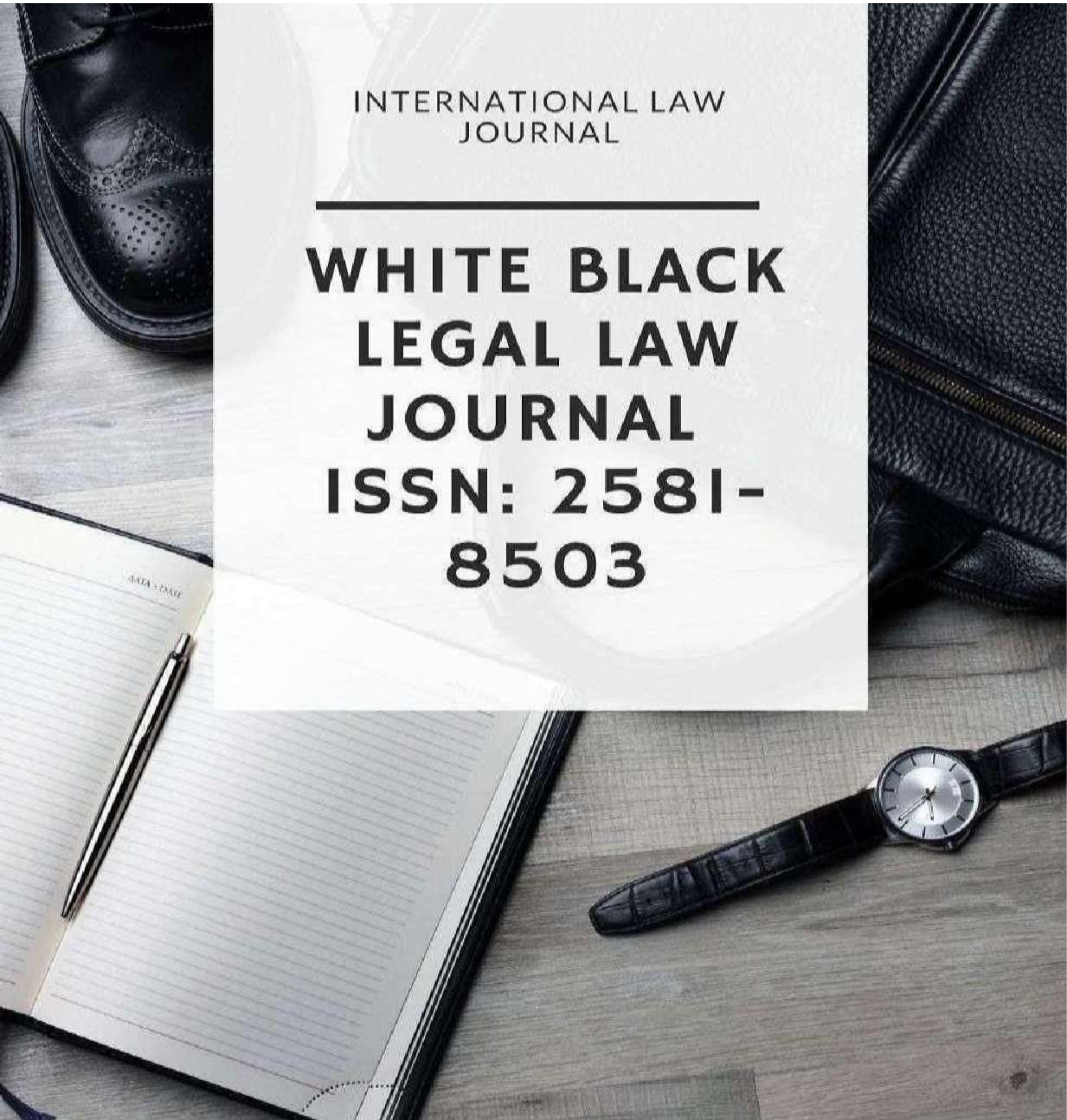

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

CYBER INTELLIGENT MARKETS & CYBERSECURITY CONCERNS VIS A VIS EVOLUTION OF ELECTRONIC VEHICLE TECHNOLOGY

AUTHORED BY - GANDHAM LAVANYA
& SIRIKONDA VISHAL VARMA

Abstract

The EV sector is now seeing a multitude of advancements due to the global energy crisis, rising demand, and the prioritization of electric cars at the national level. Electric vehiclesare equipped with a variety of sensors that serve the purpose of maintaining an environmentally sustainable setting, so contributing to the overall improvement of society and the promotion of human sustainability. Nevertheless, similar to other emerging digital technologies, these innovations are vulnerable to potential risks of security and privacy. Recent occurrences have provided evidence of the abuse of these sensors in many domains, including automobile and energy theft, financial fraud, data breach, and the occurrence of significant health and safety issues, among other detrimental consequences. This study presents a comprehensive examination of the sustainability of electric vehicles, with a particular focus on the role of digital technologies in enhancing their sustainability. Additionally, it explores the possible cybersecurity risks associated with these technologies and proposes related protection mechanisms. Three comprehensive taxonomies have been introduced to delineate the potential hazards that may impact the domains of long-term sustainability. These taxonomies include three key areas: (1) life and well-being, (2) safe environment, and (3) innovation and development. Furthermore, this study aims to assess the influence of cybersecurity risks on electric vehicles and their alignment with sustainability objectives. Thirdly, the document provides a comprehensive analysis of the effectiveness of certain security measures in addressing these risks. This analysis facilitates a seamless progression towards the establishment of safe and sustainable smart cities in the future.

The proliferation of Electric automobiles is precipitating a transition away from conventional gasoline-fueled automobiles. As a consequence, there has been an increase in the demand for Electric

Vehicle Charging Systems, resulting in substantial expansion of EVCS as both public and private charging infrastructure. The proliferation of electric vehicle charging stationshas led to a notable escalation in cybersecurity vulnerabilities associated with these systems. Within the existing environment, this study provides an analysis of cybersecurity risks pertaining to the network of Electric Vehicle Charging Stations. To provide a contextual framework for the study field, this section outlines the recent developments in the Electric Vehicle Charging Station network, as well as the prevailing trends in Electric Vehicleadaption and various charging use cases. Additionally, the cybersecurity elements of Electric Vehicle Charging Stations have been examined, taking into account vulnerabilities related to infrastructure and protocols, along with potential scenarios of cyberattacks. Furthermore, the validation of vulnerabilities in Electric Vehicle Charging Stations has been conducted by the use of real-time data-centric analysis of EV charging sessions. The study further emphasizes the identification of prospective areas of open research in the field of electric vehiclecybersecurity, serving as a valuable source of fresh insights for both scholars and practitioners in this sector.

Introduction

The Climate Change Act of 2008 has put out a target of achieving a 100% reduction in greenhouse gas emissions in the United Kingdom by the year 2050, in comparison to the emission levels recorded in 1990. Zero emission cars, particularly electric vehicles, are a pivotal component of future smart cities, hence facilitating the achievement of sustainable urban development objectives. Undoubtedly, electric vehicles have the potential to reduce our reliance on fossil fuels and contribute to the development of intelligent and adaptable power networks.

The effective administration of electric vehicles should possess the capability to avert the overloading of the electrical grid, hence reducing the need for costly infrastructure enhancements that will ultimately be borne by consumers in terms of financial consequences. The landscape of electric vehicle charging infrastructure has undergone significant transformation, transitioning from a limited number of slow chargers in localized and relatively small regions that did not need data connectivity, to the proliferation of many charging stations across urban areas (Zia Muhammad, 2023).[1]

[1] Zia Muhammad et al., *Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability*, 16 ENERGIES 1113 (2023).

These stations provide a wide range of charging options, including rapid and intelligent charging, with or without the capacity to transmit energy bidirectionally (known as vehicle-to-grid capabilities). Additionally, they provide various services that require the transmission of private information.[2] Similar to other components within a smart city, electric vehicle charging infrastructures also include intelligent capabilities and are required to prioritize cybersecurity, data privacy, and interoperability. Multiple studies have shown the significant importance of including cyber security issues into the design and implementation of electric vehicle charging infrastructure, as indicated in Section VI.

In addition to a discernible interest in the subject matter, the present analysis indicates a dearth of research pertaining to security concerns within electric vehicle charging infrastructures. This encompasses the establishment of protocols for communication between cars and chargers, as well as between chargers and other organizations such as aggregators. Furthermore, there is a lack of clarity on the specific cyber assaults that pose a greater threat and have a more significant effect on the electric vehicle charging infrastructure (DavidMorris, 2018).[3] Additionally, the current norms and standards pertaining to establishing a safe charging ecosystem remain unspecified. The objective of this study is to address the aforementioned shortcomings. A potential compromise in the security of communication devices within the electric vehicle ecosystem may have a substantial influence on the Energy and Transport industries.

Ensuring the security of the electric vehicle ecosystem is of paramount significance due to the national criticality of Energy and Transport sectors. In the United Kingdom, for instance, both sectors are among the thirteen recognized national infrastructure sectors that are deemed critical. The potential loss or compromise of critical infrastructures has the potential to significantly damage national security and the availability, integrity, and delivery of important services that are vital for the proper functioning of a modern nation and the everyday lives of its citizens. The electric vehicle ecosystem comprises several linked devices and entities, which together provide a substantial attack surface with significant vulnerabilities. The perpetrators of cyber attacks may be categorized into two main types:

[2] Bharathidasan, Mohan, et al. “A review on electric vehicle: Technologies, energy trading, and cyber security.” *Energy Reports* 8 (2022): 9662-9685.

[3] Morris, David, Garikayi Madzudzo, and Alexeis Garcia-Perez. “Cybersecurity and the auto industry: the growing challenges presented by connected cars.” *International journal of automotive technology and management* 18.2 (2018): 105-118.

insiders and outsiders. Insiders refer to individuals who possess lawful access to a company’s systems, such as employees, but engage in illicit activities by selling business data to external parties.

On the other hand, outsiders include cyber organizations supported by nation-states, who carry out attacks on various targets. Given that EV charging infrastructures are integral components of energy systems, it is pertinent to note that several cyber security and data privacy problems associated with energy systems are also applicable in this context [5, 6]. One instance is the use of intelligent electric vehicle chargers, which establish a link to the power grid. These chargers employ an extra data connection to facilitate the flow of information and control instructions among different entities within the ecosystem. Consequently, this renders them susceptible to possible cyber security threats. In order for the future smart city to operate effectively, it is essential that confidential data be transmitted while ensuring the preservation of its privacy.[4]

Data privacy concerns pertain to the transmission of messages throughout the whole of the electric vehicle charging ecosystem, facilitating a diverse range of services for users and the power grid, including supplementary services. communications of this kind include sensitive information and, as a result, need safeguards to prevent unauthorized disclosure. It is essential to use state-of-the-art cryptographic techniques to ensure the confidentiality of such communications. Additionally, these messages must be handled in accordance with established data privacy regulations, such as the General Data Protection Regulation (GDPR).[5]

One specific component of the data that is subject to manipulation includes users’ personal information, including their identity, car details, location, and bank account data, among other relevant factors. Various payment systems already utilize similar private information, relying on secure communications as an adequate safeguard. However, in the context of EV charging infrastructure, devices such as chargers and vehicles, which store private information, are frequently left unattended and vulnerable to the public for extended durations. Moreover, the inherent characteristic of electric vehicles having high mobility necessitates a reliance on charging facilities

[4] Fraiji, Yosra, et al. “Cyber security issues of Internet of electric vehicles.” *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018.

[5] El-Rewini, Zeinab, et al. “Cybersecurity challenges in vehicular communications.” *Vehicular Communications* 23 (2020): 100214.

that must be deemed trustworthy. The establishment of confidence in the infrastructure is of utmost importance. If a user lacks trust, they may choose not to engage in managed billing efforts, which might potentially disrupt the services and affect other users. The establishment of trust necessitates the simultaneous prioritization of both cyber security and data privacy.[6]

Research Questions

- In what manner can the car industry effectively reconcile the advantages associated with remote functionalities, such as over-the-air updates, with the inherent security vulnerabilities they may introduce?
- What are the potential financial consequences for manufacturers, service providers, and the automotive industry as a whole in the case of a cybersecurity incident within the domain of electric vehicle technology?
- In what ways can organisations effectively measure and control financial risks pertaining to possible cyber threats against electric vehicle systems?
- What are the issues involved in the cyber security in EV’s?

Objectives

- This study aims to identify potential vulnerabilities and security weaknesses within the software, electrical systems, and communication networks of electric vehicles.
- The primary aim of this study is to analyse the dynamic risk landscape in relation to connected and autonomous vehicles.
- This analysis aims to assess the impact of cybersecurity on the comprehensive safety of electric cars, including the well-being of passengers, as well as the safety of other motorists and pedestrians on the road.
- This analysis examines the manner in which the technology used in electric autos handles and protects personal and sensitive data generated by connected cars.
- This study aims to assess the potential for remote exploitation of electric vehicle systems, specifically focusing on unauthorised access to or manipulation of vehicle operations. The objective is to provide effective countermeasures to mitigate this security concern.

[6] *Id.*

- It is essential to establish measures that guarantee the security of the communication networks used by electric vehicles for the purpose of data sharing and receiving updates.

Hypothesis

H0: - The financial consequences of cybersecurity events within the realm of electric vehicle technology are anticipated to be significant for manufacturers, service providers, and the automotive industry as a whole. This underscores the criticality of implementing proactive security measures.

H1: - The absence of standardised cybersecurity protocols within the electric vehicle sector leads to disparities in security measures, and the adoption of standardised practises is anticipated to provide a more cohesive and efficient approach to mitigating prevalent cyber risks.

Problem Statement

The dynamic landscape created by the rapid advancement of electronic vehicle technology and the parallel expansion of cyber intelligent markets poses serious concerns around cybersecurity. Electronic vehicles are becoming more autonomous and networked, which makes them more vulnerable to cyberattacks and might jeopardize people's and businesses' safety and security.

As EVs become more widely used, there is an increased chance of hacking, data breaches, and system manipulations. Dangerous outcomes like accidents, data theft, and privacy violations could result from these dangers. Further, EVs are closely associated with the emergence of cyber intelligent markets, which are defined by digital transactions and smart technologies. Because these markets are vulnerable to cyberattacks, it is imperative to protect their security and integrity in order to prevent economic disruptions and erode customer confidence.

It is difficult to maintain appropriate cybersecurity safeguards given the EVs' quick speed of technology innovation. These advancements include the integration of IoT, artificial intelligence, and sophisticated systems—all of which are vulnerable to abuse by hostile parties.

Significance of the Study

The research article carries substantial ramifications for a multitude of crucial facets. To begin with, it assumes a pivotal function in safeguarding security and safety within the swiftly progressing domain of electric vehicle technology. Through the understanding and resolution of cybersecurity vulnerabilities associated with electric vehicles, this study makes a valuable contribution to the advancement of protective measures against possible threats. Ultimately, this ensures the security of individuals and the interests of organisations that depend on EVs.

It then discusses the robustness of contemporary markets in the era of digitalization. In an era characterised by escalating digitalization and interconnected systems, it is critical to comprehend the complex interplay between electric vehicle technology and cyber-intelligent markets. This understanding is crucial for preserving economic robustness and mitigating susceptibilities that could potentially undermine the integrity of digital transactions and market operations.

Moreover, the research exerts a substantial influence on the domain of policy and regulation. The results illuminate the significant cybersecurity obstacles that arise from the intersection of electric vehicle technology and cyber markets. These observations can provide policymakers and regulatory bodies with valuable inputs that can facilitate the development of standards and guidelines that govern the electric vehicle (EV) industry, cybersecurity practises, and digital markets in an effective manner. Moreover, the study acknowledges the swift technological progressions occurring in the electric vehicle industry and provides valuable perspectives on how technological innovation and strong cybersecurity protocols can coexist in a harmonious manner. This knowledge functions as a beacon for subsequent research and development endeavours, facilitating the fabrication of state-of-the-art electric vehicle technologies all the while guaranteeing the utmost in security.

The study concludes by examining the fundamental concern of consumer trust. It is critical to maintain consumer confidence in cyber-intelligent markets and electronic vehicles. By placing trust in the security and integrity of these systems, individuals are more inclined to embrace and profit from advancements in electric vehicle technology, as well as actively engage in the dynamic realm of cyber-intelligent markets. Therefore, this study is crucial in promoting consumer confidence, which can subsequently facilitate the extensive implementation of these revolutionary technologies.

Scope and Limitations

Scope:

- Legal and Regulatory Framework: The study thoroughly examines the legal and regulatory frameworks that control cybersecurity, market intelligence, and electronic vehicle technologies. It includes a vast array of government policy documents, rules, statutes, and case law.
- Cybersecurity Concerns: Taking into account both present and upcoming difficulties, the paper examines the many cybersecurity issues related to EV technology. It explores issues related to consumer rights, intellectual property, privacy, and data protection.
- Market Implications: This study investigates the possible social and economic effects of EV technology integration on cyber-intelligent marketplaces.

Limitations:

- Evolutionary Nature: Cybersecurity and electronic car technology are fields that are always changing. As a result, the study might not have included the most recent advancements and growing risks.
- Geographical Focus: Although an attempt is made to incorporate a worldwide viewpoint, the research mainly concentrates on cybersecurity issues and legislative frameworks in a limited number of jurisdictions, which might not include all pertinent areas.
- Industry-Specific Expertise: Although the study draws from the body of literature and professional judgements, it's possible that it didn't directly obtain access to confidential data from the cybersecurity and automobile businesses.
- Subject Complexity: The relationship between cybersecurity, market intelligence, and electronic vehicle technology is very complex. Even though the research offers a thorough examination, some subtleties might go unnoticed.
- Policy Recommendations: Although the research points out obstacles and legal loopholes, it makes no particular policy recommendations for resolving cybersecurity issues. Such suggestions would necessitate further investigation and cooperation with legislators.

Literature Review

1. **Cybersecurity for Electric Vehicle Charging Infrastructure Jay Johnson, Benjamin Anderson, Brian Wright, Jimmy Quiroz, Timothy Berg, Russell Graves, Josh Daley, Kandy Phan, Michael Kunz**[7]: **-** The electrification of the transportation sector in the United States has the potential to expose important infrastructure sectors, such as electrical systems, industry, medical services, and agriculture, to cyberattacks that specifically target vehicle charging. The issue at hand is becoming more significant due to the expansion of charging stations' power delivery capacities and their need to establish communication protocols for charging authorization, sequencing the charging process, and managing the load. This responsibility falls on various entities such as grid operators, car manufacturers, original equipment manufacturers (OEMs), and charging network operators. The research issues are many and intricate due to the involvement of multiple end users, stakeholders, and interests of software and equipment providers. The inadequate implementation of electric vehicle supply equipment (EVSE), electric vehicles, or communication systems operated by grid operators could pose a substantial threat to the widespread adoption of EVs. This is due to the potential political, social, and financial consequences of cyberattacks, or even the public perception thereof, which could have far-reaching implications throughout the industry, leaving a lasting impact. Regrettably, at now, there exists a dearth of a comprehensive strategy towards ensuring cybersecurity in Electric Vehicle Supply Equipment (EVSE).

Furthermore, the EV/EVSE sector has only embraced a limited number of best practises in this regard. There exists a limited comprehension within the industry regarding the attack surface, networked assets, and inadequately protected interfaces. In order to ensure the security of EV charging infrastructure, it is essential to provide comprehensive cybersecurity guidelines that are based on rigorous research. This project has contributed to the electricity, security, and automotive industries by establishing a robust technical foundation for safeguarding their respective infrastructures. This has been achieved via the creation of threat models, identification of technological deficiencies, and the development or identification of efficient countermeasures. The team conducted a comprehensive analysis of cybersecurity threats by developing a threat model and

[7] JAY JOHNSON ET AL., *Cybersecurity for Electric Vehicle Charging Infrastructure*, SAND2022 (2022), https://www.osti.gov/servlets/purl/1877784/ (last visited Oct 6, 2023).

conducting a technical risk assessment of Electric Vehicle Supply Equipment (EVSE) assets from various manufacturers and vendors. The objective was to enhance the protection of customers, vehicles, and power systems for automotive, charging, and utility stakeholders in response to emerging cyber threats.

2. **An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure by Roberto Metere, Zoya and Myriam**[8]: - Electric vehicles play a crucial role in mitigating our reliance on fossil fuels. It is anticipated that the future smart grid will be inhabited by a substantial number of electric vehicles that are equipped with batteries capable of meeting significant levels of energy consumption. In order to mitigate the strain on the existing electrical system, costly infrastructure enhancements are necessary. The occurrence of some upgrades may be mitigated if electric vehicle users actively engage in energy balancing measures, such as bidirectional EV charging. The rising prevalence of consumer Internet-connected gadgets, such as EV smart charging stations, has raised apprehensions over their vulnerability to hackers and the safeguarding of personal data. There is a pressing need to effectively modify and enhance our existing technology in order to address the security difficulties associated with the electric vehicle charging infrastructure. These challenges extend beyond the conventional technological applications often found within the energy and transport networks arena. The need for security must be carefully considered in conjunction with other desired attributes, like interoperability, crypto-agility, and energy efficiency. The available evidence indicates a deficiency in the existing level of knowledge about cyber security in electric vehicle charging infrastructures. This study aims to address the existing vacuum in literature by presenting a complete and up-to-date review of the difficulties pertaining to privacy and security. In order to do this, we conduct an examination of the communication protocols used within its ecosystem and propose potential security tools that may be utilised for further research endeavours.

3. **Cybersecurity Risk Analysis of Electric Vehicles Charging Stations by Safa Hamdare, Omprakash Kaiwartya, Mohammad Aljaidi, Manish Jugran, Yue Cao, Sushil Kumar,**

[8] Roberto Metere et al., *An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure*, (2022), http://arxiv.org/abs/2209.07842 (last visited Oct 6, 2023).

Mufti Mahmud, David Brown, Jaime Lloret[9]: - The proliferation of Electric automobilesis precipitating a transition away from conventional gasoline-powered automobiles. The demand for Electric Vehicle Charging Systems is increasing, resulting in substantial expansion of EVCS as both public and private charging infrastructure. The proliferation of electric vehicle charging stations has led to a notable escalation in cybersecurity vulnerabilities associated with these systems. This study provides an examination of cybersecurity risks associated with the network of Electric Vehicle Charging Stations within the given environment. To provide a contextual foundation for the study field, this section outlines the recent developments in the Electric Vehicle Charging Station network, the prevailing trends in Electric Vehicle adoption, and various charging use cases. Furthermore, the cyber security elements of Electric Vehicle Charging Stations have been examined, taking into account vulnerabilities related to infrastructure and protocols. Potential scenarios of cyber-attacks have also been discussed. Furthermore, the validation of vulnerabilities in Electric Vehicle Charging Stations has been conducted by the use of real-time data-centric analysis of EV charging sessions. The study further emphasises the identification of possible research gaps in the field of electric vehicle cybersecurity, serving as a valuable resource for both academics and professionals in this subject.

Methodology

The paper utilises a doctrinal research approach that is founded on an extensive examination of current legal, regulatory, and policy frameworks that are pertinent to the topic. The objective of this technique is to offer a comprehensive comprehension of the legal environment concerning the convergence of developing electronic vehicle technology and the developing cyber-intelligent marketplaces.

The main focus of the research is a thorough analysis of official policy papers, case law, regulations, and statutes pertaining to market intelligence, cybersecurity, and electronic vehicle technology. This comprises cybersecurity standards and recommendations set by appropriate authorities, as well as rules and regulations covering data protection, privacy, intellectual property, and consumer rights. To

[9] Cybersecurity Risk Analysis of Electric Vehicles Charging Stations - PubMed, https://pubmed.ncbi.nlm.nih.gov/37571500/ (last visited Oct 6, 2023).

support the legal analysis, scholarly papers, reports, and academic literature on the subject will also be examined.

The research will follow a methodical and controlled methodology to guarantee its doctrinal rigour. The first step of the investigation will be to identify the most important legal and regulatory provisions pertaining to cybersecurity and electronic vehicle technologies. These clauses will next be examined closely, with an emphasis on how they affect cyber-intelligent markets and the related cybersecurity issues. One tool that can be used to evaluate how other jurisdictions handle these concerns is comparative legal analysis.

Historical Perspective

Electronic vehicles originated during the early 19th century, when inventors and engineers-initiated trials utilising electric propulsion. However, the widespread adoption of electric vehicles as a more sustainable and environmentally beneficial mode of transportation did not occur until the latter half of the 20th century. The introduction of hybrid vehicles, exemplified by the Toyota Prius, marked a pivotal moment in the public's embrace of electric vehicle technology. Subsequent to that period, the electric vehicle (EV) sector has witnessed substantial expansion as a result of technological advancements and elevated environmental sustainability concerns.

Simultaneously, the proliferation of digital technologies has been inextricably linked to the evolution of cybersecurity over time. Although the advent of the internet and the information age has provided opportunities for networking and innovation, it has also exposed vulnerabilities and risks in the realm of data security. Cyberattacks, which were once considered improbable, have become more frequent and sophisticated as time has passed. As a consequence, cybersecurity has evolved into a discipline that is vital to our continued existence on the internet.

Modernly, these two trajectories converge within the framework of “Cyber Intelligent Markets.” This expression elucidates the manner in which digital technology and intelligence are employed to establish an interconnected, globally data-centric economy that transcends various market sectors. Due to the introduction of intelligent and autonomous electronic vehicles that rely on sophisticated software, sensors, and data transmission, this evolution has been significantly accelerated. The cybersecurity sector is expanding in tandem with the EV technology and cyber intelligence industries. The imperative for proactive cybersecurity measures is underscored by historical occurrences of vehicle intrusions, data breaches, and security vulnerabilities. Therefore, when examining the security and integrity of electric vehicle (EV) technology within the broader framework of cyber intelligence markets, the historical perspective underscores the growing importance and complexity of such matters.

Importance of cybersecurity in EV

Governments worldwide are increasingly endorsing the use of electric vehicles, with Europe and the United States taking the forefront in this endeavour. In pursuit of a target of 30 million electric vehicles in circulation by the year 2030, the European Union has reached a consensus to prohibit the sale of new conventional autos, devoid of electric propulsion, commencing in 2035. The Biden administration has identified the expansion of public charging infrastructure for electric cars as a key objective. The state of California is set to prohibit the sale of new vehicles powered by traditional fuels by the year 2035(Shah Khalid, 2020).

The cybersecurity vulnerabilities within the car industry have been extensively reported. Nevertheless, a significant number of individuals inside the corporate sector continue to overlook the broader perspective.

According to a recent study conducted by Deloitte Canada, there is a discernible rise in cybersecurity apprehensions within the automotive sector. The study reveals that a significant majority, namely 84%, of cyberattacks targeting automobiles are executed remotely. Furthermore, it is noteworthy that half of these assaults have transpired within the last two years. The University of Georgia conducted a study that revealed the ramifications of an attack on an electric vehicle via its charging station, which might extend to the charging station itself, the car management system, and any associated infrastructure connected to the vehicle. Based on the analysis conducted by Markets, it is projected that the automotive cybersecurity sector will attain a market value of $5.3 billion by the year 2026.

The proliferation of suppliers involved in the advancement of electric vehicles, together with the integration of sophisticated control systems, heightened connectivity, electronic control units (ECUs), and complex coding, results in a substantial vulnerability to potential attacks via several entry points. The charging station of the car as well as the electrical infrastructure might serve as possible avenues for cybercriminal infiltration.[10]

According to Stephen Meagher, the head of cybersecurity and IoT and risk consultancy at Deloitte Canada, contemporary automobiles may be likened to advanced computational devices integrated into mobile platforms. This statement was made during an interview with CTV News. There are several developers and component manufacturers, ranging from small-scale chip producers and firmware developers to control unit manufacturers and mobile application developers that provide connectivity with autos (ErayYağdereli, 2015).

Technological Theories

A framework for perceiving the dynamics and ramifications of these developments is provided by technological theories (SimonParkinson, 2017). In this discourse, we examine a selection of pivotal technological theories that are pertinent to the present investigation.

Innovation Diffusion Theory: The theory of diffusion, which was first proposed by Everett Rogers, provides an explanation of the manner in which innovations, including electric vehicle technology, permeate society. Adopters are classified as follows: laggards, innovators, early adopters, early majority, or late majority. To appraise the effects of EV technology on cyber-intelligent markets and cybersecurity, it is vital to comprehend its current position in this diffusion process.

Disruptive Innovation Theory: The theory of disruptive innovation, which Clayton Christensen popularised, emphasises the manner in which emerging technologies upheaval established markets and industries. This theory facilitates the examination of the automotive industry's ongoing transformation and its consequential impacts on the wider economy and cyber intelligence sectors, with particular reference to electric vehicles.

Complexity Theory: Complexity theory investigates the evolution and adaptation of complex

[10] Eiza, Mahmoud Hashem, and Qiang Ni. “Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity.” *IEEE Vehicular Technology Magazine* 12.2 (2017): 45-51.

systems, including the digital infrastructure of electric vehicles and cyber markets. This viewpoint is critical for comprehending the complex relationship between electric vehicle (EV) technology and cybersecurity, as well as the mechanisms by which these systems defend themselves against attacks. Technology Acceptance Model (TAM): The Technology acceptability Model (TAM) is a psychological framework utilised to evaluate the adoption and acceptability of novel technologies by individuals. Gaining insight into the perceptions and adoption patterns of policymakers, consumers, and businesses regarding electric vehicles (EVs) is critical for forecasting the ramifications of this technology on cyber intelligence markets and the related cybersecurity issues.[11]

Digital Ecosystem Theory: This theory examines the interactions and interdependencies among hardware, software, consumers, and data, among other components of a digital ecosystem. By utilising this theoretical framework to analyse the interplay between EV technology and cyber markets, one can assess the potential weaknesses and synergies that exist within the ecosystem.

Institutional Theory: Institutional theory investigates the impact of regulations, norms, and institutions on the adoption and utilisation of technology. This theory provides insight into the manner in which industry standards and government policies influence the cyber intelligence market and cybersecurity practises with regard to EV technology.

A multifaceted framework for analysing the intricate relationship between EV technology, cyber-intelligent markets, and cybersecurity concerns is provided by these technological theories. By taking into account these theoretical frameworks, the study seeks to furnish an all-encompassing comprehension of the dynamic relationship between technological progress and the digital economy, thereby providing policymakers, businesses, and researchers in these fields with invaluable insights.[12]

Securities vulnerability

Extremely complex technologies, such as those used in driverless vehicles, leave them open to cyberattacks. Inquire more about these gaps. Remote exploitation is the main point of discussion.

[11] Khatoun, Rida, and Sherali Zeadally. "Cybersecurity and privacy solutions in smart cities." IEEE Communications Magazine 55.3 (2017): 51-59.

[12] Khan, Dr Shazia W. "Cyber security issues and challenges in E-commerce." Proceedings of 10th international conference on digital strategies for organizational success. 2019.

Wireless communication systems and software technologies are crucial to the success of autonomous vehicles.[13] Attackers can gain unauthorised access to, or even take complete control of, these systems by taking advantage of flaws in their design. Weaknesses in the Wi-Fi or Bluetooth protocols, for instance, might allow an unauthorised user to remotely alter the vehicle's controls or disrupt its usual functioning. Wired highlights a scientific article in which the authors detail their demonstration of remotely hijacking a Jeep Cherokee, drawing attention to the risks associated with wireless connections (HazelLim, 2018).[14]

Sensor spoofing is the practise of intentionally creating false sensor readings to trick a monitoring system. Autonomous vehicles rely heavily on sensors like LiDAR (Laser imaging, Detection, and Ranging), radar, and cameras to gather relevant data about their surroundings for use in mapping the road ahead and making other decisions. However, it's crucial to remember that these sensors may be tricked by a spoofing attack.[15] Malicious actors have the capacity to trick a vehicle's perception systems into making erroneous decisions or gaining an inaccurate picture of its surroundings by tampering with sensor inputs. The vulnerability of sensors in autonomous cars to spoofing attacks was shown in a study conducted by researchers at the University of Michigan. The dangers associated with sensor spoofing attacks may be reduced by the deployment of redundant sensors, anomaly detection methods, and the verification of sensor data integrity.

The complexity of the software systems used by driverless vehicles is a major security risk. Paradoxically, a software flaw that allows an attacker to bypass access restrictions might be just as dangerous as a flaw that allows the attacker to bypass safety safeguards. The risks of software vulnerabilities that might affect the safety of autonomous vehicles were highlighted in a study published in the prestigious journal Science. As a result, it's more important than ever to follow strict methods of software development and perform comprehensive security checks (Dietmar Möller, 2019).[16]

[13] Parkinson, Simon, et al. "Cyber threats facing autonomous and connected vehicles: Future challenges." *IEEE transactions on intelligent transportation systems* 18.11 (2017): 2898-2915.

[14] Lim, Hazel Si Min, and Araz Taeihagh. "Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications." *Energies* 11.5 (2018): 1062.

[15] Kim, Shiho, et al. "In-vehicle communication and cyber security." *Automotive Cyber Security: Introduction, Challenges, and Standardization* (2020): 67-96.

[16] Möller, Dietmar PF, and Roland E. Haas. *Guide to automotive connectivity and cybersecurity*. Springer International Publishing, 2019.

Legal Framework- Cybersecurity

There is no stand-alone cybersecurity law in India. Instead, the foundation of the legal framework for cybersecurity is the Information Technology Act of 2000 (IT Act) and its implementing rules and regulations. The IT Act, which also includes safeguards for electronic data, information, and records, is essential in giving electronic transactions legal status and protection.[17] Specific cybersecurity crimes like hacking, denial-of-service assaults, phishing, malware attacks, identity fraud, and electronic theft are covered by important provisions of the IT Act. To reinforce and enhance the cybersecurity framework, a number of rules and regulations have been established in addition to the IT Act. These consist of:

- Information Technology (Sensitive Personal Data or Information and Reasonable Security Practises and Procedures) Rules 2011: The gathering and processing of personal or sensitive personal data must adhere to these regulations' reasonable security practises and procedures.
- The 2018 Protected System Rules (Information Technology) (Information Security Practises and Procedures for Protected System): These regulations mandate the implementation of particular information security measures by organisations that have protected systems, as specified by the IT Act.
- Guidelines for Intermediaries in Information Technology (Intermediaries Guidelines), 2011: In order to protect their computer resources and notify CERT-In of cybersecurity problems, intermediaries must follow reasonable security practises and procedures.
- Cybersecurity-related rules can also be found in other legislation, such as the Companies (Management and Administration) Rules 2014 (CAM Rules) and the Indian Penal Code 1860 (IPC).

India's cybersecurity rules and regulations mostly affect regulated businesses that work in delicate industries like banking, insurance, telecommunications, and financial services. Because of voluntary compliance with international standards and governmental action, many sectors have demonstrated greater standards of cybersecurity preparation. Significant foreign investment has been made in e-commerce and IT-enabled businesses, which have also proactively implemented strong cybersecurity

[17] Burkacky, Ondrej. *Cybersecurity in automotive*. McKinsey, 2020.

standards.[18] As digital payments have become more popular, there is a noticeable growth in payment-related cybercrimes, which makes strict cybersecurity regulations necessary (Kim Kyounggon, 2021).[19]

Acceptance of Global Guidelines

India has embraced a number of international cybersecurity standards. For example, ISO/IEC 27001 is recognised by the SPDI Rules as an authorised security standard for safeguarding personal data. Furthermore, based on worldwide standards like ISO/IEC 27001 and ISO/IEC 2702, sector-specific authorities like the Reserve Bank of India (RBI) and the Securities Exchange Board of India (SEBI) require cybersecurity requirements for their regulated firms.

Directors' and Responsible Personnel's Obligations

Information security personnel are not required by statute to inform directors about the preparedness of their organization's network; however, those in charge of an organisation must show that they have put security control measures in place in accordance with their established information security programmes and policies. According to Section 85 of the IT Act, anyone in charge of overseeing a business's operations are accountable for any violations unless they can demonstrate that they had no knowledge of the violation or took reasonable precautions to avoid it. In accordance with the CAM Rules, designated personnel are also in charge of maintaining the security and upkeep of electronic documents; neglecting to do so could be construed as a violation of their obligations (Dr Shazia WKhan, 2020).[20]

Cybercrime and Cybersecurity Definition

The IT Act defines "cybersecurity" as safeguarding different digital assets, such as data, hardware, software, and computer resources, against unauthorised access, use, disclosure, disturbance, alteration, or destruction. "Cybercrime" refers to illegal activities carried out with the purpose of causing financial loss, bodily harm, or psychological distress to individuals, groups, or organisations

[18] Xie, Yong, et al. "Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: state-of-the-art and future challenges." *Software: Practice and Experience* 51.11 (2021): 2108-2127.

[19] Kim, Kyounggon, et al. "Cybersecurity for autonomous vehicles: Review of attacks and defense." *Computers & Security* 103 (2021): 102150.

[20] Khan, Dr Shazia W. "Cyber security issues and challenges in E-commerce." *Proceedings of 10th international conference on digital strategies for organizational success*. 2019.

through the use of computers, communication devices, or computer networks.

Organisations' Minimum Protective Measures

Organisations handling sensitive personal data or information are required under the SPDI Rules to put in place "reasonable security practises and procedures." Additional security precautions are mandated by sector-specific rules, which take into account the sensitive nature of the information and industry norms. For safe financial transactions, banks must, for instance, install firewalls, SSL authentication, logical access controls, and data encryption in accordance with RBI requirements.[21]

Cybersecurity Laws for Critical Infrastructure and Intellectual Property

The IT Act addresses cyber threats to intellectual property by establishing fines for hacking, data theft, and tampering with computer source code. Furthermore, under section 70 of the IT Act, India defines specific computer resources as "protected systems," which are regarded as essential components of the vital information infrastructure (CII). In order to safeguard public health, safety, the economy, and national security, these regulations mandate precise cybersecurity practises for CII businesses.[22]

Information Sharing About Cyber threats

The Indian Supreme Court has recognised that the right to privacy applies to the sharing of cyber threat information. Nonetheless, under some conditions, including the prevention or investigation of cybercrimes, governmental and regulatory bodies are allowed access to private conversations and personally identifiable data under legislation like the Indian Telegraph Act 1885 and the IT Act.

India has rules pertaining to cybersecurity that are not just for domestic businesses. If an international organization's operations result in legal violations and involve computers, computer networks, or resources in India, they are subject to the IT Act. Therefore, in order to ensure compliance with cybersecurity standards and legal requirements, foreign organisations operating in India must follow the same regulatory duties as domestic firms.

[21] Khatoun, Rida, and Sherali Zeadally. "Cybersecurity and privacy solutions in smart cities." *IEEE Communications Magazine* 55.3 (2017): 51-59.

[22] Quintana, J. A., et al. "A Holistic Approach on Automotive Cybersecurity for Suppliers." *Proceedings of the VEHICULAR* (2023).

Cyber securities issues in EV's

By the year 2040, it is anticipated that electric automobiles would account for around 60 percent of the sales of passenger vehicles in the globe. The electronic power train components and software (SW) that are connected to the automobiles of the future are constantly being improved upon in terms of design, level of complexity, and level of safety. They maintain a high level of vigilance at all times in order to protect highly complex computerised systems, such as electric vehicles, from the potential dangers presented by hackers and other lawbreakers (JayKennedy, 2021).[23]

By the year 2030, it is anticipated that the number of linked vehicles operating on the roads will have increased to over one trillion. It is anticipated that the possibility for cyberattacks will increase in parallel with the continued evolution of these cars, which will include the addition of additional functions and improved connectivity. Over the course of the last ten years, there has been a considerable growth in the number of electric vehicle manufacturers, which has already surpassed 50. This figure takes into account both well-established original equipment manufacturers (OEMs) and new start-up businesses. During this time period, sales and marketing teams have put a higher priority on offering new features and functions. This shift in focus has often come at the cost of resolving concerns highlighted by Chief Information Security Officers (CISOs) or teams responsible for cybersecurity and functional safety (FuSa).[24]

Although it was anticipated that the recently launched UNECE certification for cybersecurity would reduce this discrepancy, it does not effectively address the number of attacks that occur on networked automobiles around once every 39 seconds. Comparing the global illicit drug trade, which is believed to be worth $400 billion, to cybercrime, which is projected to be worth $600 billion, recent evidence shows that cybercrime may be more financially rewarding. This unlawful activity entails the theft of around 75 data per second, which are subsequently traded within more than 6,000 online criminal marketplaces that have been expressly developed for the trading of ransomware.[25]

[23] Kennedy, Jay, Thomas Holt, and Betty Cheng. "Automotive cybersecurity: Assessing a new platform for cybercrime and malicious hacking." *Journal of crime and justice* 42.5 (2019): 632-645.

[24] Raimundo, Ricardo Jorge, and Albérico Travassos Rosário. "Cybersecurity in the internet of things in industrial management." *Applied Sciences* 12.3 (2022): 1598.

[25] Jawaher Fadhil & Qusay Sarhan, *Internet of Vehicles (IoV): A Survey of Challenges and Solutions*1 (2020).

Original equipment manufacturers (OEMs) have the option of taking proactive measures to prevent cyberattacks and ensuring compliance with UNECE standards, which will be required for all new vehicle types beginning in July 2022 and for all new vehicles beginning in July 2024. This is a more favourable option for OEMs than having to explain the subsequent expenses of costly recalls and the implementation of software patches and upgrades. Original equipment manufacturers have the option of taking proactive measures to prevent cyberattacks and ensure compliance with UNECE standards.[26] Original Equipment Manufacturers (OEMs) in the automobile industry face a substantial obstacle in the form of a considerable problem when it comes to the procurement of cybersecurity software and related operations. This is largely the result of their dependence on suppliers for components and software, as well as a lack of expertise or internal experience in this field, as well as a shortage of dedicated workers or defined responsibilities within different software development teams.

As automobiles become more sophisticated and move closer to becoming connected, autonomous, and electric vehicles (CAEVs), the degree to which the functioning of a vehicle is dependent on having secure communication is growing. It is essential that these connections work well, are efficient, and are protected from outside interference. Conventional Advanced Driving Assistance Systems (ADAS) are giving way to more cutting-edge forms of driver assistance technology as the field of autonomous driving moves further. This modification requires a considerable amount of data to be sent between the sensors, Electronic Control Units (ECUs), and control centres that are housed within the cars. This data sharing is being done with the intention of facilitating more effective and efficient driving, vehicle coordination, more efficient path planning, and better route and energy utilisation.[27]

An extra need for electric vehicles would include the installation of bi-directional charging and discharging capabilities, as well as the implementation of route planning and traffic management features. This requirement would be in addition to any other requirements already in place. Wireless Vehicle Communications (WVC) and Vehicular Communications Networking (VCN) the illustrated scenarios include important considerations such as the integration of a variety of applications. It is

[26] Lautenbach, Aljoscha. *On Cyber-Security for In-Vehicle Software*. Chalmers Tekniska Hogskola (Sweden), 2017.

[27] Sun, Xiaoqiang, F. Richard Yu, and Peng Zhang. "A survey on cyber-security of connected and autonomous vehicles (CAVs)." *IEEE Transactions on Intelligent Transportation Systems* 23.7 (2021): 6240-6259.

vital that the design of the wireless system be precisely adapted to suit the fundamental activities of the vehicle, while also taking into consideration the limitations that are imposed by wireless technology.[28]

The Internet of Vehicles (IoVs), sometimes known as linked vehicles, is an expansive network that connects a wide variety of nodes, such as autos, pedestrians, bicycles, and sensors. It is also often referred to as connected cars. Its major purpose is to improve driving efficiency and traffic safety, as well as to elevate the quality of the driving experience as a whole and reduce the number of collisions that take place. Intelligent vehicles (IoVs) make use of a wide variety of communication technologies, WAVE and cellular technologies. These technologies are gradually being incorporated into autonomous and electrically powered vehicles (JoachimTaiber, 2020).[29]

Customers of electric vehicles have a number of essential concerns to take into account, including range anxiety, optimum battery performance, and the availability of dynamic charging stations. As a result of this, a large number of companies have been working on the creation of simulated platforms and energy maps for connected autonomous electric cars (CAEVs). These platforms and maps want to present new services that optimise energy use by researching different routes, monitoring and controlling temperature conditions, and making predictions about battery performance.

The Internet of Electric Vehicles (IoEV), often referred to as the IoV, is a platform that enables intercommunication between automobiles and a wide variety of third parties, including but not limited to other automobiles, servers, people, traffic signals, and charging stations. The IoV is also known as the Internet of Electric Vehicles (IoEV). The employment of on-board sensors located inside the cars themselves makes it feasible for this connection to take place.[30]

Connected Autonomous Electric Vehicles, also known as CAEVs, are those that maintain consistent communication with a backend server in order to supply real-time data. This data may include, but is

[28] Bidirectional Charging and Electric Vehicles for Mobile Storage, ENERGY.GOV, https://www.energy.gov/femp/bidirectional-charging-and-electric-vehicles-mobile-storage (last visited Oct 6, 2023).

[29] Taiber, Joachim. *Unsettled topics concerning the impact of quantum technologies on automotive cybersecurity*. No. EPR2020026. SAE Technical Paper, 2020.

[30] Fadhil and Sarhan, *supra* note 6.

not limited to, information such as vehicle identification, geographical coordinates, battery cell temperature, State of Charge (SOC), HVAC status, distance to empty (DTE), and distance to destination. The server has the capability to analyse the provided information and overlay it with data pertaining to road infrastructure elements such as potholes, crevices, and speed bumps, as well as data pertaining to road traffic conditions including accidents and traffic congestion, as well as data pertaining to weather conditions such as rain, snow, and thunderstorms. Because of the integration of these data, it is now possible to develop an energy map that is especially focused on the energy consumption of electric vehicles.[31]

This map has the potential to be used by automotive original equipment manufacturers (OEMs) as well as data analytics service providers for the aim of making unique service suggestions to connected and autonomous electric cars (CAEVs). In the context of these services, “identifying the most energy-efficient route to a given destination,” “locating the closest charging stations,” and “optimising thermal management systems” are all examples of what can fall under the umbrella of “services.” (Julian Jang-Jaccard & Surya Nepal, 2014)

Vehicle-to-sensor (V2S), vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), and vehicle-to-home (V2H) communications are all included in the architecture of the Internet of Electric Vehicles (IoEV), which stands for the Internet of Electric Vehicles. In addition to this, it contains electric vehicle supply equipment-to-everything (EVSE2X) communications, more particularly electric vehicle supply equipment-to-vehicle (EVSE2EV) and electric vehicle supply equipment-to-network (EVSE2N) communications. These communication channels make it possible for connected and autonomous electric cars (CAEVs) to communicate with their environment, both internally and externally.[32]

[31] Chen, Zhaolin. “Deep learning for cybersecurity: a review.” *2020 International Conference on Computing and Data Science (CDS)*. IEEE, 2020.

[32] Chatfield, Akemi Takeoka, and Christopher G. Reddick. “A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government.” *Government Information Quarterly* 36.2 (2019): 346-357.

Cybersecurity risks to autonomous & EV industry

Electric vehicles that are technologically advanced and equipped with advanced connectivity features and intricate functionalities exhibit certain cybersecurity weaknesses.[33]

The subject matter under consideration pertains to illegal access. The issue over the possible exploitation of internet connectivity and remote-control capabilities in electric vehicles by cyber attackers is significant. The existence of vulnerabilities inside linked systems has the capacity to provide unauthorised access to critical vehicle operations. Malicious actors have the potential to exploit these vulnerabilities in order to manipulate controls, extract user data, or establish remote control over the vehicle. In a piece published by WIRED, researchers demonstrated the ability to remotely manipulate certain capabilities of a Tesla vehicle by exploiting weaknesses inside its linked systems.[34]

This paper examines the vulnerabilities that are often linked with Over-The-Air (OTA) upgrades. The use of over-the-air (OTA) updates enables manufacturers to remotely modify the software of automobiles. However, it is important to note that the vulnerability of the over-the-air (OTA) update process might potentially be exploited by hostile individuals to breach the vehicle's systems or introduce harmful software. The IOActive paper highlighted the existence of vulnerabilities in over-the-air (OTA) updates for a popular electric vehicle model, emphasising the need of establishing secure methods for upgrades and authentication.

The topic of privacy concerns is of significant academic interest. Advanced electric vehicles collect a wide range of data, such as user preferences, historical location data, and personal information, which has led to growing concerns around privacy. The absence of robust security mechanisms may lead to violations of privacy and unauthorised access to sensitive user data. The study conducted by researchers at the University of Michigan Transportation Research Institute highlighted the privacy risks related to interconnected electric vehicles, as well as the potential for location tracking and data

[33] Cybersecurity in the Autonomous Vehicle: The Next Frontier in Mobility, FINANCIALEXPRESS (Sep. 5, 2023), https://www.financialexpress.com/business/express-mobility-cybersecurity-in-the-autonomous-vehicle-the-next-frontier-in-mobility-3234055/ (last visited Oct 6, 2023).

[34] Julian Jang-Jaccard & Surya Nepal, *A Survey of Emerging Threats in Cybersecurity*, 80 JOURNAL OF COMPUTER AND SYSTEM SCIENCES 973 (2014).

exploitation.[35]

How secure are EV?

The advent of technology has led to significant advancements and increased accessibility in several aspects of human existence. However, it is important to acknowledge that with these benefits, there has been a corresponding rise in hazards to mankind. Security is an essential need throughout all aspects of human existence, including the protection of our residences, personal well-being, possessions, and other significant elements of our lives. The proliferation of information technology has led to a corresponding rise in the prevalence of internet-based security risks.[36]

- **Automated vehicles cybersecurity's**

Despite the challenges posed by the COVID-19 pandemic inside the car sector, analysts anticipate a surge in the market for electric vehicles in the next year of 2021. In the foreseeable future, there is expected to be a substantial increase in the number of electric vehicles operating on a global scale. The automotive sector has achieved notable advancements in the development of autonomous vehicles, often referred to as self-driving cars, owing to continuous improvements in technology. Hyundai, Tesla, and Google are prominent entities leading the advancement of autonomous cars.[37]

- **Autonomous cyber securities strategies**

Various machine learning techniques are used to safeguard autonomous systems from cyber attacks.[38] Autonomous systems are safeguarded by the use of diverse machine learning methods. By using these algorithms, the car acquires knowledge about the owner's pattern over a period of time. The pattern algorithm used by the owner is capable of detecting any deviations from the established norms, promptly notifying the owner and requesting the user's credentials.

Conversely, some individuals with hacking abilities are capable of falsifying user credentials,

[35] Cybersecurity in the Autonomous Vehicle, *supra* note 9.

[36] Safa Hamdare et al., *Cybersecurity Risk Analysis of Electric Vehicles Charging Stations*, 23 SENSORS 6716 (2023).

[37] EV charging points hacked to show explicit material - Cities Today, https://cities-today.com/ev-charging-points-hacked-to-show-explicit-material/ (last visited Oct 6, 2023).

[38] Elmaghraby, Adel S., and Michael M. Losavio. "Cyber security challenges in Smart Cities: Safety, security and privacy." *Journal of advanced research* 5.4 (2014): 491-497.

therefore circumventing the first barrier of protection. Professionals have the ability to use deep learning and machine learning methodologies in order to detect abnormalities within ever expanding datasets, therefore addressing this issue. Moreover, an analysis may be conducted on vehicle-to-vehicle communication in order to determine if the received data corresponds to typical driving patterns or represents a deliberate harmful intrusion.[39]

With the increasing prevalence of self-driving cars, drones, and automated industrial equipment, cybersecurity experts operating within the autonomous machine industry may expect to encounter novel challenges.

Experienced individuals with expertise in the field may significantly diminish the operational effectiveness of electric cars by decreasing their battery capacity and energy, resulting in a reduction of up to 50%. The study conducted by the researchers focused on investigating susceptibilities to cyberattacks targeting different objectives, such as energy efficiency and safety.[40] Additionally, they devised a framework for the advancement of power electronics systems in the future. Several cybersecurity concerns that might potentially impact electronic cars are outlined below:

Wireless accessibility: - Smartphone applications have garnered significant attention from cybercriminals due of their potential for unauthorised access to electric vehicles. In addition to other means, hackers possess the capability to infiltrate WiFi networks. Once infiltrated, hackers possess the capability to deactivate a vehicle’s alarm system, assume command over further systems, and exercise unrestricted authority.[41]

Recommendations & Future Study Directions

Robust and Comprehensive Cybersecurity Standards: To create strong and comprehensive cybersecurity standards for EV technology, policymakers and industry stakeholders should work together. To protect against cyber attacks, this includes intrusion detection systems, secure software

[39] Manuel Sandler, *Autonomous Vehicle Cybersecurity: An Overview*, CYRES CONSULTING (Jan. 27, 2023), https://www.cyres-consulting.com/autonomous-vehicle-cyber-security-overview/ (last visited Oct 6, 2023).

[40] Lu, Yang, and Li Da Xu. “Internet of Things (IoT) cybersecurity research: A review of current research topics.” *IEEE Internet of Things Journal* 6.2 (2018): 2103-2115.

[41] Anastasios Giannaros et al., *Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions*, 3 JOURNAL OF CYBERSECURITY AND PRIVACY 493 (2023).

upgrades, and encryption techniques.

Regulatory Framework Adaptation: Governments should modify the current regulatory framework to take into account the rapidly changing field of electric vehicle technology and how it is integrated with online marketplaces. Data privacy, responsibility, and the legal ramifications of cyberattacks on autonomous vehicles should all be taken into account throughout this adaption.

Cross-Sector Collaboration: It's critical to promote cooperation between the cybersecurity sector, tech companies, and the automotive industry. These kinds of cross-sector collaborations can promote creativity, exchange best practises, and create comprehensive defences against cyberattacks.

Future studies on the behavioural economics of EV adoption should take into account the incentives, preferences, and psychological aspects that influence consumers' decisions. This may shed light on future developments in the market for electric vehicles and related cyber technologies.

Further, research on cyber resilience techniques is essential as EVs grow increasingly autonomous and networked. It is crucial to research how these systems can resist and bounce back from cyberattacks. Examining the wider societal effects of electric vehicles (EVs) in terms of urban planning, economics, and the environment can help us understand how these cars will influence future markets and, in turn, raise cybersecurity issues.

Lastly, research on cyber liability in relation to electric vehicles is still in its infancy. Future studies can examine how cyber insurance plans are developed, how liability concerns arise, and how these factors affect the overall cyber insurance market. In the context of cyber intelligence, these suggestions and the directions for future research are essential to guaranteeing the market for electronic vehicles' continuous expansion and security. They provide a road map for navigating the intricate and dynamic environment where technology, markets, and cybersecurity combine for researchers, enterprises, and governments.

Conclusion

The consequences of a compromised automobile are significant, but, there are viable remedies. Andy Greenburg asserts that addressing the security vulnerabilities of autonomous cars necessitates fundamental alterations to their security architecture (Greenburg, n.d.). Furthermore, effective implementation would need close coordination among automotive manufacturers, security specialists, and government organisations. Consequently, the establishment of a cohesive security framework will ensue, subject to scrutiny by professionals in the field of security, and in compliance with governmental regulations. Regrettably, there is a scarcity of security expertise.

The prevailing consensus among experts is that there will be a deficit of around two million cybersecurity workers within the next years. In response to this shortage, organisations have intensified their efforts to provide the workforce with personnel who possess a high level of education and expertise, capable of safeguarding critical cyber infrastructures and information assets. The emergence of autonomous cars necessitates the presence of proficient cybersecurity professionals to address and mitigate any attacks and vulnerabilities associated with this swiftly advancing technology.

References

- Anastasios Giannaros et al., Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions, 3 JOURNAL OF CYBERSECURITY AND PRIVACY 493 (2023).
- Bharathidasan, Mohan, et al. "A review on electric vehicle: Technologies, energy trading, and cyber security." Energy Reports 8 (2022): 9662-9685.
- Bidirectional Charging and Electric Vehicles for Mobile Storage, ENERGY.GOV, https://www.energy.gov/femp/bidirectional-charging-and-electric-vehicles-mobile-storage (last visited Oct 6, 2023).
- Burkacky, Ondrej. Cybersecurity in automotive. McKinsey, 2020.
- Chatfield, Akemi Takeoka, and Christopher G. Reddick. "A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government." Government Information Quarterly 36.2 (2019): 346-357.

- Chen, Zhaolin. "Deep learning for cybersecurity: a review." 2020 International Conference on Computing and Data Science (CDS). IEEE, 2020.
- Cybersecurity in the Autonomous Vehicle, supra note 9.
- Cybersecurity in the Autonomous Vehicle: The Next Frontier in Mobility, FINANCIALEXPRESS (Sep. 5, 2023), https://www.financialexpress.com/business/express-mobility-cybersecurity-in-the-autonomous-vehicle-the-next-frontier-in-mobility-3234055/ (last visited Oct 6, 2023).
- Cybersecurity Risk Analysis of Electric Vehicles Charging Stations - PubMed, https://pubmed.ncbi.nlm.nih.gov/37571500/ (last visited Oct 6, 2023).
- Eiza, Mahmoud Hashem, and Qiang Ni. "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity." IEEE Vehicular Technology Magazine 12.2 (2017): 45-51.
- Elmaghraby, Adel S., and Michael M. Losavio. "Cyber security challenges in Smart Cities: Safety, security and privacy." Journal of advanced research 5.4 (2014): 491-497.
- El-Rewini, Zeinab, et al. "Cybersecurity challenges in vehicular communications." Vehicular Communications 23 (2020): 100214.
- EV charging points hacked to show explicit material - Cities Today, https://cities-today.com/ev-charging-points-hacked-to-show-explicit-material/ (last visited Oct 6, 2023).
- Fadhil and Sarhan, supra note 6.
- Fraiji, Yosra, et al. "Cyber security issues of Internet of electric vehicles." 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2018.
- Jawaher Fadhil & Qusay Sarhan, Internet of Vehicles (IoV): A Survey of Challenges and Solutions1 (2020).
- JAY JOHNSON ET AL., Cybersecurity for Electric Vehicle Charging Infrastructure, SAND2022 (2022), https://www.osti.gov/servlets/purl/1877784/ (last visited Oct 6, 2023).
- Julian Jang-Jaccard & Surya Nepal, A Survey of Emerging Threats in Cybersecurity, 80 JOURNAL OF COMPUTER AND SYSTEM SCIENCES 973 (2014).
- Kennedy, Jay, Thomas Holt, and Betty Cheng. "Automotive cybersecurity: Assessing a new platform for cybercrime and malicious hacking." Journal of crime and justice 42.5 (2019): 632-645.
- Khan, Dr Shazia W. "Cyber security issues and challenges in E-commerce." Proceedings of 10th international conference on digital strategies for organizational success. 2019.

- Khan, Shah Khalid, et al. "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions." Accident Analysis & Prevention 148 (2020): 105837.
- Khatoun, Rida, and Sherali Zeadally. "Cybersecurity and privacy solutions in smart cities." IEEE Communications Magazine 55.3 (2017): 51-59.
- Kim, Kyounggon, et al. "Cybersecurity for autonomous vehicles: Review of attacks and defense." Computers & Security 103 (2021): 102150.
- Kim, Shiho, et al. "In-vehicle communication and cyber security." Automotive Cyber Security: Introduction, Challenges, and Standardization (2020): 67-96.
- Lautenbach, Aljoscha. On Cyber-Security for In-Vehicle Software. Chalmers Tekniska Hogskola (Sweden), 2017.
- Lim, Hazel Si Min, and Araz Taeihagh. "Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications." Energies 11.5 (2018): 1062.
- Lu, Yang, and Li Da Xu. "Internet of Things (IoT) cybersecurity research: A review of current research topics." IEEE Internet of Things Journal 6.2 (2018): 2103-2115.
- Manuel Sandler, Autonomous Vehicle Cybersecurity: An Overview, CYRES CONSULTING (Jan. 27, 2023), https://www.cyres-consulting.com/autonomous-vehicle-cyber-security-overview/ (last visited Oct 6, 2023).
- Möller, Dietmar PF, and Roland E. Haas. Guide to automotive connectivity and cybersecurity. Springer International Publishing, 2019.
- Morris, David, Garikayi Madzudzo, and Alexeis Garcia-Perez. "Cybersecurity and the auto industry: the growing challenges presented by connected cars." International journal of automotive technology and management 18.2 (2018): 105-118.
- Parkinson, Simon, et al. "Cyber threats facing autonomous and connected vehicles: Future challenges." IEEE transactions on intelligent transportation systems 18.11 (2017): 2898-2915.
- Quintana, J. A., et al. "A Holistic Approach on Automotive Cybersecurity for Suppliers." Proceedings of the VEHICULAR (2023).
- Raimundo, Ricardo Jorge, and Albérico Travassos Rosário. "Cybersecurity in the internet of things in industrial management." Applied Sciences 12.3 (2022): 1598.

- Roberto Metere et al., An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure, (2022), http://arxiv.org/abs/2209.07842 (last visited Oct 6, 2023).
- Safa Hamdare et al., Cybersecurity Risk Analysis of Electric Vehicles Charging Stations, 23 SENSORS 6716 (2023).
- Sun, Xiaoqiang, F. Richard Yu, and Peng Zhang. "A survey on cyber-security of connected and autonomous vehicles (CAVs)." IEEE Transactions on Intelligent Transportation Systems 23.7 (2021): 6240-6259.
- Taiber, Joachim. Unsettled topics concerning the impact of quantum technologies on automotive cybersecurity. No. EPR2020026. SAE Technical Paper, 2020.
- Xie, Yong, et al. "Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: state-of-the-art and future challenges." Software: Practice and Experience 51.11 (2021): 2108-2127.
- Yağdereli, Eray, Cemal Gemci, and A. Ziya Aktaş. "A study on cyber-security of autonomous and unmanned vehicles." The Journal of Defense Modeling and Simulation 12.4 (2015): 369-381.
- Zia Muhammad et al., Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability, 16 ENERGIES 1113 (2023).