Review of ISO 15118-20 with TLS1.3 for Secure and Trustworthy EV Charging Infrastructure

Akram Salem, Mian Hammad Nazir, Leshan Uggalla, Abdulla Rahil and Khayri Abu Sayf

Abstract−Electric Vehicle Supply Equipment (EVSE) and the communication protocols that support it are essential to modern electric mobility, yet they remain vulnerable to significant cyber-physical risks. These risks largely arise from fragmented security adoption and the inconsistent use of Transport Layer Security (TLS). This paper reviews and analyses the security enhancements introduced by ISO 15118-20, with particular emphasis on the requirement for mandatory, mutually authenticated TLS 1.3 to secure end-to-end electric vehicle charging communication. Through an examination of protocol message flows and a synthesis of documented vulnerabilities, the study shows how stronger cryptographic enforcement, certificate-based authentication, and encrypted control signalling reduce the risks of replay, impersonation, man-in-the-middle, and backend exploitation attacks. The analysis also highlights the cyber-physical consequences of communication failures, demonstrating how protocol-level disruptions can result in wider operational risks. As a promoting solution, the paper concludes that the consistent implementation of ISO 15118-20, supported by effective certificate lifecycle management, is essential for developing resilient and trustworthy EV charging infrastructure. While additional advanced security approaches may further strengthen system robustness, future research is required to address additional technical, operational, and environmental factors not covered in this study.

***Keywords*− EV Charging, Cybersecurity, ISO 15118, TLS, and Cyber-attack.**

NOMENCLATURE

CSMS	Charging Station Management System
EV	Electric Vehicle
EVCS	Electric Vehicle Charging System
EVSE	Electric Vehicle Supply Equipment
HSM	Hardware Security Modules
OCPP	Open Charge Point Protocol
PnC	Plug and Charge
PKI	Public Key Infrastructure
SCADA	Supervisory Control and Data Acquisition
SoC	State of Charge
TLS	Transport Layer Security
V2G	Vehicle-to-Grid

I. INTRODUCTION

EVSE and EVs are fundamental components of sustainable transportation systems. Their widespread deployment introduces significant security challenges that must be addressed to ensure safe operation, reliable grid integration, and protection of sensitive data [1]. These challenges encompass personal and corporate privacy, secure financial transactions, and the stability of the electric grid. This may make cybersecurity a critical requirement for modern EV charging infrastructures [2].

Recent studies (e.g., [2]-[4]) reveal alarming security gaps in existing EV charging infrastructure. In [2], for instance, it was found that approximately 84% of surveyed charging stations do not implement TLS. This resulted, among others, in preventing compatibility with newer versions of the ISO 15118 standard and exposing systems to severe cyber vulnerabilities. For instance, the ISO 15118 protocol, which defines communication between EVs and EVSE, has evolved considerably to address these issues. Authors in [5] showed that earlier versions, such as ISO 15118-2, treated TLS as optional, limiting their effectiveness against advanced cyber threats. Different versions of the protocol ISO 151180-2 have been flown where some of them have become mandatory with TLS and more authentication during charging session [6], [7].

The latest standard, ISO 15118-20, represents a major advancement by mandating mutually authenticated TLS, significantly enhancing the security posture of EV charging communications. TLS ensures authentication, confidentiality, and data integrity through PKI, as demonstrated in prior research (e.g., [1], [5], [8]). This evolution enables secure services such as PnC where all V2G communications occur within a TLS-encrypted channel [6]. Such improvement thereby helps with reducing vulnerabilities and improving overall system reliability.

Despite these progresses, the rapid growth of EV adoption increases exposure to advanced cyber-attacks, highlighting the need for stronger cybersecurity mechanisms. In response to this challenge, upgrading protocols has been considered (e.g., [5],[8], [9]). In [9], for instance, some versions of OCPP have demonstrated improvements in authentication, confidentiality, and integrity. Additionally, the use of TLS 1.3 in conjunction with ISO 15118-20 has been studied in [1], [9]. However, increasing performance demands, reduced latency requirements, and heightened resilience against emerging threats necessitate further enhancements to existing security frameworks as explained in [10].

To overcome the listed issues, this paper focuses on the security enhancements introduced in ISO 15118-20, with particular emphasis on mandatory mutual TLS authentication and strengthened encryption mechanisms. A review of existing vulnerabilities in EV charging infrastructure has been conducted. The results have been structured to examine the

Manuscript received December 25, 2025; accepted May 5, 2026.
A. Salem, M.H. Nazir, L. Uggalla, A. Rahil and K. Abu Sayf are with the Department of Electric Engineering and Computer Science, University of South Wales, Cardiff, United Kingdom *(e-mail: akram.salem@southwales.ac.uk).*
Digital Object Identifier (DOI): 10.53907/enpesj.v6i1.358

role of TLS and PKI in securing V2G communications as well as evaluate and investigate the impact of the latest standard on addressing current and future cybersecurity challenges. Discussion and analyses have been included to summarise vulnerabilities and associated impacts with the aim of explaining the effectiveness of protocols in safeguarding EVSE and focusing secure, scalable, and reliable electric mobility solutions.

After an introductory part on cybersecurity research in EVSE charging systems, the remainder of this paper is organized into four main sections that together provide a comprehensive review of the literature. The first section presents a brief overview of vulnerabilities in EVSE. The second and third sections examine, respectively, the impacts of cyberattacks on EVSE cybersecurity and emerging cyber threats targeting EVSE infrastructure. The fourth section focuses on the classification of EVSE cyberattacks and corresponding defence mechanisms. An additional section is devoted to the discussion and critical analysis of related work. Finally, the paper concludes with a summary of findings and outlines directions for future research.

II. Cybersecurity in EVSE Charging Systems

The EVSE communication structure can be grouped into three main components: EV, EVSE, and CSMS. To assess and understand cybersecurity weaknesses and vulnerabilities in EVSE systems, the interactions between EV, EVSE, and CSMS must be considered. Figure 1 presents a high-level representation of the EVSE communication architecture, distinguishing between frontend communication governed by ISO 15118 and other communication paths.

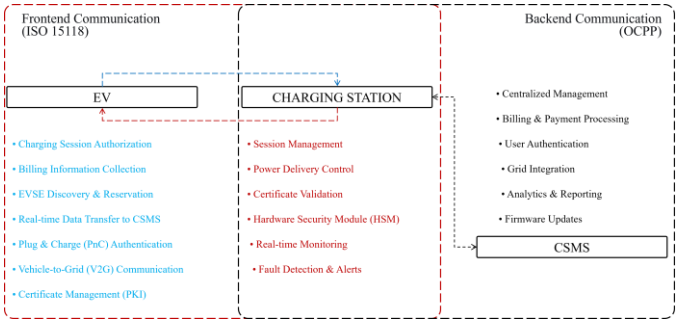

Fig. 1 Representation of EVSE Communication Structure

As shown in the figure, communication between the EV and EVSE is bidirectional. One direction includes authentication, billing, and related procedures, while the other covers session management, power delivery control, and other operational functions. The EVSE communicates with the CSMS to enable centralized management, payment processing, and additional functionalities such as grid integration and firmware updates. Security risks may occur at any communication layer and can affect one or multiple functionalities. The severity of the impact depends on factors such as the type of attack and the success of the attack.

Studies reported in [6] and [11] indicate that, at the EV layer, PnC mechanisms, certificate management processes, and real-time data exchange can be compromised through HomePlug Green PHY eavesdropping, broken-wire PLC disruption, and certificate or session manipulation arising from weaknesses in ISO 15118 implementations. In addition, the authors in [12] explain that attackers can falsify SoC values and induce denial-of-charging or unsafe charging conditions by manipulating EV-EVSE messages.

Existing research on EV charging cybersecurity provides valuable but fragmented contributions, as summarized in [1]. Early work in [2] and [5] investigates authentication and certificate-handling mechanisms within ISO 15118, identifying weaknesses in TLS configuration and certificate validation; however, these studies stop short of implementing a complete TLS 1.3 security stack. Complementary analyses in [4] examine vulnerabilities in certificate-based communication, highlighting risks associated with improper key storage and insufficient cryptographic enforcement. Broader threat-modelling efforts (e.g., [5], [6], [7], and [8]) map attack vectors across EV-EVSE communication channels, revealing threats such as spoofing, replay attacks, and supply-chain exploitation. Nevertheless, these works primarily characterize attack surfaces without proposing deployable countermeasures aligned with ISO 15118-20 [9], [24].

Further analyses in [10] and [13] clarify the operational and PKI requirements for PnC but remain largely conceptual, lacking experimentally validated protocol implementations. Research addressing backend security, including [11], [12], and [13], demonstrates that OCPP channels introduce significant risks due to weak authentication flows, insufficient message integrity verification, and vulnerable firmware-update mechanisms. However, these studies consider backend communication largely in isolation from frontend security protocols.

Hardware-based security approaches, such as those presented in [6], propose Trust EV and HSM-based key protection mechanisms, yet their effectiveness is not evaluated under the mandatory mutual TLS requirements introduced in ISO 15118-20. Finally, intelligent security approaches explored in [15] investigate machine-learning-based intrusion detection for vehicular networks, offering promise for EVCS anomaly detection, but without direct consideration of ISO 15118 message sequencing or TLS handshake behaviour.

Table 1 consolidates and synthesizes key contributions from the existing literature on EVCS cybersecurity while highlighting persistent gaps that motivate this research. Rather than providing a detailed comparison of individual studies, the table groups prior work according to core security themes, including transport-layer protection, authentication mechanisms, protocol vulnerabilities, PnC architectures, backend communication security, and data-driven detection approaches. This thematic aggregation enables clearer identification of structural limitations across the field.

Table 1. Selected Literature on TLS with Protocols

REF.	KEY ACHIEVEMENTS	IDENTIFIED GAPS / IMPROVEMENT AREAS
[2], [4], [6], [19], [20]	Definition of TLS-based security requirements; validation of certificates; analysis of TLS handshake, authentication, and encryption mechanisms; recognition of mutually authenticated TLS as a critical security enhancement	Limited analysis of certificate lifecycle management, deployment challenges, and cyber-physical impact of TLS failures on charging outcomes
[5], [3]	Implementation and validation of authentication mechanisms, including user and process authentication; exploration of behavioural biometrics as a second authentication factor	Lack of integration between authentication events and physical charging performance metrics
[6], [18], [24]	Identification of protocol-centric vulnerabilities in ISO 15118-2 communication between EV and	Absence of analysis for ISO 15118-20 upgrades and limited evaluation of

	EVSE due to weak or absent encryption	mitigation effectiveness using modern TLS configurations
[10], [14], [17], [21]	Analysis of Plug-and-Charge (PnC) ecosystem requirements; PKI architectures; trusted platform modules for secure storage of cryptographic material; V2G functional and security requirements	Insufficient evaluation of PnC security under active cyberattack scenarios and limited linkage to operational charging reliability
[8], [13], [12], [15], [7]	Comprehensive threat and vulnerability analyses of EV charging communication protocols; identification of cyberattack vectors affecting EV, EVSE, and charging infrastructure	Predominantly qualitative assessments without causal or quantitative linkage to energy delivery or battery State of Charge degradation
[11], [25]	System-of-systems and layered security approaches for isolating threats across communication layers; distributed infrastructure protection strategies	Limited integration of layered threat isolation with protocol-level security state transitions and charging dynamics
[12], [19], [28], [27]	Security analysis of OCPP-based communication between EVSE and CPOs; identification of vulnerabilities in OCPP profiles; compatibility and security profile verification	Backend security weaknesses insufficiently linked to frontend charging impacts; lack of end-to-end EV–EVSE–CSMS evaluation
[22], [23]	Machine learning applications to improve communication quality and enable intelligent, adaptive secure communication	Limited validation in safety-critical EV charging contexts and weak coupling to protocol standards and physical charging effects

Overall, the literature summarized in Table 1 demonstrates substantial progress in defining cryptographic requirements, analysing protocol vulnerabilities, and proposing layered security architectures for EV charging systems. However, most existing studies remain protocol-centric or largely qualitative, with limited investigation into how cybersecurity failures propagate into physical charging behaviour. Persistent gaps remain in certificate lifecycle management, systematic evaluation of the security enhancements introduced by ISO 15118-20, analysis of backend-to-frontend attack propagation, and understanding the causal relationship between communication-layer disruptions and charging outcomes.

From a cybersecurity perspective, as discussed in [14], the frontend layer involves the EV performing critical functions such as PnC authentication, EVSE discovery, billing data exchange, real-time session authorization, and V2G communication. These functions have been shown to be vulnerable to spoofing, session hijacking, and data manipulation when TLS is absent, optional, or misconfigured (e.g., [1], [18], [5], [19], [20]). Furthermore, work in [5] demonstrates that the EVSE acts as a central orchestration point, responsible for power delivery control, certificate validation, monitoring, and other security-critical operations, often supported by hardware anchors such as HSMs. These hardware-based mechanisms play a key role in protecting cryptographic material and enforcing PKI trust chains, as emphasized in recent studies on secure PnC and EV charging security architectures.

On the backend, the CSMS performs high-value operations including payment processing, user authentication, analytics, grid integration, and firmware updates. Studies such as [16] and [21] identify the CSMS as a prominent attack surface, where successful compromises can result in financial fraud, privacy violations, remote shutdown of charging fleets, and manipulation of grid-connected charging loads [22], [8].

The bidirectional communication flows illustrated in the figure reflect the continuous exchange of operational and billing data across EV, EVSE, and CSMS components. Consistent with prior findings, these communication paths can be exploited by adversaries to induce functional disruptions, financial and privacy compromises, safety hazards, and even large-scale power system instability [17], [23].

By situating these communication flows within a unified architectural view, the figure emphasizes that EV charging cybersecurity cannot be addressed at a single layer. Instead, effective protection requires coordinated, end-to-end security controls, including mandatory TLS, robust certificate lifecycle governance, secure firmware update mechanisms, and anomaly detection across EV, EVSE, and CSMS components. This perspective aligns with recent studies on cyber-physical risks in EV charging infrastructure and ongoing standards evolution discussed in [5], [24], [25], and [19].

III. Vulnerabilities in EVSE

More recent studies (e.g., [9], [28], [26]) extend earlier findings by examining EVSE security from a system-level perspective, demonstrating that vulnerabilities span hardware components, communication protocols, and cloud-connected services. In particular, [29] reinforces concerns regarding the persistence of insecure ISO 15118 deployments and the slow adoption of comprehensive TLS protections.

Building on this, [21] presents a detailed empirical assessment of EVSE attack surfaces, identifying exploitable weaknesses across multiple interfaces, including EV connectors, user authentication terminals, OCPP-based backend services, and maintenance ports. Rather than introducing new attack classes, these results highlight how existing weaknesses manifest simultaneously across interconnected EVSE subsystems.

Experimental evidence reported in [11] [13], [15] and [16] demonstrates how such weaknesses can be exploited in practice through communication-layer interception, PLC disruption, insecure web interfaces, and backend compromise, while [20] further documents firmware-level attacks that enable persistent adversarial control. Collectively, these studies indicate that EVSE security failures are rarely isolated and instead propagate across functional boundaries due to insufficient isolation and inconsistent security enforcement.

Importantly, recent analyses such as [27] and [28] move beyond vulnerability identification to emphasize operational consequences, showing that EVSE compromises can escalate into denial-of-charging events, falsified metering, malware dissemination, and coordinated manipulation of charging loads. These observations reinforce the need for standardized, end-to-end security controls rather than incremental or component-specific defences.

Consequently, the literature increasingly converges on the necessity of enforceable security baselines particularly mandatory TLS, coherent certificate lifecycle governance, and secure update mechanisms providing clear motivation for evaluating the security guarantees introduced by ISO 15118-20 and their effectiveness against emerging cyber–physical threats in EV charging ecosystems.

IV. Impacts of Attack on EVSE Cybersecurity

Cybersecurity vulnerabilities in EVSE can give rise to significant functional, financial, safety, and grid-level impacts, underscoring the critical importance of robust protection mechanisms across the EV charging ecosystem. At the functional level, successful cyberattacks may disrupt the availability of individual charging units, entire EVSE fleets, or vendor-managed infrastructures, thereby threatening service continuity as electric mobility expands into safety-critical domains such as emergency response, healthcare, agriculture, and industrial operations. For example, work in [32] demonstrates that malicious remote firmware updates can be leveraged to render charging networks inoperable. Manipulation of communication between the EV and EVSE further exacerbates these operational risks.

Multiple studies [33], [34] report that falsification of SoC information can result in denial-of-charging events, vehicle stranding, and broader disruptions to transportation systems. Moreover, inaccurate SoC reporting may impose excessive stress on battery management systems and increase the likelihood of unsafe charging behaviour in the absence of effective fail-safe controls [34]. Beyond operational impacts, unauthorized access to EVSE and backend systems introduces substantial financial and privacy risks. Prior work in [35] identifies threats including the exfiltration of personally identifiable information, manipulation of billing processes, and compromise of payment credentials. Independent security assessments in [36],[37] further indicate that inadequately secured EVSE deployments can serve as entry points into corporate networks, enabling espionage activities and large-scale data breaches.

Safety-related consequences arise when protective mechanisms within the EV or EVSE are degraded or circumvented. While experiments reported in [34] indicate that internal vehicle protection systems successfully prevented overcharging during a DC fast charger exploitation scenario, compromised communication channels or disabled safety interlocks could undermine these safeguards. Additionally, [38] highlights that CHAdeMO-based charging systems may permit adversarial manipulation of battery operating parameters if IEC 61851 CAN-bus messages are insufficiently validated or filtered.

Emerging charging technologies introduce further safety considerations. High-power liquid-cooled charging cables and wireless power transfer systems, for instance, raise concerns related to electromagnetic interference, including potential impacts on nearby medical devices, as documented in [38]. At the grid level, malicious manipulation of EVSE loads poses systemic risks to power system stability. Experimental investigations in [33] show that attacks targeting EVSE power electronics can induce total harmonic distortion exceeding 20%, reduce power factor below 0.8, and cause abrupt power reductions from 50 kW to 0.3 kW within 0.020 seconds.

Coordinated charging attacks further amplify these risks. Studies in [40] and [41] demonstrate that synchronized malicious charging behaviour can violate voltage constraints, overload network assets, and disrupt economic dispatch processes. At scale, such attacks may trigger under-frequency load shedding events, while [42] suggests that increasing EV penetration could enable adversary-controlled bulk frequency modulation.

EVSE cybersecurity vulnerabilities have the potential to escalate from localized disruptions to widespread functional, safety, financial, and grid-level consequences. These findings emphasize the necessity of comprehensive, end-to-end cybersecurity strategies to mitigate cascading failures and protect both transportation and power system infrastructures.

V. Emerging Cyber Threat in EVSE Infrastructure

Recent literature (e.g., [17], [28], [30],[31]) highlights a rapid increase in cyberattacks targeting critical infrastructure, emphasizing the growing need for coordinated cybersecurity strategies and incident-response frameworks at a global level. Within the EV ecosystem, these threats increasingly affect charging infrastructure and its control backbones, where disruption of communication flows can interfere with OCPP sessions and ISO 15118 authentication processes. Advanced persistent threats have been identified as a major concern, as attackers may infiltrate CSMS environments to compromise authentication credentials, extract sensitive operational data, or manipulate coordinated charging behaviour [43].

Comparable ransomware incidents in other critical sectors, such as healthcare systems [44], illustrate how similar attack strategies could be applied to EV charging networks. In such scenarios, adversaries could encrypt charging management servers, rendering billing systems, session records, and operational dashboards unavailable to EVSE operators. In parallel, the increasing use of distributed denial-of-service (also known as DDoS) attacks based on IoT botnets [45] demonstrates the feasibility of large-scale traffic flooding against EV charging infrastructures. These attacks could overwhelm OCPP communication channels, disrupt authorization services, and cause widespread service outages.

Insights from cybersecurity research on SCADA systems [46] provide further relevant parallels, particularly for EVSE–grid coordination. Manipulation of telemetry data or control signals in these environments has been shown to destabilize load management functions, raising concerns that similar attack techniques could affect EV charging systems governed by power-system security standards such as IEC 62351-7:2017.

Beyond technical attack vectors, broader cybercrime trends introduce additional governance and policy challenges for EV charging ecosystems. Studies on financial cybercrime [47], persistent social-engineering campaigns [48], and inconsistent regulatory enforcement across jurisdictions [49] reveal structural weaknesses in consumer protection, payment security, and identity management within charging services. Research on the behavioural drivers of cybercriminal activity [50], together with documented denial-of-service attacks on public and financial institutions [51]-[53], further illustrates the growing use of service disruption as a strategic objective.

In the context of EV charging networks, such large-scale and coordinated attacks could degrade authentication services, disrupt CSMS operations, and impair backend billing platforms, ultimately undermining service reliability and public trust. These developments reinforce the need for harmonized cybersecurity standards, mandatory resilience requirements, and coordinated incident-response mechanisms to support the secure and dependable deployment of electric mobility infrastructure.

VI. EVSE Cyberattacks and Defences

This work is further extended to address both cyberattacks and corresponding defence mechanisms in EVCS. To provide a general overview, Table 2 summarizes common cyberattack types relevant to EVCS, including denial-of-service, replay attacks, phishing, jamming, GPS spoofing, SQL injection, man-in-the-middle attacks, and electromagnetic interference.

Table 2. Expanded EVCS Cyberattack Types

Attack Type	Brief Description	Potential Impact on EV/EVCS	Ref
Denial-of-Service (DoS)	Overloads the charging system or backend servers with excessive requests, causing service outages.	Blocks access to charging stations, prevents charging, disrupts fleet operations.	[12, 20, 29]
Replay Attack	Captures legitimate communication messages and replays them to trick EV or EVSE.	EV may accept unauthorized commands or false authentication messages.	[11, 30]
Side-Channel Attack	Uses power consumption, EM emissions, or timing leaks to infer private keys.	Extraction of cryptographic keys used in ISO 15118 or OCPP security.	[30, 31]
Phishing Attack	Tricks users into revealing sensitive data or installing malware.	EV owners download malicious apps, firmware, or login credentials are stolen.	[20, 32]
Jamming Attack	Introduces radio interference to disrupt wireless communication channels.	Loss of connectivity in Wi-Fi, Bluetooth, PLC or wireless charging communication.	[16, 33]
GPS Spoofing	Sends falsified GPS signals to mislead navigation or location-dependent charging functions.	Misroutes EVs, affects smart-charging schedules, causes safety risks.	[31, 34]
Man-in-the-Middle (MitM)	Intercepts and manipulates communication between EV and EVSE.	Data theft, session hijacking, injection of harmful commands.	[11, 12, 35]
Buffer Overflow	Sends more data than a system can handle, triggering crashes or malicious code execution.	EVSE shutdown, firmware compromise, remote code execution.	[12, 35]
SQL Injection	Inserts malicious commands into backend database queries.	Tampering with billing data, authentication logs, or firmware configuration.	[12, 19]

As summarized in Table 2, cyberattacks on EVCS can affect confidentiality, integrity, availability, and safety across both EV and EVSE environments. The classification highlights a wide range of attack vectors, including protocol-level manipulation, backend exploitation, and human-focused attacks. This diversity of threats demonstrates that isolated or single-layer defences are insufficient and reinforces the need for comprehensive security strategies, as noted in [28] and [54].

Recent studies (e.g., [17], [10], [36], [56]) show that cyberattacks targeting EVCS are becoming increasingly sophisticated and have broader system-level consequences. Security analyses of CSMS platforms and OCPP-based backend systems reveal that attackers commonly exploit protocol weaknesses, inadequate authentication mechanisms, and insecure application programming interfaces. These vulnerabilities enable attacks such as data theft, billing manipulation, remote disabling of chargers, and large-scale service disruption.

Beyond backend systems, research in cyber-physical power systems indicates that compromised charging behaviour can propagate beyond individual charging stations. Studies in [37], [37], [39], and [41] demonstrate that coordinated load-altering attacks such as botnet-driven manipulation of charging behaviour and false data injection in EV-grid communication can destabilize distribution networks, disrupt voltage and frequency regulation, and reduce overall system reliability. These effects are further amplified under conditions of high vehicle-to-grid penetration.

One may conclude that cybersecurity risks in EVCS are inherently multi-layered, spanning physical infrastructure, communication protocols, and cloud-connected backend services. This leads to the consideration and the implementation of effective protection that may require coordinated and systematically applied security controls across all architectural layers, mainly to prevent cascading failures and mitigate operational, safety, and grid-level impacts.

In response to these challenges, several mitigation approaches are currently under investigation. Among them, the implementation of TLS is widely considered an effective means of reducing the risk of cyberattacks on EVCS communications. Figure 2 illustrates the role of TLS within the overall EVSE communication architecture. Specifically, the figure presents the end-to-end communication workflow of an EVCS, highlighting the interactions between the EV, the CS, and the CSMS under the ISO 15118 and OCPP standards.

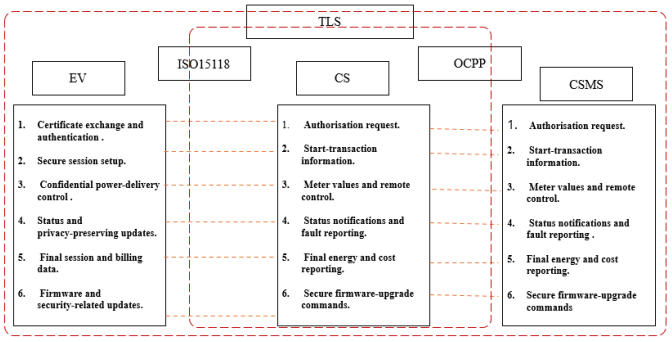

Fig. 2: End-to-End TLS-Secured Message Exchange Between EV, EVSE, and CSMS.

As can be seen in this figure, the end-to-end communication workflow among the EV, EVSE, and CSMS, depicting the structured exchange of messages throughout a charging session. The figure outlines key operational phases, including certificate-based authentication, secure session establishment, real-time control signalling, metering, billing, status reporting, and firmware updates, thereby contextualizing previously identified threat surfaces within a unified system architecture. It further demonstrates how the combined use of TLS 1.3 with ISO 15118 and OCPP provides security coverage across both frontend and backend communication paths. The mandatory mutual authentication and enhanced certificate management mechanisms introduced in ISO 15118-20 strengthen early authentication and session establishment stages that have been shown to be vulnerable to replay, impersonation, and man-in-the-middle attacks, while the encrypted and structured message exchanges defined in OCPP 2.0.1 mitigate backend threats such as unauthorized control commands, manipulation of metering data, and unauthorized access to billing or operational information. By presenting TLS as a common security layer spanning both protocol domains, the figure provides a systematic basis for evaluating how recent standard developments reduce attack surfaces and improve end-to-end security in EV charging infrastructures.

VII. Analyses and Discussion

The findings presented in this study confirm that cybersecurity in EVCS remains a critical and largely unresolved challenge, driven by fragmented protocol adoption, inconsistent enforcement of security controls, and the increasing sophistication of adversarial capabilities. As noted in the Introduction, the persistent lack of TLS deployment reported in more than 80% of operational charging stations continues to expose ISO 15118-2 and OCPP-based communication channels to attacks that compromise the confidentiality, integrity, and availability of charging services. This concern is consistently reinforced across the literature (e.g., [1]-[28]), which documents vulnerabilities in ISO 15118 message flows, misconfigured PKI infrastructures, optional or outdated encryption mechanisms, and weak backend authentication practices that collectively undermine the security posture of contemporary EVCS deployments.

A recurring limitation identified in prior work (e.g., [2], [9]-[6]) is the architectural fragmentation between frontend and backend security analyses. Frontend-focused studies primarily investigate vulnerabilities in EV–EVSE communication, such as spoofing, replay attacks, session manipulation, and PLC interception within ISO 15118, but often neglect dependencies on backend systems. Conversely, backend-oriented research (e.g., [8], [12], [10]) emphasizes exploitable APIs, weak authentication flows, insecure firmware update mechanisms, and SQL injection vulnerabilities within CSMS platforms, typically without integrating frontend protocol security considerations. This separation reveals a significant research gap, as limited work evaluates how ISO 15118-20's mandatory TLS 1.3 interacts with OCPP 2.0.1 security mechanisms within a complete, end-to-end charging workflow.

This gap is particularly consequential given that adversaries frequently exploit cross-layer dependencies. As shown in [19] and [20], compromised EVSE firmware or man-in-the-middle positioning can facilitate escalation into backend systems, while backend breaches can enable manipulation of authorization, billing, or power-delivery parameters across entire charging fleets. Beyond technical vulnerabilities, the literature clearly demonstrates the cyber-physical consequences of EVCS attacks. Studies in [24]-[29] show that EVSE compromise can disable individual chargers or entire fleets, falsify SoC values, propagate malware through firmware updates, and disrupt critical services reliant on EV mobility. These findings substantiate earlier concerns that insecure ISO 15118-2 and OCPP deployments may enable denial-of-charging events, unsafe charging conditions, inaccurate billing, and widespread service outages, alongside substantial financial and privacy risks.

Real-world assessments, including those reported in [37], further demonstrate that insecure EVSE deployments can act as entry points into corporate networks, enabling advanced intrusions and large-scale data breaches. At the grid level, studies in [29]-[34] indicate that cyberattacks targeting charging infrastructure can propagate beyond individual devices, threatening both distribution and transmission system stability. Compromised EVSE behaviour (e.g., coordinated load drops, rapid power transitions, falsified metering, and manipulated V2G dispatch) has been shown to induce voltage instability, overload network assets, disrupt generator scheduling, and trigger under-frequency load shedding events. These observations, reinforced by [51] and [52], highlight that EVCS cybersecurity risks are intrinsically linked to broader power system resilience, particularly under conditions of increasing EV penetration and expanded V2G participation.

The diversity of attack vectors summarized in Table 2 (e.g., [1], [18], [22], [43] [53][54][55]), ranging from conventional IT threats such as SQL injection and buffer overflows to cyber-physical attacks including GPS spoofing, PLC jamming, and electromagnetic interference, further illustrates the hybrid threat landscape facing EV charging systems. As emphasized in [28] and [44], the coexistence of these threat classes necessitates defence strategies capable of providing simultaneous protection across hardware, software, communication layers, and human–machine interfaces. Recent studies also indicate that these attacks are becoming increasingly automated, scalable, and adaptive, underscoring the importance of proactive detection mechanisms, secure firmware governance, rigorous PKI lifecycle management, and enhanced operational awareness among EVSE operators.

Finally, the layered architecture illustrated in Figure 1 reinforces these insights by highlighting the tight interdependencies among EVs, EVSE, and CSMS components. Vulnerabilities at any layer—such as misconfigured TLS at the EV, inadequate certificate validation at the EVSE, or insecure APIs within the CSMS—can be leveraged to compromise the integrity of the entire charging workflow. In this context, the role of hardware security modules at charging stations, as discussed in [19] and [37], is increasingly critical for protecting cryptographic keys and enforcing secure Plug-and-Charge trust chains. Similarly, the backend remains a high-value target due to its responsibility for authentication, billing, grid integration, analytics, and firmware management, as highlighted in [37] and [39]. Taken together, the findings of this work indicate that the security of electric vehicle charging ecosystems depends on the coherent and systematic enforcement of end-to-end safeguards. These safeguards include mandatory TLS 1.3, comprehensive certificate lifecycle governance, tightly controlled firmware management practices, and continuous anomaly monitoring, applied consistently across EV, EVSE, and CSMS components in alignment with evolving cybersecurity standards [39]–[42].

VIII. Conclusion

The work has shown that electric vehicle charging systems remain exposed to cyber-physical risks due to fragmented protocol adoption and inconsistent security implementation in legacy ISO 15118-2 among other factors such as OCPP deployments. The review demonstrates that ISO 15118-20 can provide substantial security improvements through mandatory mutually authenticated TLS 1.3 and strengthened public key infrastructure requirements, enabling effective mitigation of replay, impersonation, and man-in-the-middle exploitation attacks when deployed end-to-end. The findings further confirm that electric vehicle charging systems security is inherently cyber-physical, with communication failures capable of escalating from local charging disruption to wider system impacts. Secure electric mobility therefore requires more advanced techniques such as coordinated, system-wide protection across communication protocols, cryptographic key management, firmware integrity, and backend services.

Among many other work, incorporating quantitative cyber-risk assessment approaches, such as probabilistic attack modelling, can help with evaluating the likelihood and impact of attacks on EV charging infrastructure and support more effective mitigation planning.

References

[1] M. Szakály, S. Köhler, and I. Martinovic, "Current affairs: A measurement study of deployment and security trends in EV charging infrastructure," arXiv preprint arXiv:2404.06635, 2024.

[2] K. Ahmet, "Smart, secure and interoperable charging infrastructure with Plug and Charge," in Proc. 12th Int. Conf. Smart Grid (icSmartGrid), 2024.

[3] J. Sturgess et al., "CableAuth: A biometric second-factor authentication scheme for electric vehicle charging," Tech. Rep., 2023.

[4] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: A cyberattack vector?" IEEE Trans. Smart Grid, vol. 11, no. 6, pp. 5099–5113, 2020.

[5] A. Kilic, "TLS handshake for Plug and Charge in vehicular communications," Comput. Netw., vol. 243, p. 110281, 2024.

[6] P. Van Aubel and E. Poll, "Security of EV-charging protocols," arXiv preprint arXiv:2202.04631, 2022.

[7] A. Ahalawat, S. Adepu, and J. Gardiner, "Security threats in electric vehicle charging," in Proc. IEEE SmartGridComm, 2022.

[8] A. Kilic, "Plug and Charge solutions with vehicle-to-grid communication," Elect. Power Compon. Syst., vol. 51, no. 16, pp. 1786–1814, 2023.

[9] J. H. Do, J. K. Ho, and L. D. Hoon, "A study on securing communication of electric vehicle charging using combined charging system," in Proc. KICS Conf., pp. 198–200, 2021.

[10] A. Heinrich and R. Heddergott, "Secure and user-friendly EV charging: A comparison of Autocharge and ISO 15118 Plug & Charge," Hubject GmbH, Tech. Rep., Jun. 2019.

[11] J. Johnson et al., “Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses,” Energies, vol. 15, no. 11, p. 3931, 2022.
[12] Z. Garofalaki et al., “Electric vehicle charging: A survey on the security issues and challenges of the Open Charge Point Protocol (OCPP),” IEEE Commun. Surveys Tuts., vol. 24, no. 3, pp. 1504–1533, 2022.
[13] R. Baker and I. Martinovic, “Losing the car keys: Wireless insecurity in EV charging,” in Proc. 28th USENIX Security Symp., 2019.
[14] A. Fuchs et al., “HIP: HSM-based identities for Plug-and-Charge,” in Proc. 15th Int. Conf. Availability, Reliability and Security, 2020.
[15] Z. El-Rewini et al., “Cybersecurity challenges in vehicular communications,” Veh. Commun., vol. 23, p. 100214, 2020.
[16] J. Antoun et al., “A detailed security assessment of the EV charging ecosystem,” IEEE Netw., vol. 34, no. 3, pp. 200–207, 2020.
[17] A. Kilic, “Secure and manipulation-proof TLS communication with Plug and Charge,” Tech. Rep., 2023.
[18] S. Hamdare et al., “Cybersecurity risk analysis of electric vehicle charging stations,” Sensors, vol. 23, no. 15, p. 6716, 2023.
[19] K. Sarieddine et al., “Uncovering covert attacks on EV charging infrastructure,” in Proc. ACM Asia CCS, 2024.
[20] H. Jahangir et al., “Charge manipulation attacks against smart EV charging stations,” IEEE Trans. Smart Grid, 2024.
[21] F. Haidar, “Vehicle-to-grid: Towards a cyber-secure electric system including vehicle, charging points and batteries,” in Proc. SIA Powertrain & Energy Congr., 2022.
[22] E. S. Ali et al., “Machine learning technologies for secure vehicular communication in Internet of Vehicles,” Security Commun. Netw., 2021.
[23] K. N. Qureshi, A. Alhudhaif, and G. Jeon, “EV energy management and charging scheduling in sustainable cities,” Sustain. Cities Soc., vol. 71, p. 102990, 2021.
[24] H. El-Hussini et al., “A tale of two entities: Contextualizing the security of electric vehicle charging stations on the power grid,” ACM Trans. Internet Things, vol. 2, no. 2, 2021.
[25] R. M. Pratt and T. E. Carroll, “Vehicle charging infrastructure security,” in Proc. IEEE ICCE, 2019.
[26] T. Lauser, D. Zelle, and C. Krauß, “Security analysis of automotive protocols,” in Proc. ACM Comput. Sci. Cars Symp., 2020.
[27] R. Metere et al., “Cyber security and privacy in EV charging infrastructure,” arXiv preprint arXiv:2209.07842, 2022.
[28] L. Buschlinger et al., “Plug-and-patch: Secure value-added services for EV charging,” in Proc. 14th ARES, 2019.
[29] M. Kaiser, “Automating compatibility testing for integration of charge points into an EV ecosystem,” Tech. Rep., 2024.
[30] A. Z. Galbis et al., “Smart tool development for customised EV charging services,” World Electr. Veh. J., vol. 13, no. 8, p. 145, 2022.
[31] P. Aji et al., “Development of EV charging station management systems,” in Proc. IEEE ICT-PEP, 2020.
[32] S. Hsaini et al., “An OCPP-based approach for EV charging management,” Energies, vol. 15, no. 18, p. 6735, 2022.
[33] Open Charge Alliance, Open Charge Point Protocol (OCPP) 2.0.1 Specification, Dec. 2024.
[34] D. Priyasta et al., “Ensuring compliance of OCPP 1.6 messages,” J. Eur. Syst. Autom., vol. 56, no. 1, 2023.
[35] M. Mültin, “New features and timeline for ISO 15118-20,” Switch-EV, 2020.
[36] M. Shin et al., “Interoperability testing for EV chargers,” Appl. Sci., vol. 6, no. 6, p. 165, 2016.
[37] A. Pacheco et al., “Energy transition on geographic islands,” Renew. Energy, vol. 184, pp. 700–711, 2022.
[38] Z. Pourmirza and S. Walker, “EV charging station cybersecurity challenges,” in Proc. IEEE SEGE, 2021.
[39] R. Flocea et al., “EV smart charging reservation algorithm,” Sensors, vol. 22, no. 8, p. 2834, 2022.
[40] S. B. Mitikiri et al., “Cyber–physical security in EV charging infrastructure,” J. Cleaner Prod., vol. 438, p. 140347, 2025.
[41] H. R. Sayarshad et al., “Cyberattack resilience and vehicle-to-grid integration,” Transport Policy, vol. 139, pp. 158–169, 2025.
[42] S. Hamdare et al., “Cyber security for EV smart charging systems,” Conf. Paper, 2025.
[43] H. Tanyıldız et al., “Detection of cyber attacks in EV charging,” Frontiers Energy Res., vol. 13, 2025.
[44] S. B. Mitikiri et al., “Addressing vulnerabilities in the EV ecosystem,” in Proc. EVS38, 2025.
[45] Upstream Security, Automotive & Smart Mobility Global Cybersecurity Report 2025, 2025.
[46] J. Han et al., “Transfer learning for securing EV charging infrastructure,” Sci. Rep., vol. 15, 2025.
[47] A. Wahab et al., “Grid Sentinel anomaly detection framework,” Comput. Intell. Neurosci., 2025.
[48] X. Luo et al., “AI-enhanced intrusion detection for EV charging,” Alexandria Eng. J., vol. 74, no. 2, 2025.
[49] S. Chia et al., “Black-box fuzzing of EV charging protocols,” Comput. Mater. Continua, vol. 84, no. 2, 2025.
[50] R. V. Gottumukkala et al., “Cybersecurity in onboard EV charging systems,” World J. Adv. Res. Rev., 2020.
[51] J. AlFarra et al., “ML-driven distributed intrusion detection for EV charging,” CEUR Workshop Proc., vol. 3935, 2024.
[52] S. B. Mitikiri et al., “Anomaly detection of cyber attacks on EV charging ports,” Electr. Power Syst. Res., vol. 224, p. 109611, 2024.
[53] A. Wahab et al., “Machine learning empowered anomaly detection,” Comput. Intell. Neurosci., 2024.
[54] Open Charge Alliance, OCPP Information and Whitepapers, 2024.
[55] “Cyber defense in OCPP for EV charging security risks,” Int. J. Inf. Security, 2024.