Risk-Based Security Frameworks for Vanets: A Systematic Review

Anubhav Kumar[1], Dr. Devender Kumar[2]
[1]*Research Scholar, Baba Mastnath University, Rohtak*
[2]*Assistant Professor, Baba Mastnath University, Rohtak*

***Abstract*—Vehicular Ad-Hoc Networks (VANETs) are essential for intelligent transportation systems, facilitating real-time data communication between vehicles and infrastructure. Nonetheless, their decentralized and open-access characteristics render them susceptible to several cyber dangers, requiring stringent security measures. This systematic analysis analyzes risk-based security frameworks aimed at improving the resilience of VANET against attacks like spoofing, denial-of-service, and data tampering. Through the examination of existing literature, we classify security models according to quantitative risk assessment approaches, pinpointing critical vulnerabilities and corresponding mitigation strategies. The research emphasizes the significance of machine learning, cryptographic methods, and trust-centric frameworks in enhancing the security of VANETs. We also review risk assessment models that measure the likelihood and consequences of cyber threats, enabling proactive security strategies. The findings indicate that the incorporation of adaptive security methods alongside real-time risk assessments can markedly improve VANET reliability. This analysis offers insights into prospective research avenues, highlighting the necessity for scalable, efficient, and context-aware security frameworks specifically designed for automotive networks.**

***Index Terms*—Vehicular Networks, Risk Analysis, Security Analysis etc.**

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) signify a crucial development in intelligent transportation systems, facilitating decentralized communication between vehicles and roadside equipment to optimize traffic management, enhance safety, and offer convenience to users. Nonetheless, as VANETs progress, their implementation encounters considerable obstacles regarding risk and security. Quantitative risk and security analysis has become essential for tackling these difficulties and ensuring the dependability and resilience of VANET systems.

The advancement of quantitative methodologies for risk and security assessment in VANETs entails the utilization of mathematical models and analytical procedures to find, analyze, and mitigate vulnerabilities. These methods concentrate on evaluating potential hazards, including data breaches, denial-of-service attacks, hostile nodes, and communication interruptions, which may jeopardize system integrity and safety.

The ongoing enhancement of these quantitative methods allows academics and practitioners to execute efficient risk management strategies, guaranteeing that VANETs operate securely under various traffic conditions. As VANETs become more incorporated into smart city infrastructure, rigorous quantitative analysis will be essential for ensuring reliability and enhancing system performance.

A vehicular ad hoc network (VANET) is a category of mobile ad hoc network that facilitates communication between vehicles and roadside infrastructure. This communication is predominantly wireless and serves multiple functions, including traffic management, safety notifications, and passenger entertainment services. VANET systems rely on vehicles operating as nodes inside the network, creating a dynamic and decentralized communication infrastructure on the road. These technologies are designed to enhance road safety by facilitating real-time communication between cars about road conditions, traffic patterns, and potential hazards. VANET systems provide communication between vehicles and infrastructure, thereby reducing accidents, improving traffic flow, and providing drivers with critical information for informed decision-making while driving. The potential benefits

of VANET systems make them promising technology for the future of transportation and smart urban environments. In addition to improving safety and efficiency, VANET systems can reduce emissions and fuel consumption by optimizing traffic flow and mitigating congestion. As more vehicles are equipped with communication technology, the network of connected vehicles will grow, hence enhancing the capabilities of VANET systems. As technology advances and the demand for intelligent transportation solutions increases, VANET systems are poised to profoundly impact the future of mobility and urban development. As metropolitan areas advance and become more interconnected, the integration of VANET systems will be essential for creating sustainable and efficient transportation networks.

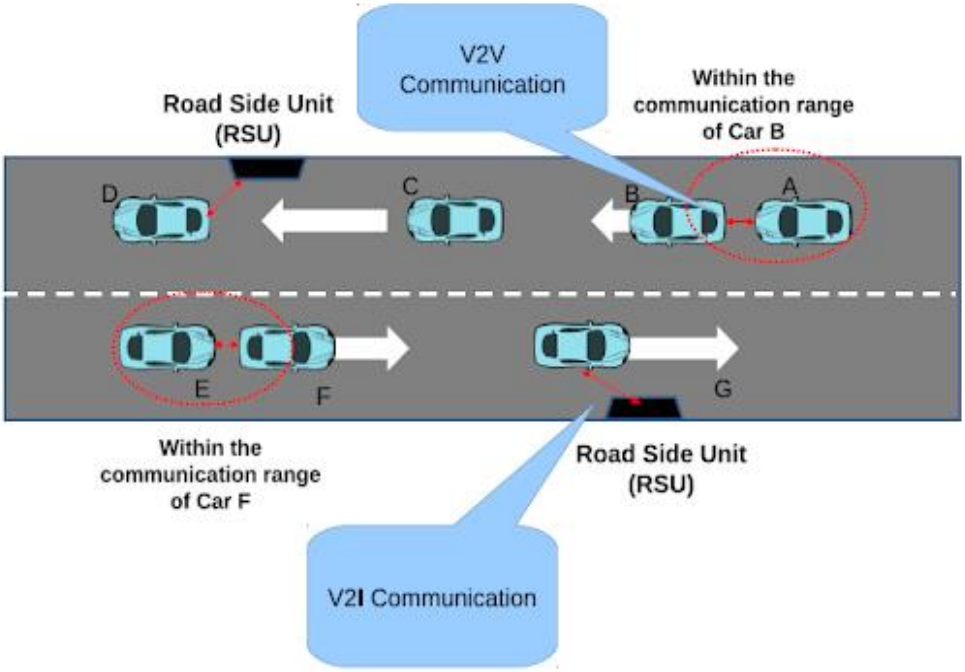

Fig 1: VANET System

(Source: http://article.sapub.org/10.5923.j.jwnc.20130303.02.html)

This integration will enhance traffic flow, alleviate congestion, promote safety, and enable more efficient routing for drivers. VANET systems can enhance traffic patterns and reduce the environmental effects of transportation by employing real-time data and enabling communication among vehicles, traffic lights, and infrastructure. Furthermore, the deployment of VANET systems can optimize the functioning of innovative mobility services, such as ride-sharing and autonomous vehicles, in metropolitan environments. The continuous development and implementation of VANET systems will be crucial for creating smarter, more linked cities that prioritize efficiency, sustainability, and safety in transportation. In a smart city employing VANET technologies, vehicles can communicate with traffic lights to adjust their speed and route in real-time, thus mitigating congestion and pollution. This technology enables the coordination of autonomous vehicles to efficiently gather passengers for ride-sharing services, hence improving urban transportation efficiency. Moreover, VANET systems enable the dissemination of information concerning road conditions, accidents, and hazards among vehicles, so allowing drivers to make educated decisions and reduce potential risks. This real-time data interchange enhances safety and increases the overall efficiency of transportation operations. The integration of VANET technology into urban infrastructure allows cities to enhance traffic flow, reduce travel times, and improve the general quality of life for residents.

VANET systems are crucial for shaping the future of smart cities and revolutionizing urban mobility.

2. INTRODUCTION OF QUANTITATIVE RISK ANALYSIS TECHNIQUES

Quantitative risk analysis methodologies are essential for guaranteeing the security and efficacy of a VANET system. Through quantitative analysis, urban planners can discern potential dangers and vulnerabilities inside the network, enabling them to execute targeted security measures to alleviate these threats. This proactive strategy not only improves the system's overall safety and stability but also fosters user trust, ultimately resulting in heightened adoption and utilization of VANET technology. In conclusion, the incorporation of quantitative risk analysis methodologies is vital for the effective growth and maintenance of a prosperous urban environment. City planners must consistently evaluate and monitor the security of the VANET system to respond to emerging risks and difficulties. By consistently upgrading and enhancing security protocols informed by quantitative risk analysis, municipalities may guarantee the sustained sustainability and efficacy of their VANET infrastructure. A proactive, data-driven approach to risk management would safeguard the system against future cyber assaults while instilling confidence and security among users, hence promoting the wider adoption and usage of VANET technology in contemporary urban settings. Cities can partner with cybersecurity experts and researchers to remain updated on developing threats and vulnerabilities within the VANET system. Investing in continuous training and education for IT and security personnel enables cities to establish a robust framework for proactive risk management and incident response. Ultimately, by integrating modern technology, strategic planning, and ongoing monitoring, communities may establish a safe and robust VANET system that improves the overall quality of life for both residents and visitors.

By cultivating collaborations with industry leaders and governmental entities, municipalities can obtain essential resources and exemplary practices to improve the security of their VANET networks. This cooperative strategy can assist cities in preempting cyber-attacks and maintaining the seamless functioning of their transportation systems. By emphasizing cybersecurity and investing in cutting-edge technologies, communities may cultivate a safer and more efficient urban environment for all inhabitants.

Moreover, municipalities might gain advantages by enforcing stringent rules and procedures that oversee the utilization of VANET networks. By implementing regulations concerning data privacy, network security, and driver conduct, municipalities can mitigate the threat of cyber assaults and guarantee the integrity of their transportation systems. Moreover, municipalities can implement emergency response protocols and communication channels to efficiently manage any disturbances or crises that may arise inside their VANET networks. By adopting a proactive and holistic strategy to cybersecurity, cities may protect their inhabitants and visitors while fostering sustainable urban development. In a city utilizing VANET technology, stringent controls can be established to encrypt important data exchanged between vehicles, so preventing illegal access. Furthermore, authorities can observe drivers conducting via the network to detect any possible hazards or infractions in real-time and implement suitable measures to ensure road safety.

3. IMPORTANCE OF RISK AND SECURITY ANALYSIS IN VANET SYSTEM

Conducting risk and security analysis in VANET systems is essential for identifying potential vulnerabilities and protecting sensitive information from cyber threats. By implementing rigorous security measures, like encryption protocols and authentication systems, communities may safeguard the integrity of their transportation networks and prevent malicious attacks. Furthermore, conducting regular risk assessments mitigates potential vulnerabilities and strengthens the resilience of VANET systems against future threats. Prioritizing risk and security evaluations in VANET systems is crucial for ensuring the reliability and effectiveness of smart city initiatives, as well as maintaining public confidence in the safety of urban mobility. By adopting a proactive approach and implementing comprehensive security measures, communities can preempt potential assaults and ensure the

uninterrupted operation of their transportation systems.

Furthermore, collaborating with diverse stakeholders, such as technology providers and cybersecurity experts, can generate essential insights and best practices to enhance the entire security framework of VANET systems. By emphasizing security, communities may create a safe and efficient transportation network that meets the needs of residents and visitors. Furthermore, investing in ongoing training and education for transportation professionals may ensure that security standards are consistently followed and updated as required. Regular audits and evaluations of security protocols can enable the detection and correction of vulnerabilities before they are exploited. By implementing a proactive security policy and fostering collaboration with industry experts, cities may effectively mitigate threats and maintain the trust of those reliant on their transportation networks. Ultimately, prioritizing security in urban transportation enhances public safety and elevates the overall quality of life in a community.

By implementing rigorous security standards, towns may create a safer environment for residents and visitors alike. This could enhance trust in using public transit and so improve the system's efficiency and dependability. Furthermore, investing in security can generate economic benefits by attracting more businesses and tourists to the region. Emphasizing security in urban mobility is essential for cultivating a thriving and sustainable urban ecosystem. The installation of surveillance cameras and the employment of security personnel in subway stations can mitigate criminal behavior and improve passenger safety. This improves the public transportation experience and fosters a sense of security, hence promoting more usage of the system, which leads to an increase in passengers and money for the city.

4. SECURITY REQUIREMENTS FOR VANET

In VANET, various security measures improve road safety and security, including system and information availability, authentication, data integrity, participation of authenticated nodes, non-repudiation, and secrecy, among others. The security specifications of the VANET are explicitly outlined in Table 1.

Table 1: Security Requirements in VANET

Security Requirements	Description
Privacy	Future and present vehicle location data cannot be accessed by third parties or unauthorized individuals, increasing driver privacy
Data Secrecy	Data exchanged in the VANET environment must be secure to maintain the data integrity level and avoid malicious attempts to modify data
Access Control	This control is essential in the VANET environment as privileges are provided so that certain roles can be performed, e.g., it allows nodes to perform certain functions when they possess authorised privileges
Authentication	Authentication ensures that only legitimate nodes can transmit and receive data in the network, thus preventing the participation of selfish nodes and increasing the security level
Integrity of Data	Having data integrity ensures that the data received by the driver is transmitted by a legitimate node and has not been modified
Nonrepudiation	This allows the VANET system to reduce the rate of message denial, i.e., the sender denies the act of transmitted data
System and Data Availability	Data and system availability are crucial in the VANET environment to achieve high QoS regarding reduced end-to-end latency, minimum waiting time, and fast response time

Source: https://www.researchgate.net/figure/Security-Requirements-in-VANETs-4_fig2_363198544

5. REVIEW OF LITERATURE

Ashrafi et al. (2022) demonstrated that this research introduced an innovative risk management strategy to formulate a Time-Cost Trade-off (TCT) mathematical model amongst fuzzy ambiguity. This work proposed a Linear Assignment Method (LAM) to rank project tasks based on the risks they incur when subjected to crashing. Secondly, activities were categorized into several classes based on their risk degree to prioritize high-risk activities. Ultimately, risk response techniques were delineated, and the outcomes are rigorously analysed. Owing to enhanced precision in addressing uncertainty and the benefits of interval type-2 fuzzy sets (IT2FS), this fuzzy set was utilized throughout the entire process. A real project from a gas sector company was utilized to assess the performance of the procedure.

Xin et al. (2023) demonstrated that Vehicle Ad-hoc Networks (VANET) were interconnected by message forwarding and exchange across vehicle nodes. VANET was particularly susceptible to security threats from various entities due to its highly dynamic architecture and wireless, heterogeneous connection style. In contrast to entity-based security authentication, it was crucial to focus on safeguarding the integrity of the data itself. To address the concerns, this study proposed an effective VANET architecture featuring a secure reputation system based on blockchain technology, termed the double-layer blockchain-based reputation evaluation and management model (DBREMM). In the DBREMM, it developed a reputation management model utilizing two parallel blockchains that operate in conjunction, referred to as the event chain and reputation chain. It proposed an indirect trust calculation utilizing the historically accumulated reputation value with an attenuation factor, alongside a secure reputation fusion scheme predicated on a numerical threshold with a fluctuation factor, aimed at mitigating the risk of attacks, including collusive attacks and false information injection. Theoretical study and comprehensive simulation studies demonstrated the effectiveness, precision, and resilience of the DBREMM security algorithm against various threats.

Fetais et al. (2023) indicated that information technology (IT) security requirements were routinely revised in a swiftly evolving technical landscape to keep abreast of emerging technologies. This study was prompted by the recognition that existing IT risk-management frameworks could offer sufficient protection for small- and medium-sized organizations (SMEs), particularly those embracing new technology. It determined that a dynamic IT risk-management framework, revised to incorporate emerging technology advancements, would enhance security and privacy for SMEs. It performed a systematic literature evaluation from 2016 to 2021, concentrating on IT risk management research across several application domains. This study demonstrated that, although existing frameworks such as NIST offer advantages, it might be more appropriately tailored to the specific requirements of SMEs because to their considerable abstractness, ambiguous standards, and insufficient adaptability to technological progress. The results indicated an urgent necessity to develop IT risk-management frameworks, especially by integrating sophisticated techniques such as system dynamics, machine learning, and technoeconomic and sociotechnological models.

Kanna et al. (2023) demonstrated that the proposed methodology uses a Residual Convolutional Neural Network (RCNN) architecture to extract characteristics from real-time traffic data obtained from VANETs. The collected features were subsequently employed to forecast traffic flow and detect potential hazards on the roadway. The RCNN model had been trained and evaluated on a real-world dataset, demonstrating superior accuracy and efficiency compared to other existing models. The study compared traditional VANET routing methods with metaheuristic methodologies and examined the VANET simulation scenario for experimental analysis. The experimental findings indicated that the GACNN method surpasses particle swarm optimization (PSO), ant colony optimization (ACO), and ad-hoc on-demand distance vector (AODV) routing protocols across three distinct VANET network models, with average improvements of 1.37%, 1.82%, and 1.41%, respectively.

Mejia et al. (2023) indicated that the integration of technologies across all industries has rendered cybersecurity risk assessment an essential component of cybersecurity risk management. Nonetheless, risk assessment could be a complex undertaking for enterprises. The primary objectives of this paper were

to: (I) delineated the distinctions (reference models and applications) and scope of the principal qualitative and quantitative models, (II) ascertained pertinent risk assessment variables, (III) proposed a risk assessment model (qualitative and quantitative) that incorporates the principal variables and sub-stages of the risk assessment phase, and (IV) solicited an evaluation of the proposed model from experts in the domain of cybersecurity. The proposal was submitted to a cohort of 28 cybersecurity professionals who endorsed the proposed variables and their significance in the cybersecurity risk assessment phase, noting a predominant utilization of qualitative tools while expressing a preference for quantitative tools.

Li et al. (2024) presented an unlikable and revocable sign cryption scheme (URSCS), employing an efficient and robust sign cryption technique for communication. This approach accommodated either numerous receivers or a single receiver through the implementation of the identifying public key, with the receiver being either roadside units (RSUs) or automobiles. A comprehensive revocation system was developed with little communication overhead, employing the Chinese remainder theorem (CRT). Both formal and informal security studies indicated that this URSCS system satisfied the anticipated security and privacy standards of VANETs.

Tariq et al. (2024) concentrated on creating effective detection techniques and countermeasures to alleviate the effects of DDoS assaults in VANETs. The study employed a blend of statistical analysis and machine learning methods, specifically Autoencoder with Long Short-Term Memory (LSTM) and Clustering with Classification, to present novel strategies for real-time anomaly detection and the development of system resilience. The emulation findings validated the efficacy of the proposed methodologies in detecting and mitigating DDoS assaults, markedly enhancing the security posture of a highly mobile ad hoc network with a 94 percent anomaly detection rate. This research advanced the attempts to protect VANETs from DDoS attacks and established a foundation for more robust intelligent transportation system architectures.

Table 2: Summary of Literature Survey

Author(s)	Year	Objectives	Results
Li et al.	2024	Proposed an unlinkable and revocable sign cryption scheme (URSCS) for VANETs using polynomial-based session keys and anonymization methods.	Achieved enhanced privacy and security while minimizing communication overhead using the Chinese remainder theorem (CRT).
Tariq	2024	Developed optimized feature selection techniques for DDoS attack detection and mitigation in SD-VANETs using machine learning methods.	Obtained a 94% anomaly detection rate, significantly improving VANET security resilience.
Hou et al.	2023	Proposed a double-layer blockchain model for VANET secure reputation evaluation and management.	Established a decentralized trust framework enhancing vehicle authenticity and communication integrity.
Al-Dosari & Fetais	2023	Developed a meta-analysis framework for risk management in SMEs with a focus on cybersecurity and information security systems.	Provided insights into optimal security configurations and risk mitigation strategies for SMEs.
Rajesh Kanna R.	2023	Identified risks and predicted traffic conditions in VANETs using AI technologies.	Improved accuracy in traffic forecasting and security risk identification.
Sánchez-García et al.	2023	Conducted a systematic mapping review on cybersecurity risk assessment methodologies.	Proposed and validated a structured risk assessment framework for cybersecurity threats.

Jyothi & Patil	2022	Developed a fuzzy-based trust evaluation framework for privacy preservation and secure authentication in VANETs.	Enhanced privacy preservation and authentication security, reducing malicious node influence.
Patel et al.	2022	Reviewed the security challenges in Internet-of-Vehicles (IoV) communications and proposed solutions.	Identified key vulnerabilities and effective security mechanisms for IoV systems.
Vetrivelan & P	2022	Proposed an enhanced security module (ESM) for traffic signal control in VANET-based smart cities.	Improved security and efficiency in traffic management using VANET-based protocols.
Zeddini et al.	2022	Examined security threats in Intelligent Transportation Systems (ITS) and their risk levels.	Categorized risk levels and provided mitigation strategies to enhance ITS security.

RESEARCH GAP

- Although numerous risk assessment frameworks are available, no globally recognized model is specifically designed for VANETs. Numerous research provides approaches; nevertheless, they frequently lack empirical confirmation.
- Many security models emphasize cryptographic methods, although they inadequately tackle multi-layer security weaknesses, especially those that extend beyond the MAC layer.
- Contemporary risk assessment methodologies frequently depend on static models that fail to adapt dynamically to the extremely fluid and unpredictable environment of VANET.
- Numerous proposed security solutions necessitate substantial processing resources, rendering them impracticable for extensive VANET implementations.
- Research on the interaction of security mechanisms across several layers of VANET communication protocols is sparse, resulting in possible inefficiencies and undetected vulnerabilities.

6. OBJECTIVES OF WORK

The main objectives of work are:

- To develop a novel technique to risk assessment in order to analyze the risk of attack against VANET availability
- To analyze a Trust Model with Group Leader (GL) based communication in VANET.

7. CONCLUSION

The systematic analysis of risk-based security frameworks for Vehicular Ad-hoc Networks (VANETs) has underscored significant breakthroughs, problems, and research deficiencies in the domain. The dynamic characteristics of VANETs, marked by high mobility, decentralized architecture, and wireless communication, necessitate sophisticated security measures that effectively evaluate, anticipate, and mitigate hazards. VANETs are particularly vulnerable to cyberattacks such as Sybil attacks, denial-of-service (DoS), data manipulation, and spoofing, hence requiring risk-based security frameworks. Current security frameworks face challenges regarding scalability and computing efficiency, rendering them unsuitable for extensive implementation. Novel methodology, such as autoencoders, deep learning models, and hybrid approaches, improve risk detection precision but are devoid of defined implementation procedures. Despite substantial advancements in risk-based security frameworks within VANETs, notable research deficiencies remain in real-time risk adaptation, cross-layer security interdependencies, and post-quantum cryptographic robustness. Future advancements must incorporate interdisciplinary methodologies, utilizing AI-driven predictive analytics, decentralized frameworks, and scalable security infrastructures to guarantee secure and efficient communication throughout VANET ecosystems.

REFERENCES

[1] Li, L.; Chen, D.; Liu, Y.; Liang, Y.; Wang, Y.; Wu, X. 2024, Unlinkable and Revocable Sign cryption Scheme for VANETs. Electronics, 13, 3164. https://doi.org/10.3390/ electronics13163164.

[2] Tariq, U. (2024), Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs. World Electrical Vehicular Journal, 15, 395. https://doi.org/10.3390/ wevj15090395

[3] Hou, B., Xin, Y., Zhu, H., Yang, Y., & Yang, J. (2023). VANET Secure Reputation Evaluation & Management Model Based on Double Layer Blockchain. Applied Sciences, 13(9), 5733. https://doi.org/10.3390/app13095733

[4] Al-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. Electronics, 12(17), 3629. https://doi.org/10.3390/electronics12173629

[5] Rajesh Kanna R., (2023), Risk identification and traffic prediction based on AI Technologies in VANET, Journal of Survey in Fisheries Sciences, pp. 4084-4089.

[6] Sánchez-García, I. D., Mejía, J., & Gilabert, T. S. F. (2023). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. Applied Sciences, 13(1), 395. https://doi.org/10.3390/app13010395.

[7] Jyothi, N., & Patil, R. (2022). A fuzzy-based trust evaluation framework for efficient privacy preservation and secure authentication in VANET. Journal of Information and Telecommunication, 6(3), 270–288. https://doi.org/10.1080/24751839.2022.2040898

[8] Patel S., Talib, M. A., Abbas, S., Nasir, Q., & Mowakeh, M. F. (2022). Systematic literature review on Internet-of-Vehicles communication security. International Journal of Distributed Sensor Networks, 14(12), 01-10. https://doi.org/10.1177/1550147718815054

[9] V, H. Vetrivelan, & P, V. (2022). Vanets Based Traffic Signals Controlling with Enhanced Security Module (ESM) In Smart Cities. Indian Journal of Computer Science and, 13(4), 1254–1263. https://doi.org/10.21817/indjcse/2022/v13i4/221304129

[10] Zeddini, B., Maachaoui, M., & Inedjaren, Y. (2022). Security Threats in Intelligent Transportation Systems and Their Risk Levels. Risks, 10(5), 91. https://doi.org/10.3390/risks10050091

[11] Haghighi, M. H., & Ashrafi, M. (2022). A new qualitative and quantitative analytical approach for risk management in energy project time-cost trade-off problem under interval type-2 fuzzy uncertainty: A case study in the gas industry. Energy Reports, 8, 12668–12685. https:// Engineering doi.org/10.1016/j.egyr.2022.09.064

[12] Pekaric, I., Sauerwein, C., Haselwanter, S., & Felderer, M. (2021). A taxonomy of attack mechanisms in the automotive domain. Computer Standards & Interfaces, 78, 103539. https://doi.org/10.1016/j.csi.2021.103539