Received: 11/08/2026, Accepted: 01/10/2026

Research Trends in CAV Intrusion Detection Systems: A Bibliometric Study of the WoS Database

Ayush Verma(ORCID: 0000-0001-7249-1011), Manju Khari(ORCID: 0000-0001-5395-5335)

Jawaharlal Nehru University, New Delhi 110067, India

ayush.k1998@gmail.com, manjukhari@yahoo.co.in

Abstract

Connected Autonomous Vehicles (CAVs) inherit the connectivity of the Internet of Things and, with it, much the same attack surface. As smart transportation infrastructure becomes increasingly exposed to cyber threats, a resilient Intrusion Detection System (IDS) is no longer optional but a basic requirement. This paper's contribution is a bibliometric mapping of how the research community has answered that need between 2014 and 2024. The corpus was drawn entirely from the Web of Science (WoS) database, with 3,775 records surviving a systematic screen of 7,996 initial results, and used to quantify four things: publication output, authorship and collaboration structure, citation behaviour, and keyword co-occurrence, through a combination of evaluative and relational bibliometric methods (fractional counting, co-authorship networks, keyword co-occurrence mapping, and citation burst detection) applied consistently at author, institution, and country level. The keyword and co-citation networks settle into a small number of stable thematic clusters, which makes it possible to say where effort has concentrated and, more usefully, where it has not. Our reading of that evidence is that the most promising direction lies in extending machine learning methods so that CAV systems recognise previously unseen anomalies rather than catalogued attacks alone. Researchers new to CAV security should find the survey useful for locating active groups, influential work, and open problems in intrusion detection. One limitation of scope deserves stating at the outset: a corpus confined to indexed scholarly literature excludes patents, technical reports, and industry publications, and their inclusion would provide a fuller account of the field.

Keywords: *Intrusion Detection System, Connected Autonomous Vehicles, Bibliometric Assessment, Internet of Things*

1. Introduction

The Internet of Things (IoT) refers to the large-scale interconnection of appliances, hardware nodes, and everyday objects equipped with sensors, embedded software, and processing capabilities. Wireless connectivity allows these devices to collect information and exchange it over the Internet, so they can coordinate with one another, monitor conditions in their surroundings, and respond to people, usually without anyone directing them step by step [1]. The category is deliberately broad. A domestic thermostat qualifies, as does a wearable monitor, a piece of factory equipment, or a connected car. Attachment to the network usually happens over Wi-Fi, Bluetooth, Zigbee, or a cellular link. Forecasts place the worldwide installed base at 30.9 billion connected units by 2025 [2], and the data generated by this population is correspondingly large; it is processed either at the edge or in the cloud, where it

*Corresponding author: Ayush Verma, Jawaharlal Nehru University, New Delhi 110067, India. (ayush.k1998@gmail.com)

is turned into insights and used to drive decisions. A good deal of that decision-making runs without human involvement. A smart home system will adjust lighting, temperature, or alarm state directly from sensor readings, while users retain the ability to intervene via voice assistants, mobile applications, or dashboards.

Adoption has accelerated sharply over the past decade. Three factors account for most of it: cheap sensors, near-universal wireless coverage, and a growing appetite for data-driven decision-making in commercial and domestic settings alike [3]. Healthcare, transportation, manufacturing, and energy have all been reached. The applications that followed have reshaped ordinary routines in ways that are easy to overlook. Clinicians monitor patients remotely via wearable devices and medication management systems. Factories run predictive maintenance and automated production lines with tighter supply chains, and municipalities apply much the same technology to traffic control, grid management, and environmental sensing.

1.1. Open Challenges in IoT

None of this expansion has been free of cost. Security weaknesses, privacy exposure, poor interoperability, and the sheer difficulty of managing and analysing data at scale all remain unresolved.

- **1.1.1. Inherent Device Vulnerabilities:** Endpoint security remains the field's most persistent weakness, and it compounds the privacy problem rather than sitting alongside it. Manufacturers optimise for unit cost and feature set; security is rarely treated as a design priority. The same consequences recur across product lines: weak or hardcoded credentials, unencrypted traffic, and untrustworthy update mechanisms.
- **1.1.2. Fragmentation and Interoperability Hurdles:** Enforcing security is considerably harder in an ecosystem with no shared standards. Vendors implement proprietary protocols and data formats, which leaves the environment fragmented and hard to reason about as a whole. That inconsistency shows up as uneven security baselines, awkward data integration, and an attack surface wider than any single vendor accounts for.
- **1.1.3. Immense Scale of Data:** Devices emit data continuously, at high velocity and in heterogeneous formats, and conventional security analytics cannot keep pace. The problem really is one of big data. Sheer volume makes threats harder to isolate, provenance harder to track, and compliance harder to demonstrate; it also frustrates the real-time analysis on which proactive defence depends.

Until these obstacles are addressed, IoT will not deliver on its promise or develop along sustainable and responsible lines.

1.2. Intelligent Transportation Systems

Advances in automotive engineering have made the vehicle one of the most visible sites of IoT deployment. Cars have become steadily more capable and more autonomous, and the trajectory points towards smart mobility, usually framed in terms of the Intelligent Transportation System (ITS) [4]. An ITS layers advanced technology onto existing transport networks to improve overall efficiency, safety, sustainability, and mobility. Several components

have to work in concert for this to happen: sensors and cameras observe, communication networks relay, and processing centres interpret, so that traffic is tracked, routes recalculated, and live information fed to drivers and transport authorities. It is the coordination between these components, more than any one of them, that allows an ITS to cut congestion, improve fuel economy, reduce environmental impact, and make journeys less taxing.

Within the ITS agenda, the development and deployment of CAVs is among the more consequential strands. CAVs differ from conventionally driven vehicles in that they exchange data with each other and with roadside infrastructure in near real time [5]. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication underpin that exchange; between them they make driving decisions more reliable and reduce the risks arising from human unpredictability. Onboard lidar, radar, and camera arrays supply an accurate model of the surroundings, which in turn supports navigation, lane-keeping, and collision avoidance. Since CAVs can also negotiate with one another and with infrastructure, they enable levels of traffic coordination, route optimisation, and safety that human-driven fleets simply cannot achieve. This article contributes a bibliometric evaluation of IDS work in the CAV setting, along with the intrusion detection techniques and tools that support it [6].

Making a car intelligent means layering in technology that improves safety, efficiency, convenience and, above all, connectivity. Progress here depends heavily on electronics, since the hardware is what makes those functions possible in the first place. A modern vehicle contains numerous electronic control units (ECUs), sensors, and communication buses that govern everything from engine management and braking to infotainment and driver assistance. The benefits of that density are real. So is the cost: greater interconnection and complexity introduce new problems, and cybersecurity is the most pressing of them.

Smart vehicles are well-connected, and that is precisely what makes them a broad target; defending them requires capable intrusion detection. A smart transportation system spans connected vehicles, roadside infrastructure, and backend servers, each of them exposed to unauthorised access, data breaches, and malicious manipulation [7]. Conventional security controls have generally proved inadequate against threats of this class. A distributed architecture, combined with hard real-time vehicle operation, means that detection and response must be fast and computationally economical simultaneously, which is a demanding pair of constraints. Advanced IDSs built specifically for the smart transportation setting are needed, and needed soon.

This study sets out to characterise research activity in CAV intrusion detection through a bibliometric reading of the WoS record. The window under examination runs from 2014 to 2024. Indicators include publication volume, subject areas, authorship patterns, and national contribution, among others. The analysis does more than describe output: it traces how the field has developed over time, identifies the authors and institutions doing the most work, and examines what the published literature actually concentrates on thematically. Taken together, the quantitative treatment is meant to give a broad view of the research landscape and to indicate where further investigation would be worthwhile.

The paper is organised as follows. Section 2 sets out the methodology used to collect and analyse the record. Section 3 examines publication structure, covering document category, publication source, and prolific institutes. Section 4 reports the co-authorship results and considers how far they can be relied upon. Section 5 covers keyword co-occurrence, Section 6

burst detection, and Section 7 the citation analysis. Section 8 draws together the principal observations, and Section 9 discusses the limitations of this work, along with directions for future research.

2. Methodology

The analysis rests on bibliographic records. These are used here to evaluate and visualise research trends in CAV, to surface the most significant publications, and to identify the leading contributors to IoT and vehicular intrusion detection. The procedure follows the approach taken by [8] in their bibliometric assessment of the cybersecurity literature, adapted to the present domain; Figure 1 sets out the steps. The process opens with a topic search in WoS, constrained by the time span adopted for this study, which returns 7,996 records. Screening then removed everything irrelevant, including book chapters, retracted publications, and several other categories, leaving 3,775 articles. Metadata for this refined set, comprising full records together with cited references, was exported. Deliberately, the analysis does not rely on a single bibliometric technique or tool: it combines evaluative and relational methods (Section 2.4) and runs them across four complementary packages the R bibliometrix package, VOSviewer, CiteSpace, and MS Excel each suited to a different part of the pipeline, from network construction to burst detection to tabulation. It is this layered combination, rather than any single tool, that constitutes the analytical architecture of the review, and the findings are presented graphically in the subsections that follow.

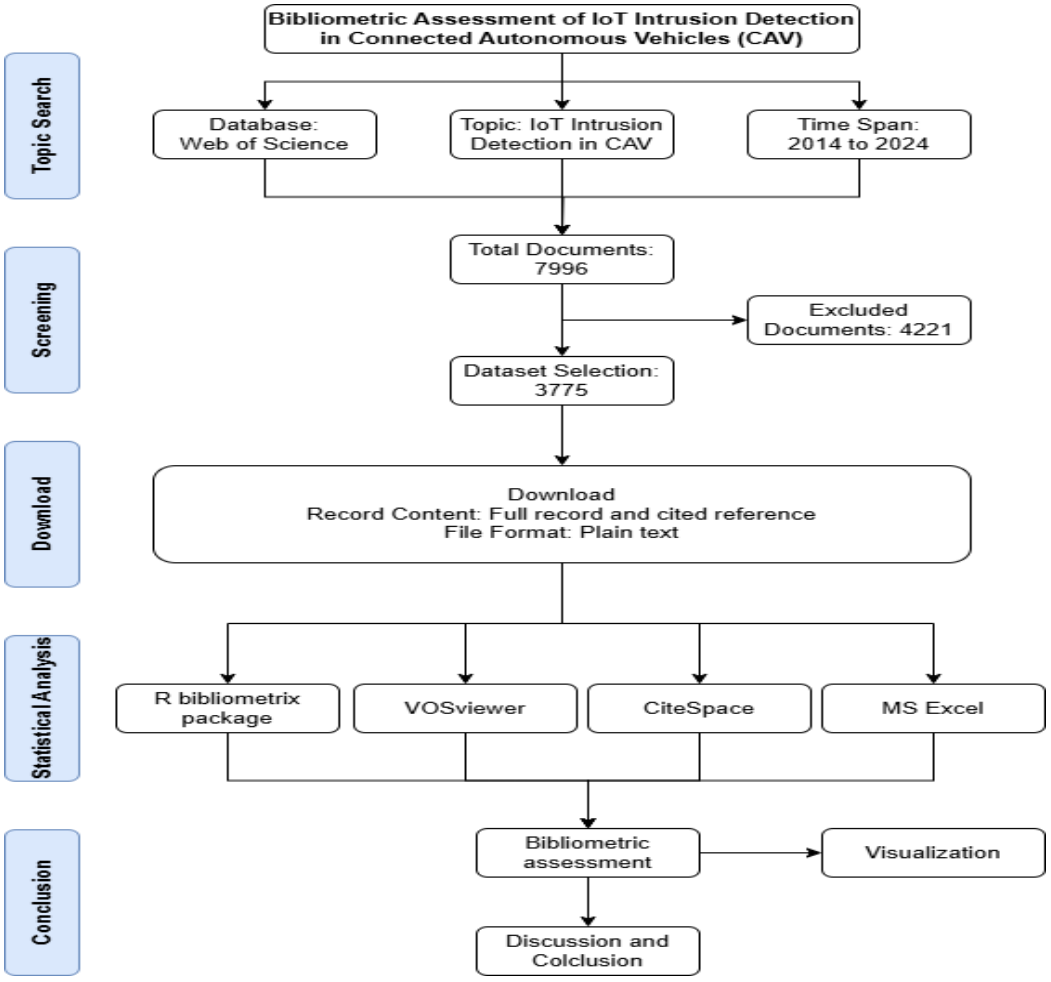


Figure 1. Methodology of the assessment

2.1. Data Gathering

Bibliometric data gathering involves systematically assembling publication records so that research output, impact, and scholarly trends can be evaluated within a defined boundary. Everything begins with a clear objective. Whether the aim is to profile a researcher, an institution, or an entire field determines which database is appropriate, be it Scopus, Web of Science, Google Scholar, or OpenAlex. A typical export includes titles, authors' names, institutional affiliations, publication years, abstracts, keywords, journal titles, citation counts, and persistent identifiers such as DOIs. Raw exports are rarely usable as they stand. Duplicates have to be removed, author names disambiguated, and journal titles and keywords standardised before the data can be trusted; where deeper analysis is intended, the records may also be enriched with altmetrics, funding data, or full text. Getting this stage right conditions everything downstream, since identifying influential researchers, mapping collaboration, and tracing thematic movement all depend on the integrity of the underlying records.

WoS served as the primary database for this assessment. Its reputation rests on the quality of the journals it indexes, and its coverage of scholarly publications dates back to 1990, giving it considerable depth as a record of academic literature. The WoS Core Collection spans the full range of indexes: Science Citation Index Expanded (SCI-EXPANDED), Emerging Sources Citation Index (ESCI), Book Citation Index Science (BKCI-S), Book Citation Index Social Sciences and Humanities (BKCI-SSH), Conference Proceedings Citation Index Science (CPCI-S), Conference Proceedings Citation Index Social Sciences and Humanities (CPCI-SSH), Social Sciences Citation Index (SSCI), and Arts and Humanities Citation Index (AHCI).

The query was built around keywords covering intrusion detection, CAV, and ITS, and restricted to the period 2014–2024. It was configured to return “full records and cited references” so that the retrieved set would support citation-level analysis. Three document types were targeted: research articles, review articles, and conference proceedings papers, with items WoS classifies as review articles also retained. Early access papers, retracted publications, and book chapters were excluded in favour of completed reviews and original research contributions. The search ran in January 2025 and yielded 3,775 publications, exported in plain text. Framing the query this way kept the retrieved set accurate and closely aligned with intrusion detection in CAV and ITS.

2.2. Search Strategy and Eligibility Criteria

The exact WoS query, entered in the Advanced Search builder as eight phrase terms joined by OR and run against All Fields (ALL=) of the WoS Core Collection, was:

ALL=("in-vehicle intrusion" OR "intrusion connected autonomous vehicles" OR "intrusion vehicular" OR "intrusion intelligent transportation systems" OR "intrusion internet of vehicles" OR "intrusion smart vehicles" OR "intrusion autonomous vehicles" OR "intrusion smart transportation")

The query was run against all eight indexes of the WoS Core Collection listed in Section 2.1, restricted to the timespan 2014–2024 and to English-language records, and executed in January 2025; it returned the 7,996 records reported in Section 2. Eligibility was then assessed at the screening stage against explicit inclusion and exclusion criteria. Records were included where they were (i) classified by WoS as a research article, review article, or conference proceedings paper; (ii) published within the 2014–2024 window; (iii) written in English; and

(iv) judged, on a title-and-abstract screen, to address intrusion detection specifically within a connected-vehicle, in-vehicle-network, or intelligent-transportation-system context. Records were excluded where they were (i) book chapters; (ii) retracted publications; (iii) early access records not yet assigned to a final issue; or (iv) records that matched the search string only superficially, for instance, general IoT or ITS papers with no intrusion-detection component, or intrusion-detection papers situated entirely outside the vehicular and transportation domain. Applying these criteria reduced the initial 7,996 records to the 3,775-record corpus used throughout the remainder of this paper.

2.3. Software Used

The bibliometric analysis was carried out using the software listed below.

- **R bibliometric package:** An open-source R package covering the full analytical pipeline, from extraction and cleaning through to network analysis and visualisation. Its strength lies in handling large record sets and supporting more demanding statistical work, which makes it particularly suited to researchers comfortable working in code.
- **VOSviewer:** A dedicated tool for constructing and displaying bibliometric networks co-citation, co-authorship, and co-occurrence alike. It produces legible maps that make the structure of a body of literature and the relations within it easy to read, which is why it is widely used to visually survey research landscapes.
- **CiteSpace:** A Java application oriented towards detecting and visualising emerging trends in scientific literature. It is especially useful for identifying citation bursts, tracing how research fronts develop, and mapping the intellectual structure of a field, allowing the dynamics of a discipline to be followed over time.
- **Excel:** Not a bibliometric package as such, but widely used in this kind of work for data manipulation, processing, and straightforward visualisation. It typically serves to collate and tidy exported records, compute simple measures, and produce preliminary charts and tables before more specialised tools take over the network analysis.

2.4. Statistical Analysis and Visualisation

Two complementary families of bibliometric methods were applied in this study:

- **Evaluative Method**: Used here to assess the research contributions of individual authors, their institutions, and the overall impact of their work. Evaluative techniques quantify output and influence for authors through publication counts, citations, and the h-index; for institutions through publication volume, citation totals, and measured research impact; for journals through indicators such as the Journal Impact Factor; and, comparably, for countries. In short, evaluative bibliometrics answers questions of magnitude and influence: how much has been produced, and how much has it mattered.

- **Relational Method**: Applied to map the relationships among authors, institutions, and research topics. Network analysis was used to expose collaboration patterns and to isolate the principal research clusters in CAV intrusion detection. Where evaluative work measures impact, relational work traces connections, reading the structure and dynamics of a field through author co-authorship, institutional collaboration, citation behaviour (via bibliographic coupling and co-citation analysis), and keyword co-occurrence. Network and co-word analyses are standard techniques. The questions it

answers are relational ones: who works with whom, and which topics travel together. Pairing this relational layer with the evaluative one above is what distinguishes a bibliometric assessment from the narrative or technical surveys of CAV intrusion detection that already exist [6], [14], [15], [16]: those catalogue methods and results qualitatively, whereas the hybrid evaluative-relational architecture used here quantifies collaboration structure, thematic concentration, and influence directly from the indexed record.

Visualisation carried much of the analytical weight in this study, both as a means of communicating results and as a way of surfacing detail that would otherwise stay buried in the numbers. Evaluative bibliometrics is quantitative by nature, but its findings become considerably clearer once rendered visually. Raw citation counts and publication totals are difficult to interpret; converted into charts, graphs, and maps, the same figures make trends, patterns, and outliers apparent. Visual treatment also highlights what matters most, whether that is the most influential authors, institutions, or journals, while exposing the relationships among them through co-authorship or co-citation networks. A well-constructed figure quickly conveys the shape of the evidence, helps identify anomalies, and communicates conclusions to a wider audience than a table would. VOSviewer 1.6.20 produced the network visualisations, and CiteSpace supported the analysis of citation and keyword trends.

2.5. Rationale for Analytical Thresholds

The numeric thresholds applied throughout the co-authorship, co-occurrence, citation, and burst-detection analyses (Sections 4–7) follow conventions established in the bibliometric literature rather than arbitrary cut-offs, and are justified individually below. The five-publication, five-citation threshold used for authors, institutions, and countries reflects the default working threshold recommended for VOSviewer analyses of corpora in the low thousands of records [27]; pilot runs at a lower threshold (three publications) produced networks too dense to interpret visually, while a higher threshold (ten publications) excluded several countries already shown in Section 3 to be active contributors. The exclusion of documents with more than 25 contributing authors follows standard practice for fractional counting: in a very large author team, each co-author's fractional contribution to a single paper becomes vanishingly small, and a handful of mega-author publications can otherwise dominate an institution's or country's apparent collaborative reach without representing genuine sustained collaboration. The five-occurrence threshold used for keyword co-occurrence (Section 5) applies the same logic to terms rather than authors: keywords occurring four times or fewer are typically idiosyncratic to a single paper or research group and do not represent a stable thematic signal for the field as a whole. For burst detection (Section 6), CiteSpace's implementation of Kleinberg's algorithm was run with its default smoothing parameters, and the 'Top N per slice' selection criterion was used in preference to a fixed absolute threshold because it adapts to the differing citation density of earlier and more recent years a necessary precaution given that the underlying corpus grows nearly six-fold between 2014 and 2024 (Figure 2), which would otherwise bias burst detection toward older, more heavily cited work.

3. Publication Structure Study

This section sets out the distribution of publications across years, categories, and source titles, and asks what those distributions reveal about CAV intrusion detection research. Leading nations, institutions, and authors in IoT intrusion detection are also identified, along with their

publication counts. All figures reported here are derived from applying the WoS analysis tools to the document collection assembled using the search strategy described above.

3.1. Study of Publications Year over Year

Figure 2 charts the annual growth of scholarly output on CAV intrusion detection as recorded in WoS. Publication counts are on the vertical axis, publication years from 2014 to 2024 on the horizontal axis, and the count for each year is printed above its bar. The trajectory leaves little room for ambiguity: output has risen substantially since 2014, indicating a marked and sustained increase in research attention to this area.

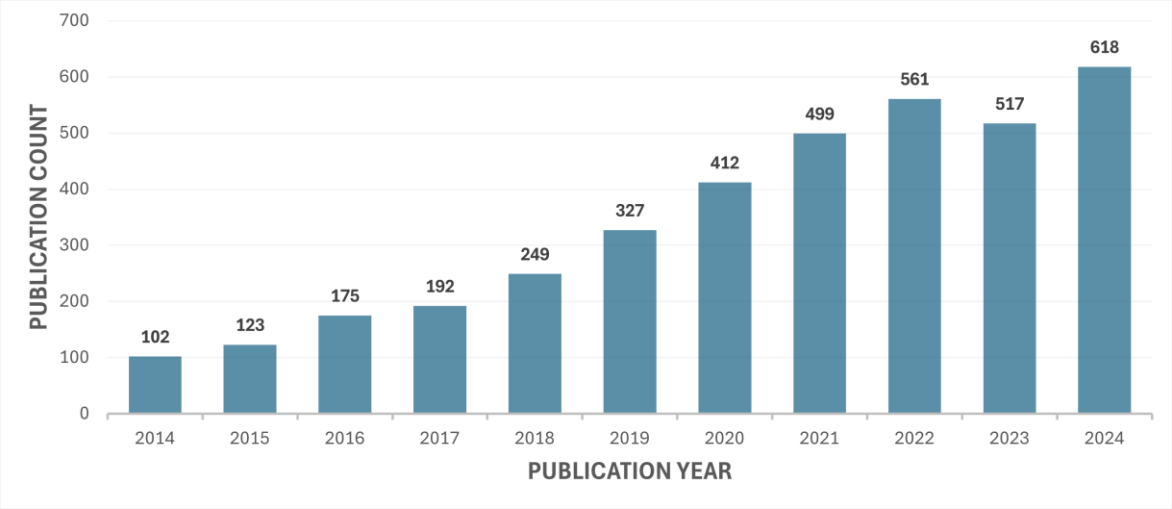


Figure 2. Progression of an annual publication count in intrusion detection in CAV from 2014–2024.

Continued strong growth in IoT connections is projected in [2]. Uptake of any technology, however, rests on the security guarantees that accompany it, which makes accelerated work on CAV intrusion detection a matter of some urgency. Figure 3 shows citations rising sharply over the same period, reinforcing how central intrusion detection has become within the IoT ecosystem. The publication categories recorded in WoS are examined next.

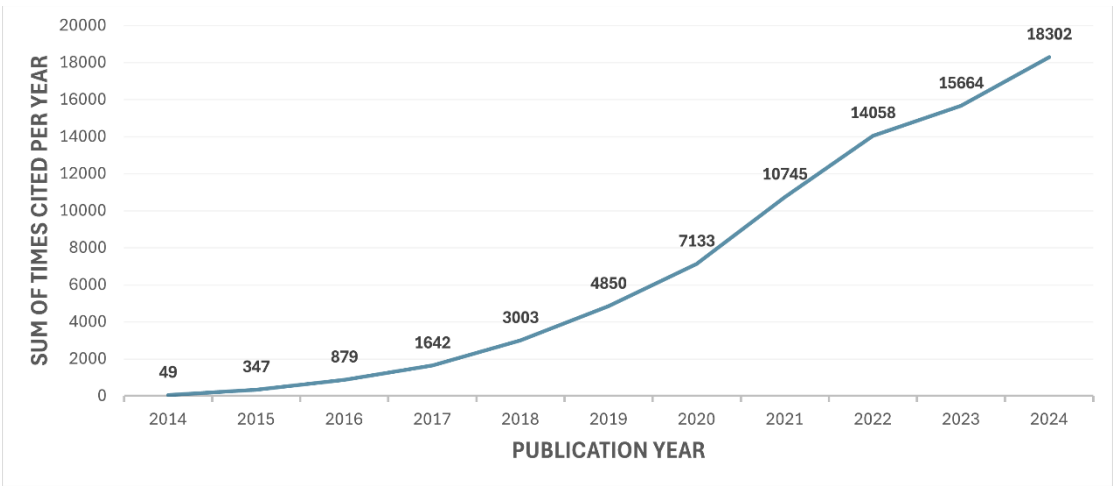


Figure 3. Total number of citations received each year by publications on Intrusion Detection in CAV within the WoS database.

3.2. Publications Category

Three document categories appear in the corpus: research articles, review articles, and conference proceedings papers. Research articles account for roughly 94% of the total, review articles 5%, and conference papers approximately 1% of the 3,775 records. Figure 4 gives the distribution together with the corresponding counts. The next subsection turns to the sources that carry out most of this research across the CAV and IoT sectors, as recorded in WoS.

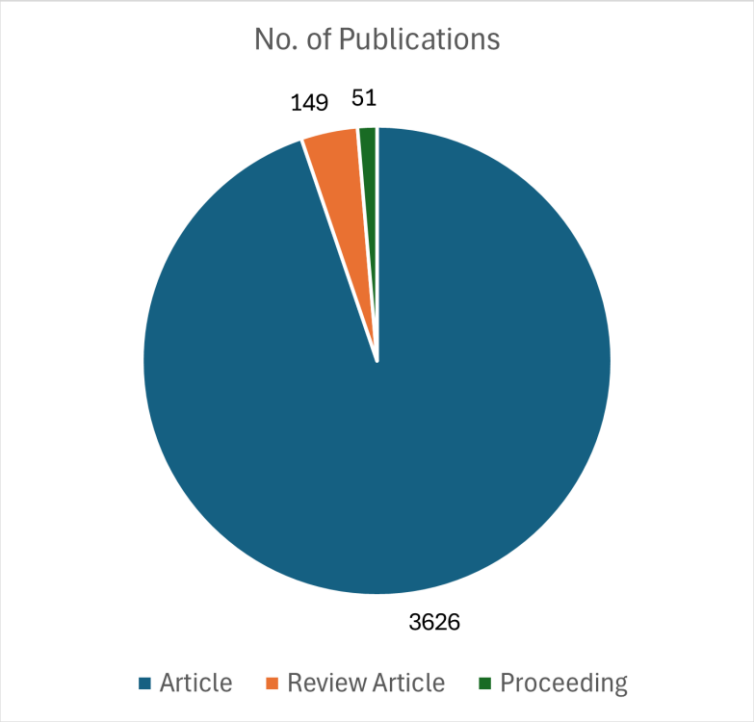


Figure 4. Publication categories in CAV intrusion detection from WoS database.

3.3. Source of Publication

'IEEE Access' leads the field with 262 publications, 25% of the top 10 sources drawn from WoS. 'Sensors' comes second with 127 publications, 12% of the top 10 record count. 'IEEE Transactions on Intelligent Transportation Systems' takes third place with 115. Behind these are 'Energies' in fourth with 109, 'IEEE Transactions on Vehicular Technology' in fifth with 103, and 'Electronics' in sixth with 79. The remainder of the top 10 comprises the 'IEEE Internet of Things Journal' in seventh with 74, 'Applied Sciences Basel' in eighth with 69, 'IEEE Journal on Selected Areas in Communications' in ninth with 69, and 'IEEE Transactions on Power Systems' in tenth with 44. Figure 5 presents these sources graphically alongside their publication counts. The institutes whose researchers contribute most heavily to the WoS record are discussed in the following subsection.

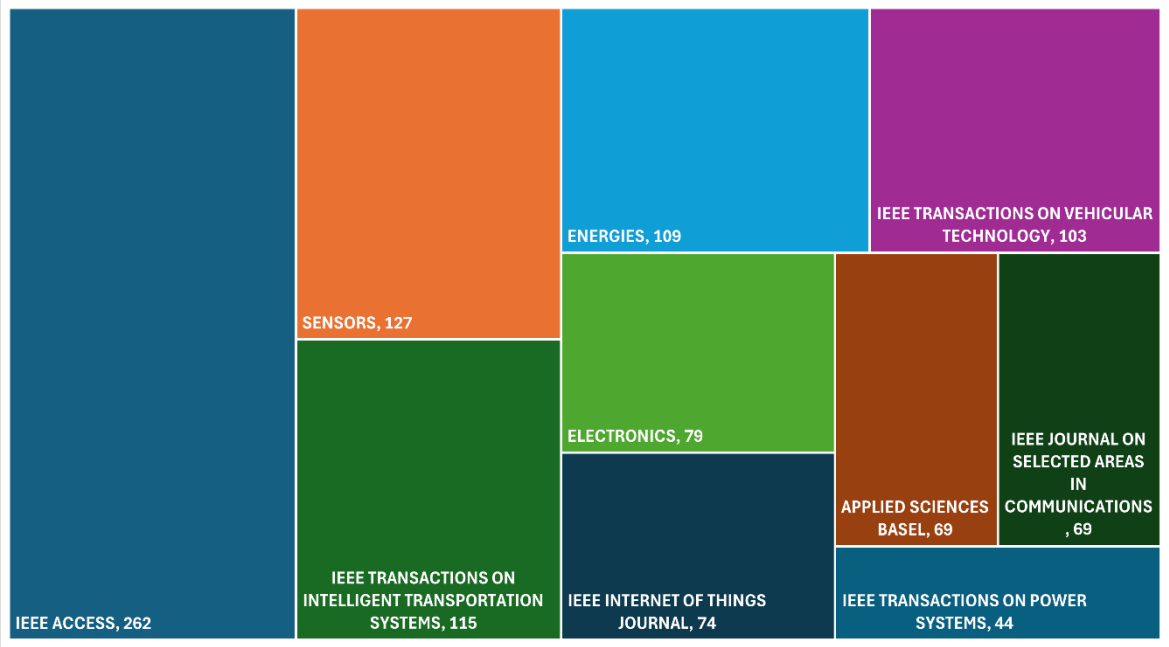


Figure 5. Top 10 leading source titles from 3,775 intrusion detection in CAV publications of the WoS database.

3.4. Prolific Institutes and Researchers

Hunan University College of Computer Science (China) heads the institutional ranking with 28 publications, with Korea University School of Cybersecurity (South Korea) close behind on 28. Nanyang Technological University College of Engineering (Singapore) and Guangdong University of Technology School of Automation (India) occupy third and fourth positions with 26 and 25 publications, respectively. Carleton University Faculty of Engineering and Design (Canada) follows with 21, and Beijing University of Posts and Telecommunications Institute of Network Technology (China) with 20. Four institutions share the remaining places with 19 WoS articles each on CAV intrusion detection: Beihang University School of Transportation Science and Engineering (China), City University of Hong Kong College of Engineering (Hong Kong), the State Key Laboratory of Networking and Switching Technology (China), and Virginia Polytechnic Institute and State University College of Engineering (United States). Figure 6 presents these ten institutes with their respective publication counts.

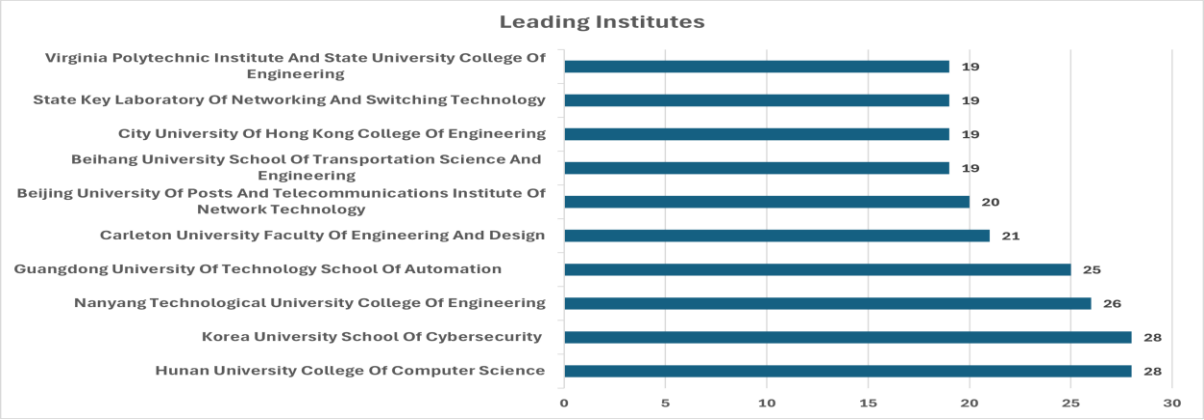


Figure 6. Top 10 leading institutes from 3,775 intrusion detection in CAV publications of the WoS database

Table 1 lists the researchers with the highest number of WoS publications in IoT intrusion detection. Four of them are based in China and two in Romania, with South Korea, Singapore, Australia, and Japan each represented by a single author.

Table 1. The top ten most prolific researchers in the field of intrusion detection in CAV.

Author	Published Institute	Nation	NPub
Xie, Guoqi	Hunan University College of Computer Science and Electronic Engineering	Peoples R China	26
Li, Renfa	Hunan University College of Computer Science and Electronic Engineering	Peoples R China	25
Groza, Bogdan	Universitatea Politehnica Timișoara, University of Siena, Inst E Austria Timisoara, Tech Univ Timisoara	Romania	18
Jo, Hyo Jin	Yonsei University, Grad Sch Informat	South Korea	17
Lee, Dong Hee Michael	NCS Pte Ltd	Singapore	15
Shi, Peng	The University of Adelaide Faculty of Engineering Computer and Mathematical Sciences	Australia	15
Guo, Zehua	Zhengzhou Res Inst, Beijing Institute of Technology Hunan University of Chinese Medicine Key Lab Intelligent Control & Decis Complex Syst, New York University, ChinaCache Northwestern Polytechnical University	Peoples R China	14
Murvay, Pal-Stefan	Universitatea Politehnica Timisoara	Romania	13
Zeng, Gang	Nagoya University Graduate School of Engineering School of Engineering	Japan	13
Dou, Songshi	University of Hong Kong Inst Technol Beijing Institute of Technology Key Lab Intelligent Control & Decis Complex Syst	Peoples R China	12

3.5. Trends in Nations

Figure 7 traces publication trends for the ten leading nations contributing to CAV intrusion detection in the WoS record. The USA produced the highest output in 2014 and 2015, with China close behind; from 2016 onwards, China took and held the lead. India rose notably in 2021–2022, trailing only China. Ranked by total articles published between 2014 and 2024, the order is People's Republic of China (1247), the United States (583), India (500), South Korea (288), Canada (219), England (217), Saudi Arabia (204), Australia (170), Iran (170), and

Italy (153). The popular research areas within IoT intrusion detection are examined in the subsections that follow.

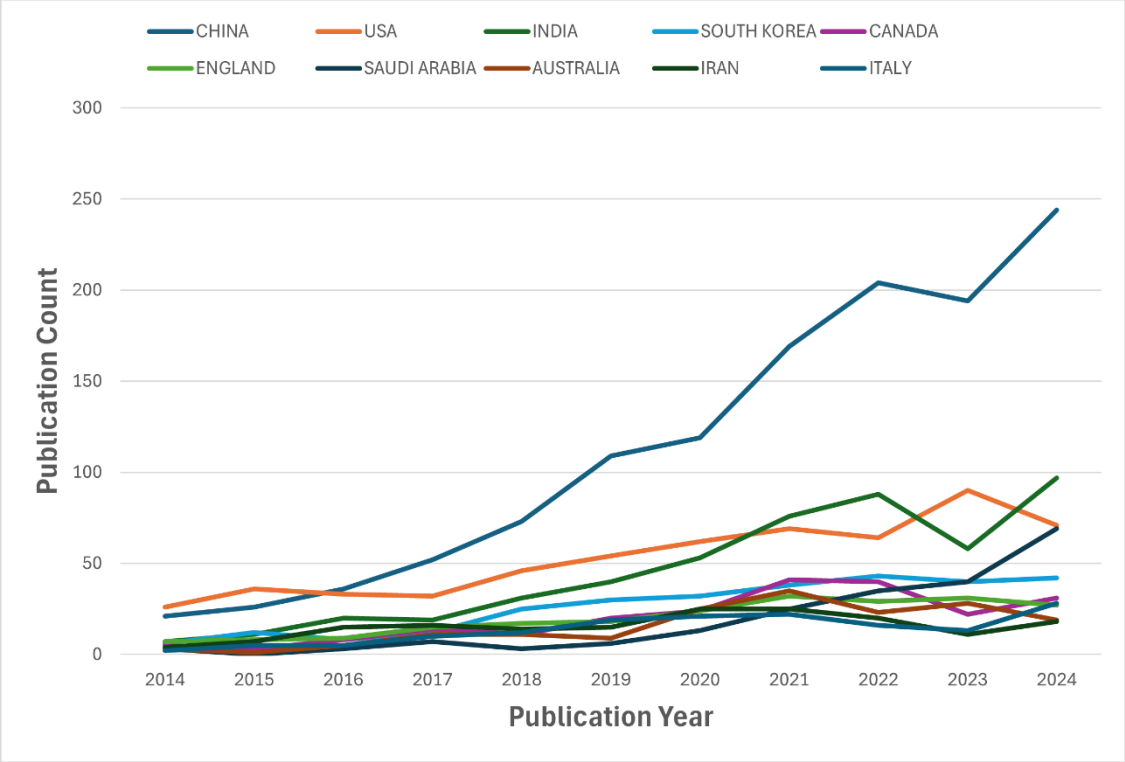


Figure 7. Trends in publications of nations from 3,775 intrusion detection in CAV publications from WOS.

3.6. Popular Research Areas

'Engineering' is the most active research area in WoS with 2,345 entries, ahead of 'Computer Science' with 1,514. 'Telecommunication' ranks third with 1,024 documents, reflecting sustained attention to security strategies for IoT-connected communication networks. A further 368 publications fall under 'Transportation', covering applications of IoT technology in that domain, particularly in intelligent industrial settings. 'Automation Control Systems' and 'Instruments and Instrumentation', with 355 and 251 WoS publications respectively, supply a multidisciplinary basis for examining intrusion risk within an IoT ecosystem. Interest in new materials and technologies for IoT security is evidenced by 226 articles indexed under 'Energy Fuels'. Chemistry follows in eighth place with 224 records and Physics ninth with 221, while Science, Technology, and Other Topics contributes a further 161 WoS papers concerned with intrusion detection in IoT. Figure 8 shows the trending study domains in CAV intrusion detection with documented counts from 2014 to 2024.

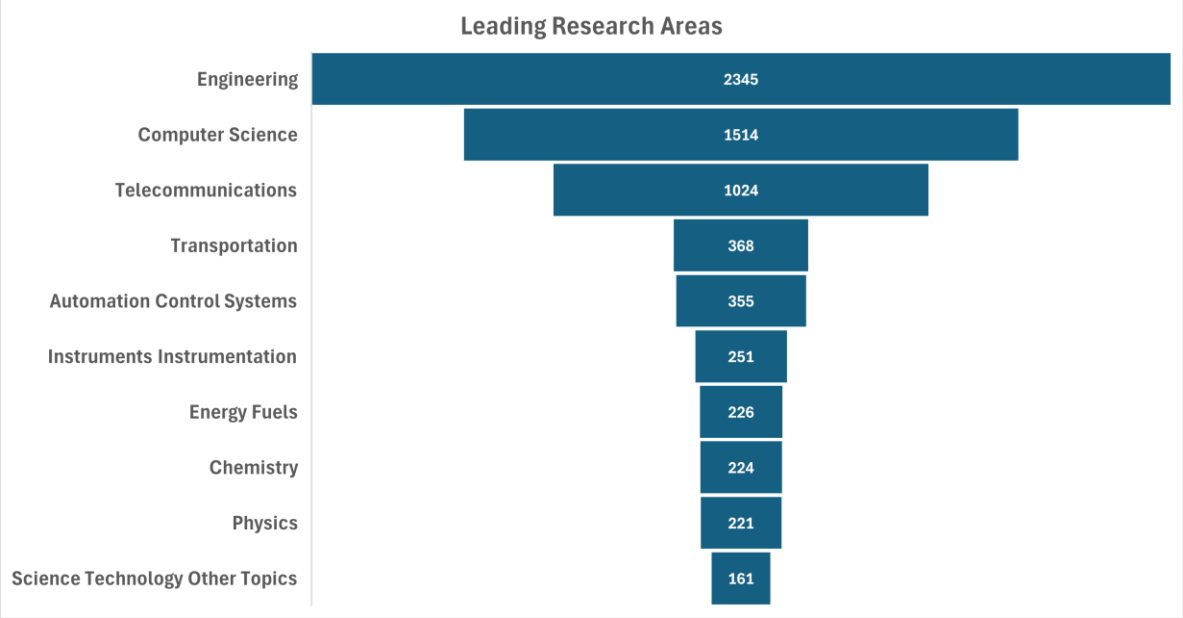


Figure 8. Leading research areas from 3,775 intrusion detection in CAV publications from WoS.

Engineering has dominated the field since 2014. Computer Science shows pronounced growth from 2018 onwards. The trend data indicate rising publication numbers and sustained expansion in Computer Science, Engineering, Telecommunications, and Transportation, alongside steadier growth in Automation Control Systems, Instruments and Instrumentation, Energy Fuels, Chemistry, Physics, and Other Science and Technology Topics. For 2024 specifically, Engineering recorded 383 publications and Computer Science 264, with Telecommunications at 191. Transportation registered 60, Automation Control Systems 54, Instruments and Instrumentation 43, Energy Fuels 25, Chemistry 35, and Physics 37, while Science Technology and Other Topics accounted for 41. Figure 9 plots these trends across the study domains named above.

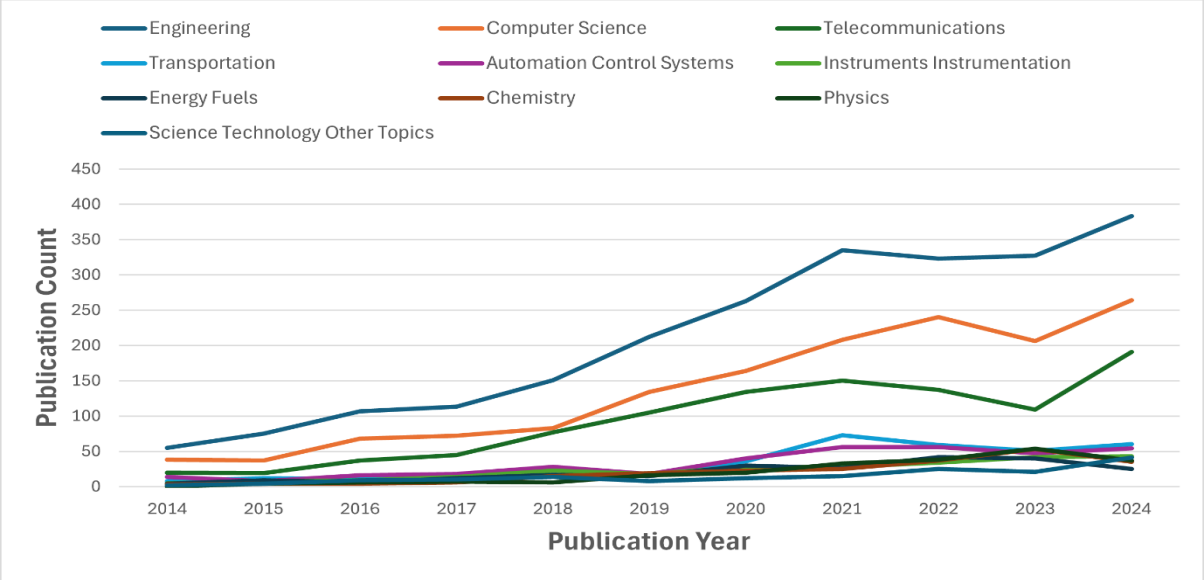


Figure 9. Trends in publication counts of research areas from 3,775 intrusion detection in CAV publications.

Table 2 breaks the publications down by study area and document type. Across every domain the research article is the dominant format. No proceedings papers are currently recorded under Instruments and Instrumentation. The distribution of research articles on CAV intrusion detection across WoS-indexed categories and publications is examined next.

Table 2. Distribution of publications by research area and paper category.

Research Area	Article	Proceeding	Review Article
Engineering	2,266	21	78
Computer Science	1,464	12	50
Telecommunications	992	4	32
Transportation	356	4	12
Automation Control Systems	346	5	9
Instruments Instrumentation	240	0	11
Energy Fuels	203	7	23
Chemistry	205	2	19
Physics	203	2	18
Science, Technology, Other Topics	144	1	17

3.7. Web of Science Categories and Indexed Publications

'Engineering Electrical Electronic' carries the largest share with 1,901 publications, followed by 'Telecommunications' with 1,024. Five of the ten leading WoS categories relate to computer science, indicating how much of the work on intrusion detection in connected and autonomous vehicles falls within that discipline. 'Computer Science Information Systems' ranks third with 900 publications, 'Automation Control Systems' fourth with 355, 'Transportation Science Technology' fifth with 355, 'Computer Science Artificial Intelligence' sixth with 269, and 'Computer Science Hardware Architecture' seventh with 261. 'Instruments Instrumentation' accounts for 251 articles. The two lowest positions in the top ten belong to 'Energy Fuels' with 226 publications and 'Engineering Multidisciplinary' with 206. Figure 10 displays these categories with their corresponding counts for CAV intrusion detection as classified by WoS.

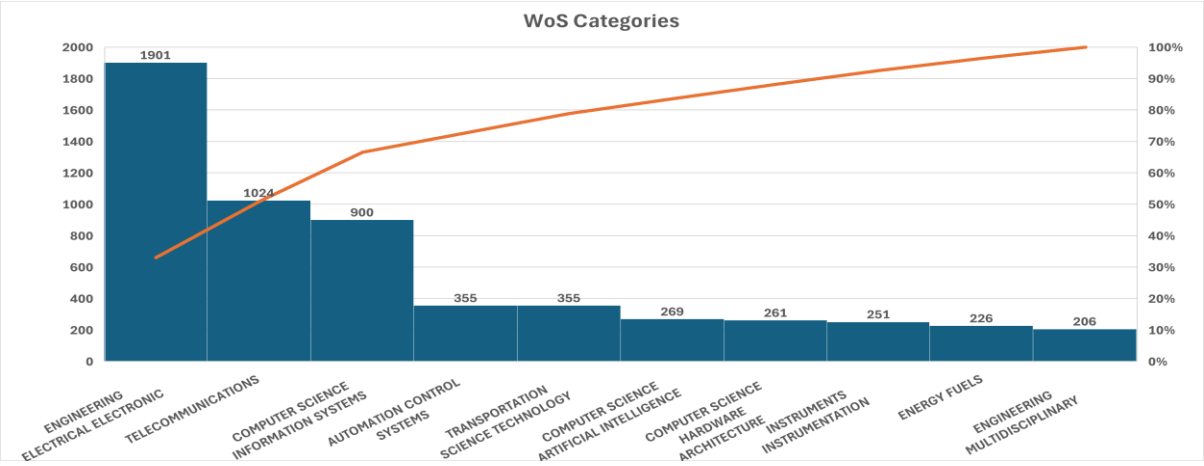


Figure 10. WoS categories from 3,775 intrusion detection documents in CAV publications.

Electrical Engineering and Electronics produced the greatest volume of documents across 2014 to 2024, with Telecommunications second. The ordering shifted in 2023, when Computer Science Information Systems moved into second place and Telecommunications into third. In 2019, the two leading categories were Electrical Engineering and Electronic and Telecommunications. By 2024, Computer Science Hardware Architecture and Computer Science Artificial Intelligence had published 40 and 41 documents, respectively. Figure 11 shows how publication patterns across WoS categories evolved between 2014 and 2024.

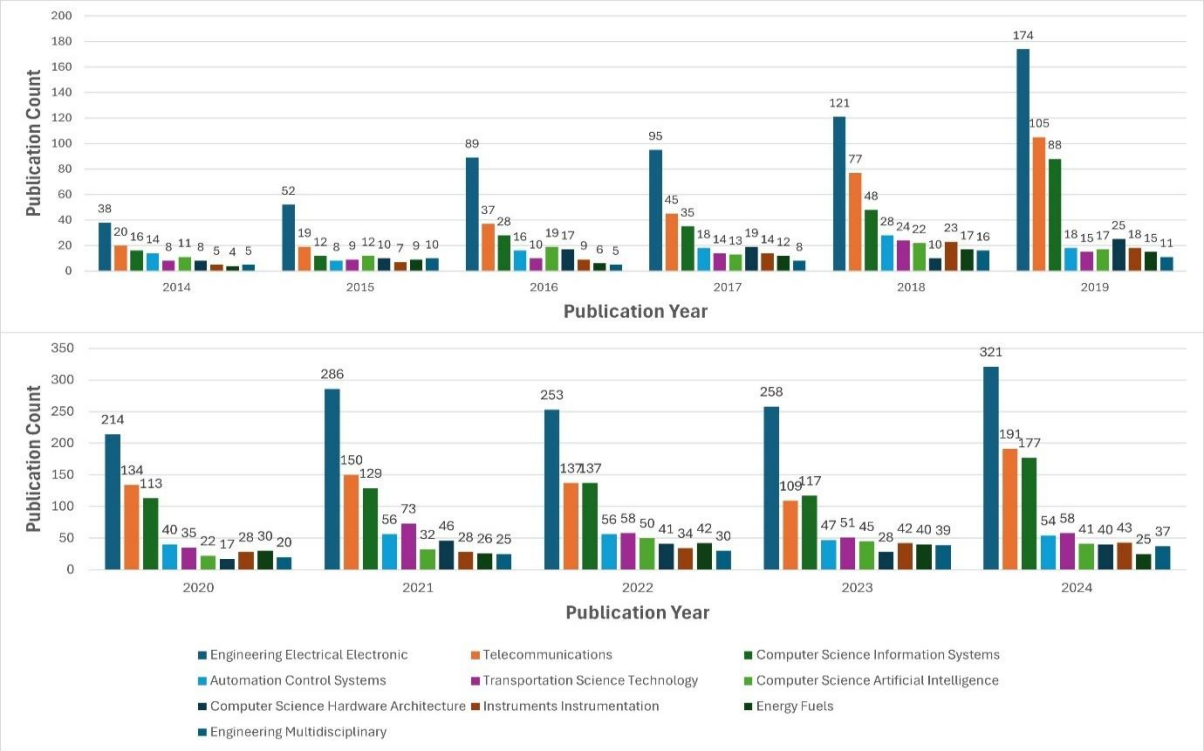


Figure 11. WoS trends from 3,775 intrusion detection papers in CAV publications.

Figure 12 breaks down the document types published on CAV intrusion detection within specific WoS categories. Research article counts increased consistently, whereas proceedings papers and review articles showed no clear trend.

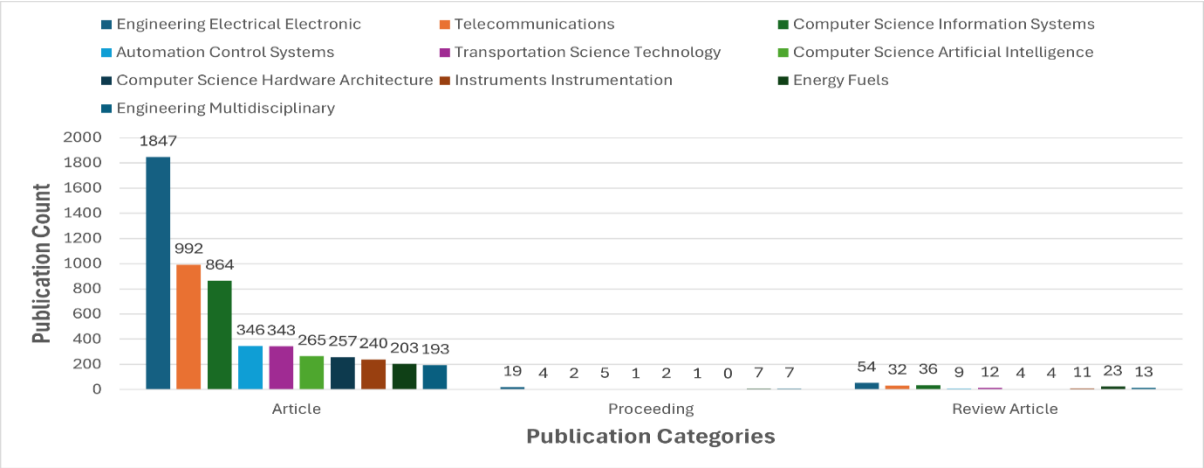


Figure 12. An analysis of document types within WoS categories, encompassing a total of 3,775 papers on intrusion detection in CAV.

Most WoS-indexed papers in the corpus originate from SCI-EXPANDED, which accounts for 3,758 publications; SSCI contributes 94 and CPCI-S a further 51. Three CAV-related intrusion detection articles appear in CPCI-SSH, and A&HCI ranks last with a single IoT-related intrusion detection article. Figure 13 sets out these publications with their corresponding counts across the WoS indexes. The leading funding sources for intrusion detection research in the Internet of Things are analysed in the following section.

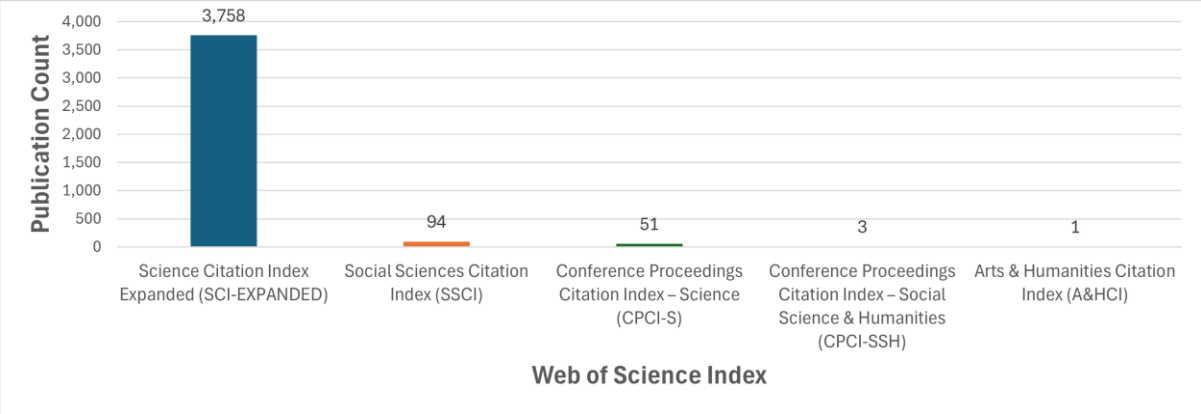


Figure 13. WoS indexes of 3,775 intrusion detection studies in CAV from the Web of Science database.

3.8. Funding Agencies

The National Natural Science Foundation of China (NSFC) is the largest single funder in CAV intrusion detection, accounting for roughly 23.623% of the 3,775 entities recorded in WoS. The National Science Foundation follows at approximately 4.27%, and the Fundamental Research Funds for the Central Universities contribute around 3.88%. Support from the National Key Research Development Program of China and from the European Union is also substantial, at 3.70% and 3.04%, respectively. Other significant funders in this area include the National Research Foundation of Korea, the China Postdoctoral Science Foundation, the Ministry of Science of the Republic of Korea, the Natural Sciences and Engineering Research Council of Canada (NSERC), and the Key Area Research and Development Program of Guangdong Province. Figure 14 shows the relative share of each funding agency alongside the distribution of publications. Open access categories are addressed in the following section.

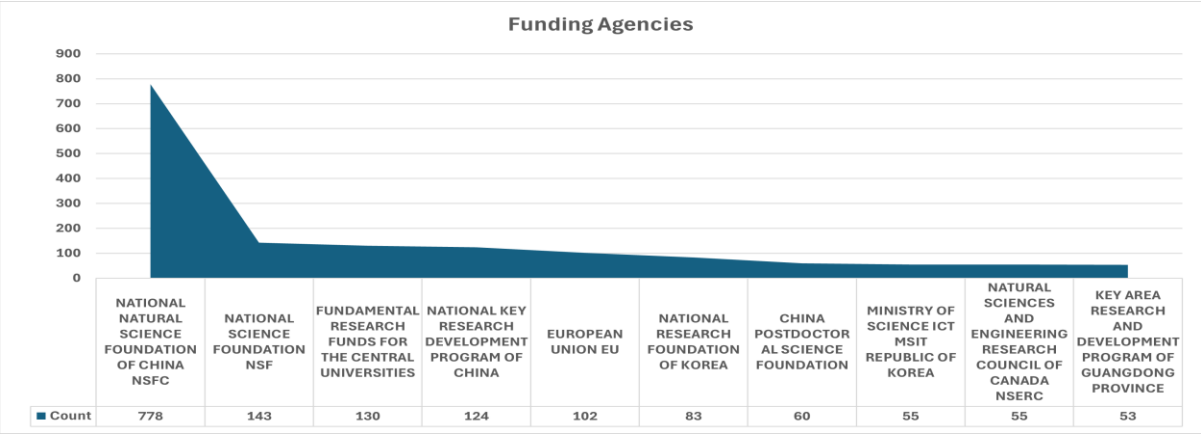


Figure 14. The top 10 funding agencies of a total of 3,775 intrusion detection in CAV publications from the WoS database.

3.9. Access Type

Open Access accounts for 46.97% of all publications in the corpus, meaning that nearly half the literature is freely available to any reader. Gold Open Access accounts for around 29.62% of entries, under which content becomes freely accessible immediately upon publication. Gold Hybrid represents approximately 4.80%: articles in conventional subscription journals that are opened to the public once the authors pay an additional charge. A further 4.77% are designated Free to Read, which grants readers temporary access following release. Green Published, Green Accepted, and Green Submitted, all found within conventional subscription-based journals, account for roughly 11.13%, 3.05%, and 10.68%, respectively. Figure 15 sets out these access categories with their corresponding counts.

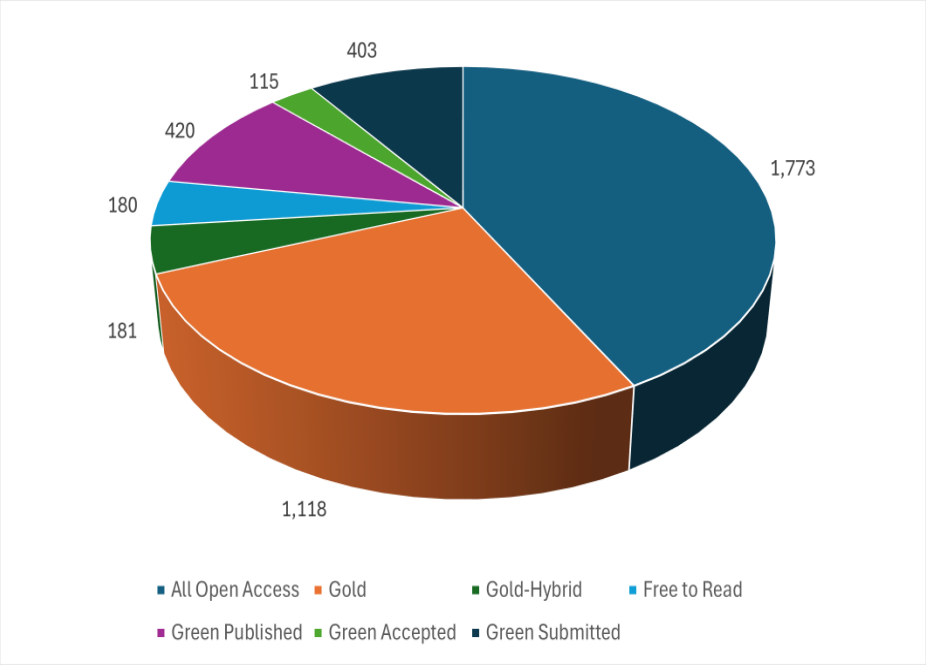


Figure 15. Distribution according to access type of a total of 3,775 intrusion detection in CAV publications from WoS

4. Co-Authorship Study

Collaboration between authors, institutions, and nations drives innovation and underpins the wider development of a research field. This section examines how those three levels of cooperation have shaped intrusion detection research in CAVs between 2014 and 2024. A fractional counting method was adopted, which accounts for both heavily and lightly cited sources within an article; the inclusion threshold was set at a minimum of five published articles and five citations per author, institution, or country, and publications with more than 25 contributors were excluded. What follows is organised by author, institution, and country in turn. Throughout, 'NPub' denotes the number of publications attributed to each entity and therefore serves as a measure of productivity in CAV intrusion detection, while Links records the number of collaborative connections between a given author, institution, or nation and others. For any publication with 'n' authors, institutions, or nations, the strength of association between any two collaborators was quantified as 1/n. The Sum of Link Strengths (SSL) aggregates collaboration strength across authors, institutions, or countries. This opening subsection deals exclusively with co-authorship among individual authors.

4.1. Author-Based Co-Authorship Study

The co-authorship network among contributing authors is analysed here. VOSviewer identified 12,513 authors active in this domain, and 1,165 publications met the criteria set for analysis. Of the papers identified, 34 fell within the most densely interconnected co-author network. Table 3 reports the 15 authors from the unconnected set with the highest co-authorship TLS values. TLS for co-authorship is always an integer, because an author's fractional link strengths sum to one across each published paper. It follows that co-authorship intensity between two authors scales directly with that author's publication count (NPub), giving a linear relationship between productivity and collaborative reach under this metric.

Table 3. The top fifteen authors have the highest TLS values

Rank	Nation	Author	NPub	Citations	TLS
1	China	Li, Renfa	25	609	24
2	China	Xie, Guoqi	24	585	22
3	South Korea	Jo, Hyo Jin	17	924	15
4	Romania	Groza, Bogdan	18	381	13
5	China	Guo, Zehua	13	117	13
6	South Korea	Lee, Dong Hoon	15	900	13
7	South Korea	Choi, Wonsuk	12	493	12
8	China	Liu, Jiajia	14	858	12
9	Romania	Murvay, Pal-Stefan	12	336	12
10	Japan	Zeng, Gang	12	276	12
11	China	Dou, Songshi	11	53	11
12	South Korea	Woo, Samuel	11	613	11
13	China	Zhang, Chuan-Ke	11	355	11
14	India	Kumar, Prabhat	10	360	10
15	Japan	Kurachi, Ryo	11	239	10

Figure 16 renders the co-authorship network, with node colour distinguishing collaborative groupings. Li, Renfa appears in blue as the leading author by TLS, Zeng, Gang in green, and so on for the remaining clusters.

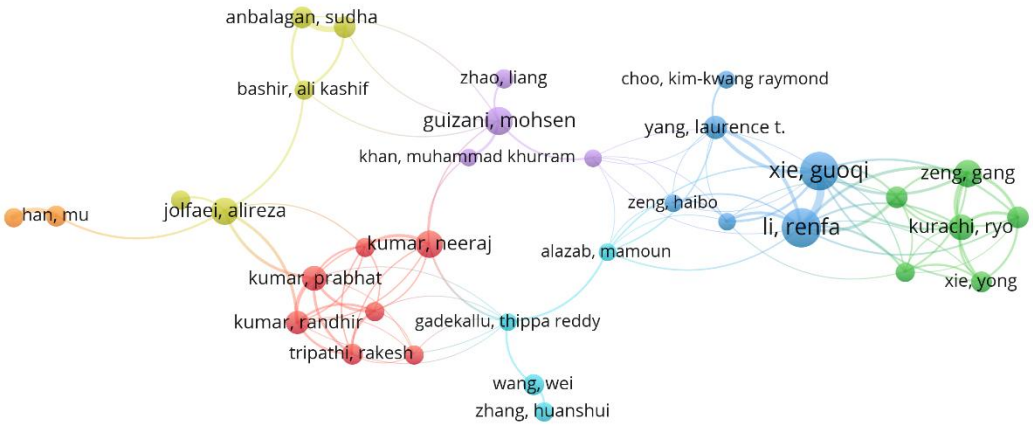


Figure 16. A visual representation of the co-authorship network among

4.2. Institute-Based Co-Authorship Study

Co-authorship between the institutions publishing CAV research is examined here. VOSviewer detected 3,702 institutions active in the field, of which only 406 satisfied the stated requirements, and 395 of those formed part of the largest integrated institutional network. Table 4 reports the ten institutions with the highest co-authorship TLS values within that set of 406. Since co-authorship strength always sums to one, institutional TLS derived from co-authorship is necessarily an integer, and in principle an institution's TLS should equal its article count (Np). Table 4 does not follow that pattern: the TLS values reported there fall below the corresponding publication totals. Hunan University illustrates the point. Ranked second by TLS, it produced 44 articles, of which 34 carried a TLS value arising from co-authorship with another institution. The remaining 10 papers either had no co-authors outside the institution or were written with partners falling below the thresholds of 5 publications and 5 citations. The same pattern recurs across the other institutions listed. Chinese institutes predominate throughout Table 4.

Table 4. The top ten institutes with the highest TLS values.

Rank	Institute	Nation	NPub	Citations	TLS
1	Chinese Academy Sciences	China	39	908	36
2	Hunan University	China	44	846	34
3	Huazhong University of Science and Technology	China	46	1717	30
4	Southeast University	China	35	666	26
5	King Saud University	Saudi Arabia	33	711	24
6	Prince Sattam Bin Abdulaziz University	Saudi Arabia	26	322	24
7	Tsinghua University	China	33	829	24
8	University of Electronic Science and Technology of China	China	41	1372	24
9	Adelaide University	Australia	26	543	23
10	Beihang University	China	40	737	21

Figure 17 shows the co-authorship structure across institutions. Colour distinguishes the research groupings within the network, and the relative thickness of each connecting link indicates the strength of the tie between institutes.

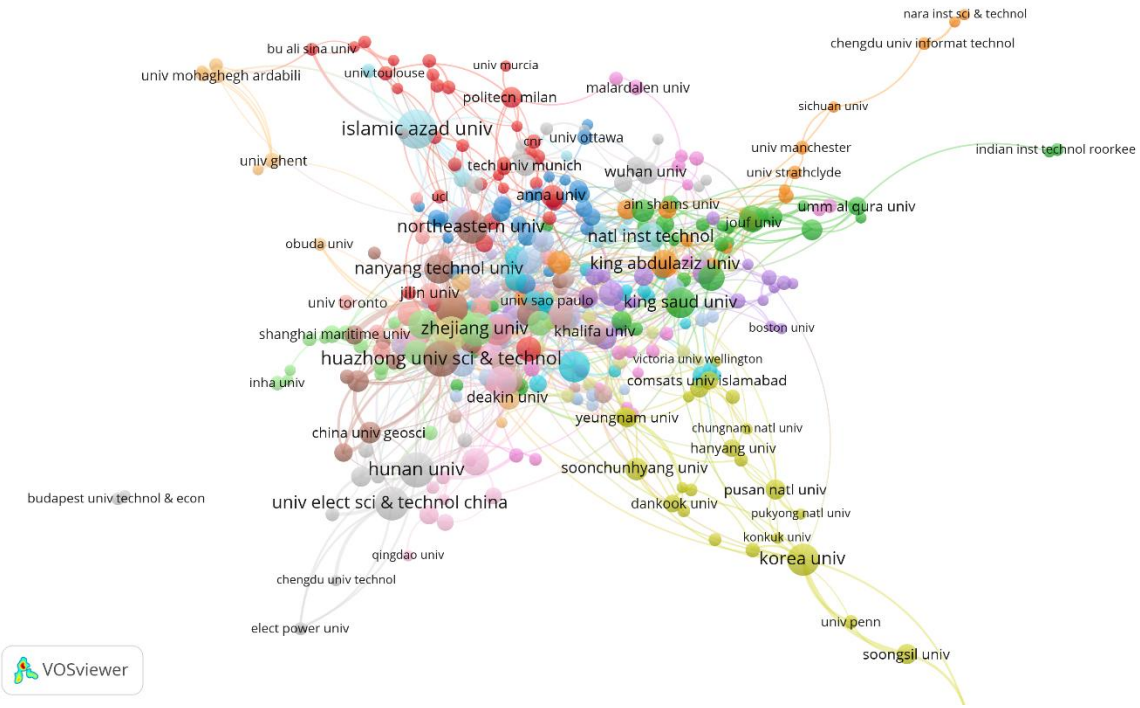


Figure 17. Co-authorship network among institutes

4.3. Nation-Based Co-Authorship Study

This subsection presents a co-authorship analysis of the countries contributing to intrusion detection research in IoT. VOSviewer identified 117 nations, of which 71 met the stated requirements. Table 5 lists the fifteen most referenced of those 71 by TLS. As with authors and institutions, national co-authorship TLS is an integer, since fractional linkages within a nation sum to one for each published work; a nation's total co-authorship strength across all its papers should therefore equal its article count, Np. Table 5 departs from this: the reported TLS values fall below the corresponding publication totals. The explanation is that some papers were published without a co-author from another country, and much of the remainder was co-authored only with nations falling below the inclusion thresholds: fewer than three papers on CAV intrusion detection and/or fewer than five WoS citations, which removed them from consideration. China illustrates the effect, with a TLS of 483 against 1,245 articles; the gap of 762 articles represents work by Chinese academics that either had no international co-authors or involved contributors from nations below the five-publication and five-citation thresholds. The USA ranks second with 550 articles and a TLS of 306, and India third with 263 publications and a TLS of 216. Saudi Arabia takes fourth place, with more than 204 publications and a TLS above 172, and Canada fifth with 218 articles.

Table 5. The 15 nations with the highest TLS values

Rank	Nation	NPub	Citations	TLS
1	China	1245	27108	483
2	USA	550	15985	306
3	India	532	8792	216
4	Saudi Arabia	204	3326	172
5	Canada	218	7207	167
6	England	216	6877	164

7	Australia	169	6652	142
8	South Korea	287	7083	107
9	Pakistan	113	2795	102
10	Italy	152	3202	83
11	France	104	2911	82
12	Germany	105	2007	67
13	Iran	169	2922	67
14	Egypt	72	1191	62
15	Japan	91	3711	61

Figure 18 maps the co-authorship network across nations. Colours mark the distinct research groupings, and link thickness indicates how strong the relationship between two countries is. The purple cluster contains China, South Korea, Japan, Thailand, Vietnam, and Nepal; the green comprises India, Norway, and Taiwan; and the red brings together England, Iran, Italy, and Australia.

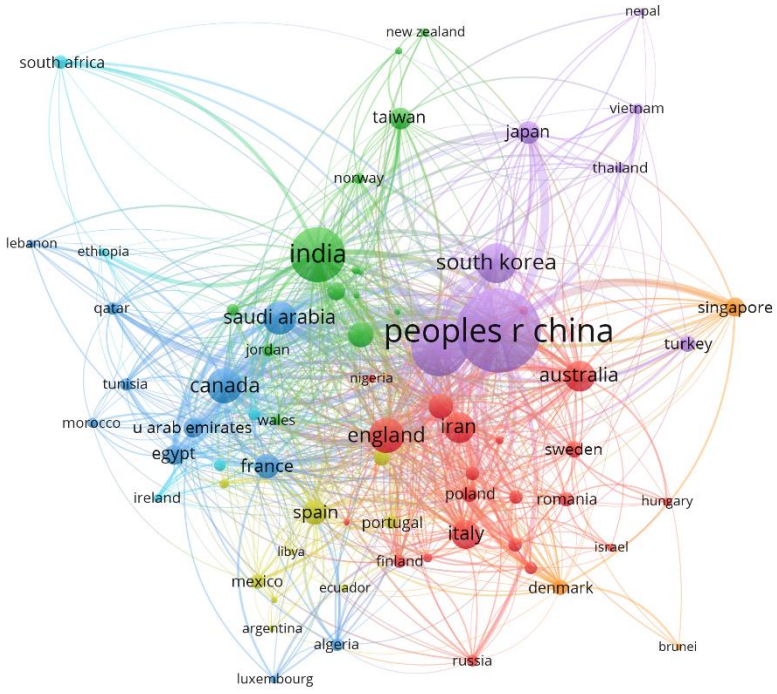


Figure 18. A visual representation of the co-authorship network among nations

5. Co-Occurrence Study

Keyword co-occurrence in the CAV intrusion detection literature recorded in WoS between 2014 and 2024 is examined in this section. The analysis applies the fractional counting method throughout, with a minimum threshold of five occurrences per term.

5.1. All Keyword-Based Co-Occurrence Study

This subsection examines co-occurrence patterns among the keywords WoS assigns to CAV intrusion detection research. The initial retrieval returned 14,723 keywords, of which 1,020 cleared the frequency threshold for analysis. Table 6 lists the top 15 co-occurring keywords ranked by TLS in descending order. ‘Intrusion Detection’ co-occurs with 464 other WoS-

indexed keywords across the analysed articles, meaning it appeared alongside each of those 464 terms at least five times. For an article containing ‘n’ such terms, the link strength between any two co-occurring keywords is 1/n, and a keyword’s TLS is the sum of these fractional strengths across all relevant publications. In theory, the fractional contribution of a keyword within a single paper sums to one, yet the TLS values in Table 6, while consistently whole numbers, fall below the actual publication counts (Np). This gap indicates cases where authors either did not use other qualifying CAV intrusion detection keywords or used terms falling below the frequency threshold. ‘Design’ is a clear example: second-highest by TLS at 424, it appeared in 122 articles without co-occurring with other qualifying WoS keywords in this domain. Taken as a group, the top fifteen point to a research focus on intrusion and anomaly detection through machine- and deep-learning-based classification in CAV security.

Table 6. The 15 keywords with the maximum co-occurrence TLS values for all keywords

Rank	Keyword	Occurrence	TLS
1	Intrusion Detection	464	464
2	Design	434	424
3	Security	383	377
4	Optimization	237	235
5	Internet	209	208
6	System	206	193
7	Model	187	184
8	Systems	181	179
9	Machine Learning	176	176
10	Algorithm	171	169
11	Controller Area Network	173	169
12	Deep Learning	168	164
13	Intrusion Detection System	163	162
14	Anomaly Detection	148	146
15	Networks	147	143

Figure 19 maps the relations among all keywords. Intrusion detection and anomaly detection appear as green nodes, while design, system, and optimization are among the terms rendered in red.

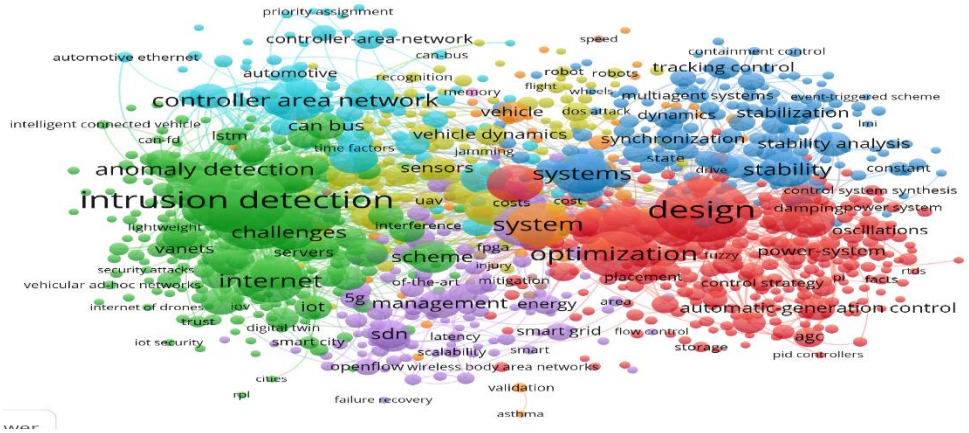


Figure 19. The co-occurrence network encompassing all keywords from the Web of Science.

5.2. Author's Keyword-Based Co-Occurrence Study

This subsection analyses co-occurrence among author-assigned terms in CAV intrusion detection publications. The search returned 11,938 author keywords, of which 635 met the criteria for co-occurrence analysis, and Table 7 lists the top 15 by TLS. The author keyword 'Intrusion Detection' co-occurs with 293 other author keywords relevant to IoT intrusion detection across the papers examined, and carries a TLS of 288 the aggregate of its appearances alongside each of those 293 terms, each occurring at least five times. As before, the link strength between two co-occurring author keywords in an article containing 'n' such keywords is 1/n, and a keyword's TLS is the cumulative strength of its co-occurrence connections across all published articles. Consistent with the method, co-occurrence TLS for author keywords is always an integer, representing the aggregation of fractional link strengths across publications.

Table 7. The 15 keywords with the maximum co-occurrence TLS values for author keywords

Rank	Author Keyword	Occurrences	TLS
1	Intrusion Detection	293	288
2	Security	281	276
3	Machine Learning	176	164
4	Deep Learning	168	151
5	Controller Area Network	146	124
6	Internet of Things	123	119
7	Intrusion Detection System	112	109
8	Protocols	95	95
9	Controller Area Network (CAN)	114	92
10	Load Frequency Control	104	79
11	Optimization	79	75
12	Anomaly Detection	78	74
13	Power System Stability	78	73
14	Delays	69	69
15	In-Vehicle Network	70	67

Figure 20 presents the VOSviewer co-occurrence map for author-supplied keywords. Purple nodes cover intrusion detection, machine learning, and IoT; blue nodes cover Controller Area Network (CAN), CAN bus, and automotive Ethernet.

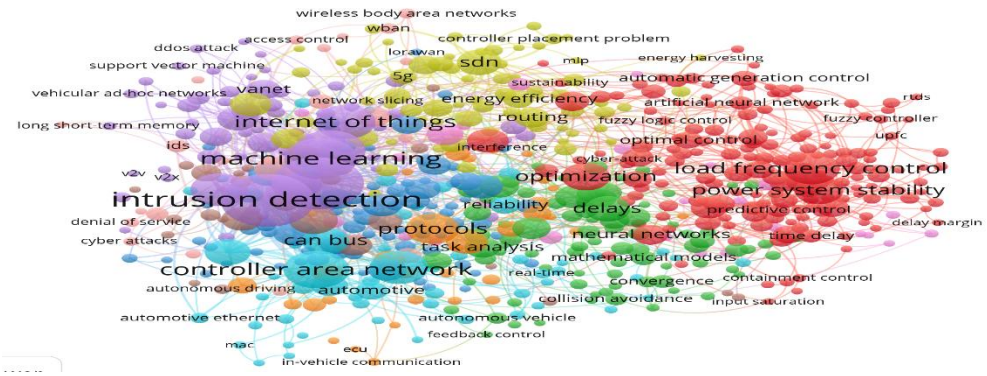


Figure 20. The co-occurrence network comprising author from the Web of Science.

6. Burst Detection Study

Burst detection was performed in CiteSpace from 2014 to 2024, and the results are reported here. The 'Top N per slice' criterion was applied to identify and examine sharp temporal increases in citation activity. This approach isolates the terms and articles that saw pronounced citation growth within particular windows. Burst detection in CiteSpace uses Kleinberg's algorithm, which picks out abrupt surges in attention. Burst strength matters here for a specific reason: it shows when a publication or keyword became temporally salient within the research community. Trends from 2014 to 2023 are compared with those emerging in 2024, bringing the most recent temporal patterns into focus.

6.1. Keyword Burst Detection

Burst detection results for keywords in CAV intrusion detection are discussed below.

6.1.1. Trends from 2014–2024

Table 13 reports the top 15 keywords ranked by burst strength between 2014 and 2024. The strongest bursts belong to 'software defined networking', 'schedulability study', and 'vehicular ad hoc networks', at 4.09, 4.03, and 3.92, respectively, across the 2016–2020 window. 'Authentication' registered 3.38 during 2021–2022. Earlier, during the 2014–2017 period, 'controller area network', 'damping controller', and 'can bus' recorded 2.88, 2.85, and 2.56, respectively. Between 2019 and 2022, four further terms peaked: 'communication' at 2.44, 'load balancing' at 2.22, 'network traffic' at 2.73, and 'artificial neural network' at 2.10. Each marks a period of concentrated research attention.

Table 13. Top 15 keywords with the strongest citation bursts.

Rank	Keyword	Year	Strength	Begin	End
1	software defined networking	2014	4.0974	2016	2020
2	schedulability study	2014	4.0387	2014	2015
3	vehicular ad hoc networks	2014	3.9298	2018	2020
4	authentication	2014	3.3878	2021	2022
5	controller area network	2014	2.8812	2016	2017
6	damping controller	2014	2.8517	2016	2017
7	can bus	2014	2.5691	2014	2017
8	communication	2014	2.448	2021	2022
9	load balancing	2014	2.2219	2019	2021
10	artificial neural network	2014	2.108	2019	2020

6.2. References Burst Detection

Burst detection, as applied to the cited CAV intrusion detection literature, is reported in this subsection.

6.2.1. Trends from 2014–2024

Table 14 lists the ten most cited papers ordered by citation burst strength. Kreutz et al. [19] recorded the strongest burst at 6.859, concentrated in a single year between 2018 and 2019. Zaidi et al. [17], published in 2019, reported 6.5048 across 2019 to 2020. Yao et al. [20] reached 6.0897 during 2018–2019, four years after publication. Lange et al. [21], published in 2015, recorded 5.6328 between 2018 and 2020, while Davis et al. [22] achieved 5.4484 across 2014

to 2016. Berde et al. [23] and Cho et al. [24] show comparable burst strengths of around 4.5, though in different windows. Sedjelmaci et al. [25] reached 4.2832 during 2019–2020. Al-Sultan et al. [26] and Choi et al. [13] recorded 3.7927 (2018–2019) and 3.513 (2022–2024), respectively.

Table 14. Top 10 references with the strongest citation bursts

Rank	Reference	Year	Strength	Begin	End
1	Kreutz D, 2015, P IEEE, V103, P14, DOI 10.1109/JPROC.2014.2371999 [19]	2015	6.859	2018	2019
2	Zaidi K, 2016, IEEE T VEH TECHNOL, V65, P6703, DOI 10.1109/TVT.2015.2480244 [17]	2016	6.5048	2019	2020
3	Yao G, 2014, IEEE COMMUN LETT, V18, P1339, DOI 10.1109/LCOMM.2014.2332341 [20]	2014	6.0897	2018	2019
4	Lange S, 2015, IEEE T NETW SERV MAN, V12, P4, DOI 10.1109/TNSM.2015.2402432 [21]	2015	5.6328	2018	2020
5	Davis RI, 2013, REAL-TIME SYST, V49, P73, DOI 10.1007/s11241-012-9167-8 [22]	2014	5.4484	2014	2016
6	Berde P, 2014, P 3 WORKSH HOT TOP S, V0, P1 [23]	2014	4.5565	2018	2019
7	Cho KT, 2016, PROCEEDINGS OF THE 25TH USENIX SECURITY SYMPOSIUM, V0, P911 [24]	2016	4.4673	2020	2021
8	Sedjelmaci H, 2015, COMPUT ELECTR ENG, V43, P33, DOI 10.1016/j.compeleceng.2015.02.018 [25]	2015	4.2832	2019	2020
9	Al-Sultan S, 2014, J NETW COMPUT APPL, V37, P380, DOI 10.1016/j.jnca.2013.02.036 [26]	2014	3.7927	2018	2019
10	Choi W, 2018, IEEE T INF FOREN SEC, V13, P2114, DOI 10.1109/TIFS.2018.2812149 [13]	2018	3.513	2022	2024

7. Citation Study

Citation-based networks that link documents, sources, authors, institutions, and nations in CAV intrusion detection are presented in this section.

7.1. Documents-Based Citation Study

This subsection reports the citation analysis of documents in CAV intrusion detection research, restricted to those with at least 5 citations each. Of the 3,775 papers retrieved, 2,303 met that criterion, and 1,141 manuscripts formed the largest set of interrelated works. Table 8 lists the ten most-cited papers from the disjoint group; most of the influential work dates from 2016 to 2020. H. Song and M. Kang appear as collaborators on several heavily referenced publications. The citation counts in Table 8 reflect the number of WoS publications that both reference these works and address intrusion detection in CAV. ‘Intrusion Detection System Using Deep Neural

Network for In-Vehicle Network Security' has attracted 400 citations, 95 of which come from WoS-published CAV intrusion detection work carrying at least five citations apiece. 'A Practical Wireless Attack on The Connected Car and Security Protocol for In-Vehicle CAN', published in 2015, has drawn 319 citations, 88 of them from WoS literature on CAV intrusion detection meeting the same threshold.

Table 8. The top 10 WoS articles with the maximum number of citation links.

Rank	Title	Source	Author	Year	Citations	Links
1	"In-Vehicle Network Intrusion Detection Using Deep Convolutional Neural Network" [9]	"Vehicular Communications"	"Song, Hyun Min; Woo, Jiyoung; Kim, Huy Kang"	2020	299	98
2	"Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security" [10]	"Plos One"	"Kang, Min-Joo; Kang, Je-Won"	2016	400	95
3	"A Practical Wireless Attack on The Connected Car and Security Protocol for In-Vehicle CAN" [11]	"IEEE Transactions on Intelligent Transportation Systems"	"Woo, Samuel; Jo, Hyo Jin; Lee, Dong Hoon"	2015	319	88
4	"A Survey of Intrusion Detection for In-Vehicle Networks" [12]	"IEEE Transactions on Intelligent Transportation Systems"	"Wu, Wufei; Li, Renfa; Xie, Guoqi; An, Jiyao; Bai, Yang; Zhou, Jia; Li, Keqin"	2020	207	83
5	"VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System" [13]	"IEEE Transactions on Information Forensics and Security"	"Choi, Wonsuk; Joo, Kyungho; Jo, Hyo Jin; Park, Moon Chan; Lee, Dong Hoon"	2018	193	80

6	"AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey" [14]	"ACM Computing Surveys"	"Rajapaksha, Sampath; Kalutarage, Harsha; Al-Kadri, M. Omar; Petrovski, Andrei; Madzudzo, Garikayi; Cheah, Madeline"	2023	57	61
7	"Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and A Meta-Taxonomy" [15]	"Electronics"	"Karopoulos, Georgios; Kambourakis, Georgios; Chatzoglou, Efstratios; Hernandez-Ramos, Jose L.; Kouliaridis, Vasileios"	2022	32	53
8	"Intrusion Detection in The Automotive Domain: A Comprehensive Review" [16]	"IEEE Communications Surveys and Tutorials"	"Lampe, Brooke; Meng, Weizhi"	2023	15	52
9	"Host-Based Intrusion Detection for VANETS: A Statistical Approach to Rogue Node Detection" [17]	"IEEE Transactions on Vehicular Technology"	"Zaidi, Kamran; Milojevic, Milos B.; Rakocevic, Veselin; Nallanathan, Arumugam; Rajarajan, Muttukrishnan"	2016	121	51
10	"Controller Area Network Reliability: Overview of Design Challenges and Safety Related Perspectives Of Future	"IET Intelligent Transport Systems"	"Ben Lakhal, Nadhir Mansour; Nasri, Othman; Adouane, Lounis; Hadj Slama, Jaleleddine Ben"	2020	15	50

	Transportation Systems" [18]

Figure 21 renders the citation graph for CAV intrusion detection derived from the WoS-published articles, with node colour and connecting links reflecting co-citation relationships.

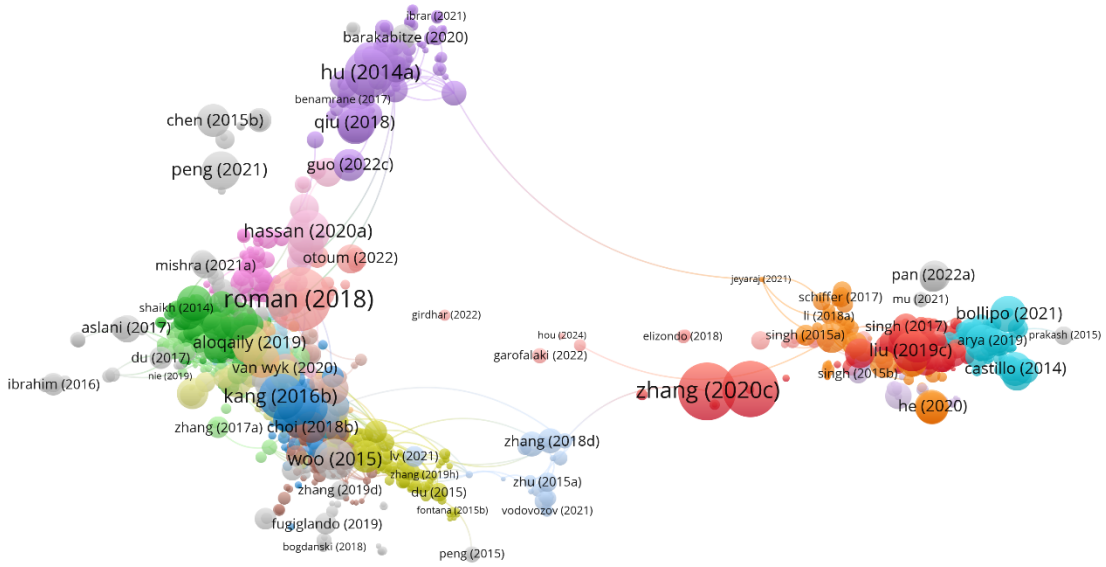


Figure 21. Depiction of citation network among documents

7.2. Source-Based Citation Study

This subsection reports the citation analysis of publications in CAV intrusion detection research. Inclusion required at least 5 publications and 5 citations per source. The initial search returned 684 sources, of which 171 satisfied that criterion. Table 9 lists the ten most frequently referenced sources ranked by TLS, together with their citation counts and publication totals (NPub). 'Ad Hoc Networks' has published 23 articles on intrusion detection in CAVs, which have collectively drawn 1089 citations from other WoS publications working in the same area. Only a minority of the sources retrieved met the five-publication, five-citation threshold.

Table 9. The top 10 sources with the highest TLS values.

Rank	Source	NPub	Citations	TLS
1	"ACM Transactions on Design Automation of Electronic Systems"	6	72	1209
2	"ACM Transactions on Embedded Computing Systems"	12	214	1207
3	"Actuators"	5	9	776
4	"Ad Hoc Networks"	23	1089	681
5	"Advances In Mechanical Engineering"	7	47	541
6	"Aims Mathematics"	6	10	449
7	"Ain Shams Engineering Journal"	8	62	426
8	"Alexandria Engineering Journal"	6	91	342
9	"Applied Energy"	16	703	280
10	"Applied Sciences-Basel"	69	665	251

Figure 22 maps the citation networks for CAV intrusion detection drawn from WoS-indexed material. Colour-coded nodes and connecting links represent co-citation relationships between sources. 'Neural Networks' and 'Energies' anchor the red network, while 'IEEE Access', 'IEEE Transactions on Vehicular Technology', and 'Computer Networks' sit within the green each grouping marking a cluster of frequently co-cited sources.

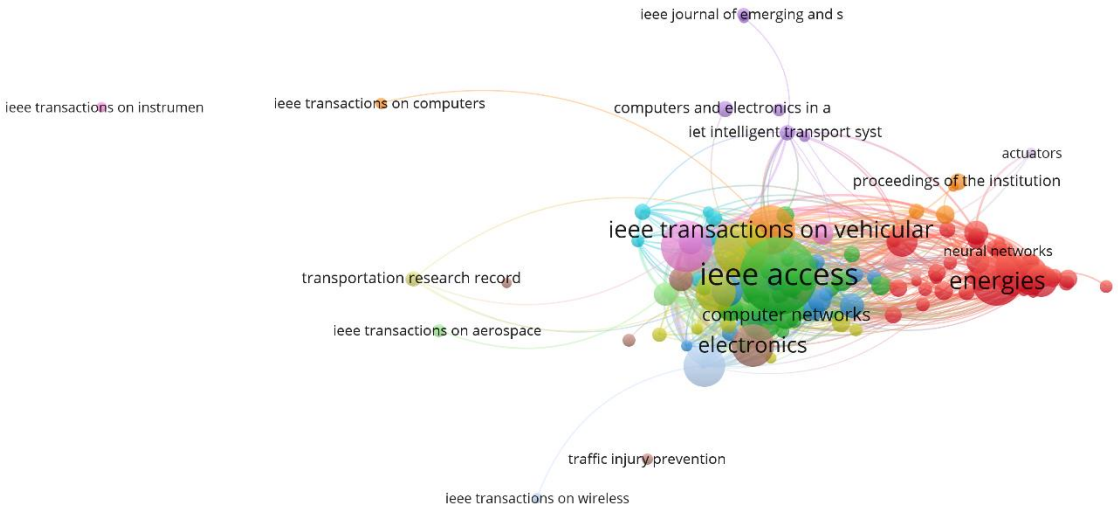


Figure 22. A visual representation of the citation network among sources

7.3. Author-Based Citation Study

Author-level citation patterns in intrusion detection research relating to the Internet of Things are analysed here. Authors were included if they had at least five publications and five citations, and documents with more than 25 co-authors were omitted. Of the 12,513 authors initially identified, 163 met these criteria, and 150 of them formed the largest interconnected network of researchers. Table 10 lists the 10 most-referenced authors from the unconnected group, ranked by TLS. The values reported indicate how many distinct WoS scholars have cited each author's contributions to IoT intrusion detection. Hyo-Jin Jo, for example, published 17 WoS-indexed works on CAV intrusion detection between 2014 and 2024 and received 924 citations from separate academics meeting the minimum of three publications and five citations, each of which establishes an individual citation link. Link strength scales with the number of citations it carries, and an author's TLS is the cumulative strength of all such linkages. The distribution in Table 10 is dominated by researchers at institutions in South Korea (four authors), China (two), and Japan (two). Renfa Li ranks fourth by TLS, with 614 citations, against a total citation count of 609.

Table 10. The top 10 authors with the highest citation TLS values.

Rank	Author	Nation	NPub	Citations	TLS
1	Jo, Hyo Jin	South Korea	17	924	686
2	Lee, Dong Hoon	South Korea	15	900	631
3	Xie, Guoqi	China	24	585	618
4	Li, Renfa	China	25	609	614

5	Choi, Wonsuk	South Korea	12	493	490
6	Groza, Bogdan	Romania	18	381	390
7	Woo, Samuel	South Korea	11	613	366
8	Murvay, Pal-Stefan	Romania	12	336	327
9	Zeng, Gang	Japan	12	276	317
10	Kurachi, Ryo	Japan	11	239	290

Figure 23 maps the citation networks for IoT intrusion detection at the author level within WoS. Node colour and connections reflect co-citation relationships. The green network includes authors such as Shi, Peng, Jiang, Jin, Li, and Yang. Jo, Hyo Jin, the principal author by this measure, appears as a blue node, while Wang, Yu, Kumar, Neeraj, and Guizani, Mohsen is shown in red.

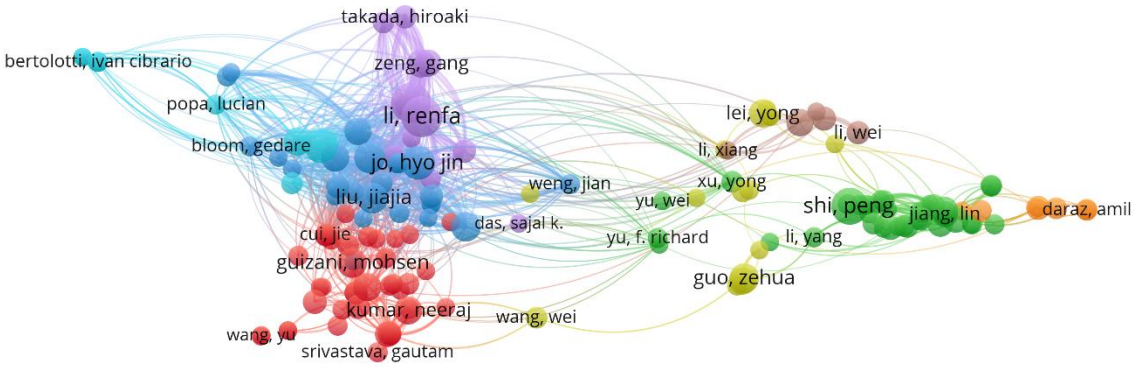


Figure 23. Depiction of the citation network among authors

7.4. Institute-Based Citation Study

Citation patterns among research institutions working on CAV intrusion detection are analysed in this subsection. Institutions were included only if they had at least 5 published documents and 5 citations, and co-authored documents across more than 25 nationalities were excluded from the analysis. A further threshold of three published works and five citations per source was also applied. VOSviewer identified 3,702 institutes that met these requirements; 406 sources ultimately satisfied the criteria, yielding an integrated network of 396 institutes. Table 11 lists the ten most-referenced institutes by TLS from the non-connected network, along with publication counts (NPub), citations, and total link strengths. China accounts for four of the institutions listed, South Korea and the USA for two each, with Saudi Arabia and Romania contributing one apiece. Korea University leads with 38 research papers, 1,907 citations, and a TLS of 1,124. Hunan University in China takes second place with a TLS of 724 across 44 articles. Northwestern Polytechnical University, despite producing more publications (NPub = 30) than Soonchunhyang University, ranks fourth with a TLS of 356. Hunan University has the largest publication count in Table 11 (NPub = 44) yet still ranks second overall, due to fewer

inter-institutional citation linkages. Beihang University, in fifth place, shows a comparable pattern.

Table 11. The top 10 institutes with the highest citation TLS values.

Rank	Institute	Nation	NPub	Citations	TLS
1	Korea University	South Korea	38	1907	1124
2	Hunan University	China	44	846	724
3	Soonchunhyang University	South Korea	19	482	418
4	Northwestern Polytechnical University	China	30	881	356
5	Beihang University	China	40	737	324
6	King Saud University	Saudi Arabia	33	711	319
7	State University of New York at New Paltz	USA	7	378	302
8	Politehnica University Timisoara	Romania	17	310	299
9	University of Pennsylvania	USA	7	415	297
10	Xidian University	China	23	1318	279

Figure 24 maps institutional citation connections in IoT intrusion detection globally, with distinct colours marking separate citation networks. Huazhong University of Science and Technology, Zhejiang University, and Shandong University of Science and Technology are picked out in green, while Beijing Institute of Technology and Princeton University appear in bright yellow.

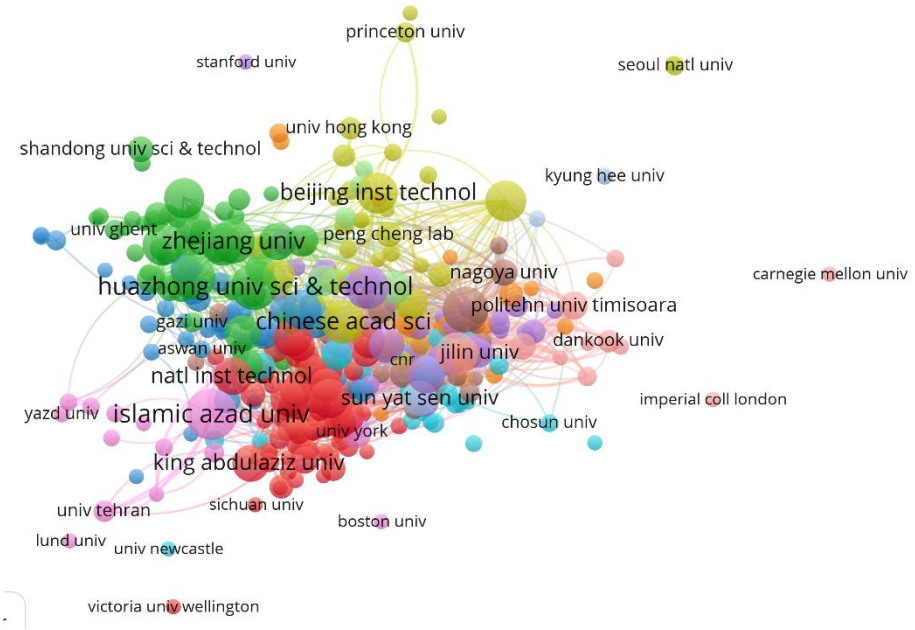


Figure 24. A graphical depiction of the interconnections formed by citations different among institutes

7.5. Nation-Based Citation Study

Citation patterns across the countries contributing to intrusion detection research in the IoT domain are examined here. Nations were included where they had at least five published documents and five citations, and documents co-authored across more than 25 nationalities were excluded. VOSviewer identified 117 nations, of which 71 satisfied the condition. Table 12 lists the ten nations with the highest TLS values. China leads with 1,245 documents and a TLS of 5,947; CAV intrusion detection work produced by China-affiliated researchers has attracted 27,107 citations and been referenced by authors from 63 distinct nations, meeting the five-document, five-citation criterion. The United States follows with 550 publications, a TLS of 3,366, and 15,987 citations.

Table 12. The ten countries with the highest total citation link strengths in the research landscape of intrusion detection for CAVs.

Rank	Nation	NPub	Citations	TLS
1	China	1245	27107	5947
2	USA	550	15987	3366
3	South Korea	287	7083	2513
4	India	532	8796	2472
5	Canada	218	7208	1758
6	Saudi Arabia	204	3327	1738
7	England	216	6878	1720
8	Australia	169	6651	1232
9	Pakistan	113	2795	925
10	France	104	2911	829

Figure 25 shows the citation network among nations publishing CAV intrusion detection research. Three principal networks are visible, denoted by red, blue, and green nodes, together with the links between them. The blue network includes China, South Korea, and Japan; the red includes India and Finland, among others.

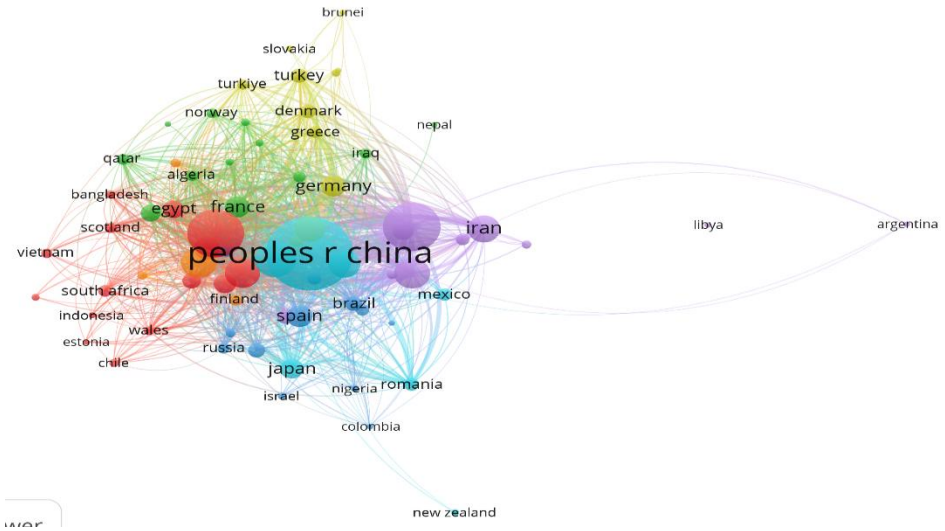


Figure 25. A graphical depiction of the interconnections formed by citations among different countries

8. Observation and Conclusions

This paper presents a bibliometric review of scholarly literature on intrusion detection in CAVs published between 2014 and 2024. The analysis worked through annual publication patterns, classifying them by document type, institution, publication source, contributing author, country of origin, and research domain. Network analytic methods, namely co-authorship, co-occurrence, and co-citation, were then applied to expose collaboration patterns, thematic linkages, and the works carrying most weight in the area; fractional counting was used throughout to produce a normalised picture of contribution. Burst detection results for articles and keywords alike were examined to identify significant temporal shifts and emerging focal points. The principal findings follow.

WoS has indexed more than 3,500 publications on CAV intrusion detection since 2020, 94% of which are research papers. IEEE Access is the single most prominent outlet, with 262 papers. China leads the field. Hunan University College of Computer Science records the highest institutional output, with 28 publications, and Guoqi Xie, also based in China, is the most prolific individual author, with 26 articles. Chinese scholars collectively produced the largest share of publications between 2020 and 2022.

Engineering is the principal research domain, with 2,266 papers; within it, 'Engineering Electrical Electronic' dominates, with 1,901 articles, ahead of 'Telecommunications' at 1,024. The National Natural Science Foundation of China (NSFC) is the leading funder, accounting for 23.623% of total funding, and roughly half of all publications are Open Access. Renfa Li of China stands out in both collaboration and influence, leading co-authorship-based TLS across 24 and 25 publications. The Chinese Academy of Sciences records the highest institutional co-authorship TLS at 36, with its articles drawing 908 citations. At the national level, the People's Republic of China ranks first, with a co-authorship TLS of 483 across 1,245 publications. Among the keywords, 'Intrusion Detection' has the highest co-occurrence TLS, at 464.

Turning to citation influence: ACM Transactions on Design Automation of Electronic Systems holds the highest source TLS at 1209. Jo, Hyo Jin of South Korea records the highest individual citation-based TLS at 686. Korea University leads institutions at 1124, and the People's Republic of China leads nations at 5947. Between 2016 and 2020, the terms 'software defined networking', 'schedulability research', and 'vehicular ad hoc networks' showed notable burst strengths, and the publication by Kreutz et al. [19] registered a burst strength of 6.859 across 2018 to 2019.

Read across the full 2014 to 2024 window, the analysis points to several clear trends, and to some prospective directions for intrusion detection research in connected and autonomous vehicles. The evidence argues for a deliberate emphasis on more sophisticated machine learning, with transfer learning, federated learning, and reinforcement learning as the obvious candidates for detecting catalogued intrusions and previously unseen anomalies alike within CAV systems. Establishing their practical value would require comparative evaluation across realistic operating contexts and threat scenarios. There is scope, too, for applying CAV intrusion detection principles to areas that remain relatively unexplored yet potentially significant: automation control systems, the physical dynamics of vehicle operation, and the mathematical models governing CAV behaviour. A dedicated bibliometric treatment of how

machine and deep learning algorithms are evolving specifically within CAV intrusion detection would, we suspect, surface trends shaping both current effort and the future of CAV security.

9. Shortcomings and Future Work

This study offers a substantive account of current trends and approaches in CAV intrusion detection as they appear in the scholarly record. Several limitations remain, and subsequent work should address them. Concentrating on academic literature necessarily leaves out part of the picture, since important practical advances and innovations originate in industry, where proprietary constraints often prevent publication in scientific journals. Relying on a single bibliographic database is a further constraint: restricting the corpus to Web of Science may omit relevant work indexed elsewhere or presented at non-indexed conferences, which limits how comprehensive the findings can claim to be. Future research should therefore draw on a wider range of data sources and adopt a more granular methodology, examining particular sub-disciplines within CAV intrusion detection individually. Narrower, targeted investigations of this kind would expose more specific difficulties and support the development of context-appropriate, practically applicable security solutions for connected and autonomous transportation.

Consent for publication - Consent for publication was obtained from all participants included in the study.
Competing interests - The authors declare no competing interests

Authors' contributions - Conceptualization, AV; writing original draft preparation, AV; writing review and editing, MK and AV; visualization, MK and AV; supervision, MK. All authors have read and agreed to the final version of the manuscript.

References

[1] Kumar, K., Khari, M. Intrusion detection system based on federated learning using layer-based privacy obfuscation. *Cluster Comput* 28, 413 (2025). https://doi.org/10.1007/s10586-025-05337-6

[2] Internet of Things (IoT) and Non-IoT Active Device Connections Worldwide from 2010 to 2025. Available online: https: //www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (accessed on 20 July 2025).

[3] Dalal, R., Khari, M. & Misra, S. Speculative Analysis of Wireless Network by Bibliometrics Tool. *Wireless Pers Commun* 135, 2039–2059 (2024). https://doi.org/10.1007/s11277-024-11064-9.

[4] Dui, H., Zhang, S., Liu, M., Dong, X., & Bai, G. (2024). IoT-enabled real-time traffic monitoring and control management for intelligent transportation systems. *IEEE Internet of Things Journal*.

[5] Biswas, A., & Wang, H. C. (2023). Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. *Sensors*, *23*(4), 1963.

[6] Nagarajan, J., Mansourian, P., Shahid, M. A., Jaekel, A., Saini, I., Zhang, N., & Kneppers, M. (2023). Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. *Peer-to-Peer Networking and Applications*, *16*(5), 2153-2185.

[7] Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., ... & Tsolis, D. (2023). Autonomous vehicles: Sophisticated attacks, safety issues,

challenges, open topics, blockchain, and future directions. *Journal of Cybersecurity and Privacy*, *3*(3), 493-543.

[8] Sharma, D., Mittal, R., Sekhar, R., Shah, P., & Renz, M. (2023). A bibliometric assessment of cyber security and cyber forensics research. *Results in Control and Optimization*, *10*, 100204.

[9] Song, H. M., Woo, J., & Kim, H. K. (2019). In-vehicle network intrusion detection using deep convolutional neural network. *Vehicular Communications*, *21*, 100198. https://doi.org/10.1016/j.vehcom.2019.100198

[10] Kang, M., & Kang, J. (2016). Intrusion detection system using deep neural network for In-Vehicle network security. *PLoS ONE*, *11*(6), e0155781. https://doi.org/10.1371/journal.pone.0155781

[11] Woo, S., Jo, H. J., & Lee, D. H. (2014). A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Transactions on Intelligent Transportation Systems*, *16*(2), 993-1006.

[12] Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., & Li, K. (2019). A survey of intrusion detection for in-vehicle networks. *IEEE Transactions on Intelligent Transportation Systems*, *21*(3), 919-933.

[13] Choi, W., Joo, K., Jo, H. J., Park, M. C., & Lee, D. H. (2018). VoltageIDS: Low-level communication characteristics for automotive intrusion detection system. *IEEE Transactions on Information Forensics and Security*, *13*(8), 2114-2129.

[14] Rajapaksha, S., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., Madzudzo, G., & Cheah, M. (2022). AI-Based Intrusion Detection Systems for In-Vehicle Networks: a survey. *ACM Computing Surveys*, *55*(11), 1–40. https://doi.org/10.1145/3570954

[15] Karopoulos, G., Kambourakis, G., Chatzoglou, E., Hernández-Ramos, J. L., & Kouliaridis, V. (2022). Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and a Meta-Taxonomy. *Electronics*, *11*(7), 1072. https://doi.org/10.3390/electronics11071072

[16] Lampe, B., & Meng, W. (2023). Intrusion detection in the automotive domain: A comprehensive review. *IEEE Communications Surveys & Tutorials*.

[17] Zaidi, K., Milojevic, M. B., Rakocevic, V., Nallanathan, A., & Rajarajan, M. (2015). Host-based intrusion detection for VANETs: A statistical approach to rogue node detection. *IEEE transactions on vehicular technology*, *65*(8), 6703-6714.

[18] Lakhal, N. M. B., Nasri, O., Adouane, L., & Slama, J. B. H. (2020). Controller area network reliability: overview of design challenges and safety related perspectives of future transportation systems. *IET Intelligent Transport Systems*, *14*(13), 1727–1739. https://doi.org/10.1049/iet-its.2019.0565

[19] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, *103*(1), 14-76.

[20] Yao, G., Bi, J., Li, Y., & Guo, L. (2014). On the capacitated controller placement problem in software defined networks. *IEEE Communications Letters*, *18*(8), 1339-1342.

[21] Lange, S., Gebert, S., Zinner, T., Tran-Gia, P., Hock, D., Jarschel, M., & Hoffmann, M. (2015). Heuristic approaches to the controller placement problem in large scale SDN networks. *IEEE Transactions on Network and Service Management*, *12*(1), 4-17.

[22] Davis, R. I., Kollmann, S., Pollex, V., & Slomka, F. (2013). Schedulability study for Controller Area Network (CAN) with FIFO queues priority queues and gateways. *Real-Time Systems*, *49*, 73-116.

[23] Berde, P., Gerola, M., Hart, J., Higuchi, Y., Kobayashi, M., Koide, T., ... & Parulkar, G. (2014, August). ONOS: towards an open, distributed SDN OS. In *Proceedings of the third workshop on Hot topics in software defined networking* (pp. 1-6).

[24] K. T. Cho and K. G. Shin. Fingerprinting electronic control units for vehicle intrusion detection. In *USENIX Security Symposium*, pages 911-927, 2016.

[25] Sedjelmaci, H., & Senouci, S. M. (2015). An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Computers & Electrical Engineering*, *43*, 33-47.

[26] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications*, *37*, 380-392.

[27] Van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(3), 523-538. https://doi.org/10.1007/s11192-009-0146-3