as Detailed in [4]

Elements	Security Threat/Attack	Blockchain-Based SSI Mitigation
EVCS	S: Hard-coded credentials/side-channel attack	Use of DIDs and VCs eliminates hard-coded credentials. Secure communication channels reduce the risk of side-channel attacks.
	R: Repudiation by manipulation and obscuration of transaction details	Immutable blockchain records provide non-repudiation and traceability of all transactions.
	E: Loss of financial/energy transaction or non-repudiation	Blockchain's immutable ledger ensures the integrity and non-repudiation of transactions.
CSS	T: Fabrication of metering and tariff information [47]/Injected a Log4Shell payload [48]	Immutable VCs and decentralized verification prevent tampering with metering and tariff information.
ISO 15118	I: Privacy concerns	User-controlled VCs enhance privacy by limiting the exposure of personal data.
IEC 61851	S: Authentication was considered outside the scope of this protocol	SSI provides a robust authentication framework, filling the gap left by the protocol.
EV Driver	S: Side-channel attack	User-controlled, encrypted credentials, and decentralized verification minimize the risk of side-channel attacks on personal data.
	I: Exposure of the EV driver's sensitive data	Blockchain-based encryption and user control over data sharing protect sensitive information.
	I: Through smartphone app access to personal EV driver and vehicle information	Decentralized authentication and encrypted communication channels protect against unauthorized access to personal data via smartphone apps.

S, Spoofing; T, Tampering; R, Repudiation; I, Information Disclosure; E, Elevation of Privilege.

2.3 Blockchain-Based SSI as a Mitigation Strategy

Based on STRIDE threat model, Table 1 presents how the application of blockchain-based SSI can minimize the possible security threats/attacks. Those threats on each component of the EVCS ecosystem are summarized in [4]. Note that in the elements column, the combined charging system is a charging system that has been developed by European and North American car manufacturers since 2011 [49]. ISO 15118 is an international standard that outlines the communication protocol between EVs and CSs [50]. It is part of the broader suite of standards for EV conductive charging systems and is crucial for the development of a seamless and efficient EV charging infrastructure. In addition to that, IEC 61851 is an international standard defining protocols for industrial communication networks, specifically for Fieldbus systems. Fieldbus is a network system for real-time distributed control, often used in manufacturing and process automation [51]. As outlined in Table 1, a blockchain-based SSI system can help mitigate attacks on multiple components that could have a major impact on service availability [52].

Furthermore, Table 2 highlights the key differences between traditional PKI and blockchain-based SSI systems. While PKI relies on centralized certificate authorities to manage trust and identity, SSI shifts control to the users themselves, leveraging DIDs and VCs recorded on blockchain networks [58]. This decentralized model enhances user privacy, supports selective disclosure, and reduces reliance on single points of failure. However, it also introduces new security and operational challenges, particularly around revocation and scalability. The comparison underscores the evolving tradeoffs between centralized and decentralized identity architectures.

3 Blockchain-Based SSI Framework

Blockchain technology offers a decentralized and immutable ledger, making it suitable for secure data management. SSI builds on this foundation, allowing individuals to create, manage, and share their digital identities securely. In the context of EV charging, SSI can ensure that only authenticated and authorized entities can access sensitive data. The proposed SSI framework includes identity creation, verification, and secure data exchange

Table 2. Comparison of Traditional PKI and Blockchain-Based SSI

Feature	Traditional PKI	Blockchain-Based SSI
Trust Model	Relies on centralized certificate authorities (CAs) to establish and validate trust [53]	Trust is distributed across participants in a blockchain network [54]
Identity Control	Identities are issued and managed by external entities like CAs or identity providers	Users generate and manage their own identifiers and credentials [55]
Revocation	Depends on Certificate Revocation Lists or the Online Certificate Status Protocol to revoke certificates [56]	Revocation can be handled through blockchain-based registries or cryptographic proofs
Authentication	Typically involves validating X.509 certificates through a CA hierarchy	Uses DIDs and VCs for trust establishment [57]
Scalability	Performance may be constrained by the central certificate infrastructure	Designed to scale with network growth and distributed verification
Interoperability	Varies based on protocol and CA compatibility	Promotes open standards such as W3C DID and VC for cross-platform use [57]
Security Risks	Centralized trust anchors are vulnerable to compromise or misuse	More resilient to centralized failure but may face smart contract and consensus risks
User Privacy	Limited control over how identity data are used; metadata exposure is common	Enables selective disclosure and improves user privacy control [54]

processes, all anchored on a blockchain platform. The integration of blockchain-based SSI into the EV charging ecosystem provides a robust solution to address security and privacy challenges. This section details the design and architecture of the proposed SSI framework, explaining how it enhances the security and privacy of EV charging systems.

3.1 Design and Architecture of the SSI Framework

The proposed SSI framework for EV charging systems consists of several key components and processes. First, DIDs are created for each user (EV owner) as unique identifiers stored on the blockchain. These DIDs are cryptographic keys that provide a secure way to reference user identities. Users manage their DIDs through digital wallets, which securely store cryptographic keys and credentials. Second, VCs are issued by trusted entities, such as EV manufacturers and CS operators, to users. These credentials contain attestations about the user, such as ownership of an EV, subscription details, and payment information. When users initiate a charging session, they present their VCs, which are cryptographically verified against the issuer's public key stored on the blockchain. The third component is the blockchain network, where a decentralized ledger records all transactions related to identity creation, credential issuance, and verification, ensuring transparency and preventing tampering. Smart contracts automate the execution of identity verification and transaction processes, ensuring that only valid transactions are recorded on the blockchain. Fourth, digital wallets securely store DIDs of users, cryptographic keys, and VCs. These wallets enable users to manage their identities and control access to their personal data, interacting with the blockchain network to authenticate users, verify credentials, and facilitate secure data sharing.

Enhancing security and privacy with SSI involves several measures. For authentication, users authenticate themselves at the CS using their DIDs and VCs stored in their digital wallets. The blockchain verifies these credentials, ensuring that only authorized users can access the charging services. This decentralized authentication process eliminates the need for centralized identity providers, reducing the risk of identity theft and unauthorized access. For data privacy, personal and billing information is encrypted and stored on the blockchain, and only authorized entities with the correct cryptographic keys can access this information. Users have complete control over their data and can decide which credentials to share and with whom, enhancing privacy and reducing the risk of data breaches. Data integrity is ensured through the immutability of the blockchain's ledger, which

guarantees that once data is recorded, it cannot be altered or deleted. This ensures the integrity of identity and transaction records, with all transactions transparently recorded on the blockchain, allowing for easy auditing and verification. Non-repudiation is achieved as all actions, including identity verifications and charging transactions, are recorded on the blockchain, providing a verifiable trail of all interactions and preventing users from denying their actions.

3.2 Compliance with UNECE R155

The proposed blockchain-based SSI framework is in line with UNECE R155, a cybersecurity regulation that mandates robust security measures for vehicles and their external interfaces, including EV charging infrastructure. To achieve compliance, a CSMS must have a clearly defined scope, conduct a systematic risk analysis, implement an action plan, and ensure continuous monitoring to mitigate cybersecurity threats. Our framework meets these compliance requirements by integrating decentralized authentication, secure identity verification, data encryption, and blockchain-based logging into the EV charging ecosystem. An important requirement of UNECE R155 is risk management, which our framework ensures through decentralized authentication and credential verification mechanisms. By using DIDs and VCs stored on a blockchain, the system eliminates the need to rely on central identity providers, reducing the risk of credential theft, spoofing attacks and unauthorized access. In addition, data protection measures can be enforced through cryptographic encryption and selective disclosure, ensuring that sensitive user and billing data remains private and only authorized entities can access the data. Our framework also addresses authentication and access control by ensuring that only verified EVs and users can initiate charging sessions. Unlike traditional identity management systems that rely on centralized trust anchors, our approach allows CSs to act as independent verifiers, reducing the risk of man-in-the-middle attacks and single points of failure. In addition, transparent auditability can be achieved through blockchain-based logging, in which all identity verifications, authentication attempts, and charging transactions are immutably recorded. This ensures tamper-proof security logs that enable auditors and regulators to verify compliance with UNECE R155 requirements for cybersecurity monitoring and incident response. Finally, compliance with UNECE R155 requires a formal certification process to confirm that all cybersecurity measures are in place. Our framework enables audit trails for regulatory certification by maintaining a blockchain-based record of all security events, risk mitigations, and policy enforcement actions. This ensures that charging infrastructure operators can demonstrate compliance with cybersecurity best practices and regulatory standards, which ultimately strengthens the overall security of EV charging ecosystems.

4 Integration of SSI with EV Charging Methods

Figure 2 presents the general structure of the blockchain-based SSI framework for EV charging security. This framework consists of several key components that work together to provide decentralized identity management, authentication, and secure transaction recording. In this architecture, the SSI blockchain is responsible for identity-related operations, including decentralized authentication, credential issuance, and verification. The Issuer (a regulatory authority or trusted entity) is responsible for issuing VCs to EVs. These credentials contain information such as the vehicle's identity, registration details, and authorization to access charging services. The EV, acting as the holder, stores these credentials in its digital wallet, which is used to authenticate at CSs without relying on centralized identity providers. To maintain a clear separation between identity management and operational data storage, a separate blockchain network is introduced for storing records of charging sessions, energy transactions and billing details. This ensures that identity verification remains independent of service usage logs, improving data privacy, scalability, and regulatory compliance. The CSMS acts as the verifier, validating the credentials presented before granting access to charging services. The blockchain network also supports real-time credential revocation and status updates, ensuring that only valid and authorized identities can participate in charging operations. The integration of blockchain-based SSI into the EV charging ecosystem significantly

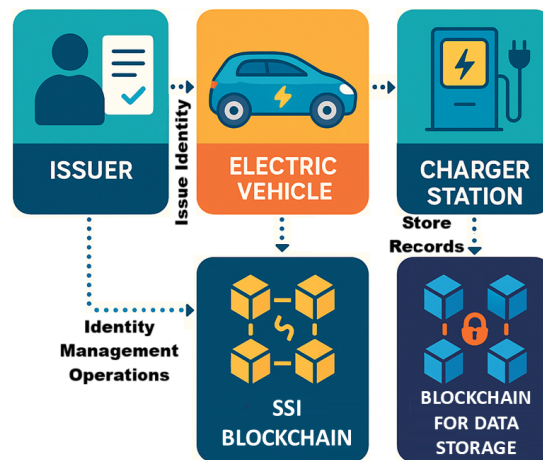


Fig. 2. The general framework for enhanced security and privacy for EVs.

enhances security and privacy. By leveraging decentralized identity management and secure data practices, the proposed SSI framework addresses existing vulnerabilities and ensures compliance with cybersecurity regulations, providing a robust solution for the future of EV charging systems. Three main categories of EV charging are defined in [4], namely conductive, inductive, and battery-swapping charging. The integration of blockchain-based SSI with various EV charging methods—conductive, inductive, and battery swapping—can provide enhanced security and privacy.

4.1 Conductive Charging

Conductive charging involves the direct transfer of electrical energy through a physical connection using electrical contacts and is divided into two subcategories: AC charging and DC charging. AC charging, which typically uses an integrated charger to convert AC to DC for battery storage, is slower and is typically used at home or at work. DC charging, on the other hand, utilizes off-board chargers to provide DC directly to the battery, which allows for faster charging speeds and is usually found at public CSs. By integrating blockchain-based SSI into conductive charging, the security and privacy of the system can be significantly improved. SSI ensures secure communication between the EV, the EVCS, and the backend systems, and only authorized users can initiate charging sessions through secure authentication mechanisms. In addition, personal data and billing information are encrypted and stored in a decentralized ledger to prevent unauthorized access. All transactions are recorded in the blockchain, which ensures transparency and prevents tampering or fraud.

Figure 3 shows the conductive charging EV ecosystem with blockchain-based SSI integration. Solid lines represent the wired connections, while dotted lines are wireless connections. The system components are as follows: The EV acts as the holder of VCs issued by a regulatory entity. The issuer is a regulatory entity responsible for issuing these VCs. The CSMS functions as the verifier, ensuring that only authenticated and authorized EVs can access the charging services. The regulatory entity certifies the identity and permissions of the EV and its owner. The blockchain network serves as a decentralized ledger that records all transactions, ensuring transparency and immutability. The digital wallet securely stores the EV's DIDs and VCs. The EV battery storage system manages battery storage and swapping operations, while the EMS oversees the distribution of energy from the power grid to the EV battery storage system.

The workflow structure of the conductive charging EV ecosystem integrated with blockchain-based SSI is as follows: The process begins with the identity and credential issuance phase. The EV owner first registers the EV

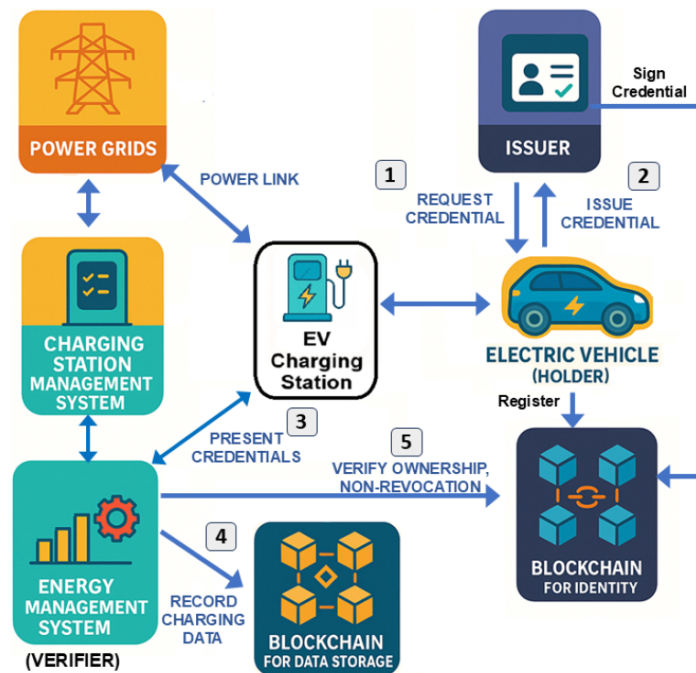


Fig. 3. A schematic structure of a conductive charging EV ecosystem integrated with Blockchain-based SSI. The illustration highlights how secure access control and encrypted transactions ensure data privacy and physical access security for conductive charging.

with the regulatory entity. The regulatory entity then verifies the EV's details and the owner's identity (step 1). Following this verification, the regulatory entity issues a VC to the EV (step 2). This credential includes essential information such as the EV's identity, registration number, and permissions. The credential is cryptographically signed by the regulatory entity and stored securely in the EV's digital wallet. In the next phase, authentication and authorization at the CS take place. When the EV arrives at the CS, it connects to the charging point and initiates a charging session request to the CSMS. Acting as the holder, the EV presents its VCs to the CSMS (step 3). This credential contains the EV's identity and authorization to use the CS. The CSMS, functioning as the verifier, receives the credential and verifies its authenticity by checking the cryptographic signature against the issuer's public key stored on the blockchain (step 4). The CSMS also validates the credential's content, including its validity and permissions. If the credential is successfully verified, the CSMS grants the EV access to the charging services and records the transaction details on the blockchain, ensuring transparency and immutability.

During the charging session management phase, the EV starts charging while the CSMS monitors the session. The CSMS records relevant data, such as the amount of energy transferred and the duration of the session, in a separate blockchain network (step 5). Upon completion of the charging session, the CSMS calculates the cost based on the energy consumed. Payment information is securely exchanged between the EV and the CSMS, leveraging blockchain technology for secure and transparent transactions. Finally, in the post-charging session phase, the CSMS records the entire charging session, including authentication and transaction details, on the blockchain. This ensures that all actions are transparent, auditable, and tamper-proof. If there are any changes in the EV's status or permissions, such as a renewal of registration, the regulatory entity can issue updated credentials. These updated credentials are stored in the EV's digital wallet and can be presented in future charging sessions, maintaining the security and integrity of the system.

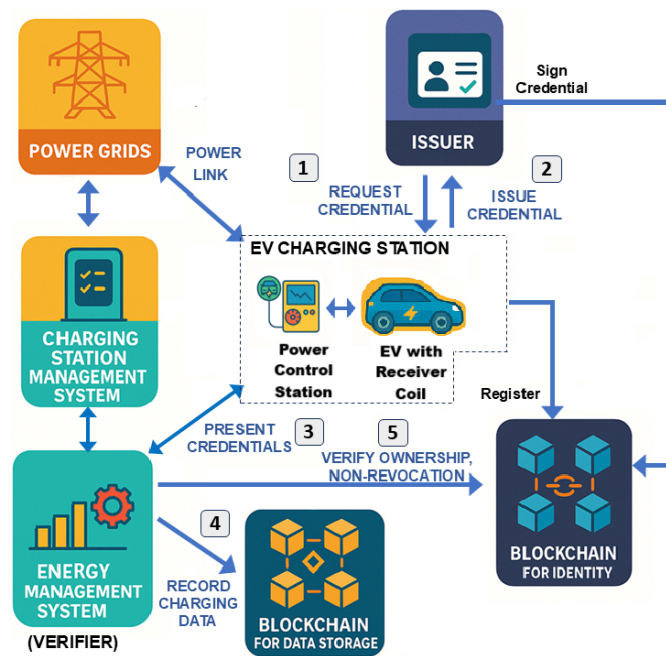


Fig. 4. A schematic structure of the inductive charging EV ecosystem integrated with Blockchain-based SSI. The figure demonstrates the framework's ability to provide anonymous authentication and secure communication for wireless energy transfer in public or dynamic settings.

The blockchain-based SSI framework provides significant value to conductive charging by mitigating risks of unauthorized physical access through robust authentication mechanisms. For example, in a home or workplace setup, this ensures that only authenticated users can utilize the CS, enhancing user confidence. Additionally, the framework's ability to encrypt personal and payment data further safeguards users against potential breaches, a critical requirement for private charging environments.

4.2 Inductive Charging

Inductive charging, also known as wireless charging, uses electromagnetic fields to transfer energy between a transmitting coil in the CS and a receiving coil in the EV. This method can be static, where the energy is transferred while the vehicle is stationary, such as in parking lots, or dynamic, where the energy is transferred while the vehicle is in motion, such as on specially equipped roads. The integration of blockchain-based SSI into inductive charging improves secure communication between the EV and the charging infrastructure and ensures data integrity. Inductive charging can benefit from the decentralized nature of blockchain, reducing the risk of centralized attack vectors. SSI also enables anonymous authentication, which protects users' identity while enabling charging. In addition, only verified and authenticated vehicles can access the inductive charging infrastructure, reducing the risk of unauthorized use. Figure 4 shows the inductive charging method integrated with blockchain-based SSI. In this diagram, charging is carried out when the EV is stopped in a public or private area so the power control station can be located in a public or private area.

The workflow for integrating BCN-based SSI in an inductive charging system involves several key steps, as shown in Figure 5. The process begins with the identity and credential issuance phase. This step is similar to the registration phase of conductive charging; however, this time, the EVCS first registers the EV with the regulatory

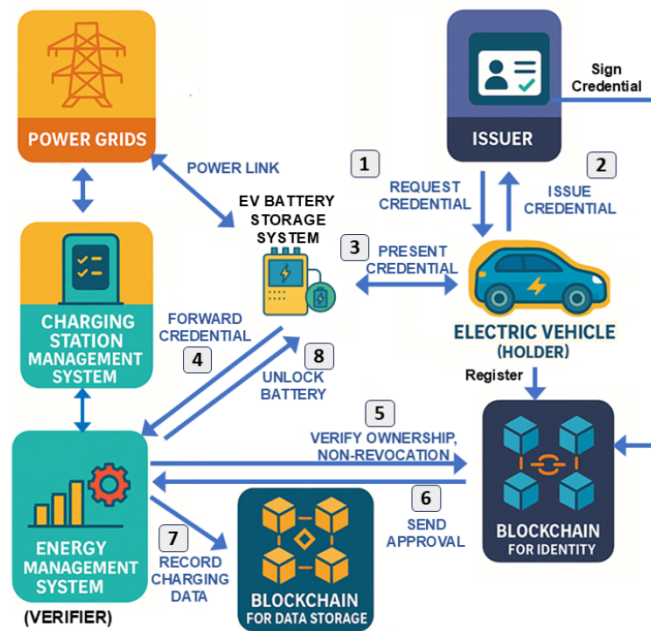


Fig. 5. A schematic structure of the EV battery-swapping ecosystem integrated with Blockchain-based SSI. The workflow emphasizes supply chain transparency and fraud prevention enabled by the immutable blockchain ledger for battery lifecycle management.

entity. The regulatory entity then verifies the EV's details and the owner's identity. Following this verification, the regulatory entity issues a VC to the EV, including essential information such as the EV's identity, registration number, and permissions. This credential is cryptographically signed by the regulatory entity and stored securely in the EV's digital wallet. In the authentication and authorization phase at the CS, the EV arrives at the inductive CS and positions itself over the transmitting coil. The EV initiates a charging session request to the CSMS. Similar to the conductive charging process, the EV presents its VCs to the CSMS, containing the EV's identity and authorization to use the CS. The CSMS, acting as the verifier, receives the credential and verifies its authenticity by checking the cryptographic signature against the issuer's public key stored on the blockchain. The CSMS also validates the credential's content, including its validity and permissions. Upon successful verification, the CSMS grants the EV access to the charging services and records the transaction details on the blockchain, ensuring transparency and immutability.

During the charging session management phase, the EV starts charging wirelessly through the inductive charging pad while the CSMS monitors the session. This step involves recording relevant data, such as the amount of energy transferred and the duration of the session, similar to the process in conductive charging. Upon completion of the charging session, the CSMS calculates the cost based on the energy consumed, and payment information is securely exchanged between the EV and the CSMS, leveraging blockchain technology for secure and transparent transactions. In the post-charging session phase, the CSMS records the entire charging session, including authentication and transaction details, on the blockchain. This ensures that all actions are transparent, auditable, and tamper-proof, mirroring the steps in the conductive charging process. If there are any changes in the EV's status or permissions, such as a renewal of registration, the regulatory entity can issue updated credentials. These updated credentials are stored in the EV's digital wallet and can be presented in future charging sessions, maintaining the security and integrity of the system.

In the case of inductive charging, the framework's unique support for anonymous authentication is particularly valuable. Wireless communication used in public or dynamic charging settings, such as highways, is prone to eavesdropping and interception. By enabling encrypted and anonymous interactions between vehicles and infrastructure, the framework minimizes exposure to such risks while maintaining seamless user experiences. These improvements are critical for public adoption of wireless charging.

4.3 Battery Swapping

Battery swapping involves the replacement of a depleted battery with a fully charged one at special battery-swapping stations. This method is fast and can be more convenient than conventional charging methods. The blockchain-based SSI integration for battery swapping ensures that users' identities are verified and that only authorized personnel have access to the batteries and can swap them, preventing unauthorized access and data breaches. Information about battery usage and user data is securely managed in a blockchain, ensuring privacy and preventing unauthorized access. In addition, the blockchain records all battery swaps and the associated transactions to prevent fraud and ensure transparency of the entire process.

The workflow for the battery-swapping system integrated with BCN-based SSI begins with the EV owner requesting VCs from the regulatory entity, known as the issuer. The EV owner provides the necessary information to the issuer to validate the identity and ownership of the EV (step 1). Once the issuer verifies this information, it issues the VCs, which include details such as the EV's identity, registration number, and permissions (step 2). These credentials are cryptographically signed by the issuer and stored in the EV's digital wallet. The credentials are also registered on the SSI blockchain, ensuring immutability and allowing for easy verification. When the EV arrives at the battery-swapping station, it presents its VCs to the EV battery storage system (step 3). The credentials are then forwarded to the CSMS for verification (step 4). The CSMS, acting as the verifier, checks the authenticity of the credentials by verifying the cryptographic signatures against the issuer's public key stored on the SSI blockchain (step 5). The CSMS also verifies the ownership, authorship, and non-revocation status of the credentials to ensure they are still valid and have not been revoked. Upon successful verification (step 1), the SSI blockchain sends approval to the CSMS, and later, it is forwarded to the EV battery storage system to proceed with the battery-swapping process. The EV battery storage system then unlocks the battery and initiates the swapping process, replacing the old battery with a fully charged one (step 6). The details of the battery swap, including the credentials verification and transaction, are recorded on the SSI blockchain to ensure transparency and immutability (step 7). By using DIDs and VCs, the identity of the EV is managed decentrally, reducing dependence on central authorities and minimizing the risk of identity theft. Blockchain also ensures that all transactions and credentials are recorded immutably, providing a transparent and tamper-proof audit trail. Finally, the EV owner retains control over their personal data and credentials and decides what information they want to share and with whom. This strengthens privacy and data protection. Each integration described above also needs to be aligned with UNECE R155 regulations to ensure compliance and robust security measures. The battery-swapping process benefits from the SSI framework's ability to maintain transparency and accountability in the supply chain. By securely recording all battery swaps on an immutable blockchain ledger, the system prevents fraud and ensures traceability of battery usage. This is particularly advantageous for fleet management operations, where reliable data on battery lifecycle and usage can optimize logistics and operational efficiency.

Note that in the above scenarios, the proposed system complies well with UNECE R155 cybersecurity regulations and ISO 15118 Plug & Charge authentication standards, ensuring regulatory compliance and interoperability with modern EV infrastructure. For example, the standard SSI models often require external verifiers (e.g., a government agency or manufacturer) to validate credentials, resulting in additional verification delays. In our framework, CSMSs act as verifiers and enable local validation of credentials without contacting an external trust authority, reducing latency and external dependencies.

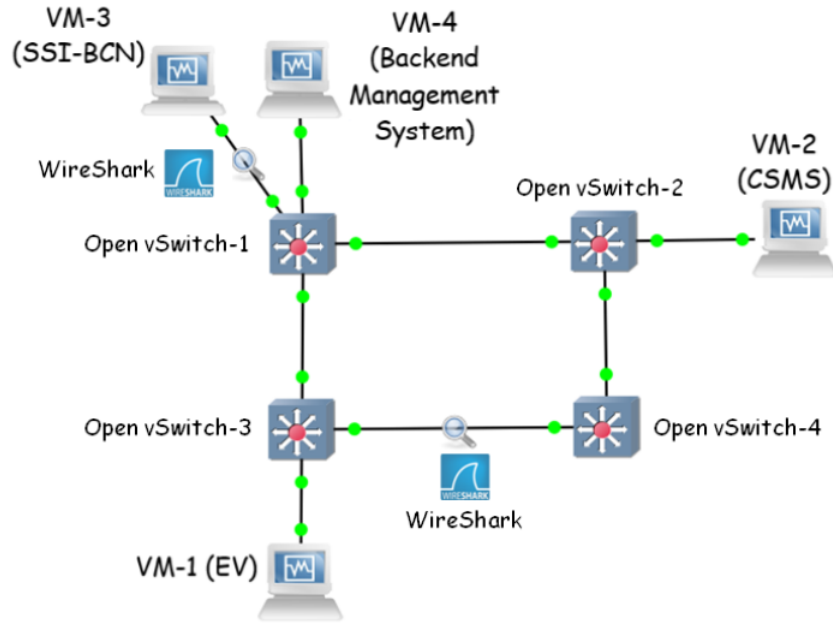


Fig. 6. Experimental setup created with the GNS3 emulation environment for validation purposes.

5 Experimental Evaluations

5.1 Test Setup

We implemented a test setup in the GNS3 emulation environment, to simulate a conductive EV charging infrastructure with blockchain-based SSI authentication and authorization. As shown in Figure 6, the setup models the interactions between an EV, CSMS, regulatory entity, and backend infrastructure, ensuring secure identity verification and transaction processing. To emulate the conductive charging network, four Open vSwitch instances were installed within the GNS3 environment, representing different network components. Additionally, four VMs running Ubuntu 16 LTS were deployed, each serving a distinct role: (i) VM-1 (EV Node in the figure) simulates the EV, managing its DID, and VCs stored in a digital wallet. The EV interacts with the CSMS to authenticate itself before initiating a charging session. (ii) VM-2 (CSMS in the figure) acts as the verifier for EV authentication requests. It queries the blockchain-based SSI network to validate the EV's credentials before authorizing charging. (iii) VM-3 (SSI blockchain network) hosts the SSI blockchain network, implemented using Von-network (Hyperledger Indy). It maintains two separate ledgers—one for CSs and CSMS and another for EVs and regulatory entities. Each device is assigned a DID and associated metadata for access control. Finally, VM-4 (backend management system in the figure) simulates the backend services for monitoring, transaction logging and management operations using OpenDaylight and Kubernetes. It retrieves authentication data from the blockchain to ensure secure and tamper-proof charging.

To manage network configuration, OpenDaylight was installed on the CSMS VM (VM-2), enabling real-time network control and policy enforcement. Kubernetes was deployed on VM-4 to orchestrate charging session management services, ensuring efficient resource allocation. The CSMS retrieves configuration parameters from the SSI blockchain network via Python scripts, allowing dynamic authentication policy updates based on revoked or newly issued credentials. For secure plug and charge authentication, Hyperledger Indy scripts have been extended to read metadata information from the digital wallets of EVs and CSMS nodes. This metadata includes charging authorizations, CSMS configuration parameters for access control, and transaction logs for authentication

Table 3. Comparison of Identity Networking Operations and Authentication Computation Costs in Time

Operation	Proposed Framework	V2G SSI Scheme [39]	SSI for EVCS [40]
Wallet Creation	≈ 200 ms	Not Evaluated	Not Applicable
Identity Verification	≈ 5 seconds	28.0 ms (EV Authentication)	487 ms
Identity Presentation	≈ 11 seconds	69 ms	69 ms
Identity Metadata Reading	≈ 3 seconds	Not Evaluated	Not Evaluated
OpenDaylight Configuration	≈ 100 ms	Not Applicable	Not Applicable
Kubernetes Deployment	≈ 40 ms	Not Applicable	Not Applicable
E2E Service Creation	≈ 3.1 seconds	45.95 ms (CS/SP Processing Time)	Not Applicable
Identity Revocation	≈ 19 seconds	Supports Dynamic Revocation, Exact Time Not Given	Not Evaluated

and billing audits. During the test, a complete E2E charging session between the EV (VM-1) and the CSMS (VM-2) was simulated. It verified the successful authentication of the EV with the VCs stored in the digital wallet, the ability of the CSMS to validate the credentials against the SSI blockchain network, the tamper-proof recording of the transaction in the blockchain, and the secure exchange of charging and billing data between the CSMS and the backend services.

5.2 Results and Discussions

We compare our proposed blockchain-based SSI framework for EV charging with the privacy-preserving authenticated key exchange protocol for V2G communications using SSI from the referenced article [39]. Our work focuses on the security of EV charging across different charging methods (conductive, inductive, battery swap), while the [39] is specifically focused on V2G energy transactions and ensures security and privacy in energy exchange. Regarding integration with EV Charging Standards, our framework is explicitly aligned with ISO 15118 (Plug & Charge) and UNECE R155 (Cybersecurity in EVs) whereas the reference paper does not explicitly consider standard compliance, though it ensures general security. Regarding the role of CSs in decentralized authorization, in our framework, CSs act as verifiers, which enables a fully decentralized trust model for peer-to-peer authentication. In [39], the SPs are still involved in key management and revocation policies, making it less decentralized.

Table 3 shows the identity networking operations of the proposed framework with the computation costs from the paper (V2G authentication scheme) [39] and in [40] (SSI for EVCS). The comparison between our proposed blockchain-based SSI framework, the V2G authentication scheme, and the SSI for EVCS framework from the referenced papers reveals significant differences in terms of performance, scope, and optimization strategies. In terms of wallet and identity operations, the V2G authentication scheme achieves the lower latency in authentication with an EV-side computation time of 28 ms, and the SSI for the EVCS framework has a 487 ms [40]. Meanwhile, for identity presentation, both of the related works have a 69 ms latency. For the CS/SP processing time of 45.95 ms, our framework exhibits higher identity verification (5 seconds) and presentation times (11 seconds). This discrepancy arises because our system involves broader identity networking tasks, including credential management and metadata verification, rather than focusing solely on cryptographic authentication. Additionally, our framework incorporates service deployment mechanisms, such as Kubernetes-based orchestration (40 ms) and OpenDaylight configurations (100 ms), which are not evaluated in the reference papers since they primarily focus on cryptographic authentication rather than system-wide identity and service management. Another notable difference lies in identity revocation, where our system requires approximately 19 seconds to revoke credentials. In contrast, one of the reference papers supports dynamic credential revocation but does not explicitly quantify its latency [39]. Meanwhile, authors in [40] do not specifically discuss about the revocation of SSI.

When considering E2E service creation, our framework exhibits a total latency of 3.100 seconds, which is significantly higher than the V2G scheme's authentication time at the CS (45.95 ms). This is expected, as our system handles network-level service instantiation and decentralized identity validation, while the V2G scheme is highly optimized for lightweight cryptographic operations in a restricted V2G authentication context. Overall, the comparisons reveal that while the V2G scheme is computationally efficient for cryptographic authentication, our proposed framework prioritizes broader identity management, service orchestration, and regulatory compliance, making it more suitable for EV charging ecosystems rather than purely V2G key exchange. Future optimizations can focus on reducing identity verification and presentation times to achieve performance levels closer to cryptographic authentication schemes while maintaining the scalability, privacy, and decentralized trust model of the proposed architecture.

6 Conclusion and Future Work

This article presents a comprehensive analysis of the integration of blockchain-based SSI with EV charging systems to improve security and privacy. The analysis covered the architecture and security model of EV charging systems, identified common security threats using the STRIDE threat model, and showed how SSI can improve security and privacy in different EV charging methods. The proposed framework addresses existing vulnerabilities and ensures compliance with cybersecurity regulations. By leveraging the decentralized and immutable nature of blockchain, the proposed SSI framework ensures secure and private data exchanges between EVs, CSs, and backend systems. The detailed design and architecture of the SSI framework highlight its capability to provide robust authentication, data integrity, privacy, and non-repudiation. This framework is implemented in various EV charging methods, including conductive, inductive, and battery swapping, demonstrating its versatility and effectiveness. Each workflow leveraged decentralized identity management and secure data practices to improve security, privacy, and transparency in the battery-swapping processes. By using DIDs and VCs, the EV's identity is managed decentrally, reducing dependence on central authorities and minimizing the risk of identity theft. The blockchain also ensures that all transactions and credentials are immutably recorded and provides a transparent and tamper-proof audit trail. In addition, the EV owner retains control over their personal data and credentials and decides what information to share and with whom, thereby enhancing privacy and data protection. In contrast to previous V2G authentication systems that focus primarily on cryptographic authentication of energy transactions, our work involves comprehensive E2E testing of a blockchain-based SSI framework tailored to the EV charging ecosystem. Our evaluation focused on identity verification, credential management, and service orchestration. The results show fast wallet creation (200 ms), efficient metadata retrieval (3 seconds), and low-latency service deployment using Kubernetes (40 ms) and OpenDaylight (100 ms), ensuring seamless identity management and secure service execution. Future research can explore advanced cryptographic techniques, cross-platform integration, and user-centric approaches to further enhance the framework.

References

- [1] Rohit Bohara, Mirko Ross, Sven Rahlfs, and Sara Ghatta. 2023. Cyber security and software update management system for connected vehicles in compliance with UNECE WP, 29, r155 and r156.
- [2] Ponnuru Raveendra Babu, Basker Palaniswamy, Alavalapati Goutham Reddy, Vanga Odelu, and Hyun Sung Kim. 2022. A survey on security challenges and protocols of electric vehicle dynamic charging system. *Security and Privacy* 5, 3 (2022), e210.
- [3] Joseph Antoun, Mohammad Ekramul Kabir, Bassam Moussa, Ribal Atallah, and Chadi Assi. 2020. A detailed security assessment of the EV charging ecosystem. *IEEE Network* 34, 3 (2020), 200–207.
- [4] Gianpiero Costantino, Marco De Vincenzi, Fabio Martinelli, and Ilaria Matteucci. 2023. Electric vehicle security and privacy: A comparative analysis of charging methods. In *2023 IEEE 97th Vehicular Technology Conference (VTC '23-Spring)*. IEEE, 1–7.
- [5] Anchali Ahalawat, Sridhar Adepu, and Joseph Gardiner. Security threats in electric vehicle charging. 2022. In *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 399–404.
- [6] Tony Nasr, Sadegh Torabi, Elias Bou-Harb, Claude Fachkha, and Chadi Assi. 2022. Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. *Computers & Security* 112 (2022), 102511.

- [7] Mohan Bharathidasan, V. Indragandhi, Vishnu Suresh, Michał Jasiński, and Zbigniew Leonowicz. 2022. A review on electric vehicle: Technologies, energy trading, and cyber security. *Energy Reports* 8 (2022), 9662–9685.
- [8] Roberto Metere, Myriam Neaimeh, Charles Morisset, Carsten Maple, Xavier Bellekens, and Ricardo M. Czekster. 2021. Securing the electric vehicle charging infrastructure. arXiv:2105.02905. Retrieved from <https://arxiv.org/abs/2105.02905>
- [9] Hamidreza Jahangir, Subhash Lakshminarayana, and H. Vincent Poor. 2024. Charge manipulation attacks against smart electric vehicle charging stations and deep learning-based detection mechanisms. *IEEE Transactions on Smart Grid* 15, 5 (Sep. 2024), 5182–5194.
- [10] Tony Nasr, Sadegh Torabi, Elias Bou-Harb, Claude Fachkha, Chadi Assi. 2023. ChargePrint: A framework for internet-scale discovery and security analysis of EV charging management systems. In *Network and Distributed System Security Symposium*.
- [11] Khaled Sareddine, Mohammad Ali Sayed, Chadi Assi, Ribal Atallah, Sadegh Torabi, Joseph Khoury, Morteza Safaei Pour, and Elias Bou-Harb. 2023. EV charging infrastructure discovery to contextualize its deployment security. *IEEE Transactions on Network and Service Management* 21, 1 (2023), 1287–1301.
- [12] Andreas Unterweger, Fabian Knirsch, Dominik Engel, Daria Musikhina, Ammar Alyousef, and Hermann de Meer. 2022. An analysis of privacy preservation in electric vehicle charging. *Energy Informatics* 5, 1 (2022), 3.
- [13] Abdullah M. Almuhaideb and Sammar S. Algothami. 2022. Efficient privacy-preserving and secure authentication for electric-vehicle-to-electric-vehicle-charging system based on ecqv. *Journal of Sensor and Actuator Networks* 11, 2 (2022), 28.
- [14] Dhaou Said and Hussein T. Mouftah. 2017. Novel communication protocol for the EV charging/discharging service based on VANETs. *IEEE Transactions on Intelligent Vehicles* 2, 1 (2017), 25–37.
- [15] Binod Vaidya and Hussein T. Mouftah. 2018. Deployment of secure EV charging system using open charge point protocol. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 922–927.
- [16] Zoya Pourmirza and Sara Walker. 2021. Electric vehicle charging station: Cyber security challenges and perspective. In *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*. IEEE, 111–116.
- [17] Pol Van Aubel and Erik Poll. 2022. Security of ev-charging protocols. arXiv:2202.04631. Retrieved from <https://arxiv.org/abs/2202.04631>
- [18] Zacharenia Garofalaki, Dimitrios Kosmanos, Sotiris Moschogiannis, Dimitrios Kallergis, and Christos Douligeris. 2022. Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp). *IEEE Communications Surveys & Tutorials* 24, 3 (2022), 1504–1533.
- [19] Cristina Alcaraz, Jesus Cumplido, and Alicia Trivino. 2023. Ocpp in the spotlight: Threats and countermeasures for electric vehicle charging infrastructures 4.0. *International Journal of Information Security* 22, 5 (2023), 1395–1421.
- [20] Khaled Sareddine, Mohammad Ali Sayed, Sadegh Torabi, Ribal Atallah, and Chadi Assi. 2023. Investigating the security of EV charging mobile applications as an attack surface. *ACM Transactions on Cyber-Physical Systems* 7, 4 (2023), 1–28.
- [21] Safa Hamdare, David J. Brown, Yue Cao, Mohammad Aljaidi, Omprakash Kaiwartya, Rahul Yadav, Pratik Vyas, and Manish Jugran. 2024. EV charging management and security for multi-charging stations environment. *IEEE Open Journal of Vehicular Technology* 5 (2024), 807–824.
- [22] Fabian Knirsch, Andreas Unterweger, and Dominik Engel. 2018. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Computer Science-Research and Development* 33 (2018), 71–79.
- [23] Mohamed Baza, Ahmed Sherif, Mohamed M. E. A. Mahmoud, Spiridon Bakiras, Waleed Alasmay, Mohamed Abdallah, and Xiaodong Lin. 2021. Privacy-preserving blockchain-based energy trading schemes for electric vehicles. *IEEE Transactions on Vehicular Technology* 70, 9 (2021), 9369–9384.
- [24] Syed Muhammad Danish, Kaiwen Zhang, and Hans-Arno Jacobsen. 2020. A blockchain-based privacy-preserving intelligent charging station selection for electric vehicles. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 1–3.
- [25] Mahmoud Abouyoussef and Muhammad Ismail. 2021. Blockchain-based privacy-preserving networking strategy for dynamic wireless charging of EVs. *IEEE Transactions on Network and Service Management* 19, 2 (2021), 1203–1215.
- [26] Yingsen Wang, Dongxu Zhang, Yixiao Li, Weihai Jiao, Guibin Wang, Juanjuan Zhao, Yan Qiang, and Keqin Li. 2024. Enhancing power grid resilience with blockchain-enabled vehicle-to-vehicle energy trading in renewable energy integration. *IEEE Transactions on Industry Applications* 60, 2 (Mar.–Apr. 2024), 2037–2052.
- [27] Prince Waqas Khan and Yung-Cheol Byun. Blockchain-based peer-to-peer energy trading and charging payment system for electric vehicles. *Sustainability* 13, 14 (2021), 7962.
- [28] Raphaëlle Akhras, Wassim El Hajj, Hazem Hajj, Khaled Shaban, and Rabih Jaber. 2023. Ecc: Enhancing smart grid communication with ethereum blockchain, asymmetric cryptography, and cloud services. In *2023 IEEE 10th International Conference on Data Science and Advanced Analytics (DSAA)*. IEEE, 1–10.
- [29] Shafkat Islam, Shahriar Badsha, Shamik Sengupta, Ibrahim Khalil, and Mohammed Atiquzzaman. 2022. An intelligent privacy preservation scheme for EV charging infrastructure. *IEEE Transactions on Industrial Informatics* 19, 2 (2022), 1238–1247.
- [30] Xiaohong Huang, Cheng Xu, Pengfei Wang, and Hongzhe Liu. 2018. LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access* 6 (2018), 13565–13574.
- [31] Hongzhi Li, Dezhi Han, and Mingdong Tang. 2020. A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing. *IEEE Systems Journal* 15, 3 (2020), 3189–3200.
- [32] Yuan Cheng Li and Baiji Hu. 2019. An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain. *IEEE Transactions on Smart Grid* 11, 3 (2019), 2627–2637.

- [33] Xiaoshuai Zhang, Chao Liu, Kok Keong Chai, and Stefan Poslad. 2021. A privacy-preserving consensus mechanism for an electric vehicle charging scheme. *Journal of Network and Computer Applications* 174 (2021), 102908.
- [34] Muhammad Tayyab Rana, Muhammad Numan, Muhammad Yousif, Tanveer Hussain, Akif Zia Khan, and Xianxian Zhao. 2024. Enhancing sustainability in electric mobility: Exploring blockchain applications for secure EV charging and energy management. *Computers and Electrical Engineering* 119 (2024), 109503.
- [35] Daniel Richter and Jürgen Anke. 2021. Exploring potential impacts of self-sovereign identity on smart service systems: An analysis of electric vehicle charging services. In *Business Information Systems*, 105–116.
- [36] Santiago de Diego, Cristina Regueiro, and Gabriel Maciá-Fernández. 2024. An authentication system based on self-sovereign identity for vehicle-to-vehicle (V2V) communications. In *International Congress on Blockchain and Applications*. Springer, 13–22.
- [37] Lukas Stockburger, Georgios Kokosioulis, Alivelu Mukkamala, Raghava Rao Mukkamala, and Michel Avital. 2021. Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications* 2, 2 (2021), 100014.
- [38] Engin Zeydan, Josep Mangues, Suayb S. Arslan, and Yekta Turk. 2023. Self-sovereign identity management for hierarchical federated learning in vehicular networks. In *2023 IEEE 24th International Conference on High Performance Switching and Routing (HPSR)*. IEEE, 191–196.
- [39] Rohini Poolat Parameswarath, Prosanta Gope, and Biplab Sikdar. 2023. A privacy-preserving authenticated key exchange protocol for v2g communications using ssi. *IEEE Transactions on Vehicular Technology* 72, 11 (2023), 14771–14786.
- [40] Adrian Kailus, Dustin Kern, and Christoph Krauß. 2024. Self-sovereign identity for electric vehicle charging. In *International Conference on Applied Cryptography and Network Security*. Springer, 137–162.
- [41] Engin Zeydan, Luis Blanco, Josep Mangues-Bafalluy, Suayb S. Arslan, Yekta Turk, Kumar Awaneesh Yadav, and Madhusanka Liyanage. 2024. Blockchain-based self-sovereign identity: Taking control of identity in federated learning. *IEEE Open Journal of the Communications Society* 5 (2024), 5764–5781.
- [42] Engin Zeydan, Suayb S. Arslan, and Yekta Turk. Exploring blockchain architectures for network sharing: Advantages, limitations, and suitability. *IEEE Transactions on Network and Service Management* 21, 2 (2023), 1791–1801.
- [43] Daniela Pöhn, Michael Grabatin, and Wolfgang Hommel. 2021. Eid and self-sovereign identity usage: An overview. *Electronics* 10, 22 (2021), 2811.
- [44] Esmeralda Broshka and Hamid Jahankhani. (Eds.). 2024. Evaluating the importance of SSI-blockchain digital identity. *Navigating the Intersection of Artificial Intelligence, Security, and Ethical Governance*. Springer Nature Switzerland, 87.
- [45] Zaina Abuabed, Ahmad Alsadeh, and Adel Taweel. 2023. Stride threat model-based framework for assessing the vulnerabilities of modern vehicles. *Computers & Security* 133 (2023), 103391.
- [46] Rafiullah Khan, Kieran McLaughlin, David Lavery, and Sakir Sezer. 2017. Stride-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 1–6.
- [47] Cabell Hodge, Konrad Hauck, Shivam Gupta, and Jesse C. Bennett. 2019. *Vehicle Cybersecurity Threats and Mitigation Approaches*. Technical Report. National Renewable Energy Laboratory (NREL), Golden, CO.
- [48] Jay Johnson, David Elmo II, George Fragkos, Junjie Zhang, Kenneth W. Rohde, and Sean C. Salinas. 2023. *Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits Using OCPP 1.6*. Technical Report. Idaho National Laboratory (INL), Idaho Falls, ID.
- [49] Puneet Kapoor, Sakshi Kaushal, and Harish Kumar. 2022. A review on architecture and communication protocols for electric vehicle charging system. In *4th International Conference on Information Management & Machine Intelligence*, 1–6.
- [50] Marc Mültin. Iso 15118 as the enabler of vehicle-to-grid applications. 2018. In *2018 International Conference of Electrical and Electronic Technologies for Automotive*. IEEE, 1–6.
- [51] K. Hänsch, A. Naumann, C. Wenge, and M. Wolf. 2018. Communication for battery energy storage systems compliant with iec 61850. *International Journal of Electrical Power & Energy Systems* 103 (2018), 577–586.
- [52] Engin Zeydan, Luis Blanco, Josep Mangues-Bafalluy, Abdullah Aydeger, Suayb Arslan, and Yekta Turk. 2024. Integrating quantum-secured blockchain identity management in open ran for 6g networks. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*. IEEE, 1–7.
- [53] Carl Ellison, Barbara Frantz, Butler W. Lampson, Ronald L. Rivest, Brian M. Thomas, and Tatu Ylonen. 2000. SPKI certificate theory. RFC Editor 2693, 1–43.
- [54] Guy Zyskind, Oz Nathan, and Alex Pentland. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*. IEEE, 180–184.
- [55] Abdullah Aydeger and Engin Zeydan. 2024. Blockchain-based self-sovereign identity in 6G non-public networks: Enhanced security in industrial cyber-physical systems. In *2024 20th International Conference on Network and Service Management (CNSM)*. IEEE, 1–7.
- [56] Michael Myers, Rich Ankney, Abhijit Malpani, Shaul Galperin, and Carlisle Adams. 1999. X.509 internet public key infrastructure online certificate status protocol - OCSP. RFC 2560, 1–40.
- [57] W3C. 2023. Verifiable credentials data model v1.1. Retrieved from <https://www.w3.org/TR/vc-data-model/>

- [58] Engin Zeydan, Luis Blanco, Josep Mangles-Bafalluy, Abdullah Aydeger, Suayb S. Arslan, Yekta Turk, Joan Bas, and Satyendra Kumar Mishra. 2024. Enhanced security with quantum key distribution and blockchain for digital identities. In *2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*. IEEE, 489–494.

Received 7 July 2024; revised 19 May 2025; accepted 28 May 2025