UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Development of Threats and Vulnerability Assessment Model for Electric Vehicles (EVs) Transportation Internet of Things (T-IoT)

Nurina Zulaikha Ghazalee[1] & Raja Zahilah Raja Mohd Radzi[2]
Faculty of Computing, Universiti Teknologi Malaysia, 81310, UTM Johor Bahru, Johor, Malaysia
Email: nurinazulaikha@graduate.utm.my[1]; zahilah@utm.my[2]

Submitted: 27/3/2025. Revised edition: 15/8/2025. Accepted: 25/8/2025. Published online: 30/11/2025
DOI: https://doi.org/10.11113/ijic.v15n2.547

***Abstract*—The paper describes the proposal of a model for threats and vulnerability assessment for Electric Vehicles (EVs) in the Transportation Internet of Things (T-IoT) model. EV systems are becoming more and more reliant on IoT devices and systems that encounter many security challenges. This reliance on many interconnected devices, sensors, and communication networks creates vulnerabilities where cyberattacks, such as hacking and data breaches, or manipulations can stem as entry points to EVs. In this study, the researcher addresses the problems outlined above by discovering orders of critical threats, evaluating the remaining approaches working to produce threat modeling and vulnerability assessments, and adapting those approaches to the requirements of EV systems. Ultimately the study details a model to provide systematic attack scenario analysis and models for vulnerability assessment to provide a solid framework of identification and risk reduction to EV security and reliability in the future of transportation networks. The model developed in this study demonstrates improved capability in predicting, identifying, and mitigating cyber threats targeting electric vehicle (EV) systems. The results provide empirical evidence of the model's capacity to strengthen protection mechanisms against evolving cyber risks, offering a tangible solution to current security challenges in EV infrastructure. This research contributes to ongoing efforts to improve cybersecurity in transportation technologies, presenting a functional approach that can be implemented in real-world scenarios. Finally, this will improve the measures of the future of security and safety for the integration of EVs into the T-IoT.**

***Keywords*—Electric Vehicles (EVs), Threat Modelling, Vulnerability Assessment, IoT Security, Transportation Internet of Things (T-IoT), Security Model**

I. INTRODUCTION

Electric Vehicles (EVs) are one of the most impressive innovations in the era of sustainable mobility, because of providing a greener alternative to standard fossil-based transportation vehicles. In comparison with the traditional vehicles, EVs feature extensive systems facilitated by the IoT applications, which leads to overall efficiency and a better experience of the users. The systems entail high-tech sensors, communication systems, battery management systems, and other technologies that enhance the working of the vehicle. Nevertheless, this heavy dependency on technology brings with it several cyber security issues. The network of many devices and sensors gives several points of entry that potential cybercriminals may use. As EVs continue to grow, it is important to familiarise oneself and resolve such weakness.

Cyber security assessments are usually based on a reactive stance as they are focused on detecting vulnerabilities after the actual act of breach, instead of focusing on preventive measures. These kinds of reactive evaluations are ineffective, considering there is constant development of cyber threats. Without active protective measures, electric vehicles (EVs) are at risk of emerging threats to trigger accidents, data loss, or interference with charging infrastructure and power systems.

Additionally, modern systems inherited security systems are adequate for regular vehicles, but often not up to the demands on hybrid vehicle and electric vehicle (EV) systems. These frameworks are too generic in nature such that they fail to recognize the special qualities of EV technology including battery management systems and their connection to charging infrastructure. The following protection gap makes it harder to identify possible vulnerabilities and leaves some weak points unmitigated exposing not only vehicles but also the supporting infrastructure to cyberattacks.

Consequently, the increased number of electric vehicles (EVs) resulted in increased dependency on Transport-oriented

Internet of Things (T-IoT) systems, requiring development of the security models that reflect the emerging environment. Such frameworks must set the precedence on progressive identification of threats and vulnerabilities before their exploitation. By creating targeted threat modelling and vulnerability assessment frameworks, the protection of EVs against cyberattacks can be enhanced. This initiative will not only ensure passenger safety but also help maintain public trust in this rapidly evolving transportation technology.

This research will majorly focus on developing systematic threat and vulnerability models against the electric vehicle (EV) transportation Internet-of-Things (IoT) ecosystem. These models list potential security threats, evaluate the possible impact of these threats, and suggest feasible solutions that will reduce the associated risks. By way of providing a consistent security framework, the study aims to provide stakeholders, consisting of policymakers, industry practitioners and cybersecurity practitioners, with the tools to understand and mitigate the unique security risks associated with interconnected EV systems. In addition to this, the current research project attempts to question and enhance foundational threat modelling as well as vulnerability assessment frameworks to appropriately align them with the unique complexities of the electric vehicle (EV) technology. The general aim is to come up with a proactive security-centered model that can complement the existing measures against cybersecurity threats besides serving as a guide in development of stronger standards and policies. To achieve this objective, the research would be expected to contribute towards achieving safe, reliable, and resilient integration of electric vehicles into a more connected transportation IoT

The scopes for this research are:

- Assess the current threat modelling and vulnerability assessment, in terms of their relevance and efficacy in terms of determining and mitigating security risk in relation to EV Transport IoT devices.
- Evaluate key aspects of threat modelling and vulnerability assessment relevant to EV Transport IoT security, including attack vectors, potential impact of successful attacks, and relevant mitigation strategies.
- Identify and evaluate potential attack scenarios associated with the unique properties of EVs.

II. BACKGROUND AND RELATED WORKS

The existing studies have indicated threat taxonomies to be a critical tool towards facilitating the processes of standardised security assessment and certification within the electric vehicle (EV) field. These frameworks facilitate compliance with regulatory requirements across diverse jurisdictions, thereby assisting manufacturers in meeting mandated security standards efficiently [1], [2]. Various tools and frameworks have been developed to streamline this process. However, the measures will be associated with significant costs in terms of financial resources and operation, especially to smaller manufacturers. These challenges are compounded by the lack of discourse regarding the aligning security models with the evolving regulatory pathways as well as the need to be collaborative across sectors in the objective of developing a unified security landscape [3].

A. Threat Modelling

The analysis of the EVs application of the security models of STRIDE, TARA, and PASTA illustrates a unitary yet discontinued collection of methodologies and implementations. Despite the fact that a few research studies acknowledge flexibility of such frameworks to EV-related case studies, a significant gap remains to be bridged regarding depth of practical application as well as level of automation. [4][5].

STRIDE has been widely used in EV security research, but many studies show poor application of this model. Several researchers have used STRIDE to find threats in charging stations, car entertainment systems, and driving controls [6][7]. The model groups threats into 6 distinct categories allowing to identify common issues a user should be aware of, including fake authentication, impaired charging infrastructure and threats causing the attack that disrupts the ability of the vehicle. Nevertheless, most literature replicates the checklist of the STRIDE without taking adequate account of the peculiarities of the architecture of EV [8][9]. Electric vehicles combine computer and physical systems, in complex ways that create new types of categories of threat that do not simply fit into the original STRIDE categories. To overcome this fact, some researchers attempt to correlate the STRIDE with car-specific threat lists, however, this usually assigns threats to the wrong categories [1]. The other shortcoming is that most of the identified threats have been focused on threats that are already known with very little regard given to how automotive systems change over time with software updates and new attack vectors that are evolving.

The TARA research of electric-vehicle (EV) security attempts to measure the risk using numerical analysis, but in the methodology, these flaws lie in its base, therefore, its findings are not trustworthy. The researchers also use risk charts, scoring and decision-making tools to set numerical values on threats [10], [11], [12]. This approach looks scientific because it produces numbers for threat severity and attack chances. However, these numbers often come from personal opinions rather than facts [13], [14]. The ratings of equal risks vary according to the professional experience and personal impressions of significance in the minds of different individuals and hence are not harmonised with certainty when the TARA is applied under different conditions by multiple stakeholders including car manufacturers, charging providers, and government agencies in relation to equal EV systems. In addition to that, TARA risk scores have tended to remain unchanged even as there has been a constant change in the nature of the threats associated with EV dialling and its changing technologies and attack strategies. As a result, a large percentage of TARA studies seem focused on identifying ways to meet the satisfaction of a governmental need rather than ways to improve the security in a substantive fashion [4].

The application of the PASTA methodology has been underrepresented in electric vehicle (EV) studies, and this oversight yields a noticeable gap in the lack of understanding of the models. Though STRIDE and TARA remain very prominent scholarly topics, PASTA is rarely discussed and rarely undergoes serious examination. Lack of thorough PASTA analysis involving all three models does not allow the researchers to assess all three of them simultaneously and conclude which is the most reliable in terms of offering the best solutions to certain EV security issues. PASTA uses a process-oriented framework that is supposed to provide solutions to some of the shortcomings of STRIDE and TARA by providing a better understanding of business needs and a real-world operating environment [15], [16]. The absence of systematic research on PASTA does not allow the field to design holistic security roadmaps that combine the advantages of each model and avoid the weaknesses of the others.

The existing research on the security of electric vehicles (EV) is too focused on automation and computer-intensive processes without paying much attention to the basic principles of security. There is a lot of research that suggest using automated TARA systems, computer generated assessment methods and machine learning methods to reveal attacks [4], [5]. [17]. These automated tools claim to work better, need less human work, and can handle complex EV systems. However, these mechanisms of automation often work only at the level of separate parts of EV systems and do not cover the whole security. The tools may give false confidence by producing detailed reports that look complete but miss essential security problems. The researchers seem to believe that advanced computer applications will solve the security problems thus delaying the demanding process of developing effective security theories and validating them critically. As a result, such technical solutions can bring complex tools based on unstable concepts instead of expanding a holistic picture of EV security problems.

B. Limitations of Current Threats Modelling

One of the most significant limitations is the heavy reliance on the STRIDE threat modelling framework, which dominates much of the existing research. At the same time, TARA and PASTA receive considerably less attention and comparative analysis [12], [18], [6], [10]. This high degree of attention on STRIDE creates methodological bias, potentially constraining the set of risk-assessment options and. underrepresentation of factors that might be better handled with TARA risk-based approach or PASTA attack-focused approach. In addition, many studies build on general automotive or cyber-physical security models applied to the context of electric vehicles without adapting or validating the frameworks in a proper manner to the unique security-related aspects of EVs [4], [14], [6], [10]. As a result, this makes the applicability of these findings to actual EV systems less valid, as EVs have specific characteristics that require specific security measures, including smart-grid connection, charging infrastructure systems and connected-car technologies.

Another limitation in the current research concerning EV security is the lack of real-world verifications and experiments of the STRIDE, TARA and PASTA models applied to the electric vehicles. Most studies remain theoretical or use small-scale case studies that do not adequately demonstrate how this security frameworks perform in operational electric vehicle systems [4], [12], [7], [13]. This limitation negates the possibility of these models being effective in circumstances where they are used in the real-world EV scenarios where complexity and process limitations will be involved. Furthermore, most studies are founded on limited or simulated data that might not represent the complexity of current EV systems, thus, restricting the applicability of the research results [4], [7], [12]. The literature also points to the insufficient funding on the process of automated creation of the tools and procedures of applying the STRIDE, TARA, and PASTA methodologies, affecting the scalability and consistency of the approaches to complex EV systems on which [4, 5, 3]. Moreover, the current study mainly focuses on the security of the charging infrastructure and conveys relatively limited interest toward in-vehicle systems, ecosystem, and pinnacle technologies, including artificial intelligence and blockchain incorporation [18], [2], [1], [8].

C. Research Gaps of Current Threats Modelling

A review of the existing studies reveals several research gaps that exist in the utilisation of threat modelling methodologies to EVs ecosystems hence highlighting the necessity of a more detailed security paradigm. The most significant gap is the fragmented application of STRIDE, TARA, and PASTA models, where each framework is typically studied in isolation rather than as complementary components of a holistic threat assessment approach [4], [13]. The field of threat categorisation as offered by STRIDE, the emphasis on risk-based analysis as provided by TARA, and the attack-centric approach provided by PASTA tackle different aspects relating to the EV security, but current research lacks the evidence on how the models can be combined to ensure complete threat coverage. This fragmentation is most especially keen in EV situations where the threat surface is highly complex and extends across in-vehicle systems, charging infrastructure, grid interconnection, and cloud services, all of which can possibly make use of the complementary capabilities of all the three frameworks. The limited use of PASTA compared to STRIDE and TARA further compounds this issue, as PASTA's attack simulation approach could provide valuable insights that complement the threat identification capabilities of STRIDE and the risk assessment focus of TARA [4], [13]. This gap suggests that current threat modelling approaches may be incomplete and that a more integrated framework combining elements from STRIDE, TARA, and PASTA could provide better coverage of the diverse threat landscape in EV environments. Additionally, the limited availability of comparative analyses that provide evaluations of comparative strengths and weaknesses of these three models in EV applications prevents understanding which method is the best to apply to specific kinds of threats or parts thereof, consequently, stalls the establishment of an optimised threat-assessment approach.

Another significant research gap is the fact that current frameworks of the threat modelling response have difficulty adjusting to the unique features and the new problems that can occur most notoriously in EV environments. Existing applications of the STRIDE, TARA, and PASTA frameworks are not completely aligned with the dynamic, cross-connected nature of the contemporary EV ecosystems where threats can spread over many different system boundaries and evolve quickly when integrating new technology [11], [13]. Through this limitation, it has become clear that there is a need to have more adaptive and holistic security models that still maintain the systematic nature that makes STRIDE, TARA and PASTA meaningful. Furthermore, there is insufficient research on how these traditional threat modelling frameworks can be enhanced or combined to address emerging EV-specific threats such as vehicle-to-grid attacks, autonomous driving system compromises, and coordinated attacks on charging infrastructure [1], [8], [15]. The lack of real-life verification of these models to a large extent curtails insights into its effectiveness when implemented in real life scenarios where EVs have high complexities both operationally and volume wise [4], [19]. This validation gap is significant, as it is a barrier to evidence-based guidance on how to make threat modelling approaches better for EV settings. The existing literature also suggests that these frameworks lack the adequate emphasis on considerations related to privacy integration since STRIDE, TARA, and PASTA historically target online security risks whereas connected EVs create as well as handle large amounts of personal and behavioural information, which requires privacy-specific threat identification [20], [21]. The above gaps collectively indicate that despite the usefulness of the existing EV threat modelling models there is obvious a need to develop more complete, and integrated security frameworks that are capable of building upon the strengths of these existing frameworks with the aim of overcoming their inherent weaknesses as well as the specific risks presented by the distinctive electric vehicle environments.

D. Vulnerability Assessment

Recent studies on assessing the vulnerability of EVs in Transportation Internet of Things (T-IoT) settings exhibit a notable set of limitations of the methodology in terms of reducing the effectiveness of recommended security systems. Existing studies focuses on individual components of the systems without paying attention to complex interdependency of modern electric vehicles [22]. Secure boot systems implemented through cryptographic frameworks, such as the one in use, are characterised by a high level of technical skill but do not take into consideration the widespread complexity of the wider software ecosystem underlying current electric vehicle platforms [23]. The result of such a compartmentalisation produces narrow security assessment where wide scope of integrated attack vectors remains untested.

Studies on communication protocol security have revealed gaps in the current evaluation strategies, especially on the strategies that do not consider the real-life situations of wireless-charging systems. [24], [25]. The use of threat-modelled frameworks demonstrates that the current threat paradigm is overly focussed in narrow and inflexible models of evaluation that cannot keep up with the ever-changing threat horizon affecting the charging infrastructure of electric-vehicles [12], [26]. Furthermore, the continued recurrence of security vulnerabilities amongst sequential protocol designations demonstrates structural flaws with the current assessment practices in current methodologies that are focused on the theoretical lists of catalogued vulnerabilities rather than practical threat prevention in operational environments [25].

The gap in vulnerability assessment approaches can be considered as a major drawback of modern research on hardware security as the current research approaches often focus on the components and overlook the overall system-wide interdependency of security issues common to the modern electric vehicle (EV) [27], [28]. The proposed cyber-physical security models does not provide the depth of analysis to look into the complexities that exist between hardware vulnerabilities and software exploitation paths that facilitate compromise of EV systems by the malicious actors [27]. Additionally, the machine learning techniques used to detect anomalies rely strongly on laboratory environments that fail to reflect the operation parameters of real-life implemented EV networks, thus, questioning the practical applicability of research findings [29], [30].

The comprehensive strategic analysis of the current state of cybersecurity standards and policy frameworks suggests the existent gap between the detected results of vulnerability studies and the establishment of implementable defence policies [31], [32]. The inflexible approach to the prescriptive use of standards like ISO/SAE 21434 and Automotive SPICE represents a rigid paradigm that fails to be in-line with the increasingly rapid development rate of the new technology trends experienced in the electric-vehicle market [31]. Moreover, the security testing of mobile applications draws upon the analysis methods that are outdated to fulfil the requirements of complex attack patterns targeting the user-interface elements permeating modern electric-vehicle ecosystems and generates flawed vulnerability measurements that extend to all areas of the vehicular technology infrastructure [33], [34].

E. Limitations of Current Vulnerability Assessment

There are various limitations in the existing literature when considering vulnerability assessment of the security models of Electric vehicles (EVs) that limit the development of complete threat assessment and vulnerability assessment models. One of the main limitations is the segmented methodology that is applied in conducting vulnerability assessment. The current research focuses on individual parts, such as Electronic Control Units (ECUs), particular communication protocols, or one-off attack vectors without implementing comprehensive methodologies that could be used to assess the vulnerability of the entire EV ecosystem [22], [27], [33]. This partial approach significantly reduces the effectiveness of the current vulnerability assessment models due to disregarding interdependencies and cascading impacts that a vulnerability created in a single component can have on the rest of the system architecture of security. Additionally, majority of risk vulnerability evaluation frameworks does not incorporate standardised risk prioritisation and threat correlation steps, an aspect that leaves the frameworks deprived of providing adequate integration between threat modelling and vulnerability identification processes [12], [29]. This overreliance on simulation-based evaluation instead of operational validation to validate existing models also limits the use of existing models to the field, where laboratory settings hardly match the complexity of the operations and emergent attack patterns of actual deployed EV infrastructure [28], [35]. Also, current strategies portray a less viable attention towards hardware-software interaction vulnerability and upcoming technologies like AI-powered attacks and blockchain-based security measures and, thus, reduce their potential to tackle the dynamic threat landscape within modern EV systems [27].

F. Research Gaps of Vulnerability Assessment

The current research gaps infer that there is an absolute necessity to conduct more extensive and combined vulnerability assessment security systems that have the potential of incorporating threat intelligence along with more organised vulnerability analysis within the electric vehicle (EV) settings. The most significant is that whereas there are specific frameworks to help assess the vulnerabilities pertaining to security issues at every level of the EV ecosystem, there are currently no comprehensive vulnerability assessment frameworks that can systematically identify vulnerabilities in multiple levels of EV ecosystem security through a multi-lateral assessment across various levels of EV ecosystem security, together with correlation to individual threats and threat-models [22], [36]. The current approaches in vulnerability assessments does not have any dynamic risk-scoring mechanism to evaluate the vulnerabilities as the threats are changing and to facilitate a real-time prioritisation of the vulnerability per the threat information sources and the operational setting, a significant need gap in adopting proactive security management of EVs [30], [37]. There is a considerable lack of established frameworks of vulnerability assessments specific to the requirements of the EV charging infrastructures, especially wireless charging systems and mobile application interfaces that have particular security issues that cannot be adequately structured in generic assessment models [24], [33]. Besides, the value of adding machine learning and artificial-intelligence tools to vulnerability assessment procedures has not been fully explored yet, though it can enhance automated vulnerability identification, impact evaluation, and vulnerability remediation prioritisation within sophisticated EV networks [38], [39]. Lack of comprehensive datasets and benchmarking measures of vulnerability assessment validation is another significant gap because it makes the researchers unable to meaningfully compare or validate their measurement techniques against benchmark measures that are well established, this act prohibits the establishment of robust and reliable vulnerability assessment security models on EV systems [30].

III. RESEARCH METHODOLGY

The research methodology to construct a model for evaluating threats and vulnerabilities in Transportation Internet of Things (T-IoT) systems associated with electric vehicles (EVs) is described within this section. This methodology provides a systematic method for addressing the complexity of securing the T-IoT system by focusing on three main areas: identifying challenges, constructing a model to get a better sense of security, and contextualizing it within real-life constraints. The research methodology consists of three levels or phases, wherein each phase is intended to inform an overall objective of improving safety and reliability of T-IoT systems for EVs. Fig. 1 depicts the research methodology model that portrays the research process to reach project aims.

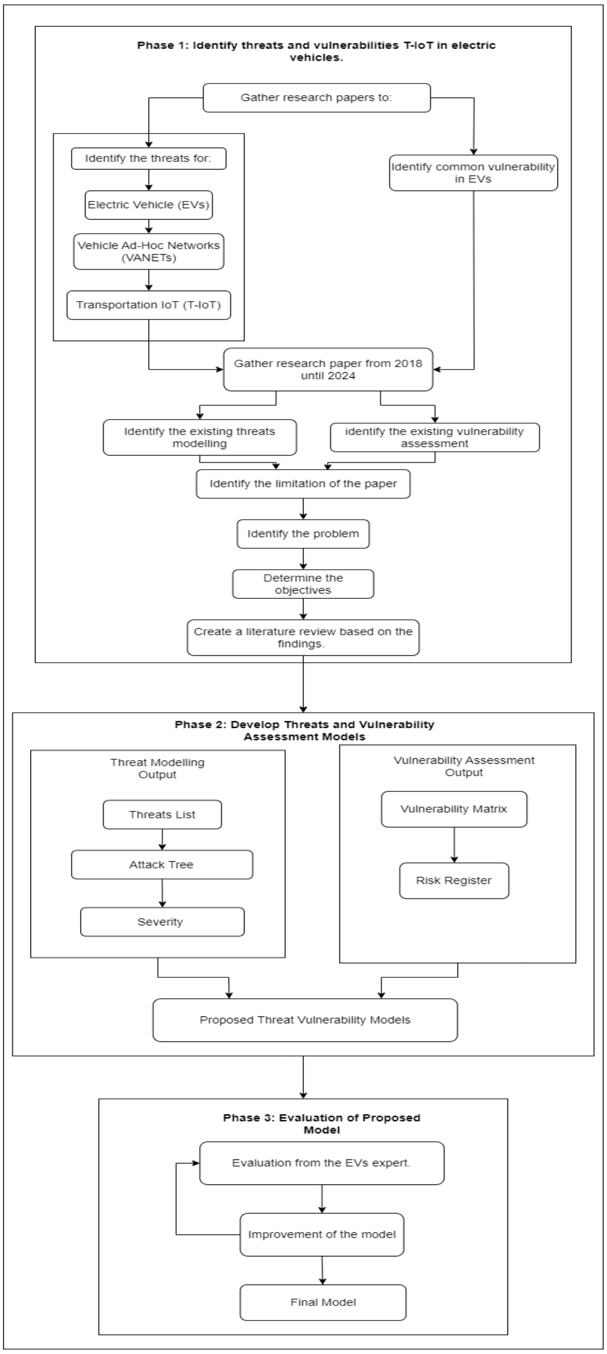

Phase 1: Identify threats and vulnerabilities T-IoT in electric vehicles.
Gather research papers to:
Identify the threats for:
Electric Vehicle (EVs)
Vehicle Ad-Hoc Networks (VANETs)
Transportation IoT (T-IoT)
Identify common vulnerability in EVs
Gather research paper from 2018 until 2024
Identify the existing threats modelling
identify the existing vulnerability assessment
Identify the limitation of the paper
Identify the problem
Determine the objectives
Create a literature review based on the findings.
Phase 2: Develop Threats and Vulnerability Assessment Models
Threat Modelling Output
Threats List
Attack Tree
Severity
Vulnerability Assessment Output
Vulnerability Matrix
Risk Register
Proposed Threat Vulnerability Models
Phase 3: Evaluation of Proposed Model
Evaluation from the EVs expert.
Improvement of the model
Final Model

Fig. 1. Research Methodology Framework

A. Phase 1

The first phase focuses on searching for existing tactics for threat modeling and vulnerability assessment specific to Transportation Internet of Things (T-IoT) systems. A comprehensive literature review of academic journal articles, technical reports, and security advisories published within a year, mainly 2018-2024, will be conducted. The objective of this first phase is to evaluate what tactics are currently being employed in the cyber security field, what their advantages or limitations are, and what certain exploitable vulnerabilities remain unaddressed. The aim of this phase is threefold: first, to find gaps in the current practices that may exploitively compromise the security of T-IoT systems; second, to gather evidence that may stem the ways in which risk analysis is performed in the future; and finally, to provide a solid platform for the research aims that follow to ensure these are logically justified to deal with the issues raised. This phase places the research within the context of existing knowledge and helps signify the importance of furthering the understanding of the security measures of T-IoT systems.

B. Phase 2

Phase 2 describes the creation of a conceptual framework that can be used to tackle security challenges related specifically to T-IoT systems in electric vehicles (EVs). This framework is enhanced from existing approaches such as STRIDE, TARA, and PASTA and is tailored to vulnerabilities in T-IoT systems. The framework results in two important outputs.

1. Threat Modelling Outputs, which include:
   a. A detailed list of threats identified through the literature review.
   b. Attack trees, which map out potential paths an attacker could use to exploit vulnerabilities.
   c. Assessments of the severity of each threat, helping to prioritise those with the greatest potential impact.
2. Vulnerability Assessment Outputs, which include:
   a. A vulnerability matrix that systematically maps weaknesses in various system components.
   b. A risk register documenting identified risks, their severity, and recommended measures to address them.

All outputs are aggregated into a comprehensive framework that outlines the most important threats and vulnerabilities with T-IoT systems for EVs.

C. Phase 3

In Phase 3, attention is devoted to validating the models in the real world to demonstrate that they work in a practical manner. This begins with a review by the cybersecurity industry experts who thoroughly evaluate models. This review is holistic and examines a variety of factors including importance and applicability of the models to assess the specific security problems addressed by T-IoT systems in electric vehicles. The experts will give valuable feedback about limitations and areas needing revision during the review process. The modifications will then be made to the models to evaluate experts' recommendations, and the models will be modified to address the issues presented. This will move towards developing models which are perceived as practical and reliable, and which are also considered developed under industry standards. This phase is very valuable for moving theory into application forms and will provide models that are ready to use in the real world and improve the security of T-IoT systems in EVs.

IV. RESEARCH DESIGN ANALYSIS AND IMLPLEMENTATION

The research starts with an in-depth discussion of related studies based on multiple sources. After that, there is an illustration of threat modelling and a risk assessment process. The anticipated threats are categorised, which include cyber-attacks, physical breaches, and vulnerability assessments of the technology and people, followed by the development and presentation of mitigation plans based on a risk register. From the detailed threat modelling, risk assessment, and evaluation of mitigation strategies, an audit checklist is generated, which considers technology and human factors associated with EV security.

A. Gathering Related Papers

The initial aspect of this study was to collect and examine appropriate, educational and technical articles that give a comprehensive understanding of the threats and vulnerabilities that exist in an Electric Vehicle (EV) and Transportation Internet of Things (T-IoT) environment. Various sources, such as Perplexity AI, Google Scholar, and the UTM library online catalog, were used to find existing research and studies that move toward threat modelling and vulnerability assessment. The research articles were evaluated with a focus on which methodologies, models, and case studies would inform or guide the project focus. The analysis collected was used to determine potential threats, for how to quantify the threats, and for planning mitigation strategies around the identified risks.

B. Threat Modelling Method

The threat modelling technique is a structured way of identifying and classifying threats to the EV and T-IoT ecosystem. This starts by creating a threat list that elaborates on the nature of potential risk, such as risks related to communications, such as unauthorised interception of information; risks described as access to systems, with insider threats as an option; and risks relating to data, such as tampering and data theft.

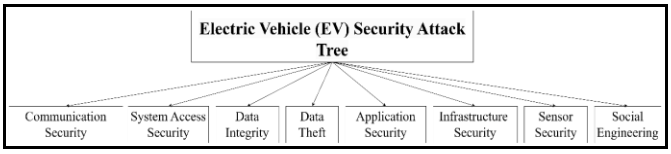


Fig. 2. Example of Attack Tree

Once the threats are established, the threats are then organised as attack trees. Attack trees are a way subset of threats to demonstrate the potential for threats to be authenticated against the original threat, starting with the generic threat and branching into specific scenarios (an example in Fig. 2). For example, communications security threats might include risks of eavesdropping or denial-of-service threats, while the application vulnerabilities may be focused on friends of the system, who are either third-party or obsolete systems/softwares.

TABLE I. EXAMPLE OF SEVERITY TABLE

Threat Category	Threats	Impact	Likelihood	Affected Persons
Communication Security	Eavesdropping on V2V and V2I communications.	High	Medium	Vehicle owners, pedestrians
	Denial of Service (DoS)	High	Medium	Vehicle owners, service providers
	Network Attacks	High	Medium	Vehicle owners, service providers
	Bluetooth Attacks	Medium	Medium	Vehicle owners
	Vehicle-to-Everything (V2X)	Medium	Medium	Vehicle owners, pedestrians
System Access Security	Unauthorised Access	High	Medium	Vehicle owners, service providers
	Physical Security	Medium	Low	Vehicle owners
	Insider Threats	High	Low	Service providers, employees
	Keyless Entry Threats	High	Medium	Vehicle owners
	Remote Access	High	Medium	Vehicle owners, service providers

The threats are then prioritised, using a severity table, for instance Table I, that describes the degree of the risk (probability) and scales it on impact and likelihood. Threats determined to be high should be immediate focus, such as risk of phishing, or risk of a breach/access to a vehicle control system. The severity table minimises exposure while prioritizing allocation for continued development and expandability of strategic risk mitigation strategies.

C. Vulnerability Assessment Method

The method of vulnerability assessment is formulated to assess vulnerabilities in the entire EV and T-IoT ecosystem. It consists of two main components.

a) The Vulnerability Matrix: Identifies weaknesses in specific system components against key security objectives regarding confidentiality, integrity, and availability. For example, the matrix will identify unauthorised access to one of the existing vehicle control systems, which can affect the integrity of data and will require strong authentication as a countermeasure.

b) The Risk Register: Developed based on the vulnerability matrix, the risk register tracks each risk with its corresponding likelihood, impact, and mitigations assigned to it. It also assigns responsibility for risks to different stakeholders, thus ensuring accountability. The risk register effectively transitions the organisation to the risk prioritisation stage and provides a structure of how to address vulnerabilities in a planned manner.

TABLE II. EXAMPLE OF VULNERABILITY MATRIX TABLE

System Component	Vulnerability	Security Parameter	Criticality
Communication Security	Eavesdropping on V2V and V2I communications .	Data Confidentiality	High
	Denial of Service (DoS)	Availability	High
	Network Attacks	Data Integrity, Availability	
	Bluetooth Attacks	Data Confidentiality	Medium
	Vehicle-to-Everything (V2X)	Data Integrity, Availability	High
System Access Security	Unauthorised Access	Authentication, Authorization	High
	Physical Security	Physical Security	Medium
	Insider Threats	Access Control	High
	Keyless Entry Threats	Access Control	High
	Remote Access	Access Control	High
	Unauthorised Access	Authentication, Authorization	High

D. Risk Management

Risk management focuses on combining the threat modelling and vulnerability assessment phases, to develop a full mitigation plan. Risk management introduces a structured approach to managing well-defined risks and involves leveraging limited resources to make proper decisions on protecting the EV and T-IoT ecosystem.

To start the process of risk management, we need to look at the threat list and the vulnerability matrix in Table II to create an appreciation for how risks can relate to one another. Then we will develop a mitigation plan to address any high-priority vulnerabilities such as creating an encrypted communication link, increasing the inseparability of authentication methods, or ensuring firmware updates are secure. Human factors related to risk management will be part of the plan as the stakeholders require training to recognise threats such as phishing and social engineering.

The risk management process also includes continual evaluation of the risk management plan on a periodic basis, to ensure the recommended methods, in fact, eliminate the risks from the identified threats. There will also be periodic updates to the mitigation strategies to accommodate the evolving threat landscape so that the security model is considered adaptable and future-proof.

V. RESULT

The result of this research is the development of a Security Audit Checklist, a comprehensive tool to ensure the security of the EV and T-IoT system.

A. Security Audit Checklist for EV

The checklist has been derived from what has been learned from the threat modelling and vulnerability assessment methods, integrating insights which came from the identification and analysis of risks. The security audit checklist is shown in Table III for EV.

TABLE III. SECURITY AUDIT CHECKLIST FOR EV

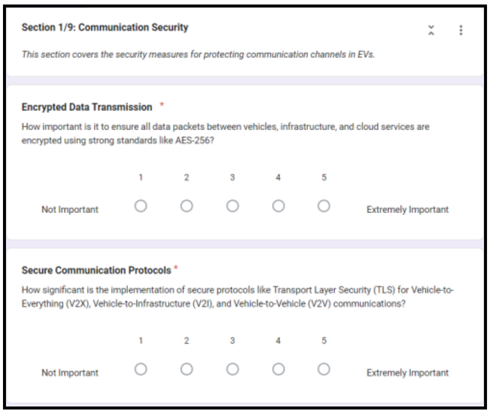
Category	Item	Description	Check
Communication Security	Encrypted Data Transmission	Ensure all data packets between vehicles, infrastructure, and cloud services are encrypted using strong encryption standards like AES-256.	□
	Secure Communication Protocols	Implement secure communication protocols such as TLS for V2V, V2I, and V2X communications.	□
	DoS Attack Mitigation	Implement rate limiting, network segmentation, and anomaly detection to prevent flooding and signal jamming.	□
	Network Attack Protection	Use IDS/IPS to detect and prevent packet sniffing, man-in-the-middle attacks, and spoofing.	□
	Bluetooth Security	Ensure secure pairing, use Bluetooth 5.0 or higher with encryption, and regularly update Bluetooth firmware.	□

The checklist incorporates key elements like encryption standards, secure access controls and software updates. Also included is an emphasis on human factors and training for users to mitigate risks related to social engineering attacks. The purpose of the checklist serves as a useful framework for an organisation in terms of implementing security measures and securing the resilience of their systems.

The Security Audit Checklist is flexible and adaptable to allow the checklist to change in response to the evolving threat landscape. Regular updates to the checklist allow it to be useful in dealing with newly identified risks, thereby helping the organisation to secure their EV and T-IoT systems.

B. Checklist Evaluation Method

The evaluation of the security audit checklist was carried out using a systematic scoring approach designed to prioritise and assess the relevance of various security measures for electric vehicles (EVs). A diverse group of participants, including professionals and experts in cybersecurity, provided feedback by rating the importance of each security item on a scale ranging from 1 to 5, with 1 being "Not Important" and 5 being "Extremely Important" as shown in Fig. 3. The checklist was carefully organised into categories, such as communication security, data integrity, and access control, enabling participants to assess specific areas of EV security comprehensively.



Section 1/9: Communication Security

This section covers the security measures for protecting communication channels in EVs.

Encrypted Data Transmission *

How important is it to ensure all data packets between vehicles, infrastructure, and cloud services are encrypted using strong standards like AES-256?

	1	2	3	4	5	
Not Important	○	○	○	○	○	Extremely Important

Secure Communication Protocols *

How significant is the implementation of secure protocols like Transport Layer Security (TLS) for Vehicle-to-Everything (V2X), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Vehicle (V2V) communications?

	1	2	3	4	5	
Not Important	○	○	○	○	○	Extremely Important

Fig. 3. Evaluation Method

During the evaluation process, respondents were encouraged to provide additional comments and suggestions on the checklist's structure and content. This feedback revealed that the checklist's clarity and categorisation were highly appreciated, making it easier to navigate and apply to real-world scenarios. However, several participants suggested incorporating emerging security challenges, such as those related to artificial intelligence in EV systems and advancements in hacking techniques, to address future vulnerabilities. This highlighted the dynamic nature of cybersecurity in EVs, emphasising the need for continuous updates to the checklist.

Overall, this structured evaluation method not only identified the most pressing security concerns but also shed light on areas where further improvements could be made. The results provided a strong foundation for refining the checklist, ensuring its applicability to evolving threats, and enhancing its effectiveness as a tool for securing EV systems

C. Security Audit Checklist for EV Result

Table IV and Table V present sample results from the questionnaire, focusing on DoS attack mitigation and network attack protection. These tables provide an overview of different job roles and their corresponding scores, offering insight into how individuals from various professions assess the importance of specific security categories. The results highlight variations in knowledge and skills, which may be influenced by experience, expertise, and exposure to security practices.

TABLE IV. RESULT OF DOS ATTACK MITIGATION

Full Name:	Job Title:	DoS Attack Mitigation
Nurhidayah	Developer	3
Lee Yi Hsing	IoT Developer	5
Nur Iqtiffah Binti Maksan @Marx's	Programmer	5
Fatin Aqilaa	IT Executive	4
Nur Athilah binti Othman	it executive	5
Jeffrey Sonsteng-Person	Sr. Security Analyst	4
Mohamamd Al Takrouri	PhD student	5

Table IV summarises the results related to DoS attack mitigation, showing varying levels of effectiveness across different job roles. The scores range from 3 to 5, indicating differences in how individuals perceive the importance of mitigating DoS attacks. The lowest score of 3 is recorded by a Developer, which may be due to a focus on software development rather than security practices. In contrast, the highest score of 5 is achieved by multiple participants, including those in IoT development, programming, IT executive roles, and PhD research. These roles often involve a stronger emphasis on security knowledge, system protection, and risk assessment, which could explain the higher ratings. IT Executives and Security Analysts given a score of 4, which may reflect experience in general IT management and security but with less direct engagement in technical mitigation strategies.

Table V presents the results for network attack protection, with scores ranging from 2 to 5. A Senior Security Analyst gave the lowest score of 2. This could indicate a more focus on broader security strategies rather than hands-on network protection. Developers and IT Executives have given scores of 3 and 4, respectively, suggesting that both groups see network security as pretty important for EV T-IoT systems, but maybe not the most critical thing compared to other security categories. The highest score of 5 is given by IoT Developers, Programmers, and PhD Students, roles that often require deeper knowledge of network security, encryption, and system vulnerabilities. IoT Developers, in particular, deal with connected devices, which are frequent targets of network attacks, necessitating a strong understanding of protection mechanisms. The variation in scores demonstrates how professional roles influence perceptions of network security's importance within EV T-IoT systems. Technical and research-oriented positions, such as IoT developers and PhD candidates, consistently assigned higher ratings, likely reflecting their direct engagement with security and system vulnerabilities. Conversely, roles with less operational involvement in security measures tended to provide more moderate assessments. This disparity suggests that hands-on experience with network protection requirements correlates strongly with recognising their criticality in electric vehicle ecosystems.

TABLE V. RESULT OF NETWORK ATTACK PROTECTION

Full Name:	Job Title:	Network Attack Protection
Nurhidayah	Developer	3
Lee Yi Hsing	IoT Developer	5
Nur Iqtiffah Binti Maksan @Marx's	Programmer	4
Fatin Aqilaa	IT Executive	4
Nur Athilah binti Othman	it executive	5
Jeffrey Sonsteng-Person	Sr. Security Analyst	2
Mohamamd Al Takrouri	PhD student	5

The findings from the security audit checklist evaluation provide an overall assessment of key security measures in EV systems. Individual results, such as those in Table IV and Table V are then combined to form a broader evaluation. This transformation helps in identifying critical areas that professionals consider important for securing EV systems. Table VI presents an overall result of the security audit checklist. The findings from the security audit checklist evaluation provided valuable insights into critical areas of EV security, highlighting key measures that professionals considered essential for safeguarding EV systems.

TABLE VI. SECURITY AUDIT CHECKLIST RESULT

Category	Item	Description	Check
Communication Security	Encrypted Data Transmission	Ensures data is transmitted securely to prevent interception or eavesdropping.	High (4-5 ratings across roles)
	Secure Communication Protocols	Uses protocols like TLS to safeguard communication.	Very High (Consistently rated 5)
	DoS Attack Mitigation	Prevents service disruption caused by denial-of-service attacks.	Moderate to High (3-5 ratings)
	Network Attack Protection	Shields networks from breaches and intrusions.	Moderate (2-5 ratings)
	Bluetooth Security	Protects Bluetooth connections from vulnerabilities.	High (4-5 ratings)

Communication security emerged as a primary concern, with encrypted data transmission and secure protocols such as TLS rated as highly important. Participants also emphasised the need for robust Bluetooth security and defences against Denial-of-Service (DoS) attacks, reflecting the increasing reliance on wireless technologies in EV systems. These measures were identified as essential for protecting real-time communications from unauthorised access and interference.

System access and data integrity were also prioritised by respondents. Measures such as multi-factor authentication, physical security protocols, and remote access safeguards were consistently highlighted as critical to preventing unauthorised access. Additionally, secure firmware updates, malware protection, and cryptographic measures were identified as vital for maintaining the integrity of EV data. While most respondents strongly supported supply chain security to address vulnerabilities during manufacturing and distribution, opinions varied based on the specific professional roles of the participants.

Finally, incident response and human factors received significant attention in the checklist results. The importance of having robust incident response plans, threat detection mechanisms, and post-incident analysis was unanimously recognised as essential for mitigating potential security breaches. Human-related vulnerabilities, such as susceptibility to phishing and social engineering attacks, were also acknowledged. Regular user training, access reviews, and awareness initiatives were deemed necessary to reduce risks arising from human error.

In conclusion, the findings from the security audit checklist placed considerable emphasis on safeguarding communication systems, strengthening access controls, and ensuring the integrity of data. Additionally, the checklist addressed critical human-related vulnerabilities and stressed the importance of enhancing incident response strategies. This evaluation highlighted the checklist's effectiveness as a structured tool for improving the cybersecurity measures within EV systems, while also identifying areas that require further enhancement to keep pace with evolving threats.

VI. CONCLUSION AND FUTURE WORKS

In summary, this study has tackled an important gap in security research for Electric Vehicle (EV) systems under the model of the Transportation Internet of Things (T-IoT). The study aimed to design a model to identify threats and evaluate vulnerabilities specific to EV systems to address their increasing risks resulting from their reliance on IoT technology. The study identified security gaps in existing EV systems by reviewing the literature and examining practice issues related to security threats. Specifically, critical gaps were identified globally in areas such as communication security, the integrity of data, and access control to the system. This was the rationale upon which a structured model was developed to assess and remediate these vulnerabilities.

The model proposed a process that systematically identified security threats and vulnerabilities to EV systems. It was evaluated through industry feedback and experimental trialing and was shown to have real-world application address security threats. Central security issues also emerged including the importance of securing communications, using multi-factor authentication, securing and verifying firmware integrity, and addressing human vulnerabilities through training and awareness activities. Overall, these findings demonstrated an understanding and opportunity for the improvement of the cybersecurity posture of EV systems, and their reliability and safeness in increasingly complex operational environments.

Future research should emphasis applying the proposed model to real-world EV systems to evaluate its better effectiveness in functional and operational environments. Testing in operational environments will better highlight the potential threat challenges and support the model in addressing security threats in real-time. Future research studies may also have a wider scope to investigate the new risks including vulnerabilities because of artificial intelligence systems and cyberattack vulnerabilities. Continued engagement with industry practitioners and researchers, cybersecurity professionals, and policy groups will also be critical in modifying the model to reflect the new technologies and standards. This will ensure the model remains relevant and fosters secure systems, as well as be resilient in the evolving nature of the transportation sector.

ACKNOWLEDGMENT

The author wishes to express heartfelt thanks to all who provided support in the completion of this thesis. The author's deepest and most profound appreciation is to the author's parents, whose endless support, prayers, and encouragement have been a tremendous source of strength throughout the whole process. Such appreciation is also extended to the author's supervisor, who provided invaluable guidance, constructive feedback, and a person of great patience, who was critical in shaping this work. The author's interest is also to express gratitude to their friends and colleagues for the support and motivation that all provided during this process and for thoughtful suggestions, which shaped this project and assisted in making it a meaningful and memorable experience. This body of work is dedicated to those who appreciate the pursuit

of knowledge and hope it advances the field and serves to inspire the thinking of others throughout their academic endeavors.

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Sommer, F., Gierl, M., Kriesten, R., Kargl, F., & Sax, E. (2024). Combining cyber security intelligence to refine automotive cyber threats. *ACM Transactions on Privacy and Security*. https://doi.org/10.1145/3644075.

[2] Costantino, G., Vincenzi, M. D., Martinelli, F., & Matteucci, I. (2023). Electric vehicle security and privacy: A comparative analysis of charging methods. *Proceedings of IEEE VTC 2023-Spring*. https://doi.org/10.1109/vtc2023-spring57618.2023.10200030.

[3] Anand, S. S., Vijayaraghavan, S., & Abhi, S. (2023). Enhancing the connected vehicle security using the SecureAuto tool. *CIISCA 2023 Proceedings*. https://doi.org/10.1109/ciisca59740.2023.00061.

[4] Din, Q. M. U., & Ahmed, Q. (2024). Automated TARA framework for cybersecurity compliance of heavy duty vehicles. *SAE Technical Paper Series*. https://doi.org/10.4271/2024-01-2809.

[5] Marksteiner, S., Schmittner, C., Christl, K., Nickovic, D., Sjödin, M., & Sirjani, M. (2023). From TARA to test: Automated automotive cybersecurity test generation out of threat modeling. *ACM Proceedings*. https://doi.org/10.1145/3631204.3631864.

[6] Abuabed, Z., Alsadeh, A., & Taweel, A. (2023). STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles. *Computers & Security, 133*, 103391. https://doi.org/10.1016/j.cose.2023.103391.

[7] Stichow, A., & Rempel, P. (2024). Securing electric vehicle charging stations: A critical analysis of authentication vulnerabilities. *IEEE REW 2024 Proceedings*. https://doi.org/10.1109/rew61692.2024.00037.

[8] Yousseef, A., Satam, S., Latibari, B. S., Pacheco, J., Salehi, S., Hariri, S., & Satam, P. (2024). Autonomous vehicle security: A deep dive into threat modeling. *arXiv Preprint*. https://doi.org/10.48550/arxiv.2412.15348.

[9] Vailoces, G., Keith, A., Almehmadi, A., & El-Khatib, K. (2023). Securing the electric vehicle charging infrastructure: An in-depth analysis of vulnerabilities and countermeasures. *ACM Proceedings*. https://doi.org/10.1145/3616392.3623424.

[10] Das, P., Asif, M. R. A., Jahan, S., Ahmed, K., Bui, F. M., & Khondoker, R. (2024). STRIDE-based cybersecurity threat modeling, risk assessment and treatment of an in-vehicle infotainment system. *Vehicles, 6*(3), 1140–1163. https://doi.org/10.3390/vehicles6030054.

[11] Wang, Y., Yinghui, W., Qin, H., Ji, H., Zhang, Y., & Jian, W. (2021). A systematic risk assessment framework of automotive cybersecurity. *Journal of Intelligent & Connected Vehicles*. https://doi.org/10.1007/s42154-021-00140-6.

[12] Bhattacharya, S., Govindarasu, M., Girdhar, M., & Hong, J. (2023). A quantitative methodology for attack-defense analysis of EV charging infrastructure. *IEEE PESGM 2023 Proceedings*. https://doi.org/10.1109/pesgm52003.2023.10252252.

[13] Ebrahimi, M., Striessnig, C., Triginer, J. M. C., & Schmittner, C. (2022). Identification and verification of attack-tree threat models in connected vehicles. *SAE Technical Paper Series*. https://doi.org/10.4271/2022-01-7087.

[14] Monica, U. D., Munjal, K., Tamas, M. P., Boi, B., Esposito, C., & Khondoker, R. (n.d.). Threat analysis and risk assessment (TARA) of an autonomous emergency braking (AEB) system. *Applied Sciences, 15*(3). https://doi.org/10.3390/app15031400.

[15] Yang, P. (2024). Electric vehicle based smart cloud model cyber security analysis using fuzzy machine learning with blockchain technique. *Computers & Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2024.109111.

[16] Kumari, T., Rakib, A., Zaslavsky, A., Jadidbonab, H., & Moghaddam, V. (2024). A context-aware framework for analysing automotive vehicle security. *ICSC 2024 Proceedings*. https://doi.org/10.1109/icsc59802.2024.00019

[17] Singh, N., & Agarwal, R. (2023). Intrusion detection system for smart vehicles using machine learning algorithms. *ICCSAI 2023 Proceedings*. https://doi.org/10.1109/iccsai59793.2023.10421298.

[18] Ganesan, S., Patel, D. K., & Chokalingam, R. (2024). Security of electric vehicle charging stations. *International Journal of Electrical and Computer Engineering Research, 4*(4), 1–7. https://doi.org/10.53375/ijecer.2024.426.

[19] Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., Brown, D. J., & Lloret, J. (2023). Cybersecurity risk analysis of electric vehicles charging stations. *Sensors, 23*(15), 6716. https://doi.org/10.3390/s23156716.

[20] Stingelová, B., Thrakl, C. T., Wrońska, L., Jedrej-Szymankiewicz, S., Khan, S., & Svetinovic, D. (2023). User-centric security and privacy threats in connected vehicles: A threat modeling analysis using STRIDE and LINDDUN. *IEEE Proceedings*. https://doi.org/10.1109/dasc/picom/cbdcom/cy59711.2023.10361381.

[21] Agustina, E. R., Hakim, A. R., & Ramli, K. (2024). Modeling data security and privacy threats for VANET using STRIDE and LINDDUN. *ICOSEIT 2024 Proceedings*. https://doi.org/10.1109/icoseit60086.2024.10497513.

[22] Luo, F., Wang, J., Li, Z., & Zhang, X. (2024). Vulnerability analysis of DoIP implementation based on model learning. *SAE Technical Paper Series*. https://doi.org/10.4271/2024-01-2807.

[23] Adly, S., Hamed, A. M., Hammad, S., & Maged, S. A. (2023). Prevention of controller area network (CAN) attacks on electric autonomous vehicles. *Applied Sciences, 13*(16), 9374. https://doi.org/10.3390/app13169374.

[24] Köhler, S., Birnbach, S., Baker, R., & Martinovic, I. (2022). On the security of the wireless electric vehicle charging communication. *SmartGridComm 2022 Proceedings*. https://doi.org/10.1109/SmartGridComm52983.2022.9961000.

[25] Alcaraz, C., Cumplido, J., & Triviño, A. (2023). OCPP in the spotlight: Threats and countermeasures for electric vehicle charging infrastructures 4.0. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00698-8.

[26] Girdhar, M., Hong, J., You, Y., & Song, T. (2022). Machine learning-enabled cyber attack prediction and mitigation for EV charging stations. *IEEE PESGM 2022 Proceedings*, 1–5. https://doi.org/10.1109/PESGM48719.2022.9916914

[27] Ye, J., Guo, L., Yang, B., Li, F., Du, L., Guan, L., & Song, W. (2021). Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions. *IEEE Journal of Emerging and Selected Topics in*

Power Electronics, 9(4), 4639–4657. https://doi.org/10.1109/JESTPE.2020.3045667.

[28] Chandwani, A., Dey, S., & Mallik, A. (2020). Cybersecurity of onboard charging systems for electric vehicles—Review, challenges and countermeasures. *IEEE Access, 8*, 226982–226998. https://doi.org/10.1109/ACCESS.2020.3045367.

[29] Yoon, S., Kim, D., Kim, K., & Euom, I. (2023). Vulnerability exploitation risk assessment based on offensive security approach. *Applied Sciences*. https://doi.org/10.3390/app132212180.

[30] Hegde, S. R., Vijayabhaskaramoorthy, V., Chandrakala, K. V., Kumar, T. G., & Shankar, V. A. (2024). Enhancing anomaly detection in electric vehicle supply equipment (EVSE) networks using classical and ensemble learning approaches. *CISCON 2024 Proceedings*. https://doi.org/10.1109/ciscon62171.2024.10696830.

[31] Acharya, S., Khan, H. A. U., Karri, R., & Dvorkin, Y. (2023). MADEVIOT: Cyberattacks on EV charging can disrupt power grid operation. *arXiv Preprint*. https://doi.org/10.48550/arxiv.2311.06226.

[32] Carlson, B., Rohde, K. W., Crepeau, M., Medam, A., & Cook, S. (2023). Consequence-driven cybersecurity for high-power electric vehicle charging infrastructure. *SAE Technical Paper Series*. https://doi.org/10.4271/2023-01-0047.

[33] Sarieddine, K., Sayed, M. A., Torabi, S., Atallah, R., & Assi, C. (2023). Investigating the security of EV charging mobile applications as an attack surface. *ACM Transactions on Cyber-Physical Systems, 7*(4), 1–28. https://doi.org/10.1145/3609508.

[34] Muhammad, Z., & Saleem, B. (2023). A cybersecurity risk assessment of electric vehicle mobile applications: Findings and recommendations. *ICAI 2023 Proceedings*. https://doi.org/10.1109/ICAI58407.2023.10136682.

[35] Mokarim, A., Gaggero, G. B., & Marchese, M. (2023). Evaluation of the impact of cyber-attacks against electric vehicle charging stations in a low voltage distribution grid. *SmartGridComm 2023 Proceedings*. https://doi.org/10.1109/smartgridcomm57358.2023.10333896.

[36] Zhou, Y., Xu, H., Liu, W., & Li, Y. (2024). Malicious mode attack on electric vehicle coordinated charging and its defense strategy. *Sustainable Energy, Grids and Networks, 39*, 101440. https://doi.org/10.1016/j.segan.2024.101440.

[37] Buedi, E. D., Ghorbani, A. A., Dadkhah, S., & Ferreira, R. (2024). Enhancing EV charging station security using a multi-dimensional dataset: CICEVSE2024. *ResearchSquare Preprint*. https://doi.org/10.21203/rs.3.rs4046330/v1

[38] Abdullah, M., Liu, S., & Zhang, X. (2024). Towards secure e-mobility: Cybersecurity of in-wheel motor electric vehicles against adversarial attacks via detection and mitigation. *INDIN 2024 Proceedings*. https://doi.org/10.1109/indin58382.2024.10774390.

[39] Albanese, E., & Terruggia, R. (2023). Secure and resilient IoT and cloud-based infrastructure for electric vehicles recharge systems. *IET Conference Proceedings*. https://doi.org/10.1049/icp.2023.1176.