Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

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

Naeem Ullah[1]
Software Engineering Research Group (SERG_UOM), Department of Computer Science & IT, University of Malakand, Pakistan
naeemullah72@gmail.com
Siffat Ullah Khan[2]
Software Engineering Research Group (SERG_UOM), Department of Computer Science & IT, University of Malakand, Pakistan
siffatullah@uom.edu.pk
Syed Muhammad Shakir Bukhari[3]
Teaching and Research Assistant, Department of Industrial Engineering, University of Engineering and Technology Peshawar
smshakirbukhari@gmail.com

Abstract

Transportation is a crucial aspect of our lives; it is needed, much like water and food, and it has an impact on our lives, but it must be handled by intelligent systems. As Automotive Vehicles (AVs) are depending on sensing, communication and artificial intelligence, therefore, AVs are attractive targets for cyber-attacks. Essentially, the amount to which automotive cybersecurity is implemented, particularly essential security that protects systems from unauthorized access, determines the safety of road users and automobiles. In the future, it will be entirely handled by objects rather than people, thus, we must begin and enhance (Vehicle-to-

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Vehicle) V2V technology in order to increase safety. The goal of research is to conduct a systematic evaluation of the literature in order to identify the security issues or risks or challenges in V2V communication and identification of practices/recommendations. Our present study established a Multivocal Literature Review (MLR) protocol to improve security challenges in the context of V2V communication. The protocol is presently in its implementation phase to improve V2V communication. This MLR is supposed to produce a list of security problems, as well as solutions to those challenges. This will also point the way for future study in this area.

Keywords: Automotive cybersecurity, automotive vehicles, V2V communication, cyber-attacks, multivocal literature review.

Introduction

What is Cybersecurity?

Cybersecurity can be defined as it related to the defense of various information systems (related infrastructure, software and hardware) the information on them and the services they provide from misuse, harmful elements and unauthorized access.

Due to the rapid growth in information technology (IT) and on another side general falling off in the cost of technology, further ICT users are joining cyberspace. According to [2] cyberspace is the dependent relationship between humans (cyber users) and linked systems (networks) which are interacting with this space. Therefore cyberspace is a virtual network where ICT devices and computers are linked with users, devices and networks [3]. For different activities cyber users are interacting to cyberspace, these activities can be, socializing, educational purposes and communication. Educational institutions are taking benefits of

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

technology to improve learning methods and educational teaching [4, 5].

When we talk about cyber offences, we generally tell about two main categories of crime: in the first a device joined the network is the target of crime this is the occurrence of various types of attacks on network integrity, availability and confidentiality. The second category have traditional crimes like cheating, forgery and theft which are performed through the help by means of computers joined the network, communication technology, associated information and computer networks. Cyber offences ranges from computer falsification, theft and fraud to violation of secrecy, the circulation of falsification of prostitution, harmful content and sorted crime [6].

In industry four, working machines are connected into the network through smart devices, due to which various types of cyber-attacks have grown rapidly [7]. As evidence the study conducted by Engineering Employees Federation in 2018 on Cyber security reveal that 48% of the constructor were identified pompous by Cyber offensive.

As Automotive Vehicles (AVs) are depending on sensing, communication and artificial intelligence, AVs are attractive targets for cyber-attacks [8]. Without formal safety automated vehicles are going. These vehicles are equipping with software and electronic technology that work flawlessly and reliably, while taking decision superior to a human. But the truth is: no protection without security. Basically the safety of road users and the safety vehicles is only as successful as the scope to which the applied automotive cybersecurity [9] and especially its important safety which preserve systems from unauthorized access.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

The area of V2V (Vehicle to Vehicle) technology is rapidly expanding and to address the demands of transportation of nationals embody the advancement of economic growth and technology. Due to development of several cities and global mobility which have importantly enlarged the amount of vehicles on roads [10]. Due to increase in the range of vehicles there is an enormous increase in pollution and waste of time is happening and the degrees of traffic freak have increased as well. However, the pedestrians also face the safety warning from traffic accidents [11]. "VANETs are posing a real security threat that has to be addressed, especially with the V2V broadcast communications. Many attacks may occur with different damage levels and threatening vehicles safety on roads" [12].

Types of Vehicular Communication

The following are various types of vehicular communication.

V2V (Vehicle-To-Vehicle)

V2X (Vehicle-To-Everything)

V2I (Vehicle-To-Infrastructure)

As reported by Upstream Security [13] By 2025 the modern vehicles will be shipped linked, possibility of not only connected or localization assistance but the acquisition of V2X (vehicle-2-X) paradigm. This phrase concerns to the car ability to exchange and communicate information with other vehicles, infrastructure and pedestrians. These types are also shown in the following diagram.

Vol. 3 No. 2 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

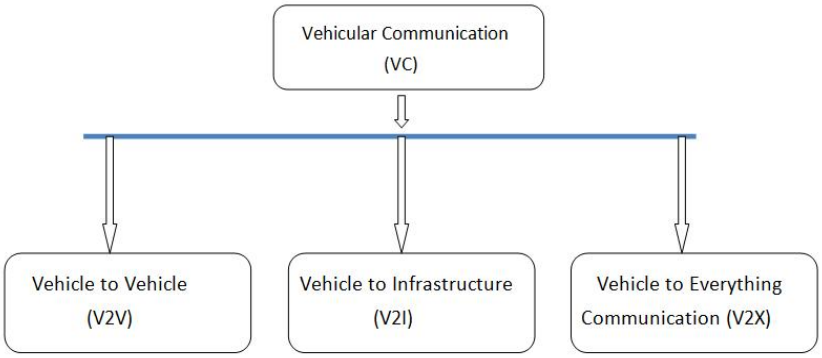


Figure 1: Types of Vehicular Communication [14]

V2V (Vehicle-To-Vehicle) Communication

It refers to IVC (inter-vehicle communication) which accepts the vehicles to communicate with each other and can share the meaningful data regarding accidents, speed limits and traffic congestion [15]. Vehicle to vehicle communication can generate the network by interlinked various devices (vehicles) using a mesh (full or partial) topology [16].

V2I (Vehicle-To-Infrastructure) Communication

It is also called roadside-to-vehicle communication (RVC) and allows the vehicle to influence with the RSUs (Road Side Units). It can help in detecting cameras, lane markers, parking meters and traffic lights [17]. The communication of vehicles with structure is wireless, bidirectional and ad-hoc [18]. The data gathered or gained from the structure are used for traffic management and supervision.

V2X (Vehicle-To-Everything) Communication

Vehicle to everything communication accepts the vehicles to interact with other nodes such as pedestrians (V2P), roadside (V2R), grid (V2G) and devices (V2D) [19]. This type of communication is used to stop road accidents with risk cyclists, motorcyclists and pedestrians [20]. This communication permit the Pedestrian

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Collision Warning (PCW) procedure to inform the traveler on roadside previously any serious accident takes place [15].

Overview of V2V

Objective of V2V is to supply drivers with important details and warn them regarding incident in real time. Using dedicated short range radio communication (DSRC) technology [21], cars will interact with each other, electronically broadcast data like the fastness of the cars, GPS location, route, track history and vehicle control information, brake status, steering wheel angle and transmission state. It is estimated that V2V communication will be common in ordinary cars or vehicles by 2020 "Although increased connectivity brings advantages in efficiency, the notion of a uniform wireless transportation infrastructure is a great concern". Before we check wireless transportation infrastructure, cybersecurity risks in today or modern vehicles deserve greater scrutiny [22]. Vehicle-to-Vehicle communication messages described by National Highway Traffic Safety Administration (NHTSA) as basic safety messages (BSMs) that correspond to messages passed between vehicles about dynamic information such as speed, location and headings [23].Some applications are discussed below.

Traffic Safety: DSRC technology can be used to improve traffic safety [24]. It allows vehicles to detect the barriers and to avoid collision accidents on the roads [25]. With the help of DSRC, the vehicle can detect a sharp curve and warn other cars [26]. If an accident happens on the road, the vehicles can transmit an alert message to other vehicles to avoid collisions.

Traffic Management System: DSRC can help establish a traffic management system which includes highway fleet management,

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

safe overtaking, etc.. The vehicles can safely overtake and maintain a desired gap during lane changes [27]. If a particular vehicle wants to change its lane, it will send the request to other vehicles for lane change. Therefore, the vehicle can perfectly manage the traffic using DSRC communication.

Vehicle Management: DSRC can be used to identify registered vehicles and provide an automatic pass to them. Hence, trespassing with a non-registered vehicle can be blocked [28].

Problem Statement and Research Questions

There are lack of comprehensive and multivocal analyses of the literature on the cyber-attacks on connected and autonomous vehicles (CAVs), predicted preparedness, mitigating techniques, and future research directions [29, 30]. "Cybersecurity, a biggest threat to AVs must be given critical importance right from the "Design" stage and embedded in the culture of development and maintenance. Cyber threats if less addressed can have severe consequences for the operations of companies (functions, reputation and assets) [31]." Transportation is an important aspect of our lives; it is essential, like water and food, and it has an impact on our lives; however, it must be managed by intelligent systems. In the future, it will be entirely managed by things rather than humans; therefore, we must begin and improve V2V and V2I technologies to improve safety [32]. Therefore in this research we will address challenges or issues in V2V communication and will provide solution or practices to these challenges. For this purpose, we formulated the below two questions. Through these questions, by RQ1, we will identify the challenges that V2V communication are facing while via RQ2, we will identify the relevant practices for the challenges that are identifying through RQ1.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

RQ1: What are the Cybersecurity challenges in V2V Communication from Software Engineering Perspective? The purpose of this question is to identify a list of cybersecurity challenges and to analyze each challenge, to be addressed.

RQ2: What are the recommendations/solutions that can be implemented to address the cybersecurity challenges? The purpose of this question is to identify the best possible solutions for addressing the cybersecurity challenges.

Constructing Search Term

We reported the PICO criteria from the literature as the first stage in creating the search string [33]. To find basic keywords and create search strings based on study questions, use PICO (Population, Intervention, Comparison, and Outcomes).

Population: Cybersecurity, Automotive cybersecurity, V2V communication

Interventions: Vehicle-To-Vehicle

Strategies/models/solutions/techniques

Comparison: The current study do not perform any comparison

Outcomes: Secure Vehicle-To-Vehicle communication

Research Methodology: Multivocal Literature Review

Multivocal Literature Review was performed during the first phase of this research. Multivocal literature review will be used to address the study Questions. We have used MLR guidelines for this study [34]. To accomplish the study aims, we performed a Multivocal Literature Review (MLR) to discover relevant studies in both the formal and grey literature. MLR procedure has been adopted by other researchers as well [35]. We discovered the cybersecurity challenges and its practices to improve secure V2V communication.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

We discussed the various phases of MLR in the subsequent sections in detail.

Search Strategy

Trial Search

We designed a search string, given below, to identify the cybersecurity risks, challenges, threats in V2V communication and practices or solutions to these challenges. We entitled this search string as Trial Search.

Trial Search: ("Cybersecurity in V2V communication" OR "V2V communication" OR "Information security in V2V communication") AND ("Cybersecurity risks" OR "Cybersecurity challenges" OR "Cybersecurity issues" OR Practices OR Solutions OR guidelines).

This query was submitted to Science Direct, IEEE Xplore, Springer Link, and ACM. We also used Google Scholar, a web-based search engine, to execute this search phrase. We squeezed the search string for Google Scholar only, as follow.

("Cybersecurity in V2V communication" OR "V2V communication" OR "Information security in V2V communication") AND ("Cybersecurity risks" OR "Cybersecurity challenges").

The number of search results for each database and search engine is shown in Table 01.

Resources to be Searched (Formal Academic Literature)

- IEEE Xplore (http://ieeexplore.ieee.org)
- ACM digital library ((http://dl.acm.org)
- ScienceDirect (http://www.sciencedirect.com)
- Springer Link (http://link.springer.com)
- Google Scholar (http://www.google.com), engine

Resources to be searched (Grey Literature)

- LinkedIn Automotive Cybersecurity groups/pages

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

- Facebook Automotive Cybersecurity groups/pages
- Annual reports generated by top 5 automotive companies in the world.
- Most popular blogs on automotive vehicles.
- Google

Facebook Automotive Cybersecurity groups/pages

Table 01: Facebook related groups about V2V communication

S.No	Name and web-links of relevant facebook groups/pages	Total number of members
01	Automotive Vehicles (https://www.facebook.com/Automotiveindustri/)	171
02	Automotive Cybersecurity (https://www.facebook.com/groups/653691448717220/?ref=share)	29
03	ASOL Automotives (https://ww.facebook.com/ASOLautomotive/)	55,060

LinkedIn Automotive Cybersecurity groups/pages

TablE 02: LinkedIn related groups about V2V communication

S.No	Name and web-links of relevant LinkedIn groups/pages	Total number of members
01	Automotive Security Research Group (ASRG) (https://www.linkedin.com/company/automotive-security-research-group/)	5,800

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

02	Mexico Automotive Industry	32,300
03	Arilou Automotive Cybersecurity (https://www.linkedin.com/company/arilou/)	3,400
04	(AIAG) Automotive Industry Action Group (https://www.linkedin.com/company/aiag/)	21,700
05	Automotive Cybersecurity Network (ACSN) (https://www.linkedin.com/company/automotive-cybersecurity-network-acsn/)	1,304
06	Automotive Industry (https://www.linkedin.com/company/automotive-industry)	5,424
07	Italy Automotive Industry	1,422
08	ISO/SAE 21434 Automotive Cybersecurity (https://www.linkedin.com/groups/893856)	547
09	Sewell Automotive Companies (https://www.linkedin.com/company/sewell-automotive-companies/)	9,205
10	Cyber Security for Automotive (https://www.linkedin.com/groups/8585300)	1,440

Search Results

Table 03: Search Results

Search string	Digital Libraries	Total Results
("Cybersecurity in V2V communication" OR "V2V communication" OR "Information security in V2V	Science Direct	880
	Springer Link	280
	ACM	245
	IEEE Xplore	534
	Google Scholar	127

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

communication") AND ("Cybersecurity risks" OR "Cybersecurity challenges" OR "Cybersecurity issues").		(Search engine)	
		Google (Search engine)	25
		Snowballing	78
Total			2169

Search Constraints and Validation

We are searching for all published papers related to our research and hence don't put any date boundaries. A prior search was conducted using a set of major search terms ("Cybersecurity in V2V communication" OR "V2V communication" OR "Information security in V2V communication") AND ("Cybersecurity risks" OR "Cybersecurity challenges" OR "Cybersecurity issues" OR Practices OR Solutions OR guidelines) and we found certain relevant papers on CiteSeer digital libraries. Prior to undertake the review process, these relevant papers will be used for the validation of search strings.

Search Documentation

Search results will be documented in the format as shown in the table below.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Table 04: Search Documentation

Name of database	Search strategy	Search string no.	Date of search	Years covered by search	No of publications found	Initial selection decision	Final selection Decision
CiteSeer Digital Library	("Cybersecurity in V2V communication" OR "V2V communication" OR "Information security in V2V communication") AND ("Cybersecurity risks" OR "Cybersecurity challenges" OR "Cybersecurity issues" OR	Trial Search	5-April-2022	All			

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

	Practices OR Solutions OR guidelines)

Search Result Management

Primary source references will be stored electronically in a separate directory. The results of each search will be stored in a directory as html pages, see Appendix-A which contains the search results of our CVVC protocol. Moreover the primary selection list will be in the following format taken from our CVVC protocol. It should be noted that the Tracing no. is the no. found for a particular paper during its search as shown in Appendix-A. If a paper is referenced in more than one database, then it will be entered once in the final selection list to avoid duplication. The "S.No" field of the final list is the primary key for a paper being selected in the review.

Table 05: Sample of Search Result Management

S.No	Tracing Number	Database	Paper Title
01	ACM-6	ACM	The Future of Autonomous Cars in the Daily Life of Cities A Systematic Mapping Study.
02	SD-73	Science Direct	Recent Advances in Machine-Learning Driven Intrusion Detection in Transportation: Survey
03	GS-15	Google Scholar	Security Study of routing attacks in Vehicular Ad-hoc

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

			Networks (Autonomous Car)
04	IEEE-3	IEEE	Cybersecurity analysis in Dedicated Short-Range Communications in vehicular networks

Publication Selection

This section contains three subsections namely inclusion criteria, exclusion criteria and the selection of primary sources, in order to choose only those search results which are relevant to the research questions. We will only consider papers/reports/books relating to cybersecurity and vehicle-to-vehicle communication. Papers/reports/books relating to vehicle-to-infrastructure and vehicle-to-everything communication will be ignored.

Inclusion Criteria

The inclusion criteria we used to determine which piece of literature (papers, technical reports, or grey literature) found by the search term will be used for the data extraction. We will only consider papers related to Cybersecurity V2V communication. The criteria are listed below as mentioned.

- Consider articles that specifically focus on cybersecurity V2V communication.
- Primary studies published in conferences, research workshops, journals and magazines.
- Studies that are available online in full text
- Studies that are written in English language
- Studies that describe challenges in Cybersecurity V2V communication.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

- Studies that describe practices/Solutions regarding Cybersecurity V2V communication.
- Studies that describe Cybersecurity V2V communication.
- Studies which focus on providing solutions/practices to build a cybersecurity V2V communication.

Exclusion Criteria

This section describes the exclusion criteria in order to decide which piece of literature found by the search term will be excluded/ignored. The criteria are listed below:

- Studies those are not relevant to the research questions.
- Studies that don't describe challenges inside cybersecurity V2V communication.
- Studies that don't describe practices for the development of cybersecurity V2V communication.
- Duplicate studies, only the most recent will be selected.
- Studies that don't fulfill the aforementioned inclusion criteria.
- Studies written in other than English languages will be excluded.

Selecting Primary Sources

Initial selection of the primary sources will be performed by reviewing the title, keywords and abstract. The purpose is to exclude/ignore only those results which have no relevance to the problem/research questions. The primary sources chosen in the initial selection process will be checked against the aforesaid inclusion/exclusion criteria by reviewing carefully through full text of the studies. The source will be sent to the secondary reviewer, for review in case of any uncertainty regarding the inclusion or exclusion decision. The record of inclusion/exclusion decision regarding each primary source will be sustained properly. This will

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

describe the reasons/justification whether or not the primary source has been included in the final review.

Quality Assessment Criteria

The assessment criteria are developed to evaluate the quality of the selected primary studies and remove the research bias. The quality assessment phase interprets the significance and completeness of each selected primary study [36, 37]. The QA criteria checklist provided by Kitchenham and Charters [36] are analyzed and designed the QA questions. Each selected primary study evaluated against the quality assessment criteria (QA1-QA8). Score 1 assigned if the study comprehensively addresses the quality assessment criteria. Similarly, 0.5 points are assigned to those who have partially addressed the QA criteria. Studies with no evidence of addressing the QA criteria are assigned 0 points. The measurement of quality is performed after final selection of publications. The quality of publications is assessed in parallel at the time of data extraction. The quality checklist contains the following questions:

Table 06: Quality Assessment Criteria's for the Formal Literature

No	Quality Assessment Criteria's	Choices
QA1	Does the adopted research method address the research problem?	1/0.5/0
QA2	Does the study have clear research objectives?	1/0.5/0
QA3	Does the study explicitly discuss the proposed research approach?	1/0.5/0
QA4	Is the study clearly reported the findings?	1/0.5/0

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

QA5	Does the study present the real-world implications of the research?	1/0.5/0
QA6	Is it clear how the challenges/practices, in cybersecurity V2V communication at industry level, were identified/ measured/ evaluated? (i.e. whether the mentioned challenges in the paper are based on a sound methodology or not?	1/0.5/0
QA7	Is the paper published in conference proceeding?	1/0.5/0
QA8	Is the paper published in a journal?	1/0.5/0

In order to achieve the reliability and quality of grey literature, we will perform quality assessment evaluation as shown in Table 07.

Table 07: Quality Assessment Criteria's for the Grey Literature

No	Criteria	Answer
GL-1	Has organization published the study/report?	1/0.5/0
GL-2	Does the study have a clear objective?	1/0.5/0
GL-3	Does the study use a clear methodology?	1/0.5/0
GL-4	Does the study have a unique contribution?	1/0.5/0
GL-5	Are the cybersecurity challenges presented clearly?	1/0.5/0

Data Extraction Strategy

Primary Study Data

The purpose of the study is to collect the data, from the publications, which is focused on satisfying the research questions for the review. The following data will be extracted from each publication.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

The following table presents the data to be captured in the data extraction form.

Table 08: **Data Extraction Form**

Data to be Extracted
• paper ID: • Title: • Conference/ journal: • Digital library: • Methodology (interview, case study, report, survey, etc): • Year of Publication: • Country where the study is conducted: • Challenges/Issues affecting cybersecurity V2V communication. • Practices/Solutions in development of cybersecurity V2V communication.

Data Extraction Process

The review will be undertaken by a single researcher, who will be responsible for the data extraction. A secondary reviewer will be approached for guidance in case of an issue regarding the data extraction. secondary reviewer will select few publications randomly from the list of publications already chosen by the primary reviewer. The secondary reviewer will independently extract the data from the randomly selected publication. The results will then be compared with the results produced by the primary reviewer. Primary Reviewer: Our supervisor at the University of Malakand, Pakistan.

Data Storage

The summarized data for each publication will be kept as a Microsoft Word/SPSS document and will be stored electronically.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Data Synthesis

Due to two research questions, the synthesis will also be categorized into two parts. For the Research Question1, the data will be synthesized by creating one summary table having the columns (S.No, Challenges, Frequency, Percentages) showing the list of all the challenges along with their frequencies and percentages. The complete detail of every challenges mentioned in the Summary table will be recorded in a separate table which will hold the following the columns (Challenges group name, S.No of reference, Challenges subgroups, Paper reference/Paper title). For the Research Question2, the same process will be performed as for the RQ1 mentioned above.

Analysis and Classifications

Extracted data item information will be tabulated and given a theme during analysis. The paper related to each theme will be counted and analyzed. Total extracted data will be saved in Excel sheets and data will be analyzed using statistical tools, SPSS.

Protocol Validation

The protocol was jointly developed by the authors and then presented to Software Engineering Research Group (SERG_UOM) for validation. The underlined comments were incorporated and the protocol was revised accordingly.

Findings

We designed a search string, given below, to identify the cybersecurity risks, challenges, threats in V2V communication and practices or solutions to these challenges. We entitled this search string as Trial Search. Trial Search: ("Cybersecurity in V2V communication" OR "V2V communication" OR "Information security in V2V communication") AND ("Cybersecurity risks" OR

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

"Cybersecurity challenges" OR "Cybersecurity issues" OR Practices OR Solutions OR guidelines).

This query was submitted to Science Direct, IEEE Xplore, Springer Link, and ACM. We also used Google Scholar, a web-based search engine, to execute this search phrase. We squeezed the search string for Google Scholar and Google only, as follow. ("Cybersecurity in V2V communication" OR "V2V communication" OR "Information security in V2V communication") AND ("Cybersecurity risks" OR "Cybersecurity challenges").

The number of search results for each database and search engine is shown in Table 3

Review Timetable

Table 09: Review Timetable

Task	Date
Start of the protocol	05-February-2022
Completion of search	12/April/2022
Submission of the protocol for review	12-August-2022
Completion of the protocol	30/November/2022
Completion of primary study selection	5/January/2023
Completion of Data Extraction	14/March/2023
Completion of Data Synthesis	10/August/2023
Completion of Review Report	15/December/2023

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Divergences

In case of any divergence from the protocol, which may occur during the study, we will record any change in a new Appendix to this document.

Conclusion

It is clarified from the findings of the search phase of the multivocal literature review that no multivocal literature review (MLR) or systematic literature review (SLR) is published till now that can identify the V2V communication challenges or risks or threats and its solution. In this work, we provide the results of the MLR protocol, which is the single component of our planned study. The MLR protocol is currently being implemented. We intend to achieve the following as our ultimate aim in the future:

- Using MLR and empirical research in the automotive sector, identify the Vehicle to Vehicle communication problems, risks, and issues, as well as their practices or solutions for V2V communication.
- By implementing the practices and guidelines as we will identifying via literature and validating through an empirical survey may help the companies to achieve specific goals regarding V2V communication improvement. To create a Cybersecurity Challenges Mitigation Model (CCMM) to help various companies in the automobile sector to assess their readiness for V2V communication development.

Acknowledgment

We are grateful to the fellows of Software Engineering Research Group (SERG-UOM) at University of Malakand and reviewers of the WSE-2022 for their valuable suggestions in validation process of the MLR protocol.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

References

[1] A. Rashid, G. Danezis, H. Chivers, E. Lupu, A. Martin, M. Lewis, *et al.*, "Scoping the cyber security body of knowledge," *IEEE Security & Privacy,* vol. 16, pp. 96-102, 2018.

[2] R. Ottis and P. Lorents, "Cyberspace: Definition and implications," in *International Conference on Cyber Warfare and Security*, 2010, p. 267.

[3] M. Grobler, J. Jansen van Vuuren, and J. Zaaiman, "Preparing South Africa for cyber crime and cyber defense," 2013.

[4] N. Phutela and S. Dwivedi, "Impact of ICT in education: students' perspective," in *Proceedings of International Conference on Digital Pedagogies (ICDP)*, 2019.

[5] S. von Solms and R. von Solms, "Towards Cyber Safety Education in Primary Schools in Africa," in *HAISA*, 2014, pp. 185-197.

[6] L. Schnider, "Scene of the cybercrime," ed: Syngress Publishing, 2002.

[7] T. C. Mahoney and J. Davis, "Cybersecurity for Manufacturers: Securing the Digitized and Connected Factory," 2017.

[8] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent transportation systems,* vol. 16, pp. 546-556, 2014.

[9] E. Knauel, J. Gramm, and J. Holle, "Automotive Cybersecurity-Efficient Risk Management for the Entire Life Cycle of Vehicles," *ATZelectronics worldwide,* vol. 15, pp. 18-22, 2020.

[10] M. Hannan, M. M. Hoque, A. Mohamed, and A. Ayob, "Review of energy storage systems for electric vehicle applications: Issues and challenges," *Renewable and Sustainable Energy Reviews,* vol. 69, pp. 771-789, 2017.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[11] L. Zhenyu, P. Lin, Z. Konglin, and Z. Lin, "Design and evaluation of V2X communication system for vehicle and pedestrian safety," *The Journal of China Universities of Posts and Telecommunications,* vol. 22, pp. 18-26, 2015.

[12] Y. Maalej and E. Balti, "Integration of Vehicular Clouds and Autonomous Driving: Survey and Future Perspectives," *arXiv preprint arXiv:2201.02893,* 2022.

[13] M. Scalas and G. Giacinto, "Automotive cybersecurity: Foundations for next-generation vehicles," in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, 2019, pp. 1-6.

[14] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, and M. Hafeez, "A survey of autonomous vehicles: enabling communication technologies and challenges," *Sensors,* vol. 21, p. 706, 2021.

[15] F. Arena and G. Pau, "An overview of vehicular communications," *Future Internet,* vol. 11, p. 27, 2019.

[16] P. M. d'Orey and M. Ferreira, "ITS for sustainable mobility: A survey on applications and impact assessment tools," *IEEE Transactions on Intelligent Transportation Systems,* vol. 15, pp. 477-493, 2013.

[17] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin*, et al.*, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access,* vol. 4, pp. 5356-5373, 2016.

[18] G. Xie, Y. Li, Y. Han, Y. Xie, G. Zeng, and R. Li, "Recent advances and future trends for automotive functional safety design methodologies," *IEEE Transactions on Industrial Informatics,* vol. 16, pp. 5629-5642, 2020.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[19] K. Lee, J. Kim, Y. Park, H. Wang, and D. Hong, "Latency of cellular-based V2X: Perspectives on TTI-proportional latency and TTI-independent latency," *IEEE Access,* vol. 5, pp. 15800-15809, 2017.

[20] J.-R. Lin, T. Talty, and O. K. Tonguz, "On the potential of bluetooth low energy technology for vehicular applications," *IEEE Communications Magazine,* vol. 53, pp. 267-275, 2015.

[21] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE,* vol. 99, pp. 1162-1182, 2011.

[22] R. J. Duplechin, "The emerging intersection of products liability, cybersecurity, and autonomous vehicles," *Tenn. L. Rev.,* vol. 85, p. 803, 2017.

[23] A. Demba and D. P. Möller, "Vehicle-to-vehicle communication technology," in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, 2018, pp. 0459-0464.

[24] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety," *IEEE communications magazine,* vol. 44, pp. 74-82, 2006.

[25] R. Sevlian, C. Chun, I. Tan, A. Bahai, and K. Laberteaux, "Channel characterization for 700 MHz DSRC vehicular communication," *Journal of Electrical and Computer Engineering,* vol. 2010, 2010.

[26] E. G. Strom, "On medium access and physical layer standards for cooperative intelligent transport systems in Europe," *Proceedings of the IEEE,* vol. 99, pp. 1183-1188, 2011.

[27] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications:

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

A survey," *IEEE transactions on vehicular technology,* vol. 65, pp. 9457-9470, 2016.

[28] J. F. de Valgas, D. Martín-Sacristán, and J. Monserrat, "5G New Radio Numerologies and their Impact on V2X Communications," *Waves, Univesitat Politecnica de Valencia,* pp. 15-22, 2018.

[29] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accident Analysis & Prevention,* vol. 148, p. 105837, 2020.

[30] 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.

[31] A. Seetharaman, N. Patwa, V. Jadhav, A. Saravanan, and D. Sangeeth, "Impact of Factors Influencing Cyber Threats on Autonomous Vehicles," *Applied Artificial Intelligence,* vol. 35, pp. 105-132, 2021.

[32] M. El Zorkany, A. Yasser, and A. I. Galal, "Vehicle To Vehicle "V2V" Communication: Scope, Importance, Challenges, Research Directions and Future," *The Open Transportation Journal,* vol. 14, 2020.

[33] D. Budgen, M. Turner, P. Brereton, and B. A. Kitchenham, "Using Mapping Studies in Software Engineering," in *Ppig*, 2008, pp. 195-204.

[34] V. Garousi, M. Felderer, and M. V. Mäntylä, "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering," *Information and Software Technology,* vol. 106, pp. 101-121, 2019.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[35] H. Al-Matouq, S. Mahmood, M. Alshayeb, and M. Niazi, "A Maturity Model for Secure Software Design: A Multivocal Study," *IEEE Access,* vol. 8, pp. 215758-215776, 2020.

[36] B. Kitchenham and S. Charters, "Source:"Guidelines for performing Systematic Literature Reviews in SE "Kitchenham et al Guidelines for performing Systematic Literature Reviews in Software Engineering Source," *Guidelines for performing Systematic Literature Reviews i,* pp. 1-44, 2007.

[37] 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.

[38] Mosaddeque, A., Rowshon, M., Ahmed, T., Twaha, U., & Babu, B. (2022). The Role of AI and Machine Learning in Fortifying Cybersecurity Systems in the US Healthcare Industry. *Inverge Journal of Social Sciences*, *1*(2), 70-81.

[39] Ahmed, T., Mosaddeque, A., Hossain, A., Twaha, U., Rowshon, M., & Babu, B. (2022). The Dynamics of AI and Automation in Financial Forecasting, Human Resources Planning, and Resources Optimization for Designing an Effective National Healthcare Policy. *Journal of Business Insight and Innovation*, *1*(2), 78-88.

[40] Ahmed, A., Rahman, S., Islam, M., Chowdhury, F., & Badhan, I. A. (2023). Challenges and Opportunities in Implementing Machine Learning For Healthcare Supply Chain Optimization: A Data-Driven Examination. *International journal of business and management sciences*, *3*(07), 6-31.

[41] Rahman, S., Sayem, A., Alve, S. E., Islam, M. S., Islam, M. M., Ahmed, A., & Kamruzzaman, M. (2024). The role of AI, big data and predictive analytics in mitigating unemployment insurance

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

fraud. *International Journal of Business Ecosystem & Strategy (2687-2293)*, *6*(4), 253-270.

[42] Badhan, I. A., Hasnain, M. N., Rahman, M. H., Chowdhury, I., & Sayem, M. A. (2024). Strategic Deployment of Advance Surveillance Ecosystems: An Analytical Study on Mitigating Unauthorized US Border Entry. *Inverge Journal of Social Sciences*, *3*(4), 82-94.

[43] Butt, M. A. J., Latif, A., & Ali, S. (2022). Indian Hegemonic Attitude towards Neighbor States: The Growing Influence of China in South Asia. *Journal of Policy Research (JPR)*, *8*(3), 422-430.

[44] Shakeel, M., Khan, K., & Latif, A. (2023). Role of Finnacial Inclusion, Institutional Quality and Human Capital in Economic Growth: An Empirical Analysis from Selected Asian Countries. *Journal of Policy Research (JPR)*, *9*(2), 274-278.

[45] Iqbal, S., Latif, A., & Bashir, R. (2023). A Comparative Analysis of the Differences in Mental Health in Aged Men and Women. *Journal of Policy Research (JPR)*, *9*(2), 565-572.

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

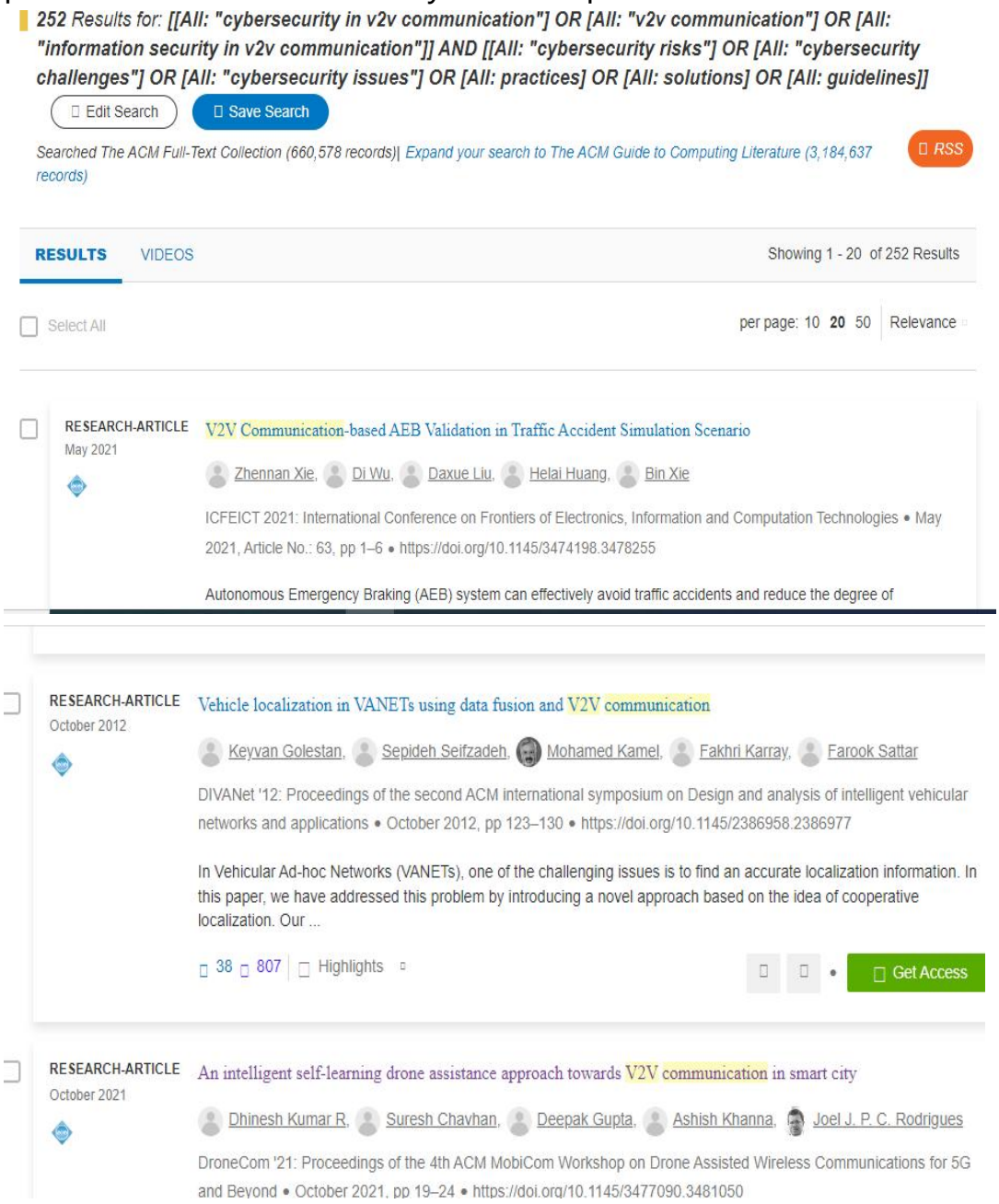
SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Appendix-A (Search Results of Cybersecurity challenges for V2V communication (CCVVC) protocol)

See the attached html pages please. Or contact me on the provided email addresses if you have queries.



252 Results for: [[All: "cybersecurity in v2v communication"] OR [All: "v2v communication"] OR [All: "information security in v2v communication"]] AND [[All: "cybersecurity risks"] OR [All: "cybersecurity challenges"] OR [All: "cybersecurity issues"] OR [All: practices] OR [All: solutions] OR [All: guidelines]]

Edit Search | Save Search | RSS

Searched The ACM Full-Text Collection (660,578 records)| Expand your search to The ACM Guide to Computing Literature (3,184,637 records)

RESULTS VIDEOS Showing 1 - 20 of 252 Results

Select All per page: 10 20 50 Relevance

RESEARCH-ARTICLE
May 2021

V2V Communication-based AEB Validation in Traffic Accident Simulation Scenario

Zhennan Xie, Di Wu, Daxue Liu, Helai Huang, Bin Xie

ICFEICT 2021: International Conference on Frontiers of Electronics, Information and Computation Technologies • May 2021, Article No.: 63, pp 1–6 • https://doi.org/10.1145/3474198.3478255

Autonomous Emergency Braking (AEB) system can effectively avoid traffic accidents and reduce the degree of

RESEARCH-ARTICLE
October 2012

Vehicle localization in VANETs using data fusion and V2V communication

Keyvan Golestan, Sepideh Seifzadeh, Mohamed Kamel, Fakhri Karray, Farook Sattar

DIVANet '12: Proceedings of the second ACM international symposium on Design and analysis of intelligent vehicular networks and applications • October 2012, pp 123–130 • https://doi.org/10.1145/2386958.2386977

In Vehicular Ad-hoc Networks (VANETs), one of the challenging issues is to find an accurate localization information. In this paper, we have addressed this problem by introducing a novel approach based on the idea of cooperative localization. Our ...

38 807 Highlights Get Access

RESEARCH-ARTICLE
October 2021

An intelligent self-learning drone assistance approach towards V2V communication in smart city

Dhinesh Kumar R, Suresh Chavhan, Deepak Gupta, Ashish Khanna, Joel J. P. C. Rodrigues

DroneCom '21: Proceedings of the 4th ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond • October 2021, pp 19–24 • https://doi.org/10.1145/3477090.3481050

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Showing 1-25 of 557 for
("Cybersecurity in V2V communication" OR "V2V communication" OR "Information security in V2V communication") AND ("Cybersecurity risks" OR "Cybersecurity challenges" OR "Cybersecurity issues" OR Practices OR Solutions OR guidelines)

Conferences (395) Journals (130) Early Access Articles (16) Magazines (14)
Books (2)

Show
All Results
Open Access Only

Year
Single Year Range
2005 2022

Select All on Page
Sort By: Relevance

Comparison of two coding technique dedicated to UWB V2V communication ystem
Y. El Hillali; R. Elassali; F. Boukour; A. El Abed; A. Rivenq
2009 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST)
Year: 2009 | Conference Paper | Publisher: IEEE
Cited by: Papers (1)

It may have been moved, edi
deleted.

Design of a Blockchain Enabled Secure Vehicle-to-Vehicle Communication System
Debashis Das; Sourav Banerjee; Pushpita Chatterjee; Uttam Ghosh; Wathiq Mansoor; Utpal Biswas
2021 4th International Conference on Signal Processing and Information Security (ICSPIS)
Year: 2021 | Conference Paper | Publisher: IEEE
Abstract HTML

Secure Privacy-Preserving V2V Communication in 5G-V2X Supporting Network Slicing
Hyeran Mun; Minhye Seo; Dong Hoon Lee
IEEE Transactions on Intelligent Transportation Systems
Year: 2021 | Early Access Article | Publisher: IEEE
Abstract

Cybersecurity analysis in Dedicated Short-Range Communications in vehicular networks
Michael Stepzinski; Shamik Sengupta

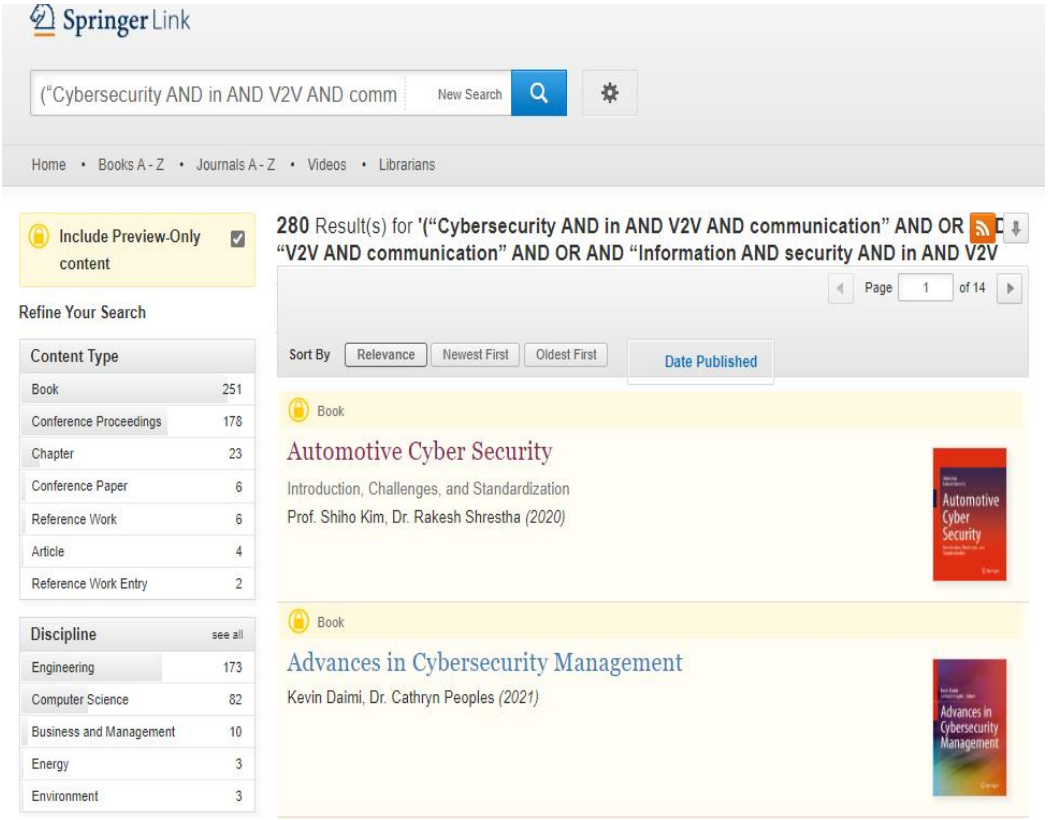
Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X



Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Advances in Security, Networks, and Internet of Things

Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20

Dr. Kevin Daimi... in *Transactions on Computational Science and Computational Intelligence (2021)*

Book and Conference Proceedings

Computer Safety, Reliability, and Security

SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Turku, Finland, September 10, 2019, Proceedings

Alexander Romanovsky... in *Lecture Notes in Computer Science (2019)*

Book

Advances in Computing, Informatics, Networking and Cybersecurity

A Book Honoring Professor Mohammad S. Obaidat's Significant Scientific Contributions

Assoc. Prof. Petros Nicopolitidis... in *Lecture Notes in Networks and Systems (2022)*

Book and Conference Proceedings

Advances in Information and Communication

Proceedings of the 2022 Future of Information and Communication Conference (FICC), Volume 2

Prof. Dr. Kohei Arai in *Lecture Notes in Networks and Systems (2022)*

Book