

## Identification of cyber threats in IoV communication: A systematic literature review

Naeem Ullah<sup>1</sup>, Iftikhar Ahmad<sup>2</sup>, Abdulaleem Ali Almazroi<sup>3</sup>, Mujeeb Ur Rahman<sup>4</sup>

<sup>1</sup>Software-Engineering-Research-Group (SERG-UOM), Department of Computer Science and IT, University of Malakand, Pakistan,

<sup>2</sup>Centre for Autonomous and Cyberphysical Systems, Cranfield University, Bedford MK43 0AL, UK

<sup>3</sup>Department of Information Technology, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Rabigh 21911, Saudi Arabia

<sup>4</sup>School of Computer Science and Informatics, De Montfort University, LE1 9BH, Leicester, UK

### Abstract

Internet of Vehicles (IoV) plays an essential role in the intelligent transportation system that contributes to traffic congestion reduction, road safety, pollution reduction, and efficient travel. However, the growing reliance on communication technologies subjects IoV to a wide range of cyber threats, such as privacy violations, message malware, spoofing, and denial-of-service attacks. The paper involves a Systematic Literature Review (SLR) to determine and evaluate cyber threats in the IoV communication. After a systematic search and quality evaluation, 83 primary research studies were examined, and as a result, eight key categories of threats were identified. According to the findings, denial-of-service and distributed denial-of-service (DDoS) attacks, spoofing and impersonation, and falsified information attacks are the most reported risks. These insights represent a broad view of the existing vulnerabilities in the communication of the Internet of Vehicles and countermeasures are required to address the identified cyber-threats. The findings of this review would inform other researchers, policy makers, and industry practitioners to establish effective countermeasures to enhance IoV security before its wide-scale implementation.

**Keywords:** Cyber threats, Internet of Vehicles, Vehicular communication, Security, Intelligent Transportation Systems

## 1 Introduction

The Internet of Vehicles (IoV) is a complicated system of vehicles communicating with each other by means of the Internet. It uses communication technologies to facilitate synchronization between the vehicles, roadside units and pedestrians. However, the propagation of connected vehicles poses numerous cyber threats that should be taken into consideration as they may severely affect road safety and cause traffic congestion and accidents. [1]. The report of the Federal Highway Administration of the USA claims almost 16,000 highway accidents in the USA daily [2]. Moreover, IoV has now become an important element of contemporary communication, which has drawn significant attention from practitioners and researchers [3]. The statistical reports show that in 2019, the autonomous vehicles market value amounted to 131.9 billion US dollars globally [4]. In IoV environments, sensors gather pertinent data and send it via cloud storage to process it. Some of the IoV applications include reduced traffic congestion, collision prevention, and best route selection [5].

To achieve these benefits, IoV data should be authentic and reliable. Confidentiality and security in vehicular communication are thus a necessity for user trust and safety. Any falsified or manipulated safety information can result in traffic jams and accidents because even a single bit of manipulation can change the interpretation of the whole message [5].

Additionally, IoV is a new concept that should be properly investigated before being widely implemented. It is essential to determine the possible cyber threats and ways to mitigate them. IoV security is actively being developed by researchers across the globe, though the recent challenges, as well as the current solutions to them, still constitute an urgent concern. As a directive towards this research, the following research questions were developed.

**RQ1:** What are the recent cyber threats in the IoV vehicular communication? Such a question aims at finding a list of potential cyber threats based on a systematic review.

**RQ2:** Do the identified threats vary based on publication year, sources nature and geographical distribution of sources?

## 2 Related Work

Harsha Vasudev et al. [6] paid special attention to the security of message transmission within the systems of the IoV, and they suggested a lightweight protocol which is aimed at protecting against different types of attacks. These communication standards focus on various IoV elements, which are V2V, and Vehicle-to-Infrastructure (V2I). Jin Cui et al. [7] provide the review of security attacks and autonomous vehicle countermeasures. Their work gives a detailed study of the found attacks to promote knowledge of the found vulnerabilities and their related countermeasures.

According to Surbhi Sharma and Baijnath Kaushik [8], described that the world today has approximately one billion existing commercial and passenger vehicles, which are likely to be two billion by 2035. In the context of such fast development, better road safety and comfort of passengers, as well as traffic surveillance, are required to avoid accidents. Besides the examination of the security threats and mitigation, the authors suggested a lightweight authentication protocol of the Radio Frequency Identification (RFID) devices on the basis of the argument that the lightweight authentication protocol enhances the performance of the IoV with regard to the use of CPU, memory, and detection time. Nevertheless, they also pointed out that there are numerous IoV issues that are yet to be addressed.

The authors of the article in [9], noted that the IoV is also categorized by serious challenges in areas of privacy, reliability, and safety because it relies on such types of communication as V2V, V2I, Vehicle-to-Roadside (V2R), and Vehicle-to-Pedestrian (V2P). They are susceptible to eavesdropping, spoofing, denial of service (DoS) and replay attacks. To overcome these threats, they came up with a Fine Tree-based Intrusion Detection System (IDS). However, due to the enthusiasm in the development of the IoV systems, new threats are bound to arise, and it is important to detect and mitigate them in time.

In [10], an IoV wireless sensor network was offered a customized communication security framework, which handles technical and scientific issues in the context of an efficient encryption model. Since a vehicle is constantly collecting and transmitting sensitive information like speed, position and brake condition, there is a need to have secure protocols in place to ensure that the information is not mistreated. The structure will provide the privacy wherein the cryptographic keys are produced without revealing the parameters and the session keys are relayed in encrypted format.

According to the literature above, it is evident that the detection of recent cyber threats occurring in the IoV communication systems plays a critical role. As the system of IoV is based on various communication platforms and connectivity, which is operated by sensors, new vulnerabilities can be expected to emerge. Researchers and stakeholders are required to continue their work in order to ensure that they develop robust solutions to the new cyber threats to the IoV systems.

### 3 Research Methodology

We adopted a Systematic Literature Review (SLR) in this study. SLR is a form of scientific evidence synthesis to respond to the developed research questions. SLR is open and replicable, whereas it aims to incorporate all the available published evidence on the subject and the quality of that evidence. In the SLR approach, we carefully look through the literature about the identification of cyber threats with them in the context of IoV communication. The protocol development is the initial stage of SLR. First, we have created the protocol and discussed it in [11]. The SLR was conducted according to the recommendations presented in [12], which were altered to be implemented in transport/smart mobility systems [13, 14].

#### 3.1 Search Strategy

In order to select relevant sources, we utilized a structured search strategy for the SLR. The search strategy is outlined as follows:

- Search terms were constructed upon the documentation of the Population, Intervention, and Outcome (PICO).
- Associated synonyms and alternative spellings were identified.
- Verified keywords from related studies were incorporated.
- Boolean operators were applied to refine and broaden the search as necessary.

The inclusion/exclusion criteria and quality assessment checklist are vital and documented upon the suggestions provided in [15]. This approach has been adopted by other researchers [16-18]. Table 1 illustrates the elements of Population, Intervention, and relevant Outcomes taken as the PICO criteria.

**Table 1.** PICO criteria

| PICO                  | Results                                              |
|-----------------------|------------------------------------------------------|
| Populations           | IoV, Vehicular Communication                         |
| Intervention          | Enhancing IoV communication security                 |
| Experimental Design   | Systematic Literature Review                         |
| Significance Outcomes | List of threats within the IoV communication system. |

The research question is designed as presented below:

[What are the cyber threats in the IoV communication system? To recognize threats and address each threat to enhance the IoV communication security?].………….”INTERVENTION”

within [IoV communication].………….”POPULATION”

To be used for [IoV communication security].………….”SIGNIFICANCE OUTCOMES”

PICO criteria, as shown in Table 1, assist us in generating a search string using the researched questions and we got a minimum of 6 search terms. We applied these keywords in the scholarly databases, as well as, Google search engine and identified synonyms used in the articles that were found. These synonyms are linked with Boolean operators as they appear in Table 1. Eventually, we were able to come up with the search string as given below to locate the threats in the IoV communication system:

(Issues OR Challenges OR threats) AND (“IoV communication” OR “vehicular communication” OR “V2V communication” OR “V2X communication”).

Table 2 and Table 3 show the study strategy (keywords, synonyms and SLR results), respectively. The research design involved an intensive review of each stage of the search method and the publication by specialists. The design of the review did not indicate any major problem.

**Table 2.** Keywords synonyms

| Keyword                    | Synonyms                                                                                                                           |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| “Secure IoV communication” | Issues OR<br>Threats OR<br>“IoV communication” OR<br>“Vehicular Communication” OR<br>“V2V Communication” OR<br>“V2X Communication” |

In these libraries, the following digital libraries used the search string to search relevant literature:

- IEEE Xplore
- Wiley Online Library
- ScienceDirect
- Google Scholar (Search Engine)

**Table 3.** SLR Search Results

| Search string                          | Digital Libraries | Total Results | Initial Selection | Final Selection |
|----------------------------------------|-------------------|---------------|-------------------|-----------------|
| (Issues OR Challenges OR threats) AND  | Science Direct    | 780           | 73                | 19              |
| AND (“IoV communication” OR “vehicular | Springer Link     | 180           | 23                | 07              |
| communication” OR “V2V communication”  | ACM               | 235           | 63                | 21              |
| OR “V2X communication”).               | IEEE Xplore       | 435           | 105               | 18              |
|                                        | Google Scholar    | 135           | 37                | 13              |
|                                        | (Search engine)   |               |                   |                 |
|                                        | Snowballing       | 42            | 31                | 05              |
| Total                                  |                   | 1807          | 332               | 83              |

The snowballing technique was adopted as a post-search technique to fetch the other relevant literature that was possibly omitted during the initial search in databases. It was conducted with the use of forward and backward snowballing (the review of the reference list of the existing sources and new sources that are followed, which are cited in the chosen works respectively). With this, it was possible to identify more relevant responses and thus enhanced the sample size [19-21]. The method has been used by other researchers as well in making their literature reviews more comprehensive [22-25]. The overall description of the SLR procedure is presented in Figure 1.

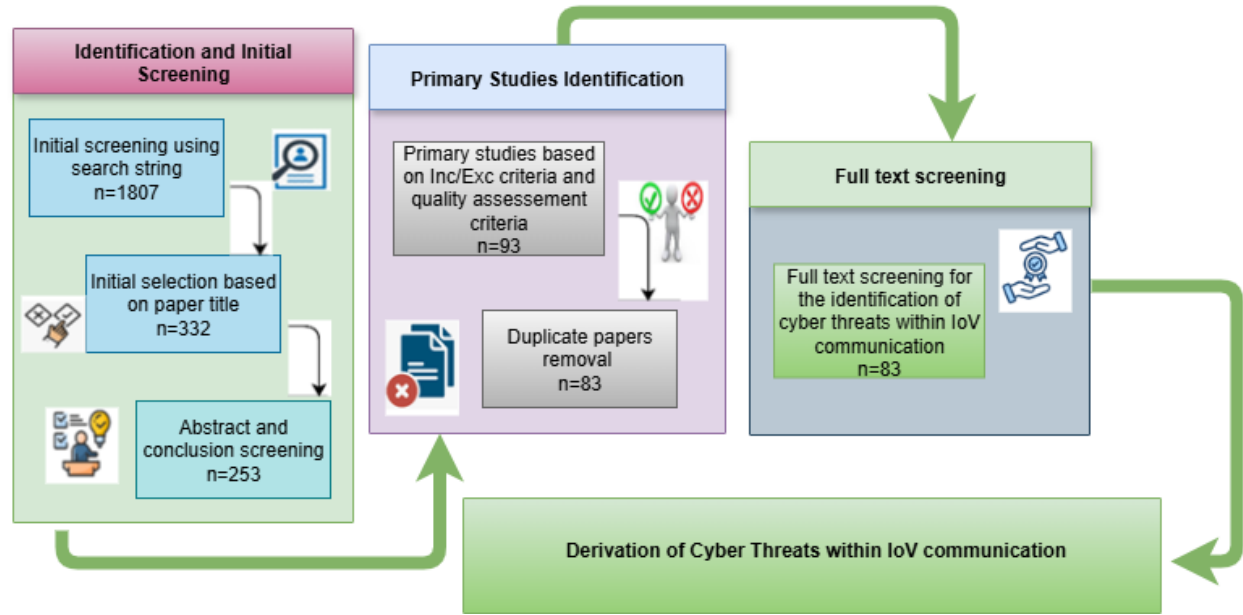


**Fig 1.** SLR process overview

### 3.2 Inclusion/Exclusion Criteria

To strengthen the final sample quality, we applied well-defined inclusion/exclusion criteria to filter the retrieved articles, as shown in Table 4. These criteria were designed to extract only the most pertinent studies related to IoV communication systems, particularly in terms of enhancing communication security.

**Table 4.** Inclusion and Exclusion Criteria

| Inclusion Criteria                                                             | Exclusion Criteria                                                                                    |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Articles that specifically focus on cyber threats within IoV communication.    | Articles unrelated to predefined research queries.                                                    |
| Articles in the English language.                                              | Articles that don't define any issue or relevant solution regarding secure IoV communication systems. |
| Published articles in journals or conferences.                                 | Studies those are not fully accessible online.                                                        |
| Articles addressing challenges, risks related to the IoV communication system. | In cases of duplicate content, only the most recent publication was retained.                         |

### 3.3 Quality evaluation

To measure the final sample quality and reduce the possible bias, we established a list of evaluation parameters with the help of which we assessed which studies were relevant and conditional [26, 27]. Here, we adhered to the checklist suggested by Kitchenham and Charters [26, 28], to design the Quality Assessment (QA) criteria. Table 5 shows the QA questions that are applied in the assessment of the published articles.

**Table 5.** Quality Assessment Criteria

| No   | Quality Assessment Criteria                                                                                | Answer  |
|------|------------------------------------------------------------------------------------------------------------|---------|
| QA-1 | Does the selected article respond to the study problem?                                                    | 1/0/0.5 |
| QA-2 | Does the article possess a clear research purpose?                                                         | 1/0/0.5 |
| QA-3 | Does the article accurately describe the intended research technique?                                      | 1/0/0.5 |
| QA-4 | How were the problems in the IoV communication systems in the article identified, determined or evaluated? | 1/0/0.5 |
| QA-5 | Is the article a journal or conference publication?                                                        | 1/0/0.5 |

As part of the quality assessment process, each question in the QA checklist was evaluated using a three-point scale: 1, 0.5 and 0 for each article. This scoring approach was applied to formal literature. According to the evaluation, the primary studies that scored above 60 percent in answering the QA questions were 13, 23 percent scored above 70 percent and 21 articles scored above 80 percent. Such findings suggest that the chosen primary sources were mostly pertinent and of reasonable quality in terms of the research questions. Sources with a quality score of less than 2/5 (i.e. less than 40 percent) were out of the scope of the further analysis because of the lack of evidence. Three studies were hence excluded in the process as part of quality screening to have a refined dataset to be analyzed later. Criteria used to evaluate the quality were developed to determine the publication scores and these criteria were used to devise the final published articles list. The primary purpose of the quality assurance was to eliminate the low-quality studies and maximize the validity of the evidence applied in this review [29, 30].

### 3.4 Papers Selection

The source screening was first performed after the title and abstract of the search results were screened. The last step in the selection process was achieved in the second step where the full-text articles that had been found during the first step underwent further scrutiny. Further, the data were extracted using the sources that were also selected in accordance with the inclusion and exclusion criteria and the quality evaluation criteria. 83 publications in total were finally chosen in formal literature.

### 3.5 Extraction of Data

The application of the primary sources in the ultimate research procedure enabled us to assemble the required data to respond to the fundamental objectives of this research. As a summary of the identified challenges, along with their incidences and proportions in answering the research questions, we did a synthesized tabular summary (with columns titled (including columns titled Threats ID, Threats Name, Frequency, and Percentage) as presented in Table 6. The primary reviewer synthesized the data, and it was then reviewed by a second reviewer. The second reviewer sampled the list of reviewed articles randomly and independently retrieved the information on the articles reviewed by the first reviewer. The findings were then compared to the past results of the original reviewer and no significant results were found. The main reviewer first determined 12 threats. Upon additional consideration of the secondary reviewer, we integrated the recommended changes and came up with a final list of 8 different threats that have been displayed in Table 6.

## 4 Results and Discussion

As a response to RQ1, we defined a group of threats in the systems of the IoV communication with the help of SLR, and this is provided in Table 6. The most common one is CT-2: denial and distributed denial of service (DDoS) attacks, which were reported in 47% of the studies. Eight major problems were then identified and synthesized out of the 83 studies sampled. There were 12 cyber threats that were identified during data synthesis, however, through

meticulous review and the combination of like terms, the list was narrowed down to eight threats. These completed threats, as indicated in Table 6, give a holistic view of cyber threats in the systems of IoV communication.

**Table 6.** Cyber threats within the IoV communication system

| Threats ID | Threats Name                                     | Frequency | Percentage |
|------------|--------------------------------------------------|-----------|------------|
| CT-1       | Falsified-Information Attack                     | 29        | 35%        |
| CT-2       | Denial and distributed denial of service attacks | 47        | 57%        |
| CT-3       | SQL and fuzzy injection attacks                  | 9         | 11%        |
| CT-4       | Lack of software and hardware protection         | 13        | 16%        |
| CT-5       | Ransom-ware Attacks                              | 11        | 13%        |
| CT-6       | Message replay and spamming attacks              | 23        | 28%        |
| CT-7       | Spoofing and impersonation attacks               | 43        | 52%        |
| CT-8       | Lack of communication channel reliability        | 7         | 8%         |

Examining Table 6, DOS and DDoS attacks seem to be the most prevalent in the literature. This attack should be mitigated to avoid interference in communication, especially in times of emergency [31]. It is thus advisable that researchers and decision-makers apply machine learning methods to address these threats. In the second position are spoofing and impersonation attacks, 52 percent of the studies reviewed mentioning them. In IoV communication, there is a possibility of accidents and the latency to transmit messages due to false signals and spam messages [32-34]. Machine learning-based countermeasures are also necessary to counter these attacks. Similarly, falsified information attacks are ranked third. Under these circumstances, it is important to ensure that VANETs are secured because an attacker can use them to invade the privacy of drivers or passengers [8].

To address RQ2, the detailed sources are represented in the figures given below. The year-wise publication distribution is depicted in Figure 2, with the X-axis represent the years whereas the Y-axis represent the published articles frequency in a particular year. The highest point was observed in 2024, and it can be seen that the issue of IoV security has increased more significance and the efforts to respond the recent threats in cyberspace are being more actively researched. The nature of sources is shown in Figure 3 and includes 56 journals and 27 conference papers. Figure 4 shows the geographical distribution where the majority of articles are in Europe, then Asia and then America. The publications are divided into two categories in Figure 5: 2012-2018 (30 articles) and 2019-2024 (53 articles). This is because of the increased number of recent publications, which shows that researchers and decision-makers are already attempting to solve the problem of the security of IoV even before it is widely implemented. Overall, this paper systematically demonstrated recent cyber threats in the area of IoV communication. Researchers and stakeholders have a responsibility to make sure that such threats are mitigated at an earlier stage of large-scale implementation of IoV in order to minimize the risks and prevent accidents.

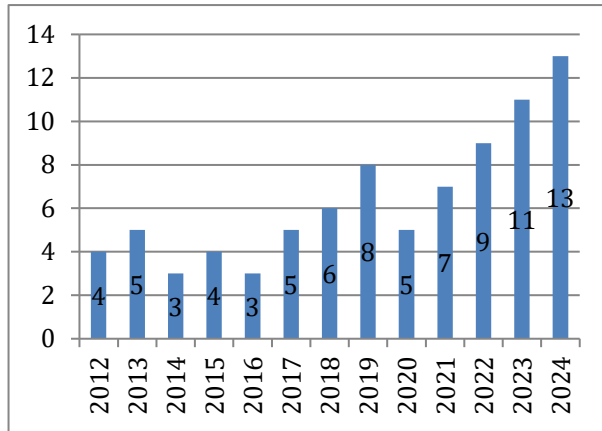


**Fig 2.** Year-wise publication sources

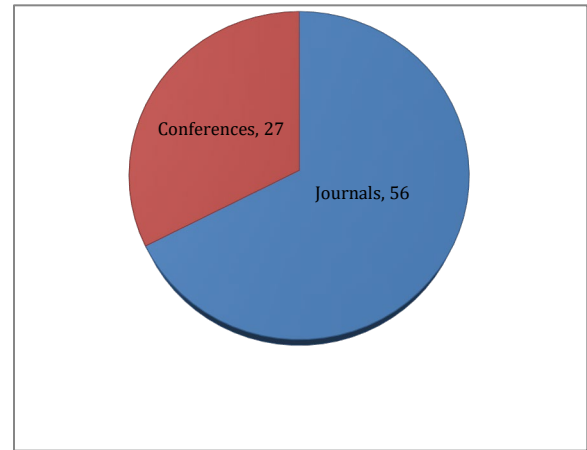


**Fig 3.** Nature of sources

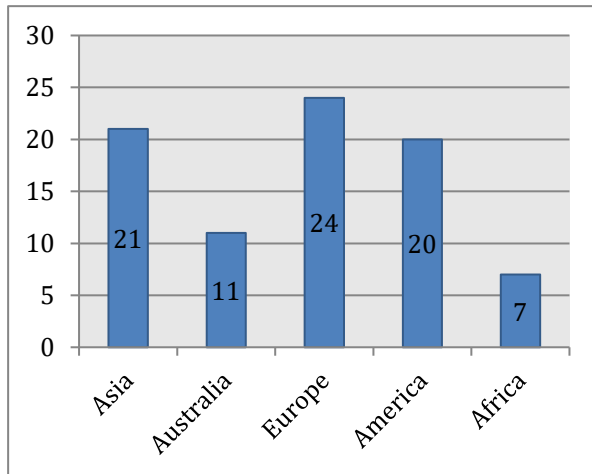


**Fig 4.** Geographical distribution of sources

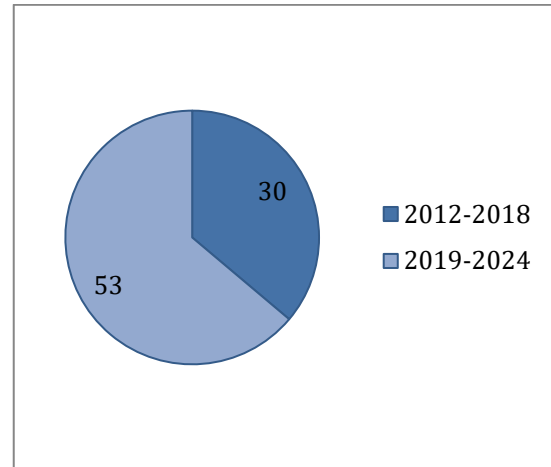


**Fig 5.** Period of sources

## 5 Conclusion

In this study, we have systematically reviewed 83 articles that are relevant to vehicular communication systems. The SLR helped us in the identification of eight major cyber threats to IoV communication system as shown in Table 6. The most mentioned threats are the denial and distributed denial of service attacks, the spoofing and impersonation attacks, and the falsified information attacks. The paper has provided various analyses such as year of publication, type of sources, geographical spread and period covered by the studies. We intend to empirically confirm the SLR results in the future by conducting an online survey of people with expertise in the area of automotive communication to determine any similarities and differences between the literature and the perspective of the

practitioners. We intend to carry out another SLR to explore mitigation measures to address these cyber threats so that the security of IoV communication can be strengthened. Finally, the author intends to develop a Cyber Threat Mitigation Model (CTMM) based on the results of the SLR and expert opinions in order to assist automotive organizations evaluate their readiness to secure vehicular communication systems.

## References

1. K. Lin, C. Li, G. Fortino, and J. J. Rodrigues, "Vehicle route selection based on game evolution in social internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, pp. 2423-2430, 2018.
2. K. Hartman and J. Strasser, "Saving lives through advanced vehicle safety technology: Intelligent vehicle initiative," United States. Federal Highway Administration, 2005.
3. K. Guan, D. He, B. Ai, D. W. Matolak, Q. Wang, Z. Zhong, et al., "5-GHz obstructed vehicle-to-vehicle channel characterization for internet of intelligent vehicles," *IEEE Internet of Things Journal*, vol. 6, pp. 100-110, 2018.
4. N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE internet of things journal*, vol. 1, pp. 289-299, 2014.
5. I. García-Magariño, G. Palacios-Navarro, R. Lacuesta, and J. Lloret, "ABSCEV: An agent-based simulation framework about smart transportation for reducing waiting times in charging electric vehicles," *Computer Networks*, vol. 138, pp. 119-135, 2018.
6. H. Vasudev, D. Das, and A. V. Vasilakos, "Secure message propagation protocols for IoVs communication components," *Computers & Electrical Engineering*, vol. 82, p. 106555, 2020.
7. J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Networks*, vol. 90, p. 101823, 2019.
8. S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, p. 100182, 2019.
9. P. K. Tiwari, S. Prakash, A. Tripathi, T. Yang, R. S. Rathore, M. Aggarwal, et al., "A secure and robust machine learning model for intrusion detection in internet of vehicles," *IEEE Access*, 2025.
10. A. Venčkauskas, M. Taparuskas, Š. Grigaliūnas, and R. Brūzgienė, "Enhancing communication security an in-vehicle wireless sensor network," *Electronics*, vol. 13, p. 1003, 2024.
11. N. Ullah, S. U. Khan, and S. M. S. Bukhari, "Multivocal Literature Review Protocol for the Identification of Cybersecurity Challenges and its Solutions in the Context of Vehicle-to-Vehicle Communications from Software Engineering Perspective," *Spectrum of engineering sciences*, vol. 3, pp. 58-89, 2025.
12. B. Kitchenham, R. Pretorius, D. Budgen, O. P. Brereton, M. Turner, M. Niazi, et al., "Systematic literature reviews in software engineering—a tertiary study," *Information and software technology*, vol. 52, pp. 792-805, 2010.
13. M. Petticrew and H. Roberts, *Systematic reviews in the social sciences: A practical guide*: John Wiley & Sons, 2008.
14. E. Karger, A. Rothweiler, T. Brée, and F. Ahlemann, "Mapping the Future of Urbanization: A Bibliometric Analysis of Artificial Intelligence in Smart Cities," Available at SSRN 5010171.
15. D. Budgen, M. Turner, P. Brereton, and B. A. Kitchenham, "Using Mapping Studies in Software Engineering," in *Pp*, 2008, pp. 195-204.
16. S. Keele, "Guidelines for performing systematic literature reviews in software engineering," ed: Technical report, ver. 2.3 ebse technical report. ebse, 2007.
17. S. U. Khan, M. Niazi, and R. Ahmad, "Barriers in the selection of offshore software development outsourcing vendors: An exploratory study using a systematic literature review," *Information and Software Technology*, vol. 53, pp. 693-706, 2011.
18. M. Niazi, S. Mahmood, M. Alshayeb, M. R. Riaz, K. Faisal, N. Cerpa, et al., "Challenges of project management in global software development: A client-vendor analysis," *Information and Software Technology*, vol. 80, pp. 1-19, 2016.
19. C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, 2014, pp. 1-10.
20. S. Ahmadisakha and V. Andrikopoulos, "Architecting for sustainability of and in the cloud: A systematic literature review," *Information and Software Technology*, p. 107459, 2024.
21. M. U. Rehman, "Quantum-enhanced chaotic image encryption: Strengthening digital data security with 1-D sine-based chaotic maps and quantum coding," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, p. 101980, 2024.
22. H. Gunatilake, J. Grundy, R. Hoda, and I. Mueller, "The impact of human aspects on the interactions between software developers and end-users in software engineering: A systematic literature review," *Information and Software Technology*, p. 107489, 2024.
23. G. Márquez, M. Pacheco, H. Astudillo, C. Taramasco, and E. Calvo, "Inclusion of individuals with autism spectrum disorder in software engineering," *Information and Software Technology*, p. 107434, 2024.

24. N. Ullah, S. Khan, M. Niazi, M. Esposito, A. A. Khan, and J. A. Nasir, "Solutions to cybersecurity challenges in secure vehicle-to-vehicle communications: A Multivocal Literature Review," *Information and Software Technology*, p. 107639, 2024.
25. M. M. Hazzazi, M. U. Rehman, A. Shafique, A. Aljaedi, Z. Bassfar, and A. B. Usman, "Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach," *Scientific Reports*, vol. 14, p. 12277, 2024.
26. B. Kitchenham and S. Charters, *Guidelines for performing systematic literature reviews in software engineering (EBSE 2007-001)*. Keele University and Durham University Joint Report. 2007.
27. A. A. Khan, S. Badshah, P. Liang, B. Khan, M. Waseem, M. Niazi, et al., "Ethics of AI: A systematic literature review of principles and challenges," *arXiv preprint arXiv:2109.07906*, 2021.
28. B. Kitchenham, L. Madeyski, and D. Budgen, "How should software engineering secondary studies include grey material?," *IEEE Transactions on Software Engineering*, vol. 49, pp. 872-882, 2022.
29. N. Dissanayake, A. Jayatilaka, M. Zahedi, and M. A. Babar, "Software security patch management-A systematic literature review of challenges, approaches, tools and practices," *Information and Software Technology*, vol. 144, p. 106771, 2022.
30. T. Dybå and T. Dingsøy, "Empirical studies of agile software development: A systematic review," *Information and software technology*, vol. 50, pp. 833-859, 2008.
31. M. M. Hamdi, L. Audah, M. S. Abood, S. A. Rashid, A. S. Mustafa, H. Mahdi, et al., "A review on various security attacks in vehicular ad hoc networks," *Bulletin of Electrical Engineering and Informatics*, vol. 10, pp. 2627-2635, 2021.
32. A. S. Al Hasan, M. S. Hossain, and M. Atiquzzaman, "Security threats in vehicular ad hoc networks," in *2016 international conference on advances in computing, communications and informatics (ICACCI)*, 2016, pp. 404-411.
33. S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, pp. 217-241, 2012.
34. I. A. Sumra, H. Hasbullah, I. Ahmad, and Jamalul-lail bin Ab Manan "Forming vehicular web of trust in VANET," in *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, 2011, pp. 1-6.



**DSpace**

<https://dspace.org/>

## **Identification of cyber threats in IoV communication: a systematic literature review**

**Ullah, Naeem; Ahmad, Iftikhar; Almazroi, Abdulaleem Ali; Rahman, Mujeeb Ur**

**2025-11-25**

Springer

[https://doi.org/10.1007/978-3-032-23035-5\\_15](https://doi.org/10.1007/978-3-032-23035-5_15)

Ullah N, Ahmad I, Almazroi AA, Rahman MU. (2026) Identification of cyber threats in IoV communication: a systematic literature review. In: Proceeding of the Advances in Intelligent Computing Techniques and Applications II (IRICT 2025): Intelligent Systems, Health Informatics, Data Analytics and Internet of Things, Volume 2, 25-26 November 2025, Casablanca, Morocco, Lecture Notes on Data Engineering and Communications Technologies, Volume 293, pp. 159-169