Computer Modeling in Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.066727

ARTICLE

Data-Driven Digital Evidence Analysis for the Forensic Investigation of the Electric Vehicle Charging Infrastructure

Dong-Hyuk Shin[1], **Jae-Jun Ha**[1] **and Ieck-Chae Euom**[2,*]

[1]System Security Research Center, Chonnam National University, Gwangju, 61186, Republic of Korea
[2]Graduate School of DataScience, Chonnam National University, Gwangju, 61186, Republic of Korea

*Corresponding Author: Ieck-Chae Euom. Email: iceuom@jnu.ac.kr

Received: 16 April 2025; Accepted: 13 June 2025; Published: 30 June 2025

ABSTRACT: The accelerated global adoption of electric vehicles (EVs) is driving significant expansion and increasing complexity within the EV charging infrastructure, consequently presenting novel and pressing cybersecurity challenges. While considerable effort has focused on preventative cybersecurity measures, a critical deficiency persists in structured methodologies for digital forensic analysis following security incidents, a gap exacerbated by system heterogeneity, distributed digital evidence, and inconsistent logging practices which hinder effective incident reconstruction and attribution. This paper addresses this critical need by proposing a novel, data-driven forensic framework tailored to the EV charging infrastructure, focusing on the systematic identification, classification, and correlation of diverse digital evidence across its physical, network, and application layers. Our methodology integrates open-source intelligence (OSINT) with advanced system modeling based on a three-layer cyber-physical system architecture to comprehensively map potential evidentiary sources. Key contributions include a comprehensive taxonomy of cybersecurity threats pertinent to EV charging ecosystems, detailed mappings between these threats and the resultant digital evidence to guide targeted investigations, the formulation of adaptable forensic investigation workflows for various incident scenarios, and a critical analysis of significant gaps in digital evidence availability within current EV charging systems, highlighting limitations in forensic readiness. The practical application and utility of this method are demonstrated through illustrative case studies involving both empirically-derived and virtual incident scenarios. The proposed data-driven approach is designed to significantly enhance digital forensic capabilities, support more effective incident response, strengthen compliance with emerging cybersecurity regulations, and ultimately contribute to bolstering the overall security, resilience, and trustworthiness of this increasingly vital critical infrastructure.

KEYWORDS: Electric vehicle charging infrastructure; digital forensics; incident investigation; charging network; vulnerability analysis; threat modeling; open-source intelligence (OSINT)

1 Introduction

The global energy paradigm is undergoing a significant transformation, with a pronounced shift towards electrified transportation as a cornerstone of achieving a zero-carbon economy and enhancing the integration of renewable energy sources [1]. This transition is catalyzing the rapid expansion and increasing sophistication of the electric vehicle (EV) charging infrastructure. More than just power dispensers, these deployments are evolving into complex cyber-physical systems (CPS) that integrate diverse hardware components, a variety of communication protocols, and multiple software layers, establishing critical interfaces with national power grids, financial payment networks, and advanced vehicle management platforms [2]. The economic magnitude of this sector is substantial; the global EV charging market is projected for exponential

expansion, which firmly underscores the strategic importance of these systems within critical national infrastructure paradigms. As this infrastructure matures, it not only facilitates the primary function of EV charging but also paves the way for advanced functionalities such as vehicle-to-grid (V2G) capabilities, which position EVs as distributed energy resources capable of bolstering grid stability and improving operational efficiency, particularly when harmonized with fluctuating renewable energy outputs.

However, the intricate interconnectivity inherent in the EV charging infrastructure, while enhancing functionality and user convenience, concurrently creates an expanding attack surface. The rapid expansion of charging networks, characterized by heterogeneous components and interconnected systems, presents an increasingly expansive attack surface vulnerable to sophisticated cyber threats [3]. This heightened risk environment is not merely theoretical; automotive cyber incidents and vulnerabilities are increasing annually, with high-profile attacks exploiting weaknesses in charging protocols, communication standards, and devices highlighting the diverse threat landscape [4]. Such security incidents can precipitate significant consequences, ranging from direct financial losses for both charging operators and end-users to the potential disruption of power grid stability, and, critically, an erosion of public trust in EV technology. In recognition of this escalating criticality and the potential systemic risks, regulatory frameworks are beginning to mature. A notable example is the European Union's Network and Information Security (NIS) 2 Directive [5], which explicitly categorizes EV charging operators as essential entities. This directive mandates the implementation of comprehensive cybersecurity measures, encompassing robust risk management practices and formal incident response protocols. Such regulatory endeavors are largely driven by the mounting evidence of tangible cybersecurity risks within the EV charging ecosystem.

1.1 Motivation and Problem Statement

Despite the growing recognition of cybersecurity risks and the evolution of regulatory frameworks like the NIS 2 Directive, existing cybersecurity measures within the EV charging domain have predominantly emphasized prevention and vulnerability mitigation. Standards such as ISO 15118 and the Open Charge Point Protocol (OCPP) focus significantly on preventive security mechanisms like authentication and encryption. However, a critical gap persists concerning structured and standardized methods for performing digital forensic analysis after a security incident has occurred in these complex EV charging ecosystems. While regulations acknowledge the importance of securing this infrastructure, they often lack specific guidance on post-incident digital forensic procedures, leaving a void in standardized response capabilities.

This deficiency in post-incident analysis capabilities presents a significant problem. It severely hinders effective incident response, makes the reliable attribution of malicious activities exceptionally challenging, and complicates the processes for legal recourse or insurance claims following security breaches. The problem is further compounded by several inherent characteristics of the EV charging infrastructure. Forensic investigations frequently concentrate on the Electric Vehicle Charging Station (EVCS) as a primary target or point of compromise in security incidents. However, significant challenges impede such investigations. These challenges stem from the inherent heterogeneity of EVCS hardware, firmware, and the diverse range of EVs and Charging Station Management Systems (CSMSs) involved. Pertinent digital evidence related to a single incident is often distributed across multiple entities—the EVCS, the connected EV, and the backend CSMS—making evidence correlation and holistic incident reconstruction inherently difficult. These difficulties are frequently exacerbated by the technical intricacies of the governing communication protocols (e.g., ISO 15118 for EV-EVCS interactions and OCPP for EVCS-CSMS connections), potentially deficient or inconsistent logging mechanisms within these systems, and the practical challenges encountered in data acquisition, especially from proprietary EVCS components [6]. The often optional nature of crucial security logging

features in prevailing standards also leads to inconsistent security postures and further hinders effective investigation across different vendor systems.

1.2 Related Work

While significant efforts have focused on preventive cybersecurity in the EV charging infrastructure, comprehensive forensic investigation methods explicitly tailored to incidents involving EVCSs remain considerably underdeveloped. Framework profiles, such as NIST IR 8473, have been developed to enhance the cybersecurity of EV fast charging networks [7]. These profiles offer recommendations for forensic considerations, including logging, yet they often lack detailed digital evidence analysis methodologies suitable for the intricacies of EVCS incidents. The bulk of existing research on digital forensic methods has traditionally centered on conventional information technology systems, industrial control systems (ICS), or broader automotive systems. This focus leaves a notable gap concerning EVCSs, which uniquely integrate characteristics from multiple domains (automotive, power grid, payment systems), presenting distinct challenges for digital investigators [8,9].

Addressing this specificity, Girdhar et al. [10,11] highlighted that despite the existence of forensic frameworks for related areas like smart grids and automated vehicles, no established forensic investigation framework had been explicitly adapted to the nuances of EVCSs. In response, they proposed an incident analysis framework employing the "Who, What, When, Where, Why, and How" (5W1H) model, complemented by stochastic anomaly detection methods, to investigate cyberattacks and abnormal operations within EVCSs. This structured approach emphasizes systematic evidence collection and the chronological analysis of logs and system data, aiming to facilitate root cause identification and effective incident response.

Nonetheless, current methods, including those proposed, exhibit limitations in their practical application, largely due to the inherent complexities of the EV charging ecosystem. A significant issue is that studies have rarely explored comprehensive digital evidence identification across the various architectural layers (physical, network, application) of EVCSs in a holistic manner. While general recommendations for acquiring digital evidence from physical hardware, network communication logs, and application-level data exist, clearly defined digital evidence taxonomies or structured mappings between threats and evidence—designed explicitly for the EV charging infrastructure—remain largely absent [12,13]. Consequently, existing approaches often fall short in terms of ensuring adequate forensic readiness, enabling systematic digital evidence identification, and supporting effective incident response tailored to EVCSs. For instance, present forensic frameworks seldom incorporate comprehensive digital forensic readiness from the design and deployment phases of EVCSs, leaving these systems ill-equipped to generate and preserve the necessary digital evidence crucial for effective post-incident investigations. These gaps underscore the need for a more specialized and data-driven forensic framework.

1.3 Research Scope and Contributions

The scope of this research is to propose and evaluate a structured, data-driven framework for the analysis of digital evidence to support forensic investigations of security incidents within the Electric Vehicle Charging Infrastructure (EVCI). This study focuses on addressing the identified deficiencies in post-incident analysis by providing a systematic approach tailored to the EVCI's specific operational and technical characteristics.

The primary contributions of this work are:

- **Development of a Structured Digital Forensic Framework for EVCI:** this paper introduces a structured, data-driven digital forensic framework designed for the EVCI environment. It considers the complexities arising from its diverse components and multi-stakeholder interactions.
- **Systematic Identification and Classification of Digital Evidence:** the framework outlines a methodology for systematically identifying and classifying forensically relevant digital evidence across the physical, network, and application layers of EVCSs. This process incorporates information from protocol specifications, relevant datasets, and Open-Source Intelligence (OSINT).
- **Establishment of Threat-Evidence Mappings:** the research proposes the development of structured mappings between identified cybersecurity threats common in the EVCI ecosystem and the corresponding digital evidence these threats are likely to generate. This aims to facilitate more targeted investigations.
- **Formulation of Adaptable Forensic Investigation Workflows:** adaptable forensic investigation workflows are presented, which include systematic system modeling, threat analysis, strategies for digital evidence acquisition, and considerations for evidentiary value assessment.
- **Analysis of Digital Evidence Availability Gaps:** the study identifies and analyzes existing gaps in the availability of crucial digital evidence within current EVCS implementations. This analysis aims to highlight limitations in forensic readiness and suggest areas for future improvements in logging standards and practices.
- **Integration of OSINT into Forensic Processes:** the framework emphasizes the integration of OSINT techniques throughout the forensic investigation process, including system modeling, data collection, and threat analysis, to supplement traditional data sources.

The remainder of this paper is organized as follows. Section 2 provides a detailed overview of the EV charging infrastructure, covering its core components, operational stakeholders, the layered network architecture crucial for understanding potential points of evidence, and a review of the prevalent cybersecurity threat landscape. Section 3 meticulously presents the proposed data-driven digital evidence analysis framework, detailing its systematic phases: system modeling, data collection strategies including OSINT integration, threat analysis methodologies, and specific techniques for digital evidence identification and assessment. Section 4 validates the practical applicability of the framework through comprehensive case studies, encompassing both empirically derived scenarios and diverse virtual incidents. Section 5 discusses the key findings from the case studies, evaluates the effectiveness of the proposed method, and critically examines the identified gaps in digital evidence availability. Finally, Section 6 concludes the paper by summarizing the main contributions and proposing avenues for future research in this rapidly evolving domain.

2 Background

2.1 Overview of the Electric Vehicle Charging Ecosystem

The EV charging infrastructure represents a complex cyber-physical ecosystem comprising multiple interconnected components and stakeholders, as illustrated in Fig. 1. Users interact with this infrastructure by plugging their EVs into charging stations, initiating a sophisticated network of interactions that involve payment systems, charging management entities, and the broader electrical grid. These systems operate using various standards and protocols that facilitate vehicle authentication, automated billing processes, and real-time operational management.

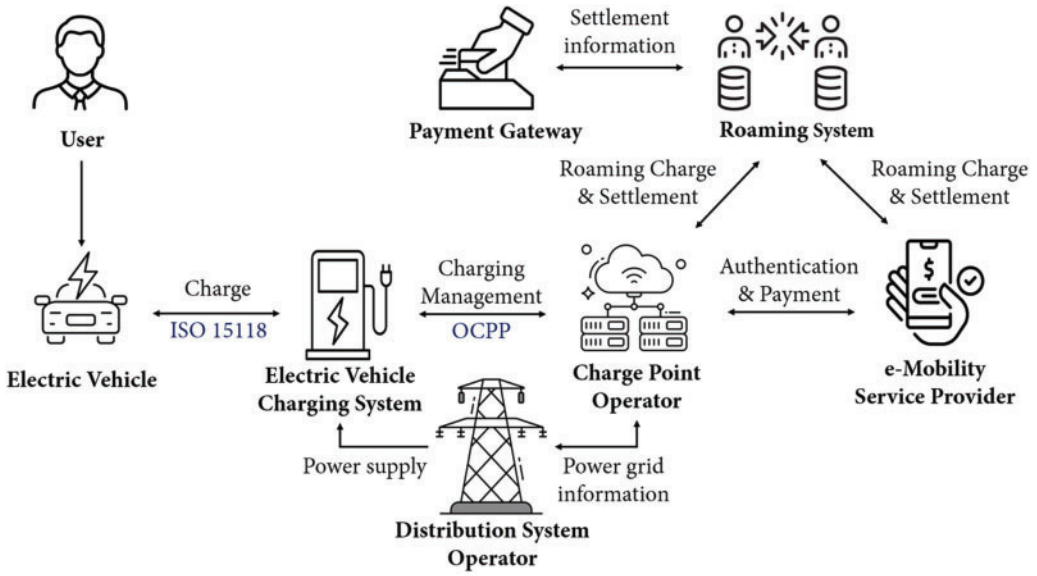

Figure 1: Overall electric vehicle charging ecosystem

- **Users:** primary stakeholders initiate charging sessions by physically connecting their EVs to EVCSs. Modern EVs incorporate technology, such as V2G, allowing them to function as energy consumers and providers, returning energy to the grid under certain conditions.
- **Electric Vehicle Charging Stations:** physical interfaces connect the electric grid and EVs, delivering electrical power through specialized charging terminals equipped with power supply systems and network communication equipment. Advanced EVCSs that are compliant with ISO 15118 support "Plug & Charge," enabling automatic authentication and billing without user intervention, streamlining user experience but introducing cybersecurity considerations.
- **Charge Point Operators (CPOs):** entities manage EVCSs via backend management platforms. The CPOs handle charge session management, real-time operational data transmission, firmware updates, and remote command execution via OCPP. These operations produce significant datasets and logs for forensic investigations.
- **Distribution System Operators (DSOs):** these operators are responsible for managing electrical power distribution networks supporting EV charging infrastructures. The DSOs employ demand-response strategies for load balancing during peak usage periods and coordinate with V2G-enabled EVs to manage grid stability and energy distribution.
- **E-Mobility Service Providers (e-MSPs):** providers manage user authentication, transaction processing, and customer service. The e-MSPs facilitate a seamless user experience by offering platforms to locate charging stations, process payments, manage user accounts, and provide value-added services, such as loyalty programs and tariff discounts.
- **Payment Gateways:** systems securely process financial transactions initiated by users via e-MSP platforms. They integrate with EV roaming systems, enabling effective transaction management and cross-provider financial settlements.
- **EV Roaming Systems:** platforms enhance interoperability across diverse charging networks managed by CPOs. They handle automated authentication, payments, and transaction settlements among operators, significantly improving user convenience and operational efficiency.

This intricate interplay between numerous stakeholders and the extensive data interactions occurring across the ecosystem inherently underscores the necessity of developing and applying structured forensic methodologies. Such methodologies are essential to thoroughly investigate security incidents, attribute actions, and effectively mitigate the diverse cybersecurity risks present in this critical infrastructure.

2.2 Electric Vehicle Charging Network Architecture

The EV charging infrastructure comprises two main domains: the physical layer with hardware components, such as EVs, charging stations, and grid interfaces, and the cyber layer covering software systems and communication networks [14]. This architecture can be extended by referencing models from smart grids, cyber-physical systems, or Internet of Things (IoT) architectures [15–17]. In addition, Fig. 2 illustrates the cyber-physical system-based EV charging architecture in this study, highlighting the structured interactions and data exchanges between the physical hardware, network communications, and application software layers.

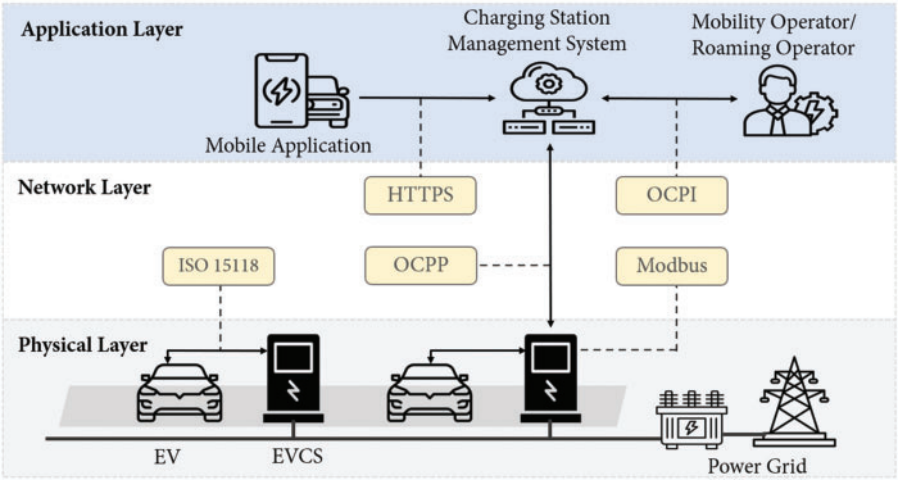

Figure 2: Electric vehicle charging infrastructure network architecture

2.2.1 Physical Layer

The physical layer encompasses the hardware components and direct physical interactions involved in the charging process. This layer includes EVs, EVCSs, and the Power Grid. EVs connect to EVCSs via standardized physical connectors. EVCSs manage the physical power transfer and perform essential real-time monitoring of operational parameters for control and safety.

2.2.2 Network Layer

The network layer provides the communication infrastructure enabling data transfer between physical devices and application layer systems, as well as internally within complex devices like the EVCS. Key protocols facilitating these interactions include:

- ISO 15118: governs communication between the EV and the EVCS, enabling secure authentication, authorization, and charging parameter exchange.
- OCPP: manages communication between the EVCS and the CSMS for session management, status reporting, and remote commands.

- Hypertext Transfer Protocol Secure (HTTPS): secures data exchange between the user's Mobile App and the CSMS.
- Open Charge Point Interface (OCPI): facilitates interoperability and data exchange between the CSMS and Mobility Operator or Roaming Operator platforms.
- Modbus: often employed internally within the EVCS for communication between different hardware modules (e.g., controllers), enabling detailed status monitoring and internal control functions.

2.2.3 Application Layer

The application layer comprises high-level software platforms and services managing overall system operations and user interactions. Key components shown at this layer are:

- Mobile Application: provides end-user interfaces to locate stations, initiate charging sessions, and manage accounts through interaction with the CSMS.
- CSMS: A central backend system managing EVCSs. Its functions include configuration, monitoring, session authorization, firmware updates, and aggregation of operational data received via OCPP.
- Mobility Operator/Roaming Operator: Entities providing services potentially across different charging networks. They interact with the CSMS via OCPI to handle aspects like user authentication, authorization for roaming, and billing data aggregation.

2.3 Cybersecurity Threat Analysis in the Electric Vehicle Charging Infrastructure

Cybersecurity threats to the EV charging infrastructure are diverse and can be effectively analyzed by categorizing them according to the three-layer architecture detailed in Section 2.2. Research has increasingly focused on specific threats at these distinct layers as the infrastructure's complexity and criticality have grown.

At the physical layer, studies have explored a range of hardware and firmware vulnerabilities. These include risks associated with unauthorized firmware updates, direct physical tampering with charging equipment, the presence of hardware backdoors, and weaknesses in cryptographic practices implemented in charging hardware. Johnson et al. [18] examined such hardware-related risks, with a particular emphasis on vulnerabilities found in charger firmware and associated maintenance interfaces. Ronanki and Karneddi [19] contributed through case studies illustrating sabotage scenarios, such as modification and interference attacks targeting hardware operations, firmware integrity, and the overall operational stability of chargers. Furthermore, empirical studies on deployed infrastructure, like the work by Szakály et al. [20], have revealed practical challenges such as the widespread lack of transport layer security (TLS) encryption in some systems and potential weaknesses in key management and communication establishment processes, leaving systems vulnerable.

Research focusing on the network layer has become increasingly specific, concentrating on detailed analyses of communication protocols critical to EV charging operations, notably the OCPP and ISO 15118. Hu et al. [15] presented a survey identifying various protocol-specific vulnerabilities. These include man-in-the-middle (MITM) attacks, replay attacks, denial-of-service (DoS) threats, and side-channel attacks that exploit weak encryption or insecure implementations of these communication standards.

Concerning the application layer, recent studies have significantly focused on vulnerabilities within mobile applications and backend software systems. This includes extensive evaluations of insecure application programming interfaces (APIs), insufficient authentication methods, and compromised payment processing mechanisms. Concurrently, research by Sarieddine et al. [21] identifies mobile applications as a distinct and significant attack surface, revealing prevalent deficiencies in areas like vehicle ownership

verification and authorization processes for critical operations, which could potentially facilitate the remote hijacking of charging sessions.

Table 1 provides a summary of critical cyberattacks identified across these three architectural layers of the EV charging infrastructure. It maps common attack vectors to the affected components, outlines their potential effects, and lists supporting literature.

Table 1: Types of cyberattacks on the electric vehicle charging infrastructure

Layer	Object	Vulnerability/Attack	Effects	Reference
Physical	EV	Relay attack	Unauthorized vehicle control	[22,23]
		GPS spoofing	Manipulating location information	
	EVCS	Firmware tampering	Data leakage, charging schedule manipulation	[24–26]
		Communication interface	Charging service suspension	[20,27]
	Power grid	power outage/overload	Disruption of power grid stability	[25,28,29]
Network	EV-to-EVCS	Side-channel attack	Charging session interruption	[30]
	EVCS-to-CSMS	MITM attack	Data tampering, authentication bypass	[31,32]
		Packet replay	Abnormal charging activities	[33]
		MITM attack	User authentication and payment information theft	[34–36]
		DoS/DDoS	Charging service suspension	[25,34]
		API and web service vulnerabilities	Data leakage, system control	[37]
	Vehicle-to-Grid	Relay attack	Unauthorized energy theft	[38]
		Delayed charging attack	Sudden surge in power grid load	[39]
		DDoS	Power grid stability impairment	[40]
Application	CSMS	Malware injection	Remote control of the EVCS	[14,24]
		Data leaks and manipulation	User information and payment information leaks	[18,41]

(Continued)

Table 1 (continued)

Layer	Object	Vulnerability/Attack	Effects	Reference
	Mobile app	Remote charging session hijacking	Grid instability	[21]

Notes: MITM: man in the middle, DoS: denial of service, DDoS: distributed DoS, GPS: global positioning system.

3 Proposed Digital Evidence Analysis Method

To address the complexities inherent in investigating security incidents within the EVCI, this section introduces a systematic, multiphase method for the analysis of digital evidence. This method, which integrates OSINT as a cross-cutting element, provides a structured approach to decompose system intricacies, guide evidence collection, facilitate comprehensive analysis, and enable robust incident reconstruction. Fig. 3 outlines the core of this method, which consists of four foundational phases: (1) system modeling, (2) data collection, (3) threat analysis, and (4) digital evidence identification. The outputs of these phases converge into a final investigative synthesis. This structured progression is designed to allow investigators to systematically navigate the complexities of EV charging ecosystems, ensuring a thorough, evidence-based, and repeatable forensic process.

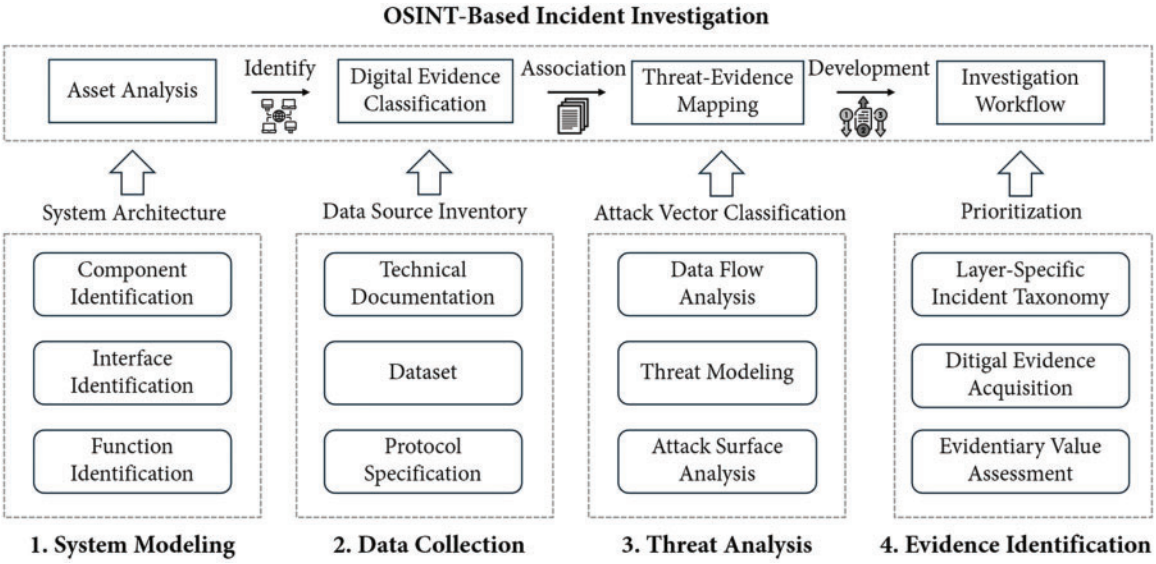

Figure 3: Digital evidence analysis method for the electric vehicle charging infrastructure

To further articulate the procedural logic of this method, Algorithm 1 is presented as a detailed illustration of a potential workflow. This algorithm systematically guides an investigation, commencing with the formal modeling of the target system and the identification of critical assets. Based on this model, it proceeds through structured data collection and threat analysis, which includes attack surface mapping and the correlation of threats with potential digital evidence. The core analytical phase then involves identifying, evaluating, and correlating relevant forensic digital evidence to reconstruct incident timelines and events. Ultimately, these results are synthesized into structured investigation findings. Algorithm 1 thus details an

exemplary sequence of operations and the flow of information between the phases depicted in Fig. 3, offering a computationally grounded and repeatable procedure for conducting forensic investigations in this domain.

Algorithm 1: Digital evidence analysis process for EV charging infrastructure

Input: Incident Information (I_{info}), System Knowledge Base (KB_{sys}), Threat Taxonomy (T_{tax}), Evidence Definitions (A_{def}), OSINT Sources (S_{osint})
Output: Investigation Findings ($Findings_{report}$)
Procedure: SystemModeling(KB_{sys}, I_{info})
Identify System Components C, Interfaces I from KB_{sys}, I_{info}
Construct Formal System Graph G = (C, I)
Map System Functions F onto Graph G
Identify Critical Assets $Assets_{crit}$ within G using F, I_{info}
Return G, $Assets_{crit}$ ▷ Define formal system structure (G) and identify critical assets
End Procedure
Procedure: DataCollection(G, $Assets_{crit}$, KB_{sys}, S_{osint}, A_{def})
Gather Relevant Data Sources (Docs, Datasets, Specs) guided by G, $Assets_{crit}$, S_{osint}
Compile Data Source Inventory DSI
List Potential Digital evidence A_{pot} by scanning DSI using A_{def}
Return DSI, A_{pot} ▷ Gather data sources and list potential digital evidence based on system model
End Procedure
Procedure: ThreatAnalysis(G, I_{info}, T_{tax}, DSI, A_{pot})
Analyze Data Flow pathways on G
Identify relevant Threats T_{id} using T_{tax}, I_{info}
Map Attack Surface AS onto G based on T_{id}
Generate Threat-Digital evidence Map M_{TE} correlating T_{id} with A_{pot}
Return T_{id}, AS, M_{TE} ▷ Analyze threats, attack surface, and generate Threat-Digital evidence Map (M_{TE})
End Procedure
Procedure: EvidenceAnalysis(I_{info}, G, $Assets_{crit}$, DSI, M_{TE}, T_{id}, A_{def})
Select Candidate Digital evidence $A_{candidate}$ based on M_{TE}, I_{info}
Acquire Candidate Digital evidence as $A_{acquired}$ from DSI sources
For each Evidence A in $A_{acquired}$:
Calculate Evidentiary Value E(A)
Filter $A_{acquired}$ yielding $A_{relevant}$ where $E(A) \geq E_{threshold}$
Correlate $A_{relevant}$ using temporal, spatial, and G-based analysis
Reconstruct Incident Timeline TL from correlations
Determine Investigation Findings and supporting Evidence from $A_{relevant}$, TL
Return TL, Findings, Evidence ▷ Consolidate results and produce final structured findings
End Procedure
Procedure SynthesizeFindings(I_{info}, TL, Findings, Evidence, G, AS)
Consolidate TL, Findings, Evidence with context (G, AS, I_{info})

(Continued)

Algorithm 1 (continued)

Produce structured Investigation Findings $\text{Findings}_{\text{report}}$
Return $\text{Findings}_{\text{report}}$
End Procedure

The subsequent subsections will detail the specific procedures, formalisms, and data utilized within each phase of this proposed method.

3.1 System Modeling

The system modeling phase establishes the structural foundation for the proposed forensic investigation framework. Its objective is to create a precise and manageable model of the target EV charging infrastructure, explicitly identifying components, interfaces, their functions, and critical data flows pertinent to post-incident analyses. This comprehensive architectural decomposition is crucial for navigating the complexities of distributed and often proprietary charging systems, enabling investigators to effectively target relevant data sources and potential points where digital evidence may be generated.

3.1.1 Component Identification

This initial step identifies all relevant hardware and software elements within the investigation's scope. Formally, we define the set of components as $C = \{c_1, c_2, \ldots, c_n\}$, where each $c_i \varepsilon C$ represents a distinct system element. The process involves reviewing available technical documentation, analyzing network topology data, conducting controlled network discovery, and consulting system diagrams to enumerate components such as specific EVCS models c_{evcs} CPO backend servers (c_{csms}), e-MSP platforms (c_{emsp}), communication gateways (c_{gw}), databases (c_{db}), and the associated EVs (c_{ev}). Each component (c_i) can possess attributes like type, vendor, model, and version, contributing to the detailed system understanding.

3.1.2 Interface Identification

The next step is to map the communication links and protocols that connect the identified components. The system's interaction structure is formally modeled as a directed graph $G = (C, I)$, where C is the set of vertices (components) and I is the set of edges representing the interfaces. An interface $i \in I$ is defined as a tuple (c_{src}, c_{dst}, p), where $c_{src}, c_{dst} \in C$ are the source and destination components, respectively, and $p \in P$ is the communication protocol (from a set of relevant protocols P) utilized over that interface; thus, $I \subseteq C \times C \times P$. Identifying these interfaces involves analyzing protocol information from documentation (e.g., specific versions like OCPP 1.6J, ISO 15118-2), reviewing network configurations, and potentially analyzing network traffic samples. This helps in understanding how data, including potential digital evidence, are exchanged.

3.1.3 Function Identification

This step involves documenting the critical operational functions performed by the identified components and interfaces, particularly those relevant to potential security incidents. A set of critical functions $\mathrm{F} = \{\mathrm{f}_1, \mathrm{f}_2, \ldots, \mathrm{f}_\mathrm{m}\}$ is defined. Each function $\mathrm{f}_\mathrm{k} \in \mathrm{F}$ can be formally mapped to the set of components responsible for its execution $\mathrm{Map}_{\mathrm{F}\to\mathrm{C}}: \mathrm{F} \to 2^{\mathrm{C}}$ and the set of interfaces utilized $\mathrm{Map}_{\mathrm{F}\to\mathrm{I}}: \mathrm{F} \to 2^{\mathrm{I}}$. For instance, an authentication function f_{auth} might involve components $\{\mathrm{c}_{\mathrm{ev}}, \mathrm{c}_{\mathrm{evcs}}, \mathrm{c}_{\mathrm{csms}}\}$ and utilize interfaces associated with protocols $\mathrm{p}_{\mathrm{iso15118}}$ and $\mathrm{p}_{\mathrm{ocpp}}$. This mapping, derived from protocol specifications, user manuals, and system requirements, allows investigators to anticipate where digital evidence related to specific actions (e.g., authentication failures, unauthorized commands) might be generated within the formal model G.

The intended output of this system modeling phase is a formalized initial asset analysis. Based on the modeled graph $G = (C, I)$ and the function mappings $\mathrm{Map}_{\mathrm{F}\to\mathrm{C}}, \mathrm{Map}_{\mathrm{F}\to\mathrm{I}}$, this analysis identifies critical system assets. A criticality score, $\mathrm{Crit}(\mathrm{x})$, can be assigned to each element $\mathrm{x} \in \mathrm{C} \cup \mathrm{I}$. This assignment considers factors such as its role in critical system functions (derived from F), its potential to store sensitive data or operational logs (information typically part of the System Knowledge Base, KB_{sys}), and its direct relevance based on the preliminary incident information (I_{info}). Critical assets, $Assets_{crit}$, are then identified as those elements meeting or exceeding a certain criticality threshold, θ; formally, $Assets_{crit} = \{\mathrm{x} \in \mathrm{C} \cup \mathrm{I} \mid \mathrm{Critx} \geq \theta\}$. It is important to note that while this describes a formalized approach, the practical assignment of criticality scores and determination of thresholds may be adapted based on the specific investigative context, available information, and experienced judgment, potentially incorporating qualitative assessments alongside or in place of strict quantitative scoring. Regardless of the specific evaluation method, the clearly identified set $Assets_{crit}$ and the formal graph G are the key outputs of this phase passed to subsequent procedures.

3.2 Data Collection

Following the system modeling phase, the data collection process focuses on systematically gathering diverse data sources essential for the subsequent data-driven analysis of potential digital evidence. This phase is guided by the formal system model (G) and the identified critical assets ($Assets_{critical}$) from Section 3.1, ensuring that data gathering is both targeted and efficient. A significant challenge in EVCI forensic investigations is often the limited access to internal data within closed, proprietary systems; therefore, this process emphasizes supplementing available internal data with crucial external intelligence, notably through Open-Source Intelligence methods (S_{osint}). While OSINT can provide valuable contextual information, investigators must acknowledge its limitations in scenarios involving highly proprietary system details or outdated public information; these practical considerations are further discussed in Section 5.4.

The primary categories of data sources to be considered include technical documentation, compliance requirements, operational datasets, and specific communication protocol standards relevant to the interfaces (I) in G. The goal is to compile a comprehensive Data Source Inventory (DSI) and identify a list of potential digital evidence (A_{pot}) using predefined digital evidence definitions (A_{def}). Table 2 provides illustrative examples of common data sources in EVCI investigations, their potential forensic value, and acquisition considerations, serving as a general guide.

Table 2: Data sources for electric vehicle charging infrastructure investigations

Data source	Name/Identifier	Forensic Relevance/Digital evidence focus	Considerations
Technical documentation	Vendor manuals, datasheets	Hardware specifications, vendor-specific log formats, error codes, sensor details	Proprietary—requires vendor access/cooperation
	Standards and requirements	Evidence related to mandated security controls, diagnostic logging, operational reporting	Depends on compliance by region/program

(Continued)

Table 2 (continued)

Data source	Name/Identifier	Forensic Relevance/Digital evidence focus	Considerations
Dataset	Multifaceted Analysis of EV charging data [42]	Detection of anomalous transactions via regional usage patterns	Retrospective data lacking confirmed security incidents
	DESL-EPFL data [43]	Analysis of power-related digital evidence and SoC anomalies in DC fast-charging	Controlled sessions may differ from public usage
	DOE EV charging data [44]	Correlation of vehicle- and charger-based digital evidence at fleet scale	Requires data normalization and time synchronization
	Workplace charging for electric vehicles [45,46]	Contextualizes user behavior digital evidence in workplace charging environments	Scenario specific to workplaces
	ACN-data [47]	Evaluation of managed charging algorithms and API interactions	Research setting may not reflect production conditions
Protocol specification	OCPP	Primary EVCS–CSMS communication (sessions, metering, security events)	Depends on the protocol version; optional security features affect the Digital evidencescope
	ISO 15118	Authentication (PnC/EIM), V2G interactions, TLS handshakes between EV and EVCS	Multivendor interoperability can complicate analysis

Notes: PnC/EIM: plug and charge/external identification means, DC: direct current, CAN: controller area network, SoC: state of charge.

3.2.1 Technical Documentation

This involves gathering specific documents describing the target system's implementation, focusing on critical assets ($Assets_{crit}$). Sources include vendor manuals, system requirements, firmware notes, security advisories, and component datasheets, often found via OSINT (S_{osint}) or direct requests.

3.2.2 Dataset

The Data Source Inventory (DSI) should incorporate operational data (e.g., logs from CPOs/CSMSs, EVCSs, network devices, databases, particularly from $Assets_{crit}$) acquired through authorized procedures, and comparative datasets from public repositories or OSINT (S_{osint}) to provide analytical context and baseline behaviors.

3.2.3 Protocol Specification

Precise technical specifications for communication protocols ($p \in P$) identified in G (e.g., ISO 15118, OCPP) are essential for accurately interpreting communication-related digital evidence from the DSI. They define message structures, data fields, and forensically relevant information, forming a basis for analysis.

3.3 Threat Analysis

The threat analysis phase undertakes a systematic identification and evaluation of cyber threats pertinent to the EV charging infrastructure, as formally modeled by the system graph G. This phase applies the outputs from system modeling (G) and data collection (DSI, A_{pot}) to establish a contextualized threat landscape, guiding subsequent forensic activities. S_{osint} methods are integrated here to enrich the analysis with publicly available information regarding known vulnerabilities, relevant attack vectors, and potential threat actor tactics associated with the system components (C) and communication protocols (P) used in interfaces (I). The principal outputs of this phase, which inform the subsequent digital evidence identification procedures, are a set of identified relevant threats (T_{id}), a delineated attack surface map (AS), and a formalized Threat-Evidence Map (M_{TE}) that links threats to potential digital evidence.

3.3.1 Data Flow Analysis

This initial step scrutinizes the communication pathways and data exchanges between system components ($ci \in C$) as delineated in the system model G. Applying the collected protocol specifications (part of DSI) corresponding to interfaces ($i_k \in I$), the flow of critical data types across these defined interfaces is examined. This process can be visualized using data flow diagrams (DFDs) to identify potential junctures for data interception or manipulation, delineate attack vectors predicated on data flow characteristics, and anticipate the location of potential digital evidence generation within G. Fig. 4 provides an example of such a DFD for a representative EV charging infrastructure, illustrating how this technique can map out data movements between various entities and processes. S_{osint} can contribute by providing intelligence on known protocol implementation weaknesses or common misconfigurations affecting data flow security.

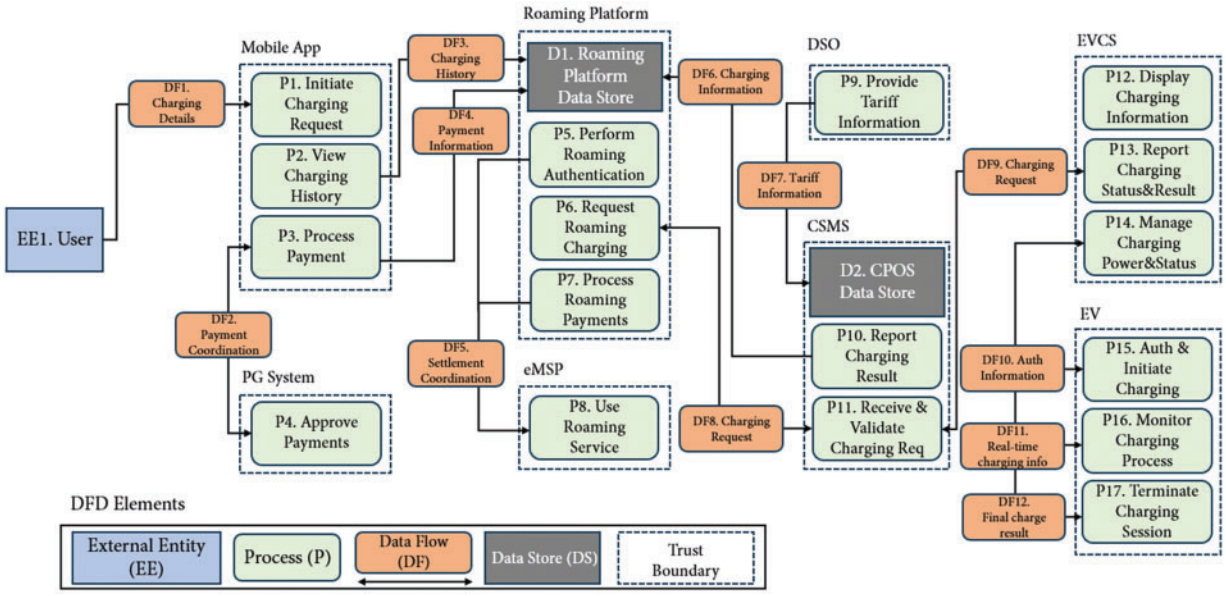

Figure 4: Data flow diagram of electric vehicle charging infrastructure

3.3.2 Threat Modeling

Threat modeling extends the insights from data flow analysis by applying established methodologies, such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege), to categorize and identify potential threats relevant to the EVCI, possibly drawing from a predefined threat taxonomy [22,31]. This approach links identified data flows and system elements to potential threat vectors. For example, spoofing threats might compromise EV-to-EVCS authentication processes (potentially related to interfaces using $p_{iso15118}$), while tampering could alter metering data transmitted via OCPP. This structured analysis helps reveal how adversaries might exploit system weaknesses and results in the identification of a set of relevant threats for the investigation, guiding the subsequent search for associated forensic evidence.

3.3.3 Attack Surface Analysis

The attack surface analysis synthesizes the findings from data flow analysis and the identified threats to provide a comprehensive mapping of the system's attack surface. This involves identifying all interfaces and components in G through which the system could potentially be accessed or influenced by the threats in T_{id}. Each identified element of the attack surface is correlated with specific threats and associated vulnerabilities. For instance, communication channels susceptible to interception or components prone to tampering are highlighted. Fig. 5 conceptually demonstrates how an attack surface can be identified within the EV charging infrastructure, focusing forensic efforts on the most significant vulnerabilities defined within AS. The Threat-Evidence Map is then generated by correlating these identified threats and attack surface elements with the list of potential digital evidence compiled during data collection.

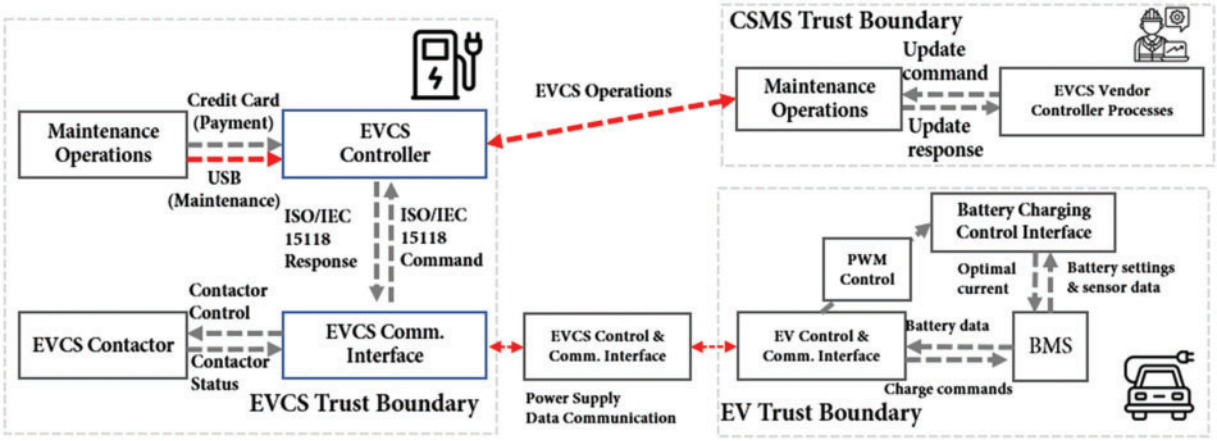

Figure 5: Identifying the attack surface in the EV charging infrastructure

3.4 Digital Evidence Identification

This final core phase of the proposed framework focuses on enumerating, acquiring, and evaluating digital evidence with forensic value. The process is critically guided by the Threat-Evidence Map generated in the preceding Threat Analysis phase (Section 3.3), which links identified threats to potential digital evidence. Utilizing M_{TE} ensures that digital evidence identification, acquisition, and subsequent analysis are targeted and relevant to the specific incident context and the modeled system. This section outlines the general

steps involved, including the use of incident taxonomies, evidence acquisition strategies, and an approach to evidentiary value assessment.

3.4.1 Layer-Specific Incident Taxonomy

To effectively utilize the M_{TE} and guide the search for digital evidence, a structured taxonomy of potential incident types, categorized by the affected architectural layer, is a useful tool. This classification schema can be derived from the threats T_{id} identified during threat analysis (Section 3.3.2) and mapped onto the layered system architecture. Such a taxonomy facilitates a structured investigative approach by enabling investigators to associate observed anomalies or alerts with specific incident categories, thereby refining the focus within the M_{TE} to pinpoint types of digital evidence most likely to be relevant.

- **Physical layer:** physical layer incidents include hardware tampering, unauthorized physical access, or power grid disruptions. For instance, tampering with EVCS units (c_{evcs}) might involve altering charging parameters or injecting malicious firmware.
- **Network layer:** network layer incidents encompass attacks on communication protocols ($p \in P$). Examples include man-in-the-middle attacks, protocol manipulation, or DoS attacks targeting network interfaces ($i_k \in I$).
- **Application layer:** application layer incidents involve breaches at the software level, such as unauthorized access to management systems (c_{csms}), data theft, or fraudulent activities (e.g., manipulating transaction records or stealing user credentials).

3.4.2 Evidence Acquisition

This step details the process of identifying and acquiring specific digital evidence pertinent to the forensic investigation. Guided by the Layer-Specific Incident Taxonomy and the M_{TE}, candidate digital evidence ($A_{candidate}$) is selected from the pool of potential digital evidence. Acquisition procedures are then employed to retrieve these $A_{candidate}$ items from the sources cataloged in the DSI, often prioritizing sources associated with critical assets. The resulting set of collected digital evidence is denoted as $A_{acquired}$. The identification of specific relevant digital evidence within A_{pot} involves a systematic analysis of collected data (DSI, including protocol specifications, datasets, documentation), categorized across the architectural layers. The following tables (Tables 3–10) present a comprehensive catalogue of digital evidence types identified as potentially valuable for forensic investigations within the EVCI. This catalogue is intended to guide investigators on what to look for and serves as a baseline for establishing forensic readiness.

Table 3: Electric vehicle-related digital evidence identified via the ISO 15118 protocol analysis

Category	Identified digital evidence	Source message type	Investigation value
Battery information	Battery state-of-charge data	ChargingStatusReq/Res	Charging state verification, anomalous charging detection
	Requested voltage parameters	ChargeParameterDiscovery Req/Res	Validation of requested electrical parameters
	Maximum power/voltage capabilities	ChargeParameterDiscovery Req/Res	Vehicle capability baseline establishment

(Continued)

Table 3 (continued)

Category	Identified digital evidence	Source message type	Investigation value
Charging parameters	Real-time power/voltage measurements	ChargingStatusReq/Res	Operational condition verification
	Cumulative energy delivery	MeteringReceiptReq/Res	Energy usage validation
Vehicle information	Electric vehicle ID	AuthorizationReq/Res	Session attribution, vehicle tracking
	Vehicle certificate data	CertificateInstallationReq/Res CertificateUpdateReq/Res	Authentication verification
Status information	Vehicle operational status	ChargingStatusReq/Res	Condition monitoring, anomaly detection

Table 4: Electric vehicle charging station-related digital evidence identified via a dataset comparison

Evidence type	Identified digital evidence	Dataset coverage*	Significance and value
Session information	Session start/end timestamps	5/5	Temporal correlation, session reconstruction
	Session ID	3/5	Uniquely identifying transactions
Charging power parameters	Requested power and maximum power	3/5	Anomalous power request detection
	Battery state of charge	2/5	Battery condition monitoring
Billing information	Total energy delivered	5/5	Charging transaction verification
	Session payment amount	1/5	Financial transaction validation
Identity information	User ID	3/5	User attribution
	Vehicle ID	1/5	Vehicle tracking and correlation
Infrastructure information	Charger ID	4/5	Equipment attribution
	Charger location data	3/5	Geographic correlation

Note: *Number of datasets containing the digital evidence out of the five analyzed datasets.

Table 5: Electric vehicle to charging station network communication digital evidence

Communication element	Identified digital evidence	Data source	Significance and value
Physical connection signaling	Control pilot signal parameters, PWM duty-cycle measurements	ISO 15118-3 [48] specification	Detection of signal manipulation, connector tampering
Network handshake mechanisms	EXI encoded message sequences, V2G session establishment parameters	ISO 15118-2 [49] (Section 8.3)	Authentication integrity verification, session manipulation, identification
Transport layer security	Certificate exchange records, TLS cipher suite negotiations	ISO 15118-2 [49] (Section 7.9)	Cryptographic integrity verification, security downgrade detection
Connection management	Session initiation/termination events, error recovery sequences	ISO 15118-2 [49] (Section 8.7)	Connection disruption analysis, communication interference detection

Notes: PWM: Pulse Width Modulation, EXI: Efficient Extensible Markup Language Interchange.

Table 6: OCPP-based electric vehicle charging station to management system communication digital evidence

Message category	Identified digital evidence	Significance and value
Authentication	AuthorizeRequest/Response messages, IdToken validation records	Authentication integrity verification, credential misuse detection
Transaction management	StartTransaction/StopTransaction messages, MeterValues records with timestamps	Session boundary verification, energy measurement validation
Status reporting	StatusNotification messages, ErrorCode fields, connector status changes	System state transition analysis, anomalous condition detection
Remote operations	RemoteStartTransaction/RemoteStopTransaction messages, triggering entity identifiers	Administrative action verification, unauthorized control detection
Security events	SecurityEventNotification messages, SignedMeterValue fields	Security incident verification, data integrity validation

Table 7: Authentication-related digital evidence

Evidence type	Data elements	Significance and value
User identification	User ID values, IDToken parameters	User attribution, session ownership verification
Authorization records	Authorization requests/responses, authorization status	Authentication attempt verification, access control validation
Session tokens	Session identifiers, session contexts	Session tracking, session hijacking detection
Authentication timestamps	Login/logout events, authentication attempts	Temporal correlation, access pattern analysis

Table 8: Transaction management digital evidence

Evidence type	Data elements	Significance and value
Session records	Session ID values, transaction start/stop messages	Session boundary verification, transaction reconstruction
Consumption measurements	Energy delivered (kWh), meter values	Energy delivery verification, consumption anomaly detection
Financial data	Payment amounts, billing parameters	Financial transaction validation, fraud detection
Transaction timestamps	Start/stop times, meter reading intervals	Temporal analysis, charging pattern verification

Table 9: Status notification digital evidence

Digital evidence type	Data elements	Significance and value
Operational states	Charger status codes, connector states	System condition verification, abnormal state detection
Control indicators	Controlled session flags, management intervention records	External control verification, unauthorized management detection
Connection states	Connection/disconnection timestamps, charging state changes	Session timeline reconstruction, usage pattern analysis
Fault indicators	Error codes, diagnostic information	Fault condition analysis, system integrity verification

Table 10: System management digital evidence

Digital evidence type	Data elements	Significance and value
Remote commands	RemoteStartTransaction/RemoteStopTransaction records	Administrative action verification, unauthorized control detection
Configuration changes	GetConfiguration/ChangeConfiguration messages	System configuration analysis, setting modification detection
Firmware management	UpdateFirmware notifications, firmware status	Software integrity verification, unauthorized update detection
Diagnostics	DiagnosticsStatusNotification, log retrieval records	System health analysis, tampering evidence identification

Physical layer digital evidence originates from hardware components ($c_i \in C$) and their operational data. Based on the analysis of protocol specifications like ISO 15118 and examination of various datasets within DSI, critical physical layer digital evidence can be identified:

- **EV-related digital evidence:** analysis of standards such as ISO 15118-2 reveals message types generating valuable digital evidence [49]. Message structures identified (e.g., from specific standard sections) yield digital evidence detailed in Table 3, representing critical evidence for physical layer incidents.

EVCS-related digital evidence: comparative analysis of multiple charging session datasets (examples referenced in Table 2 and detailed in Appendix A) enables the identification of common digital evidence generated across diverse charging systems (c_{evcs}). Table 4 shows this digital evidence, providing essential evidence for incidents involving charging equipment.

Network layer digital evidence comprise data generated during communications between components over interfaces ($I_k \in I$). Critical forensic evidence is identified across primary communication segments:

- **EV-to-evcs communication digital evidence:** analysis extends beyond the ISO 15118 message content (as referenced for physical digital evidence) to include network-level communication traces with significant forensic value, detailed in Table 5. These encompass physical connection signals, handshake parameters, security mechanism traces, and connection events.
- **EVCS–CSMS communication digital evidence:** the OCPP protocol governs standardized communication between c_{evcs} and c_{csms}. Table 6 presents systematically identified OCPP-generated digital evidence categorized by message type, crucial for analyzing interactions over this interface.

Application layer digital evidence encompass data generated by management systems (c_{csms}), user applications, and related services. Systematic analysis identifies several categories of application-level digital evidence with significant forensic value:

- **Authentication digital evidence:** the OCPP generates several authentication-related digital evidence for forensic investigation as detailed in Table 7.
- **Transaction management digital evidence:** Table 8 shows consistent transaction-related digital evidence across implementations, vital for verifying session details and financial data.
- **Status notification digital evidence:** critical evidence regarding system conditions, derived from OCPP status notifications, is presented in Table 9.

- **System management digital evidence:** management-level digital evidence documenting administrative actions via OCPP are outlined in Table 10.

The collection and categorization of these diverse digital evidence ($A_{acquired}$) across all layers, guided by M_{TA} and the incident context, provide the foundation for the subsequent evidentiary value assessment (Section 3.4.3). Investigators can reconstruct complex incident scenarios, attribute malicious activities to specific actors, and document the effects of security events on charging operations by collecting and analyzing these digital evidence.

3.4.3 Evidentiary Value Assessment

Following the acquisition of potentially relevant digital evidence ($A_{acquired}$), a critical phase involves the formalized assessment of their evidentiary value. This assessment provides a quantitative basis for prioritizing analytical efforts, focusing resources on digital evidence most likely to contribute significantly to the investigation. The evaluation is based on established forensic criteria—Relevance, Reliability, Temporal Fidelity, and Completeness—considered within the specific context of the EV charging infrastructure incident, and utilizes a structured quantitative model.

We define the Evidentiary Value $E(A)$ for each Digital evidence $A \in A_{acquired}$ using a multi-criteria decision analysis approach, specifically a weighted sum model as presented in Eq. (1). This model was chosen initially for its clarity, while acknowledging the potential for more complex models in future work.

$$LE(A) = w_R \cdot f_R(A) + w_L \cdot f_L(A) + w_T \cdot f_T(A) + w_C \cdot f_C(A) \tag{1}$$

where f_R, f_L, f_T, f_C represent scoring functions that quantify the digital evidence's Relevance, Reliability, Temporal Fidelity, and Completeness, respectively. A critical step for practical application, which is beyond the scope of the current definitions provided in this paper, is the development of specific, objective rubrics or mathematical formulas to operationalize each function $f_X(A)$, mapping diverse digital evidence attributes onto a normalized scale (e.g., [0, 1]). The weights w_R, w_L, w_T, w_C represent the relative importance of each criterion, determined contextually for the specific investigation, satisfying $\sum w_i = 1$.

- **Relevance (f_R):** this function must quantify the direct linkage between Digital evidence A and the incident hypothesis or investigative questions. Defining the scoring mechanism requires establishing rules based on factors like the evidence's ability to confirm/refute specific questions (e.g., event timing, actor identity).
- **Reliability (f_L):** this function must quantify the trustworthiness and integrity of A. Operationalization involves creating a scoring system based on source credibility, creation process integrity, potential for tampering (e.g., hash verification status), and chain of custody documentation.
- **Temporal Fidelity (f_T):** this function must quantify the accuracy, precision, and synchronization of timestamps associated with A. Defining this function requires assessing timestamp source reliability, precision level, and potential temporal discrepancies using a consistent method.
- **Completeness (f_C):** this function must quantify the sufficiency of detail and context provided by A. Operationalization involves assessing whether the Digital evidence captures an event adequately or presents only a fragment, considering the presence of necessary contextual information.

A critical consideration for the practical application of Eq. (1) is the necessary development of specific, objective rubrics or detailed mathematical formulas to operationalize each scoring function $f_X(A)$. Defining these functions rigorously is a complex task and is considered beyond the scope of the current paper's primary contributions, representing an area for significant future research. Therefore, in the context of this paper and its case studies, the assessment of evidentiary value is primarily guided by these criteria in a qualitative

or conceptual manner, rather than through strict quantitative calculation using Eq. (1). The aim is to filter $A_{acquired}$ to yield $A_{relevant}$ where $E(A)$ is deemed sufficiently high based on these guiding criteria and a conceptually applied threshold. Subsequent analysis involves correlating $A_{relevant}$ to reconstruct the incident timeline and determine findings.

4 Case Study

This section validates and demonstrates the practical applicability of the data-driven forensic method proposed in Section 3. The efficacy of the method is illustrated through its application to credible threat scenarios, some derived from empirical security research targeting EVCSs and others elaborated as representative virtual incident investigation scenarios. These case studies demonstrate the application of the structured forensic workflow. This workflow is conceptually guided by the phases outlined in Fig. 3 and the procedural logic illustrated in Algorithm 1, integrating system modeling, OSINT-informed data collection, threat analysis, digital evidence identification, conceptual evidentiary value assessment, and systematic investigation principles. The objective is to substantiate the method's capacity to address complex forensic challenges within contemporary EV charging ecosystems, thereby aiming to enhance forensic readiness and response capabilities.

4.1 Digital Evidence Analysis Based on Demonstrated Threat Scenarios

This first case study focuses on the forensic investigation process for incidents corresponding to threat vectors whose viability and influence were empirically confirmed by the Electric Vehicle Secure Architecture Laboratory Demonstration (EV SALaD) project [27]. The significance of using these EV SALaD findings is their empirical validation. The project moved beyond theoretical vulnerabilities to demonstrate tangible attack consequences on real-world extremely fast charging systems. Therefore, the observable outcomes documented during these demonstrations represent high-fidelity examples of potential security incident manifestations.

Table 11 presents these empirically observed outcomes as potential incident scenarios that a forensic investigator might encounter. The descriptions focus on the observable results of the incident, facilitating the forensic task of determining the cause. This approach aligns with the initial investigation phase, where the primary information is often the manifestation of the problem itself.

Table 11: Incident scenarios derived from demonstrated threats

#	Incident scenario description	Affected component	Potential impact
1	Displays abnormal charging amount and power values	Human-machine interface	Misleading information, user confusion, potential billing errors, unnecessary service interruption
2	"Emergency Shutdown" message appears on the display during an active charging session		
3	"You've Been Hacked" message appears on the display		
4	Unstable power delivery with observable fluctuations during the charging session	Power conversion system	Degraded charging quality, EV battery stress

(Continued)

Table 11 (continued)

#	Incident scenario description	Affected component	Potential impact
5	Charging cable temperature increases abnormally during charging	Thermal management system	Safety hazard, automatic power reduction, and equipment reliability concerns
6	Charging cable cooling system makes irregular on-off sounds during operations		
7	AC input contactors unexpectedly open during high-power charging, causing abrupt session termination	Power management system	Charging service interruption, charging failure
8	Vehicle charges much slower than selected with the wrong battery level displayed	EV-EVCS communic ations	Extended charging duration
9	Charging session unexpectedly terminates or will not start despite proper connection		Charging service interruption
10	Charger interface behavior unexpectedly changes after vehicle connection		
11	Charging session automatically ends without apparent cause or error message	EVCS–CSMS communications	

4.1.1 System Modeling for Digital Evidence Analysis

Following the method outlined in Section 4.1 and the System Modeling procedure in Algorithm 1, we constructed a detailed system model relevant to the scenarios in Table 11. This involved identifying the key system components (C) and their communication interfaces (I), formally conceptualized as a graph $G = (C, I)$. Table 12 provides an overview of the primary components and interfaces considered in this case study's system model.

Table 12: Components and interfaces in the case study system model

Type	Element ($c \in C$ or $i \in I$)	Description/Protocol ($p \in P$)	Relevant scenarios
Component	Electric vehicle	The vehicle being charged	8, 9
	EVCS controller	Central processing unit of the charging station	1–11
	HMI	Human-Machine Interface (Display/Input)	1, 2, 3, 10
	Power module	Converts and delivers electrical power	4, 7, 8

(Continued)

Table 12 (continued)

Type	Element ($c \in Cori \in I$)	Description/Protocol ($p \in P$)	Relevant scenarios
	Thermal management	Cooling system (e.g., cable cooling)	5, 6
	AC input contactor	Connects/disconnects AC power input	7
	Charging station management system	Backend system managing multiple EVCSs	11
	EV-EVCS interface	Communication between EV and EVCS	8, 9, 10
Interface	ISO 15118/CCS/CHAdeMO		
	EVCS internal interface	Communication between internal EVCS modules	1–7
	CAN bus, Modbus, Ethernet		
	EVCS-CSMS interface	Communication between EVCS and Backend	11
	OCPP		
	EVCS maintenance interface	Port for diagnostics/updates (e.g., USB, Ethernet)	1–7

This model synthesizes the architectural representations in Figs. 1 and 2. Regarding the physical layer, relevant hardware components identified in Table 12 include the HMI display systems, power conversion modules, cooling management subsystems, and input contactors. The interface mapping identified critical communication pathways, such as the internal bus between the HMI display and the central controller (relevant to Scenarios 1–3) and interfaces controlling the power module and cooling system (relevant to Scenarios 4–7). The function identification process revealed that these components execute critical operations like power delivery control, thermal regulation, and safety monitoring, generating forensically significant data. The model also captures network layer interfaces like the EV-EVCS communication (using CCS/CHAdeMO) and the EVCS-CSMS communication (using OCPP), relevant to Scenarios 8–11.

4.1.2 Data Collection Application

This phase focused on gathering diverse data sources essential for the investigation. The collection was specifically targeted towards obtaining information related to the key system components and interfaces identified in the system model (Table 12). The primary goal was to compile a comprehensive Data Source Inventory (DSI) and subsequently identify a list of Potential Digital evidence (A_{pot}) by analyzing the DSI based on predefined Digital evidence definitions (A_{def}). This involved gathering technical documentation, relevant datasets, and specific communication protocol standards governing the identified interfaces.

The technical documentation analysis focused on specifications like ISO 15118 and OCPP, which define the communication structure pertinent to the interfaces listed in Table 12. These specifications supply detailed message formats, data fields, and parameter definitions crucial for interpreting communication digital evidence potentially present in the collected data.

The dataset analysis incorporated multiple datasets identified during data collection (examples referenced in Table 2 and detailed in Appendix A), including the Multifaceted Analysis of EV charging data, DESL-EPFL data, and DOE EV charging data. These datasets provided baseline behavioral patterns for charging operations related to the modeled components (EV, EVCS), enabling the identification of anomalous activities characteristic of the security incidents described in Table 11.

The examination of the protocol specifications (part of the *DSI*) revealed substantive differences in security-relevant data fields between protocol versions, directly impacting the A_{pot} derivable from communications over interfaces like the EVCS-CSMS link (Table 12). For example, OCPP 1.6 implementations often omit critical security event logging capabilities present in OCPP 2.0, whereas implementations of ISO 15118 vary significantly in certificate handling and authentication mechanisms. These variations substantially affect the forensic digital evidence available during investigations and require tailored analysis approaches for different deployment scenarios impacting the components and interfaces modeled in Table 12. Table 13 summarizes the key differences between protocol versions and their implications for forensic investigations.

Table 13: Protocol version differences and forensic implications

Protocol	Version	Security features	Digital evidence available	Limitation
OCPP	1.6J	Basic authentication, Optional TLS	Authorization logs, Transaction records, Basic status notifications	Limited security event logging, No mutual authentication records, No firmware security logs
	2.0.1	Mutual authentication, Mandatory TLS, Security events Security event notifications, Firmware integrity checks, Transaction signatures	Enhanced authentication logs,	Rarely implemented in current charging infrastructure
ISO 15118	−2	Basic TLS, Certificate exchange	Certificate exchange logs, Basic charge parameter records	Limited authentication details, Basic session management logs
	−20	Enhanced Public Key Infrastructure (PKI), Plug & Charge security	Certificate validation records, Comprehensive session security logs, Contract certificate records	Not widely implemented, Backward compatibility issues limiting adoption

4.1.3 Threat Analysis Based on Incident Scenarios

The threat analysis procedure utilized the system model and the collected data sources and potential digital evidence from the previous phase as primary inputs, along with incident information (I_{info}) derived from Table 11 scenarios and a predefined threat taxonomy (T_{tax}). The objective was to systematically identify relevant threats (T_{id}), delineate the attack surface (AS) pertinent to the modeled system, and critically, generate the Threat-Digital Evidence Map (M_{TE}) that links identified threats to A_{pot}, guiding the subsequent digital evidence identification phase.

The data flow analysis scrutinized communication pathways between the system components and across interfaces defined in Table 12. For Scenarios 1 to 3 involving HMI anomalies, we mapped the flow of display instructions from the EVCS Controller to the EVCS HMI, identifying potential interception points on the EVCS Internal Interface. For Scenarios 4 to 7 affecting power and thermal systems, we traced control signals between the EVCS Controller, Power Module, and Thermal Management system via internal interfaces, highlighting vulnerable points where malicious commands could be injected. For communication-related scenarios (8 to 11), we analyzed the bidirectional data flows over the EV-EVCS and EVCS-CSMS interfaces, identifying potential protocol vulnerabilities.

Threat modeling then classified each scenario according to its predominant threat category using the STRIDE framework (drawing from T_{tax}), explicitly linking threats to the components and interfaces in Table 12. This classification, summarized in Table 14, connects T_{id} to their likely manifestations in system data and guided the generation of the M_{TE}.

Table 14: Threat classification of incident scenarios

Protocol	Scenarios	Threat	Affected system elements	Potential attack vectors
HMI Aanomalies	1–3	Tampering, Information disclosure	Display subsystem, Controller-HMI interface	Maintenance interfaces, USB port
Power & Thermal system manipulation	4–7	Tampering, Denial of service, Elevation of privilege	Power conversion modules, Thermal management system, Input power contactors	Maintenance interfaces, Firmware update mechanisms
Communication protocol exploitation	8–11	Spoofing, Tampering, Denial of service	Certificate exchange logs, Basic charge parameter records	Protocol implementation flaws, Communication channel interception, Lack of message authentication

The attack surface analysis integrated these findings to map the system's overall AS comprehensively. As illustrated conceptually in Fig. 6, this involved correlating the identified vulnerable components and interfaces from Table 12 (e.g., EVCS Maintenance Interface, EV-EVCS and EVCS-CSMS communication link) with the T_{id} relevant to the scenarios. This analysis highlighted that maintenance interfaces, physical

connectors (related to EV-EVCS interface), protocol implementations (affecting all communication interfaces), and administrative access mechanisms (potentially via EVCS-CSMS interface) represent the most significant elements of the *AS* for these scenarios.

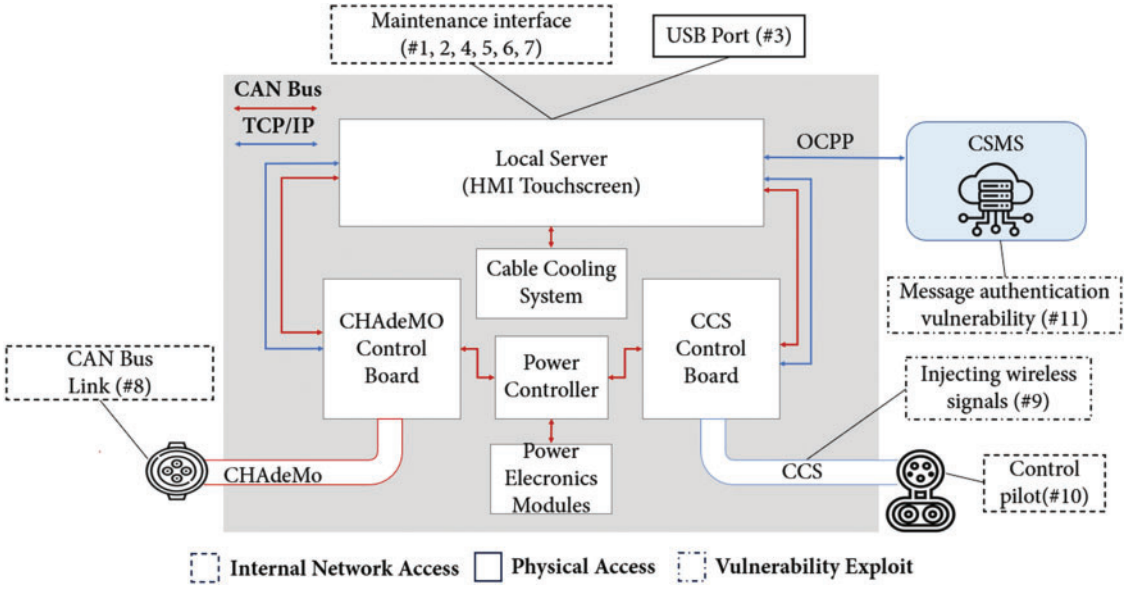

Figure 6: Attack surface identification for EV charging infrastructure incident scenarios

The key output of this phase, the M_{TE}, formally links the identified threats (T_{id}) and attack surface elements (AS) to the A_{pot} listed in the previous step, providing a crucial input for the evidence analysis in the next section.

4.1.4 Layer-Specific Digital Evidence Identification

This procedure systematically processes potential evidence based on the findings from the preceding threat analysis phase. Key inputs for this procedure, as defined in Algorithm 1, include the M_{TE}, I_{info}, G, $Assets_{crit}$, DSI, and A_{def}. The core of this analysis begins by selecting Candidate Digital evidence ($A_{candidate}$) pertinent to the scenario, guided by the M_{TE}, followed by acquiring these candidates ($A_{acquired}$) from DSI. Subsequently, the Evidentiary Value ($E(A)$) of acquired digital evidence is conceptually evaluated using the criteria from Eq. (1), and only those meeting the required evidentiary threshold are filtered as Relevant Digital evidence ($A_{relevant}$). These relevant digital evidence are then correlated using temporal, spatial, and system-model-based analysis. This correlation enables the reconstruction of the incident timeline and the determination of findings based on the consolidated evidence. The relevant digital evidence ($A_{relevant}$) identified through this process for the case study scenarios are discussed below, organized by architectural layer.

For HMI-related incidents (Scenarios 1 to 3), the Evidence Analysis procedure, guided by the relevant part of M_{TE}, focused on identifying digital evidence from the EVCS Controller and HMI components (Table 12). Key $A_{relevant}$ identified included controller-HMI communication logs (from EVCS Internal Interface), system status codes indicating component communication errors, external device connection records (via EVCS Maintenance Interface), and command history logs. HMI-controller communication logs were assessed (conceptually, via $E(A)$) as having high evidentiary value for distinguishing system

malfunctions from malicious manipulations. For example, a simplified logical check applied during the correlation step to detect potential display tampering in these logs can be formulated. In the following expression in Eq. (2), cmd represents an individual command or log entry within the log:

$$IsTampered\left(Log_{HMI}\right) = \exists cmd \in Log_{HMI}; \text{s.t;} \left(cmd.source \notin TrustedSources\right) \vee \left(\neg VerifyChecksum\left(cmd\right)\right) \tag{2}$$

For power and thermal management incidents (Scenarios 4 to 7), the analysis targeted digital evidence related to the EVCS Power Module, Thermal Management system, and Input Contactor. Relevant digital evidence identified through the process included power module control signals, real-time power/voltage measurements (potentially derived from ISO 15118 messages exchanged over the EV-EVCS interface, if logged), thermal management system logs documenting cooling system behavior, state transition records, and internal network traffic captures (EVCS Internal Interface). However, our analysis, stemming from the difficulty in acquiring sufficient $A_{acquired}$ for evaluation, highlighted a critical digital evidence gap: detailed thermal management data such as cooling pump operation status, fan activation patterns, and precise cable temperature sensor readings are often not systematically recorded or available in the DSI of current implementations. This lack of granular data severely hampers the forensic analysis and conclusive determination (timeline reconstruction) of thermal incidents.

For communication protocol incidents (Scenarios 8 to 11), the focus was on digital evidence generated during communications over the EV-EVCS and EVCS-CSMS interfaces. Significant $A_{relevant}$ identified included Controller Area Network (CAN) bus communication packets documenting protocol-level interactions, control pilot signal data detailing pulse-width modulation signals and duty-cycle patterns, charging session timing information, battery SoC reporting data, and network traffic patterns potentially revealing attacks like Man-in-the-Middle or replay on either interface. The Evidence Analysis process again revealed significant gaps: CAN bus communication packets and detailed pilot wire signal logs were identified as potentially high-value digital evidence (high potential $E(A)$) but are not consistently captured or available in the DSI from existing systems. This represents a significant limitation in current forensic capabilities for investigating attacks targeting these communication layers.

The analysis revealed substantive patterns in digital evidence availability and utility across these scenarios. Physical layer digital evidence provided the most direct evidence of system manipulation but were often inadequately logged in existing implementations. Network layer digital evidence offer the most consistent forensic value, particularly when protocol-level traffic is comprehensively captured. Application layer digital evidence vary significantly in forensic utility depending on implementation-specific logging practices, with substantial inconsistencies across charging networks. These patterns strongly highlight the need for improved standardization of forensic logging practices across the EV charging ecosystem to ensure sufficient high-value digital evidence ($A_{relevant}$) can be reliably identified, acquired, and analyzed using this method, thereby enhancing overall investigative capabilities.

4.2 Case Studies Based on Virtual Scenarios

This section extends the application of the forensic method proposed in Section 3 beyond the empirically derived scenarios presented in Section 4.1. We explore four hypothetical yet plausible incident scenarios in the EV charging infrastructure, each representing a distinct category of security threats with significant forensic implications. These scenarios were selected primarily to demonstrate the adaptability of our forensic method's analytical logic and procedural flow across diverse investigative contexts that charging infrastructure operators and forensic analysts might encounter. It is important to note that these virtual scenarios, while designed for plausibility, are illustrative and serve to explore the method's application under

assumed data conditions; they do not represent empirical validation based on real-world incident data. The analytical checks and equations (Eqs. (3)–(6)) presented within these scenarios operate on conceptual data inputs. Table 15 provides an overview of the four virtual scenarios explored. Unlike the scenarios in Section 4.1, these virtual scenarios often represent complex, multi-stage security events, allowing for a broader exploration of the method's potential application.

Table 15: Virtual incident scenarios for forensic method application

#	Incident scenario description	Affected component	Potential impacts
1	Fire incident at EVCS during an active charging session	EVCS hardware, Power systems, Connected EV	Equipment damage, Safety hazard, Service disruption, Potential liability issues
2	Coordinated attack targeting multiple charging stations to disrupt the power grid	Multiple EVCSs, Grid connection points, CSMS	Grid instability, Power outages, Cascading infrastructure failures
3	Tracking a stolen EV through its charging activities at various stations	EV, Multiple charging stations, Authentication systems	Identification of unauthorized usage patterns, Evidence for criminal investigation
4	Unauthorized access to charging network resulting in data theft and system manipulation	EVCS network, CSMS, User data repositories	Personal data exposure, Payment information theft, Network compromise

4.2.1 Investigation of an Electric Vehicle Charging Station Fire Scenario

This first virtual scenario involves a fire incident at an EVCS. The potential causes are varied, including EVCS malfunction, EV battery faults, user actions, or external environmental factors. Applying the structured forensic method proposed herein, the goal of the investigation is to determine the root cause. The process involves identifying and acquiring critical digital evidence, such as battery SoC information from the EV, EVCS data, and corresponding user authentication/payment data from the CSMS. The subsequent analysis phase examines these identified digital evidence for anomalies and correlations indicative of the fire's origin. For example, scrutinizing power logs (Log_{Power}) for overcurrent conditions preceding the incident could involve the illustrative check shown in Eq. (3). In this equation, T_{window} represents the specific time window being analyzed within the power log, and $I_{maxlimit}$ denotes the predefined maximum current threshold considered safe for the EVCS operation:

$$DetectOvercurrent\left(Log_{Power}, T_{window}\right) = \exists t \in T_{window}; \text{s.t.}; Current\left(Log_{Power}, t\right) > I_{max\_limit} \tag{3}$$

Further analysis would involve examining EVCS status codes and EV SoC data for electrical faults (overvoltage, overcurrent, overcharging), analyzing power logs for other abnormal requests or delivery patterns, reviewing available environmental sensor data (temperature, water ingress), and correlating CSMS data with the incident timeline to assess user actions. Finally, synthesizing the findings from the correlated evidence allows inferring the most probable cause.

4.2.2 Investigation of a Grid Attack Scenario via Charging Stations

This scenario considers a coordinated attack leveraging the EV charging infrastructure to disrupt the electrical grid. Guided by the proposed systematic method, the investigation aims to identify the attack vector, method, and involved entities. Critical digital evidence identified during the evidence analysis phase include EV SoC data, EVCS power logs, charger status codes, EVCS-CSMS communication logs (OCPP), session timing data, and CSMS logs (user authentication, network traffic, OS access).

The analysis phase focuses on detecting anomalies indicative of such a coordinated attack across multiple chargers. As an example of specific logic that could be applied, detecting potentially coordinated high charging demands might involve a check like the one defined in Eq. (4). In this equation, C_{subset} represents the subset of chargers under scrutiny within a specific time window t_{window}, $IsHighDemand\,(Log_c, t_{window})$ is a function evaluating if an individual charger c's log indicates high demand during that window, and $Demand_{threshold}$ is a predefined threshold representing the minimum ratio of chargers in the subset that need to show high demand simultaneously to trigger suspicion:

$$DetectCoordinatedDemand\,(Logs, C_{subset}, t_{window})\,L = \left(\frac{1}{|C_{subset}|}\sum_{c\in C_{subset}} IsHighDemand\,(Log_c, t_{window})\right) > Demand_{threshold} \tag{4}$$

Beyond such specific checks, the broader analysis involves scrutinizing power logs and status codes for abnormal grid feedback or simultaneous faults. Communication logs and session timing data are analyzed for patterns suggesting orchestrated commands or communication jamming. CSMS logs are assessed for evidence of unauthorized access or command injection targeting grid interaction parameters. Correlating suspicious network activity with authentication data helps identify compromised accounts or actors involved. Consolidating the evidence then confirms the nature and source of the attack.

4.2.3 Investigation Tracking a Stolen Electric Vehicle

This scenario involves tracking a stolen EV using charging station data. Following the defined forensic process, the investigation focuses on reconstructing the vehicle's location and movement patterns. Essential digital evidence identified during the investigation include the stolen vehicle's unique identifier (EV_{stolen}), its battery SoC data recorded during charging sessions, charger IDs and their physical location data, requested power logs, session timestamps, and relevant CSMS data (like user authentication and network logs).

The core of the analysis involves querying CSMS and EVCS logs using the (EV_{stolen}) to retrieve all associated charging events. The locations from these events are then mapped chronologically to reconstruct the vehicle's path. The logic for this path reconstruction can be represented by Eq. (5). In this equation, QueryLogsByEV_ID(EV_{stolen}) retrieves the relevant session records for the EV_{stolen}, the Map function extracts the timestamp ($session.timestamp$) and location ($session.location$) from each session record ($session$), and $Sort_{time}$ orders these timestamp-location pairs by time to produce the final path sequence ($Path$):

$$Path = Sort_{time}(\text{Map}(\text{QueryLogsByEV\_ID}(EV_{stolen}), \lambda session: (session.timestamp, session.location))) \tag{5}$$

In addition to path reconstruction, the SoC data recorded at the start and end of the identified sessions can help estimate the travel range and predict potential subsequent locations. Analysis of the requested power data might also help distinguish the stolen vehicle's unique charging signature. Furthermore, user

authentication information and network logs associated with these sessions can provide clues regarding the perpetrator's methods or location. Integrating these digital findings with physical evidence (e.g., CCTV footage from charging sites) completes the investigation picture.

4.2.4 Investigation of Charging Station Hacking and the Data Breach Scenario

This scenario addresses a compromise of the charging network or CSMS for data exfiltration or manipulation. Following the proposed structured approach, the investigation aims to determine the intrusion vector, breach scope, data manipulation, and trace attacker activities. Relevant digital evidence identified during the analysis include potentially compromised data (EV IDs, SoC logs), charger/location info, OCPP logs, session times, and critical CSMS logs (authentication, network traffic, OS access, database audit, firewall).

The analysis phase focuses on identifying the breach point and potential data exfiltration pathways. For instance, network traffic logs (Log_{Net}) are examined for suspicious outbound connections. An example rule applied during this analysis to flag potentially suspicious network flows ($flow$) is given in Eq. (6). Here, $flow.dest$ is the flow's destination address, $TrustedDestinations$ is a predefined set of legitimate destinations, $flow.protocol$ is the protocol used, P_{exfil} represents protocol(s) potentially used for exfiltration (e.g., FTP, specific TCP ports), $flow.volume$ is the data volume transferred, and $V_{exfil_threshold}$ is a volume threshold indicating potential large data transfer to an untrusted destination:

$$IsSuspiciousFlow\,(flow) = (flow.dest \notin TrustedDestinations) \wedge \left(flow.protocol = P_{exfil}\right) \wedge \left(flow.volume > V_{exfil\_threshold}\right) \tag{6}$$

In addition to network traffic analysis, CSMS access logs are examined for unauthorized access attempts or privilege escalation. OCPP communication logs are reviewed for signs of data tampering or unauthorized command injections directed at charging stations. Database audit logs are crucial for identifying any unauthorized record modification or deletion. Comparing potentially exfiltrated data with original system records helps determine the scope of the breach and any data manipulation. Correlating various logs allows reconstruction of the attacker's actions, identifying compromised accounts or systems, and potentially tracing the attack origin. The final phase involves synthesizing the findings into a comprehensive report on the breach.

5 Results and Discussion

This section presents the key findings derived from the application and evaluation of the data-driven digital forensic method proposed in this research, which is designed for the complexities of the EV charging infrastructure. The application of this method, conceptually demonstrated through the case studies (Section 4), yielded insights into digital evidence identification, overall analysis capabilities, and, significantly, the critical limitations imposed by current data logging practices within EV charging systems. The following subsections will discuss these findings in detail, assess the effectiveness of the proposed forensic method, elaborate on identified implementation challenges and digital evidence gaps, and outline the limitations of this study along with directions for future work.

5.1 Findings and Effectiveness

The application of the proposed data-driven forensic method, as illustrated through the diverse case studies (Section 4), yielded significant insights into the utility of this structured approach and highlighted the current state of forensic readiness within the EV charging infrastructure. The systematic evaluation of scenarios based on both empirically demonstrated threats and representative virtual incidents confirmed

the method's capability to guide effective investigations, even while simultaneously identifying critical limitations inherent in existing EVCS implementations.

A key finding is that the structured approach, particularly the systematic digital evidence taxonomy developed in Section 3.4, is effective in directing investigators toward high-value evidence sources across all three architectural layers (physical, network, and application) of an EVCS. The method facilitates the identification and classification of diverse forensically relevant digital evidence, including, but not limited to, battery State of Charge data from EVs, operational status codes from charging stations, transaction records from management systems, and protocol-level communication data across various interfaces.

The case studies conceptually demonstrated the strengths of this method in:

- Guiding systematic evidence collection across organizational boundaries and diverse technical domains.
- Facilitating the correlation of digital evidence generated at various architectural layers through a structured and systematic analytical process.
- Supporting comprehensive timeline reconstruction even when evidence sources are distributed.
- Aiding investigators in differentiating between malicious activities and system malfunctions when sufficient digital evidence is available and analytical checks (such as those conceptualized in Eqs. (2)–(6)) can be effectively applied.

For instance, as notionally explored in the virtual fire incident investigation (Section 4.2.1), the method would guide the correlation of physical anomalies (e.g., abnormal charging rates potentially flagged by logic similar to Eq. (3)) with system logs (e.g., error codes) and communication records. Similarly, in the conceptual EV theft investigation (Section 4.2.3), the method's approach would facilitate cross-network evidence correlation (as illustrated by Eq. (5)) to establish movement patterns. These examples underscore the method's potential to improve the consistency and reliability of forensic investigations in this domain.

5.2 Implementation Challenges and Digital Evidence Gaps

Despite the potential strengths of the proposed forensic method, its practical application, as indicated by the analysis underlying the case studies (Section 4) and a review of current EV charging infrastructure characteristics, faces significant implementation challenges. These challenges primarily stem from critical gaps in the availability and consistency of digital evidence across existing EV charging systems. Such gaps can severely limit the depth, certainty, and efficiency of forensic investigations, regardless of the analytical method employed. Table 16 summarizes several critical digital evidence gaps that were identified as commonly present or likely in current EV charging systems. The table details these gaps across different architectural layers, outlines their potential adverse effects on forensic analyses, and indicates their typical implementation status.

Table 16: Critical digital evidence gaps and their effects on forensic investigations

Architectural layer	Digital evidence gap	Effects on investigations	Implementation status
Physical	HMI-controller communication logs	Unable to distinguish between system errors and malicious display manipulation	Rarely implemented

(Continued)

Table 16 (continued)

Architectural layer	Digital evidence gap	Effects on investigations	Implementation status
	Thermal management system status data	Cannot verify cooling system tampering or trace thermal anomalies	Inconsistently implemented
	Power module control signal history	Limited ability to detect unauthorized command injection	Vendor-specific implementation
Network	CAN bus traffic captures (CHAdeMO)	Reduced visibility into protocol manipulation in EV-EVCS communications	Rarely implemented
	Control pilot signal data	Cannot detect PWM signal manipulation or interference	Virtually nonexistent
	Session establishment metrics	Limited ability to diagnose communication disruptions	Partial implementation
Application	Detailed administrative action logs	Difficulty tracing unauthorized commands to specific accounts	Basic implementation is common
	Configuration change history	Cannot establish a baseline for detecting unauthorized modifications	Inconsistent implementation
Cross-layer	Temporal correlation mechanisms	Challenges in establishing a precise event sequence across components	Rarely implemented

These identified digital evidence gaps significantly impede the ability to conduct comprehensive forensic investigations. For example:

- At the physical layer, the common absence of detailed HMI-controller communication logs (as noted in Table 16) makes it exceedingly difficult to definitively distinguish between genuine system errors and malicious display manipulation in incidents like Scenarios 1–3 (Table 11), even when conceptual analytical checks (e.g., similar to Eq. (2)) are considered. Similarly, insufficient logging of thermal management component states (e.g., cooling pump status, fan activation patterns, precise sensor readings) hinders conclusive determination regarding potential tampering versus hardware failure in thermal incidents (relevant to Scenarios 5 and 6, Table 11).
- Within the network layer, the limited availability of detailed CAN bus traffic captures for protocols like CHAdeMO hampers the investigation of potential protocol manipulation during EV-EVCS communications (related to Scenario 8, Table 11). Furthermore, the near-universal absence of detailed logging for CCS control pilot signal parameters (PWM signals, duty-cycle patterns) impedes the analysis of attacks targeting that specific physical/electrical signaling interface (relevant to Scenarios 9 and 10, Table 11).
- In the application layer, while basic administrative logs might be present, they often lack the granularity necessary to effectively trace unauthorized commands or configuration modifications back to specific accounts or to establish a reliable baseline for detecting unauthorized system alterations.

These examples, drawn from the analysis of potential incident scenarios and the recognized state of current logging practices, underscore systemic challenges in digital evidence availability within many contemporary EVCS implementations. Addressing these gaps is crucial for enhancing forensic readiness and the overall effectiveness of any investigative method. The implications of these gaps for the proposed method and potential avenues for future work, including strategies for dealing with incomplete data, are further discussed in Section 5.4.

5.3 Method Effectiveness Assessment

The application of the proposed data-driven forensic method, as illustrated through the case studies (Section 4), indicates notable improvements in the investigative process, particularly when contrasted with conventional *ad hoc* or less structured mainstream forensic practices. The method demonstrably enhances the structure, explicitness, and systematic nature of investigations. This structured approach provides investigators with a repeatable and logically organized process, which can be particularly beneficial in complex EVCI environments where mainstream techniques might rely more heavily on individual investigator experience or a disparate set of tools without a unifying analytical workflow. Key aspects of its effectiveness, offering advantages over less systematic approaches, include:

- **Enhanced digital evidence management:** the method promotes more complete identification and classification of potential digital evidence within the bounds of available data. Its systematic nature helps investigators to methodically consider evidence sources across different architectural layers, increasing the likelihood of uncovering relevant traces that might be missed in less structured approaches.
- **Improved correlation and contextualization:** by guiding a systematic approach to system modeling, data collection, and threat analysis, the method inherently supports more robust correlation of disparate digital evidence. This allows for better contextualization of individual pieces of evidence and aids in reconstructing a more coherent narrative of events.
- **Systematic approach to complex environments:** even when faced with challenges such as data gaps or novel attack patterns, the method's methodical phases encourage a comprehensive survey of the system and potential threat vectors. This systematic process can help in forming more informed hypotheses, identifying what crucial evidence is missing and more clearly documenting the knowns and unknowns, leading to a more rigorous assessment of investigative certainty than purely intuitive methods.

Despite these enhancements to the investigative process itself, the ability to reach definitive forensic conclusions with high certainty is often influenced by factors external to the methodology. The pervasiveness of digital evidence gaps in current EVCS implementations remains a fundamental constraint on the ultimate conclusiveness of any investigation. Therefore, while the proposed method offers a robust and systematic approach to optimize the analysis of available information and improve the rigor of the investigation, its overall success in achieving definitive outcomes is significantly influenced by the availability, quality, and granularity of the digital evidence generated and preserved by the EVCS in question.

5.4 Limitations and Future Work

This study presents a structured method for digital forensic investigations in EVCI, yet several areas define its current boundaries and offer avenues for future research.

- **Validation scope and real-world data:** the method's validation relied on case studies using specific empirically-derived scenarios and illustrative virtual incidents. Broader validation with diverse real-world incident data across various proprietary EVCS platforms is a key priority for future work to assess practical effectiveness and generalizability more comprehensively. Furthermore, such future work should

include comparative studies or benchmarking of the proposed method against established mainstream forensic techniques using common datasets or controlled scenarios to provide practitioners with a clearer understanding of its relative performance, efficiency, and resource requirements.

- **OSINT in proprietary contexts:** the utility of OSINT can be reduced in highly proprietary EVCS environments with limited public technical data or encrypted communications. Future research could focus on advanced OSINT techniques or complementary data inference methods for such closed systems.
- **Addressing novel attack vectors:** the current method is primarily oriented towards known threat categories. Enhancing its capability to address entirely novel or zero-day attacks, potentially by integrating adaptive security mechanisms like ML-based anomaly detection, is an important area for future development.
- **Managing digital evidence gaps:** significant digital evidence gaps are common in current EVCSs. While this method aids in analyzing available evidence, future research should focus on robust algorithmic solutions for investigation with incomplete or sparse data, such as data imputation or probabilistic reasoning.
- **Operationalizing evidentiary value assessment:** the quantitative model for evidentiary value is conceptual, as its scoring functions require mathematical operationalization. Future work should develop and validate objective rubrics for these functions to enable practical, quantitative assessment.
- **Standardization and automation:** the development and adoption of standardized logging profiles for EVCSs are crucial for improving forensic readiness by addressing identified evidence gaps. Further research into automated techniques for large-scale digital evidence correlation and anomaly detection is also needed to enhance practical forensic capabilities.

6 Conclusion

The rapid global adoption of electric vehicles necessitates robust security measures and effective digital forensic capabilities to safeguard the expanding and increasingly complex EV charging infrastructure. Traditional forensic approaches often struggle within these heterogeneous cyber-physical systems, largely due to system diversity and inconsistent data logging practices. This paper addressed these challenges by proposing and evaluating a structured, data-driven method for the analysis of digital evidence specifically tailored to the EV charging domain.

The proposed method offers a systematic approach integrating system modeling, OSINT-informed data collection, threat analysis, and layered digital evidence identification. As illustrated through representative case studies, this approach enhances the structure and repeatability of the forensic process, aiding in the correlation of digital evidence and the reconstruction of incident timelines.

However, a critical challenge underscored by this research is the significant and pervasive gaps in the availability of crucial digital evidence within current EVCS implementations. These deficiencies—particularly concerning detailed internal system communications, low-level protocol interactions, and granular administrative logs—substantially hinder conclusive forensic analysis and can complicate the definitive differentiation of malicious attacks from system failures, even when a systematic method is applied.

This study provides a foundational method for advancing digital forensic capabilities within the EV charging infrastructure. While the proposed method offers a pathway toward more rigorous investigations, achieving comprehensive forensic readiness across the ecosystem requires concerted industry efforts and regulatory guidance to implement improved and standardized data logging practices. Addressing these identified digital evidence gaps is paramount for enabling the consistent and effective application of systematic analytical techniques, ensuring accountability, facilitating effective incident response, and ultimately bolstering the security and trustworthiness of this vital and rapidly growing critical infrastructure.

Acknowledgement: We would like to express our sincere gratitude to our colleagues at the System Security Research Center in Chonnam National University for their helpful discussions and support. Additionally, we would like to acknowledge the reviewers for their meticulous and constructive feedback, which helped improve the quality of our work.

Funding Statement: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (RS-2023-00242528, 50%) and supported by a grant from the Korea Electric Power Corporation (R24XO01-4, 50%) for basic research and development projects starting in 2024.

Author Contributions: The authors confirm contribution to the paper as follows: conceptualization, Dong-Hyuk Shin and Ieck-Chae Euom; methodology, Dong-Hyuk Shin; validation, Dong-Hyuk Shin, Jae-Jun Ha and Ieck-Chae Euom; investigation, Dong-Hyuk Shin; data curation, Dong-Hyuk Shin; resources, Jae-Jun Ha; writing—original draft, Dong-Hyuk Shin; writing—review & editing, Jae-Jun Ha and Ieck-Chae Euom; visualization, Dong-Hyuk Shin; supervision, Ieck-Chae Euom; project administration, Ieck-Chae Euom; funding acquisition, Ieck-Chae Euom. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the first and corresponding author upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Appendix A Dataset Field Analysis for Digital Evidence Identification

This appendix provides a detailed analysis of the datasets employed during the data collection process (Section 3.2), documenting field specifications and their corresponding forensic significance.

Appendix A.1 Multifaceted Analysis of EV Charging Dataset

This dataset originates from the 2023 research publication "Multi-faceted Analysis of Electric Vehicle Charging Transactions" [42]. It contains 72,856 charging session records from 2337 EV users and 2119 charging stations, collected via OCPP with 30-s data transmission intervals.

Table A1: Multifaceted analysis of electric vehicle charging dataset fields

Field	Data type	Description	Forensic value
User ID	Integer	User identifier (0 for nonmembers, 1–2337 for members)	User attribution and session ownership verification
Charger ID	String	Unique charging station identifier	Equipment identification and location correlation
Charger company	Binary	Charging station operator classification (0 = own company, 1 = other)	Operational responsibility attribution
Location	String	Charging station installation location	Geographical context establishment

(Continued)

Table A1 (continued)

Field	Data type	Description	Forensic value
Charger type	Binary	Charger classification (0 = standard, 1 = fast charger)	Equipment capability verification
Start day	Date	Session connection start date (YYYY-MM-DD)	Temporal context establishment
Start time	Time	Session connection start time (HH:MM:SS)	Session initiation timing
End day	Date	Session connection end date (YYYY-MM-DD)	Session termination dating
End time	Time	Session connection end time (HH:MM:SS)	Session termination timing
Start datetime	Date Time	Combined connection start timestamp	Session boundary verification
End datetime	Date Time	Combined connection end timestamp	Session boundary verification
Duration	Integer	Connection duration in minutes	Session length validation
Demand	Float	Energy delivered to vehicle (kWh)	Energy consumption verification

Appendix A.2 DESL-EPFL Level 3 Electric Vehicle Charging Dataset

This dataset was published by the Distributed Electrical Systems Laboratory (DESL) at École Polytechnique Fédérale de Lausanne (EPFL) in 2022 [43]. It contains charging session data from DC fast-charging stations in southwestern Switzerland, collected from April 2022 to July 2023.

Table A2: Distributed electrical systems laboratory at école polytechnique Fédérale de Lausanne dataset fields

Field	Data type	Description	Forensic value
Session	Integer	Unique charging session identifier	Session correlation and event sequencing
CCS	String	Connector identifier (CCS1/CCS2)	Physical connection documentation
Arrival	Date Time	Vehicle arrival time	Session initialization context
Departure	Date Time	Vehicle departure time	Session termination context
Stay	Integer	Vehicle presence duration (minutes)	Physical presence verification

(Continued)

Table A2 (continued)

Field	Data type	Description	Forensic value
Energy	Float	Energy delivered to vehicle (kWh)	Energy delivery verification
Pmax	Integer	Maximum charging power during session (W)	Power delivery capability verification
Preq_max	Integer	Maximum power requested by vehicle (W)	Vehicle power request verification
Controlled session	Binary	Session control status (0 = uncontrolled, 1 = controlled)	Charging management intervention
Total capacity	Float	Vehicle battery total energy capacity	Vehicle capability baseline
Bulk capacity	Float	Vehicle battery usable energy capacity	Operational capacity verification
SoC arrival	Float	Battery state-of-charge at arrival (%)	Initial charge state verification
SoC departure	Float	Battery state-of-charge at departure (%)	Final charge state verification
Energy capacity	Integer	Approximate vehicle energy capacity (Wh)	Vehicle capability estimation

Appendix A.3 Department of Energy Electric Vehicle Charging Dataset

This dataset was released by the US Department of Energy's Office of Scientific and Technical Information in 2024 [44]. It contains vehicle–charger interaction data collected by CALSTART from multiple vehicles and charging stations.

Table A3: Department of energy electric vehicle charging dataset fields

Field	Data type	Description	Forensic value
Vehicle ID	String	Unique vehicle identifier	Vehicle attribution and fleet correlation
Charger ID	String	Unique charging station identifier	Equipment identification
Local connect time	DateTime	Vehicle-charger connection timestamp	Connection initialization verification
Local disconnect time	DateTime	Vehicle-charger disconnection timestamp	Connection termination verification

(Continued)

Table A3 (continued)

Field	Data type	Description	Forensic value
Charge start time	DateTime	Actual charging process start timestamp	Charging operation initiation
Charge end time	DateTime	Actual charging process end timestamp	Charging operation termination
Average power	Float	Average power delivery during session (W)	Power delivery profile verification
Max power	Float	Maximum power delivery during session (W)	Peak power consumption documentation
Total energy delivered	Float	Total energy transferred to vehicle (kWh)	Energy consumption verification
Starting SoC	Float	Battery SoC at charging start (%)	Initial battery state verification
Ending SoC	Float	Battery SoC at charging end (%)	Final battery state verification
SoC charged	Float	Battery SoC increases during the session	Charging effectiveness verification

Note: SoC: state of charge.

Appendix A.4 Adaptive Charging Network Data Electric Vehicle Dataset

This dataset was published by the California Institute of Technology in 2019 [47], collected from the Adaptive Charging Network (ACN) at Caltech and NASA's Jet Propulsion Laboratory (JPL), providing charging data from 2018 onwards.

Table A4: Adaptive charging network dataset fields

Field	Data type	Description	Forensic value
_id	String	Unique record identifier	Record integrity verification
ClusterID	String	Charging network or station cluster identifier	Network segment identification
ConnectionTime	DateTime	Vehicle-charger connection timestamp	Connection initialization verification
DisconnectTime	DateTime	Vehicle-charger disconnection timestamp	Connection termination verification
DoneChargingTime	DateTime	Charging completion timestamp	Charging operation termination

(Continued)

Table A4 (continued)

Field	Data type	Description	Forensic value
kWhDelivered	Float	Energy delivered during session (kWh)	Energy consumption verification
SessionID	String	Unique charging session identifier	Session correlation and event sequencing
SiteID	String	Charging location identifier	Geographical context establishment
SpaceID	String	Specific parking space identifier	Physical location verification
StationID	String	Charging station identifier	Equipment identification
Timezone	String	Time zone for timestamp interpretation	Temporal context verification
UserID	String	User identifier	User attribution and session ownership
UserInputs	Object	User-provided information before charging	User intention documentation

Appendix A.5 Departement of Energy Workplace Charging Dataset

This dataset, published on the Harvard Dataverse in 2019 [45,46], was collected by Georgia Tech's Asensio Lab to analyze charging behavior and vehicle usage patterns in workplace environments. It comprises 3395 charging sessions from 85 EV drivers.

Table A5: Department of energy workplace charging dataset fields

Field	Data type	Description	Forensic value
SessionID	String	Unique charging session identifier	Session correlation and event sequencing
kwhTotal	Float	Energy delivered during session (kWh)	Energy consumption verification
Dollars	Float	Payment amount for session (USD)	Financial transaction verification
Created	DateTime	Session creation timestamp	Session initialization context
Ended	DateTime	Session termination timestamp	Session termination context
StartTime	Integer	Hour of session start (HH)	Temporal pattern analysis
EndTime	Integer	Hour of session end (HH)	Temporal pattern analysis

(Continued)

Table A5 (continued)

Field	Data type	Description	Forensic value
ChargeTimeHrs	Float	Session duration in hours	Session length verification
Weekday	String	Day of week for session	Weekly pattern analysis
Platform	String	Platform used for session management (android/iOS/web)	Interface usage pattern verification
Distance	Float	Distance between user home and charging location (miles)	User proximity verification
UserID	Integer	8-digit user identifier	User attribution
StationID	Integer	6-digit station identifier	Equipment identification
LocationID	Integer	6-digit location identifier	Geographical context establishment
MangerVehicle	Binary	Fleet vehicle status (1 = manager vehicle, 0 = other)	Usage categorization
FacilityType	Integer	Facility classification (1 = manufacturing, 2 = office, 3 = research and development, and 4 = other)	Environmental context establishment
ReportedZip	Binary	User ZIP code reporting status (1 = reported, 0 = not reported)	User information verification

References

1. Rehman AU, Zia MF, Khalid H, Said Z, Muyeen SM. Wind and grid energy-based onshore beach charging station for electric vehicles: an integration infrastructure with techno economics, sustainable mobility, and environmental protection. Results Eng. 2025;26(2):105113. doi:10.1016/j.rineng.2025.105113.
2. Khalid HM, Flitti F, Muyeen SM, Elmoursi MS, Sweidan TO, Yu X. Parameter estimation of vehicle batteries in V2G systems: an exogenous function-based approach. IEEE Trans Ind Electron. 2022;69(9):9535–46. doi:10.1109/TIE.2021.3112980.
3. Dehrouyeh F, Yang L, Badrkhani Ajaei F, Shami A. On TinyML and cybersecurity: electric vehicle charging infrastructure use case. IEEE Access. 2024;12:108703–30. doi:10.1109/ACCESS.2024.3437192.
4. Oberti F, Abrate F, Savino A, Parisi F, Carlo SD. Navigating the road to automotive cybersecurity compliance. In: Proceedings of the 2024 IEEE 30th International Symposium on On-Line Testing and Robust System Design (IOLTS); 2024 Jul 3–5; Rennes, France. Piscataway, NJ, USA: IEEE; 2024. p. 1–4. doi:10.1109/IOLTS60994.2024.10616052.
5. European Union. Directive (EU). 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014

and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). OJL. 2022;333:80–152. doi:10.4337/9781800372092.00013.
6. Hamdare S, Kaiwartya O, Aljaidi M, Jugran M, Cao Y, Kumar S, et al. Cybersecurity risk analysis of electric vehicles charging stations. Sensors. 2023;23(15):6716. doi:10.3390/s23156716.
7. McCarthy J, Grayson N, Brule J, Cottle T, Dinerman A, Dombrowski J, et al. Cybersecurity framework profile for electric vehicle extreme fast charging infrastructure. Gaithersburg, MD, USA: National Institute of Standards and Technology; 2023.
8. Mohamed N, Al-Jaroodi J, Jawhar I. Cyber-physical systems forensics: today and tomorrow. J Sens Actuator Netw. 2020;9(3):37. doi:10.3390/jsan9030037.
9. Lutta P, Sedky M, Hassan M, Jayawickrama U, Bakhtiari Bastaki B. The complexity of internet of things forensics: a state-of-the-art review. Forensic Sci Int Digit Investig. 2021;38(1):301210. doi:10.1016/j.fsidi.2021.301210.
10. Girdhar M, Hong J, You Y, Song TJ, Govindarasu M. Cyber-attack event analysis for EV charging stations. In: Proceedings of the 2023 IEEE Power & Energy Society General Meeting (PESGM); 2023 Jul 16–20; Orlando, FL, USA. Piscataway, NJ, USA: IEEE; 2023; p. 1–5. doi:10.1109/PESGM52003.2023.10252504.
11. Girdhar M, You Y, Song TJ, Ghosh S, Hong J. Post-accident cyberattack event analysis for connected and automated vehicles. IEEE Access. 2022;10:83176–94. doi:10.1109/ACCESS.2022.3196346.
12. Montasari R. A standardised data acquisition process model for digital forensic investigations. Int J Inf Comput Secur. 2017;9(3):229–49. doi:10.1504/IJICS.2017.085139.
13. Shin DH, Han SJ, Kim YB, Euom IC. Research on digital forensics analyzing heterogeneous internet of things incident investigations. Appl Sci. 2024;14(3):1128. doi:10.3390/app14031128.
14. Sarieddine K, Sayed MA, Assi C, Atallah R, Torabi S, Khoury J, et al. EV charging infrastructure discovery to contextualize its deployment security. IEEE Trans Netw Serv Manag. 2024;21(1):1287–301. doi:10.1109/TNSM.2023.3318406.
15. Hu X, Jiang X, Zhang J, Wang S, Zhou M, Zhang B, et al. Electric vehicle charging network security: a survey. J Syst Archit. 2025;159(12):103337. doi:10.1016/j.sysarc.2025.103337.
16. Ahmed MA, Guerrero L, Franco P. Network modeling and analysis of internet of electric vehicles architecture for monitoring charging station networks—a case study in Chile. Sustainability. 2024;16(14):5915. doi:10.3390/su16145915.
17. Januário F, Cardoso A, Gil P. A distributed multi-agent framework for resilience enhancement in cyber-physical systems. IEEE Access. 2019;7:31342–57. doi:10.1109/ACCESS.2019.2903629.
18. Johnson J, Berg T, Anderson B, Wright B. Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. Energies. 2022;15(11):3931. doi:10.3390/en15113931.
19. Ronanki D, Karneddi H. Electric vehicle charging infrastructure: review, cyber security considerations, potential impacts, countermeasures, and future trends. IEEE J Emerg Sel Top Power Electron. 2024;12(1):242–56. doi:10.1109/JESTPE.2023.3336997.
20. Szakály M, Köhler S, Martinovic I. Current affairs: a measurement study of deployment and security trends in EV charging infrastructure. arXiv:2404.06635. 2024.
21. Sarieddine K, Sayed MA, Torabi S, Atallah R, Assi C. Investigating the security of EV charging mobile applications as an attack surface. ACM Trans Cyber-Phys Syst. 2023;7(4):1–28. doi:10.1145/3609508.
22. Akshitha K, Subran S, Sankaran S, Sutraye P, Nishad AK. Threat modeling and attack simulation of charging infrastructures in electric vehicles. In: Proceedings of the International Conference on Computer Communication and Network Technology (ICCCNT); 2024 Jun 24–28; Kamand, India, Piscataway, NJ, USA: IEEE; 2024. p. 1–7. doi:10.1109/icccnt61001.2024.10725968.
23. Brighente A, Conti M, Donadel D, Poovendran R, Turrin F, Zhou J. Electric vehicles security and privacy: challenges, solutions, and future needs. arXiv:2301.04587. 2023.
24. Nasr T, Torabi S, Bou-Harb E, Fachkha C, Assi C. ChargePrint: a framework for internet-scale discovery and security analysis of EV charging management systems, Feb 27-Mar 3. In: Proceedings of the 2023 Network and Distributed System Security Symposium (NDSS); 2023 Feb 27–Mar 3; San Diego, CA, USA. p. 1–17. doi:10.14722/ndss.2023.23084.

25. Gupta K, Panigrahi BK, Joshi A, Paul K. Demonstration of denial of charging attack on electric vehicle charging infrastructure and its consequences. Int J Crit Infrastruct Prot. 2024;46(3):100693. doi:10.1016/j.ijcip.2024.100693.
26. Acharya S, Khan HAU, Karri R, Dvorkin Y. MaDEVIoT: cyberattacks on EV charging can disrupt power grid operation. In: Proceedings of the 2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT); 2024 Feb 19–22; Washington, DC, USA. p. 1–5.
27. Rohde KW, Carlson BR, Crepeau MJ, Salinas SC, Guidry JM, McCarthy DD, et al. EV SALaD 2023 demonstration: best practices and mitigations for protecting EVSE infrastructure. Idaho Falls, ID, USA: Idaho National Laboratory (INL); 2024.
28. Aljohani T, Almutairi A. A comprehensive survey of cyberattacks on EVs: research domains, attacks, defensive mechanisms, and verification methods. Def Technol. 2024;42(10):31–58. doi:10.1016/j.dt.2024.06.009.
29. Sarieddine K, Sayed MA, Torabi S, Atallah R, Assi C. Edge-based detection and localization of adversarial oscillatory load attacks orchestrated by compromised EV charging stations. Int J Electr Power Energy Syst. 2024;156(5):109735. doi:10.1016/j.ijepes.2023.109735.
30. Köhler S, Baker R, Strohmeier M, Martinovic I. Brokenwire: wireless disruption of CCS electric vehicle charging. In: Proceedings of the 2023 Network and Distributed System Security Symposium (NDSS)2023 Feb 27–Mar 3; San Diego, CA, USA, p. 1–14. doi:10.14722/ndss.2023.23251.
31. Johnson J, Anderson B, Wright B, Quiroz J, Berg T, Graves R, et al. Cybersecurity for electric vehicle charging infrastructure. Albuquerque, NM, USA: Sandia National Laboratories; 2022.
32. Costantino G, De Vincenzi M, Martinelli F, Matteucci I. Electric vehicle security and privacy: a comparative analysis of charging methods. In: Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring); 2023 Jun 20–23; Florence, Italy. Piscataway, NJ, USA: IEEE; 2023. p. 1–7. doi:10.1109/VTC2023-Spring57618.2023.10200030.
33. El-Rewini Z, Sadatsharan K, Selvaraj DF, Plathottam SJ, Ranganathan P. Cybersecurity challenges in vehicular communications. Veh Commun. 2020;23:100214. doi:10.1016/j.vehcom.2019.100214.
34. Elmo D, Fragkos G, Johnson J, Rohde K, Salinas S, Zhang J. Disrupting EV charging sessions and gaining remote code execution with DoS, MITM, and code injection exploits using OCPP 1.6. In: Proceedings of the 2023 Resilience Week (RWS); 2023 Nov 27–30; National Harbor, MD, USA. Piscataway, NJ, USA: IEEE; 2023. p. 1–8. doi:10.1109/RWS58133.2023.10284654.
35. Garofalaki Z, Kosmanos D, Moschoyiannis S, Kallergis D, Douligeris C. Electric vehicle charging: a survey on the security issues and challenges of the open charge point protocol (OCPP). IEEE Commun Surv Tutor. 2022;24(3):1504–33. doi:10.1109/COMST.2022.3184448.
36. Alcaraz C, Lopez J, Wolthusen S. OCPP protocol: security threats and challenges. IEEE Trans Smart Grid. 2017;8(5):2452–9. doi:10.1109/TSG.2017.2669647.
37. Smart car chargers. Plug-n-play for hackers? [Internet]. 2021 [cited 2025 Jun 1]. Available from: https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/.
38. Conti M, Donadel D, Poovendran R, Turrin F. EVExchange: a relay attack on electric vehicle charging system. In: Atluri V, Di Pietro R, Jensen CD, Meng W, editors. Computer security—ESORICS 2022. Cham, Switerland: Springer International Publishing; 2022. p. 488–508. doi:10.1007/978-3-031-17140-6_24.
39. Guo S, Chen H, Rahman M, Qian X. DCA: delayed charging attack on the electric shared mobility system. IEEE Trans Intell Transp Syst. 2023;24(11):12793–805. doi:10.1109/TITS.2023.3287792.
40. Aljohani T, Almutairi A. Modeling time-varying wide-scale distributed denial of service attacks on electric vehicle charging stations. Ain Shams Eng J. 2024;15(7):102860. doi:10.1016/j.asej.2024.102860.
41. Nasr T, Torabi S, Bou-Harb E, Fachkha C, Assi C. Power jacking your station: in-depth security analysis of electric vehicle charging station management systems. Comput Secur. 2022;112(6):102511. doi:10.1016/j.cose.2021.102511.
42. Antoniou C, Giannakopoulou K, Pelechrinis K, Zacharia A. A dataset for multi-faceted analysis of electric vehicle charging transactions. Sci Data. 2024;11(1):262. doi:10.1038/s41597-024-02942-9.
43. Distributed Electrical Systems Laboratory (DESL), École Polytechnique Fédérale De Lausanne (EPFL). DESL-EPFL/Level-3-EV-charging-dataset [Internet]. 2024 [cited 2025 Jun 2]. Available from: https://github.com/DESL-EPFL/Level-3-EV-charging-dataset.

44. LeCroy C, Dobbelaere C. DOE EV data collection—charging data [Internet]. 2025 [cited 2025 Jun 2]. Available from: https://doi.org/10.15483/1989855.
45. Asensio OI, Alvarez K, Dror A, Cammarata E, Perzanowski D. Electric vehicle charging stations in the workplace with high-resolution data from casual and habitual users. Sci Data [Internet]. 2021 [cited 2025 Jun 2]. Available from: https://www.nature.com/articles/s41597-021-00956-1.
46. Asensio OI, Alvarez K. asensio-lab/workplace-charging-experiment [Internet]. 2021 [cited 2025 Jun 2]. Available from: https://github.com/asensio-lab/workplace-charging-experiment.
47. Lee ZJ, Li T, Low SH. ACN-Data: analysis and applications of an open EV charging dataset. In: Proceedings of the Tenth ACM International Conference on Future Energy Systems; 2019 Jun 25-28; Phoenix, AZ, USA. New York, NY: ACM; 2019. p. 139–49. doi:10.1145/3307772.3328313.
48. ISO 15118-3:2015. Road vehicles–vehicle-to-grid communication interface—part 3: physical and data link layer requirements. Geneva, Switzerland: ISO; 2015.
49. ISO 15118-2:2014. Road vehicles–vehicle-to-grid Communication interface–part 2: network and application protocol requirements. Geneva, Switzerland: ISO; 2014.