Mesopotamian journal of Cybersecurity
Vol.5, No.3, **pp**. 1165–1183
DOI: https://doi.org/10.58496/MJCS/2025/062; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Global Research Trends and Collaboration in MITRE ATT&CK Framework: A Bibliometric and Network Analysis in Cybersecurity

Asad Maqsood [1], Syifak Izhar Hisham [2,*], , Ahmad Firdaus [2]

[1] *University of Engineering & Technology, Peshawar, KPK, Pakistan*

[2] *Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, 26600, Pekan, Pahang, Malaysia*

ARTICLEINFO

Article History

Received 16 Jun 2024
Revised 08 Aug 2025
Accepted 18 Sep 2025
Published 14 Oct 2025

Keywords

MITRE ATT&CK Framework

Threat Intelligence
Cybersecurity

Bibliometric Analysis
Network Analysis

Industrial Control Systems (ICS)

ABSTRACT

The MITRE ATT&CK framework has become a foundational tool for organizing adversarial behaviors and techniques in cybersecurity. While its adoption in practice and academia has grown significantly, no prior bibliometric review has comprehensively mapped the global research landscape surrounding this framework. This study addresses that gap by conducting a systematic bibliometric and network analysis of publications related to ATT&CK indexed in Scopus from 2017 to 2025. Using VOSviewer and quantitative bibliometric methods, we analyzed 391 publications to identify trends in research output, influential works, key contributors, thematic areas, and patterns of collaboration. Results show exponential growth in studies related to ATT&CK, with North America, Europe, and Asia as major contributors. Network analysis revealed highly interconnected author clusters, while keyword mapping identified five dominant research themes, including threat intelligence, adversary emulation, and machine learning-based detection. Citation analysis further identified inspiring publications that have significantly influenced the field. This review clarifies the intellectual structure and collaborative dynamics of ATT&CK research, offering insights into its development and pointing to future opportunities in interdisciplinary cybersecurity research.

1. INTRODUCTION

Cybersecurity has evolved significantly in response to increasingly sophisticated cyber threats. A pivotal advancement in this area is the MITRE ATT&CK framework (Adversarial Tactics, Techniques, and Common Knowledge), introduced by the MITRE Corporation in 2013[1]. Initially, it was used as an internal research initiative, aimed at profiling advanced persistent threats (APTs) targeting Windows enterprise environments. It was publicly released in 2015. The framework initially featured 96 techniques across nine tactical objectives [2] and subsequently expanded to include macOS, Linux, pre-attack stages (PRE-ATT&CK), mobile platforms, cloud services, and, notably, industrial control systems (ICS)[3].

Due to its systematic approach to categorizing adversarial behaviors into standardized tactics, techniques, and procedures (TTPs), the MITRE ATT&CK framework has quickly become indispensable to cybersecurity practitioners [2]. It has been extensively utilized across various sectors for critical functions such as threat modelling, adversary emulation, incident response planning, and proactive security strategies [4].

The practical foundations of such adversarial mapping are deeply rooted in intrusion detection research. Aljanabi et al. [25] provided a comprehensive review of intrusion detection systems, outlining host-based, network-based, and hybrid approaches that inform the mechanisms, later captured in frameworks like ATT&CK. Similarly, Mohammed et al. [26] proposed a hybrid fusion model for intrusion detection that highlights the importance of benchmarking and evaluation, which closely mirrors how ATT&CK techniques are systematically validated in research. Together, these studies show how advances in intrusion detection laid the groundwork for structured adversary behavior models like ATT&CK, effectively connecting traditional IDS approaches with modern threat intelligence frameworks.

A recent search of the Scopus database reveals that MITRE ATT&CK publications have grown from fewer than ten papers in 2017 to over 100 annually by 2023, reflecting its central role in the cybersecurity research community. However, despite its popularity, only limited efforts have been made to synthesize the growing body of work comprehensively. Initial review efforts by [5] provided a classification of ATT&CK applications in research and practice, while[6] qualitatively assessed over 50 publications related to ATT&CK to summarize current trends and challenges. These studies highlighted a range of

*Corresponding author. Email: syifakizhar@umpsa.edu.my

applications of ATT&CK from threat intelligence and simulation to security evaluation and automation. They also emphasize the need for a more structured, data-driven overview of the developing field.

Despite the framework's widespread adoption and growing body of research, comprehensive and systematic analyses of the ATT&CK literature using quantitative bibliometric methods have been lacking. Previous reviews have primarily employed qualitative approaches, offering limited insights into global research trends, influential publications, thematic evolution, and international collaborations [5][6].

To date, no bibliometric study has systematically examined the MITRE ATT&CK research landscape. Unlike narrative or thematic literature reviews, bibliometric analysis enables researchers to quantify and map trends in publication output, citation patterns, collaboration networks, and the evolution of keywords[23]. A bibliometric approach is thus essential for identifying the most influential works, contributors, and institutions, as well as for revealing hidden structures and gaps in literature. This study addresses this critical gap by providing a comprehensive bibliometric and network analysis of scholarly work employing the MITRE ATT&CK framework, published in Scopus-indexed sources between 2017 and 2025. Using advanced bibliometric methodologies and visualization tools, like VOSviewer, we quantitatively explore publication trends, key contributions, thematic concentrations, author networks, and international collaboration patterns. By illuminating these dimensions, our research clarifies the intellectual structure surrounding MITRE ATT&CK research, identifies influential studies and contributors, and highlights emerging opportunities for interdisciplinary and international collaboration, thereby contributing to both theoretical development and practical cybersecurity applications.

1.1 RESEARCH OBJECTIVES

This study aims to answer the following research questions:

RQ1: What is the current publication trend in MITRE ATT&CK in cybersecurity?

RQ2: Which are the most influential articles on MITRE ATT&CK?

RQ3: Which themes involving MITRE ATT&CK are the most popular among scholars?

RQ4: Who are the most influential authors on MITRE ATT&CK?

RQ5: What is the current state of collaboration involving MITRE ATT&CK?

RQ6: What is the intellectual structure of current research on MITRE ATT&CK?

RQ7: What kinds of issues hamper research on MITRE ATT&CK?

RQ8: What areas involving MITRE ATT&CK need additional study?

Through these research questions, the study seeks to map the intellectual landscape of MITRE ATT&CK research, highlighting publication growth, identifying key contributors and thematic concentrations, analyzing international collaboration patterns, and uncovering challenges and opportunities for future exploration. This review is based on Scopus-indexed publications (2017–2025)[7] and is supported by foundational reports and peer-reviewed survey articles.

1.2. CONTRIBUTIONS

The main contributions of this study are as follows:

- It provides the first large-scale bibliometric and network analysis of the MITRE ATT&CK research landscape (2017–2025).
- It identifies influential publications, key authors, institutions, and global collaboration patterns.
- It maps five major thematic clusters using co-word and citation analysis, including threat intelligence, adversary emulation, and machine learning.
- It uncovers research gaps in the area, such as real-world validation, cloud, IoT, and ICS security.
- It proposes a reproducible methodology using Scopus and VOSviewer, offering a model for future bibliometric research in cybersecurity.

2. METHODS

This study utilized a bibliometric approach to quantitatively review the MITRE ATT&CK research landscape. We began by retrieving all relevant publications from the Scopus database (Elsevier) covering the period 2017 through early 2025. The query targeted the term "MITRE ATT&CK" (including variations such as the ATT&CK framework) in titles, abstracts, and keywords to ensure comprehensive coverage of relevant literature. This yielded a dataset of 391 documents after removing duplicates and non-relevant items. All document types were included (e.g., journal articles, conference papers, book series

contributions, etc.) to provide a complete picture of the field's output. For each record, bibliographic data (title, authors, affiliations, source, year, keywords, citations, etc.) were downloaded from Scopus. The timespan was chosen to start in 2017, as this is when the first publications related to the ATT&CK were published, and to capture the latest available data (as of May 2025), reflecting the field's evolution. The Scopus subject categories and document type classifications for each publication were preserved for later analysis of disciplinary reach and dissemination channels. Citation counts for each document were recorded as provided by Scopus (reflecting citations accumulated up to 2025).

Before analysis, the data were carefully cleaned and standardized. Author names and affiliations were checked for consistency (e.g., merging spelling variants of the same author or institution). Likewise, keywords were reviewed to unify synonyms (for instance, "Cybersecurity" vs. "Cyber Security") and to ensure the MITRE ATT&CK context (terms unrelated to the ATT&CK framework were excluded if inadvertently retrieved). The final literature of 391 publications, along with their metadata, formed the basis for the subsequent bibliometric analyses.

2.1 Bibliometric Analysis and Visualization

We carried out both descriptive statistical analysis and network-based analysis to address the research questions (RQ1–RQ6). For publication trends (RQ1), we analyzed the annual output of publications and their citation counts. Using the metadata from Scopus, we tallied the number of publications per year related to ATT&CK and plotted their growth rate. Total citations per year were also aggregated to observe how influence has grown over time. Additionally, we examined the distribution of publications by venue and type, i.e., each source of the document was classified as a conference proceeding, journal article, book series, etc., and as an article, review, conference paper, etc., according to Scopus's categorization. The statistics were compiled using an Excel spreadsheet, providing outputs such as Table 1 (sources by type) and Table 2 (document type distribution). Summary indicators such as average citations per paper and the field's h-index and g-index were computed from the citation data to gauge overall impact (Table 9). The h-index represents the number of papers h with at least h citations each, while the g-index is the largest number g such that the top g papers receive together at least g^2 citations. These metrics helped identify the influence and maturity of the ATT&CK research domain as of 2025.

To uncover the key thematic areas (RQ3 and RQ6), we performed a keyword co-occurrence analysis. We relied on VOSviewer software (version 1.6.20), a tool designed for bibliometric mapping and visualization [14]. Author-provided keywords from all documents were extracted and analyzed for frequency and co-occurrence patterns. We set a minimum threshold of 5 occurrences for a keyword to be included in the co-occurrence network, focusing on significant and recurring topics. VOSviewer constructed a network map where each node represents a keyword, and links between nodes indicate that two keywords appear together in the same publication. The strength of co-occurrence (how often keywords co-appeared) determined the proximity of nodes on the map. We applied the Linlog/modularity clustering algorithm in VOSviewer to detect clusters of related keywords, which were later interpreted and labeled according to their thematic focus (as reported in the Results, e.g., Threat Intelligence & Ontology, Risk & ICS Security, Machine Learning Analytics, etc.). A similar term co-occurrence analysis was conducted on the titles of the papers to complement the keyword analysis. For the title analysis, a binary counting method was used (each term counted at most once per title to avoid bias from repeated words in a single title). Common stop words and generic terms were removed, and the remaining significant terms (after stemming and normalization) were mapped into a network to visualize the dominant concepts appearing in the paper titles (see Figure 4 in the Results). The content analyses revealed the intellectual structure and popular research themes within the ATT&CK literature.

Next, to identify key contributors and collaboration patterns (RQ4 and RQ5), we analyzed authorship and affiliation data. We ranked productive authors, institutions, and countries by their total publications and citations (as shown in Tables 6–8). Collaboration networks were then visualized to understand how researchers and organizations connect in this field. Using VOSviewer's co-authorship analysis, we created a network of co-authors where nodes represent individual authors and edges represent co-authored publications. We employed fractional counting for co-authorship, which means that each co-authored paper contributes a fraction of credit to each author, thus preventing authors with many collaborators from disproportionately dominating the network. For clarity, a minimum productivity threshold was established to display only authors with at least n publications (or a certain number of co-authorship links); this filter excludes one-time authors and highlights the core collaborative groups. The resulting author network (Figure 5) allowed us to identify major collaboration clusters and research teams (for example, a prominent cluster centered on researchers from National Yang Ming Chiao Tung University, Taiwan, was observed).

We also mapped collaboration at the country level. The author affiliations of each publication were used to tag the countries involved, and a country co-authorship network was generated in VOSviewer. In this network, nodes represent countries, and a link between two country nodes indicates the number of publications co-authored by researchers from those countries. We included countries with a minimum of 5 publications in our dataset to ensure the network focused on the most active nations in ATT&CK research. The thickness of the links corresponds to the strength of collaboration (number of shared papers). This visualization (Figure 6) helped identify international collaboration patterns, such as the central role of the United States and the formation of regional collaboration clusters (e.g., between certain Asian and European countries).

Finally, to explore the intellectual lineage and influential works (RQ2 and RQ6), we conducted a citation network analysis among the ATT&CK publications. Using Scopus citation data, we build a directed network where nodes represent the documents in our literature, and an edge from paper A to paper B indicates that A cites B in its references. VOSviewer was used to visualize this citation network (Figure 7), highlighting how ideas propagated and which papers serve as key reference points in the field. We did not apply a strict citation threshold for inclusion, however, in the visualization, we emphasized clusters around highly cited papers to interpret the major knowledge streams. Through this network, we identified influential papers that were frequently cited by subsequent studies, as well as clusters of papers that cite each other, indicating sub-communities of research (for instance, a cluster of works focusing on industrial control system security with ATT&CK, anchored by an influential 2021 paper, was identified). Additionally, we computed indicators based on citations for each document (total citations and whether it meets the h-index threshold of the literature) to measure influence quantitatively.

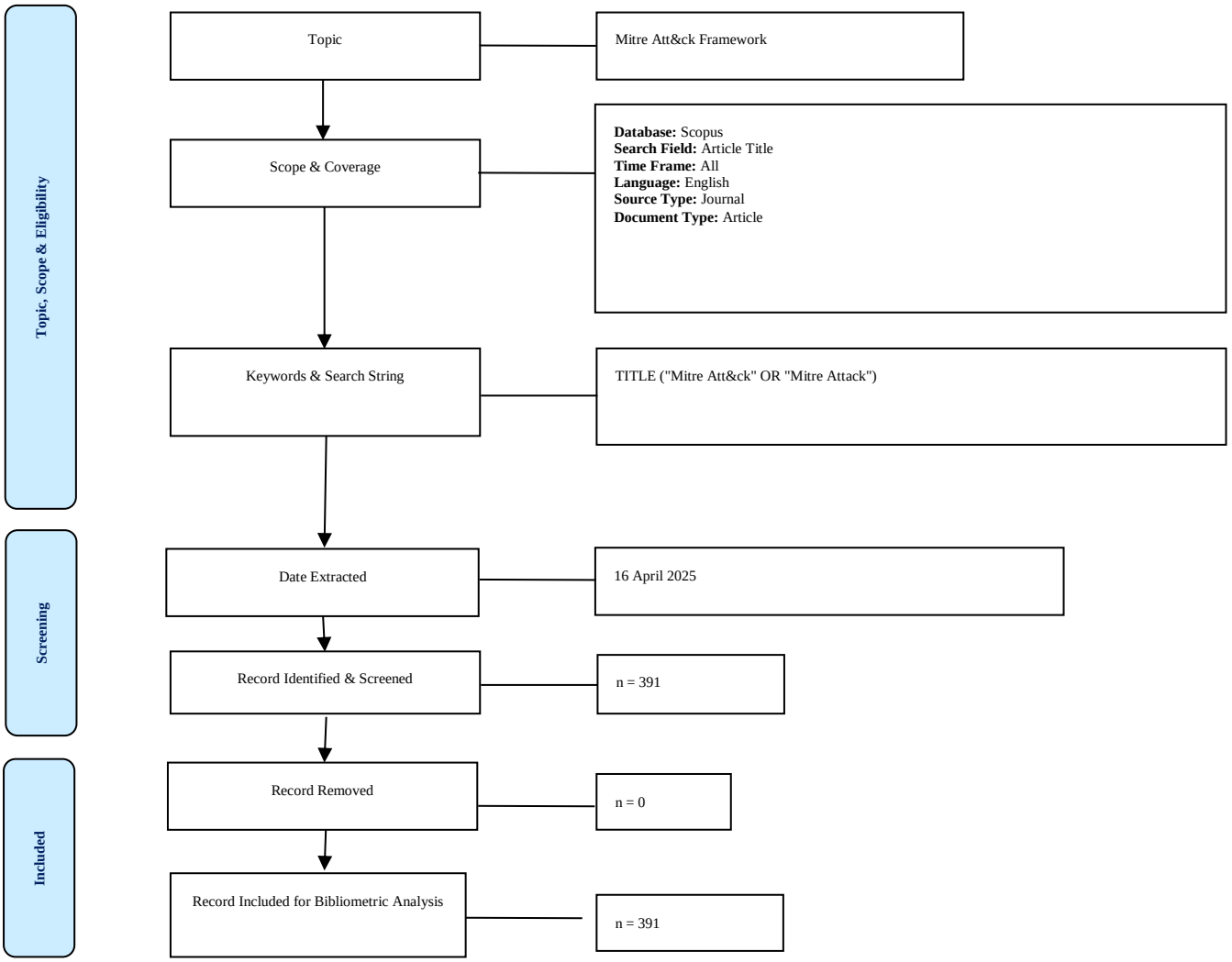

Fig. 1. PRISMA-inspired flow diagram of the literature selection process for the bibliometric analysis of MITRE ATT&CK research (2017–2025).

3. RESULTS

This section presents the bibliometric findings on MITRE ATT&CK research in alignment with the study's research questions, including publication trends (RQ1), prominent themes (RQ3), key contributors and collaborations (RQ4–RQ5), as well as the intellectual structure and influential works in the field (RQ2, RQ6). The analysis encompasses 391 Scopus-indexed documents (2017–2025) and uses VOSviewer for network visualizations. Figures and tables referenced correspond to those in the original manuscript.

3.1 Publication Trends and Dissemination (RQ1)

3.1.1 Growth of Publications

MITRE ATT&CK research has expanded exponentially. Fig. 2 shows the annual output of ATT&CK-related papers and their citations, revealing a steady start (fewer than 10 papers in 2017) followed by aggressive growth from 2020 onward. Notably, publication counts increased fourfold from 2022 to 2024 compared to the late 2010s, reflecting a scholarly interest. This spike coincides with key developments such as the public release of ATT&CK for ICS around 2019–2020, which broadened the framework's scope and attracted new researchers. The rising citation counts (orange line in Fig. 2) indicate that recent works are rapidly accumulating influence. However, the field's overall citation rate (≈4.8 citations per paper) remains modest, consistent with an emerging research area (Table 9). This sharp upward trend in publications and citations directly addresses RQ1, demonstrating that MITRE ATT&CK has transformed from a niche topic into a mainstream subject of cybersecurity research in under a decade.

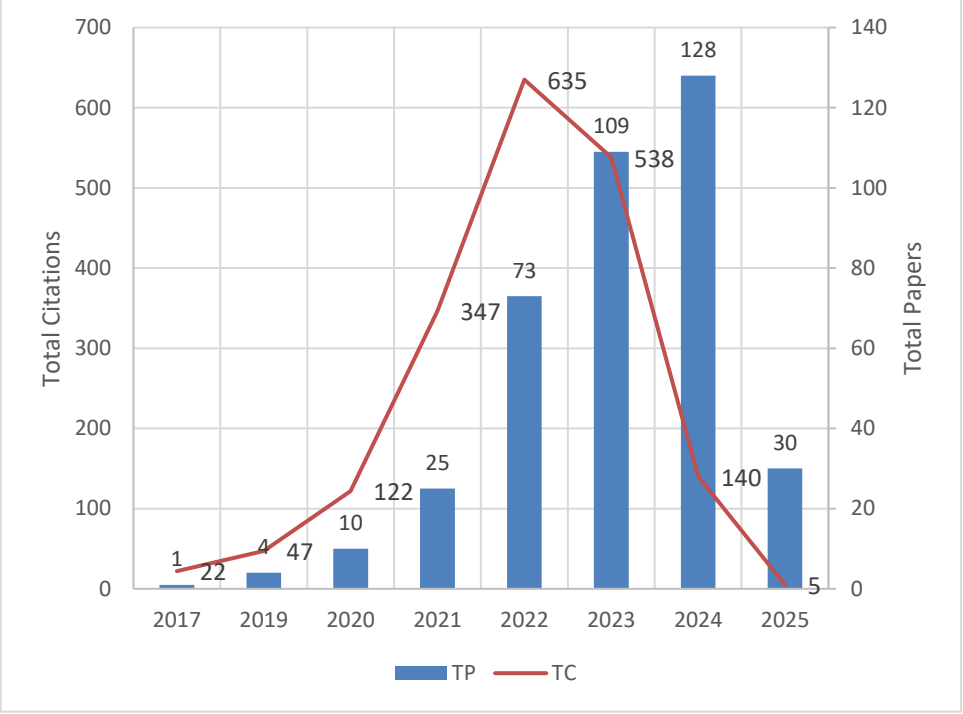

Fig. 2. Total Publications and Citations by Year

3.1.2 Publication Venues and Document Types

The dissemination of ATT&CK research spans a mix of fast-track conference outputs and rigorous journal articles. Table 1 shows that nearly half of all publications (≈48%) are in conference proceedings, highlighting a community preference for rapid, peer-to-peer knowledge exchange of cutting-edge findings. Journals account for about 39% of publications, indicating that a substantial portion of research has matured into archival literature with longer-term impact. The remaining outputs are smaller in share, including book series (~11%), and few standalone books (~1.5%).

TABLE I. SOURCES FOR MITRE ATT&CK RESEARCH

Source Type	Total Publications (TP)	Percentage (%)
Conference Proceedings	189	48.34%
Journal	152	38.87%
Book Series	44	11.25%
Book	6	1.53%
Total	391	100.00

Table 2 further breaks down document types, i.e., conference papers dominating (57.29% of documents), followed by standard research articles (36.83%). Notably, review articles are rare (1.02%), and data papers are even less common (0.26%), indicating a gap in synthesized knowledge and open data resources within this domain. This distribution suggests that the field is still in a growth phase, where most contributions report new technical advances (often in conference form),

and comprehensive surveys and shared benchmarks remain rare. The dominance of conference publications, typically in fast-evolving cybersecurity domains, suggests that researchers prioritize rapid dissemination and timely feedback. However, the increasing proportion of journal publications in recent years signals a shift toward more rigorous and consolidated contributions, reflecting the field's maturation. RQ1's focus on publication trends is addressed by a pattern of accelerating output across diverse venues, initially emphasizing quick dissemination, and gradually shifting toward more journal publications as ATT&CK research gains academic maturity.

TABLE II. DOCUMENT TYPES FOR MITRE ATT&CK RESEARCH

Document Type	Total Publications (TP)	Percentage (%)
Conference Paper	224	57.29%
Article	144	36.83%
Conference Review	9	2.30%
Book Chapter	6	1.53%
Review	4	1.02%
Book	3	0.77%
Data Paper	1	0.26%
Total	391	100.00

3.1.3 Leading Sources

The most active source title publication (Table 3) include high-impact outlets in both conference and journal categories. IEEE Access tops the list with 26 papers (236 total citations), reflecting its role as a popular open-access journal for ATT&CK studies. The broad-based ACM International Conference Proceedings Series contains 22 papers (151 citations), illustrating that many conferences, although not individually indexed in Scopus, have hosted ATT&CK research as part of this series. Among journals, Computers & Security stands out with 17 papers and a strong citation impact (CiteScore 12.4), affirming it as a leading scholarly journal for cybersecurity frameworks. Despite the notable source being Lecture Notes in Computer Science (LNCS), which, despite only 10 ATT&CK-related papers, amassed 405 citations, an average of approximately 40 citations per paper, suggesting that seminal early work appeared in this Springer series and garnered significant attention. In summary, ATT&CK research is published in a mix of high-throughput conferences and reputable journals, indicating both the urgency of sharing practical techniques and the drive to establish a lasting academic foundation.

TABLE III. MOST ACTIVE SOURCE TITLE

Source Title	TP	TC	Publisher	Cite Score	SJR 2023	SNIP 2023
IEEE Access	26	236	IEEE	9.8	0.96	1.44
ACM International Conference Proceedings Series	22	151	ACM International Conference Proceedings Series	N/A	N/A	N/A
Computers and Security	17	137	Elsevier	12.4	1.566	2.163
Lecture Notes in Computer Science Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics	10	405	Springer Nature	2.6	0.606	0.590
Electronics (Switzerland)	9	22	Multidisciplinary Digital Publishing Institute (MDPI)	5.3	0.644	0.993
Lecture Notes in Networks and Systems	8	8	Springer Nature	0.9	0.171	0.282
Sensors	7	153	Multidisciplinary Digital Publishing Institute (MDPI)	7.3	0.786	1.247
CEUR Workshop Proceedings	7	5	NA	1.1	0.191	0.235
Applied Sciences (Switzerland)	7	32	Multidisciplinary Digital Publishing Institute (MDPI)	5.3	0.508	0.924
Communications in Computer and Information Science	6	11	NA	1.1	0.203	0.246
Proceedings of the 2023 IEEE International Conference on Intelligence and Security Informatics.	4	4	IEEE	9.8	0.96	1.44
IFIP Advances in Information and Communication Technology	4	12	Springer Nature	1.6	0.242	0.346
IEEE Transactions on Dependable and Secure Computing	4	32	IEEE	11.2	2.222	2.406
European Conference on Information Warfare and Security, ECCWS	4	5	NA	1	0.141	0.115

3.2 Key topics in MITRE ATT&CK Research (RQ3, RQ6):

3.2.1 Subject Areas

In terms of disciplinary reach, MITRE ATT&CK research is heavily grounded in Computer Science and Engineering. Table 4 shows that 90.28% of the publications fall under computer science, often with a secondary classification in engineering (51.41%). This reflects the technical, applied nature of the ATT&CK study, which frequently involves software development, security engineering, or system implementation. A significant subset is also tagged as Mathematics (20.46%) and Decision Sciences (17.39%), referring to the use of formal models, algorithms, and decision support techniques (e.g., optimization, analytics) in ATT&CK-related work. Smaller portions in areas like Materials Science (9.46%) and Physics (7.16%) likely stem from niche applications (e.g. hardware security or fundamental research on attack impacts), where Social Sciences (9.21%) and Business, Management and Accounting (2.56%) indicate a growing recognition of human factors, organizational strategy, and economics in applying ATT&CK. Collectively, this subject area spread portrays ATT&CK research as anchored in computer science yet increasingly interdisciplinary, aligning with the framework's expansion into diverse domains (e.g., critical infrastructure, policy, education). It also addresses RQ6 (intellectual structure) by showing that while the core knowledge base is technical, contributions from diverse peripheral fields enrich the overall research landscape.

TABLE IV. SUBJECT AREA

Subject Area	Total Publications (TP)	Percentage (%)
Computer Science	353	90.28%
Engineering	201	51.41%
Mathematics	80	20.46%
Decision Sciences	68	17.39%
Materials Science	37	9.46%
Social Sciences	36	9.21%
Physics and Astronomy	28	7.16%
Energy	15	3.84%
Medicine	11	2.81%
Business, Management, and Accounting	10	2.56%
Chemistry	10	2.56%
Biochemistry, Genetics, and Molecular Biology	9	2.30%
Chemical Engineering	8	2.05%
Environmental Science	3	0.77%
Earth and Planetary Sciences	2	0.51%
Health Professions	2	0.51%
Multidisciplinary	2	0.51%
Economics, Econometrics, and Finance	1	0.26%

3.2.2 Keyword Co-Occurrence and Clusters

A network visualization of author keywords (Figure 3) highlights the main research topics and their connections around the central concept of "MITRE ATT&CK." In the VOSviewer keyword map, "MITRE ATT&CK" appears as the largest node at the center, reaffirming its role as the unifying reference point across studies. Five distinct but closely related clusters radiate from this center (each color-coded in Fig. 3), representing the primary thematic areas in literature.

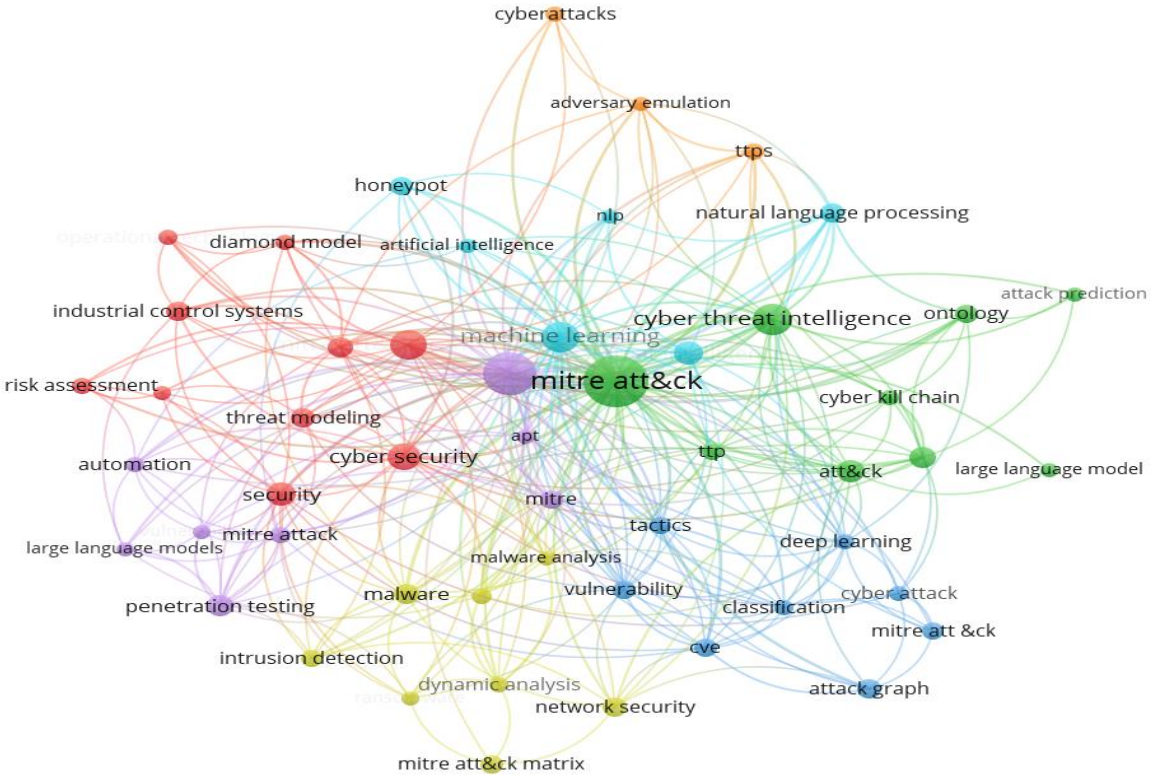

Fig. 3. Network visualization map of the author keywords with at least 5 occurrences.

Threat Intelligence & Ontology (Green Cluster): Keywords like "cyber threat intelligence (CTI), TTP, cyber kill chain, ontology" co-occur here. This cluster represents research that leverages ATT&CK to structure and reason over threat information – for example, mapping unstructured reports or feeds into standardized tactics and techniques. Such work often involves knowledge graph construction and ontologies to integrate ATT&CK with threat intelligence data, enabling automated reasoning about adversary behaviors. This theme underscores ATT&CK's importance in threat intelligence and threat hunting contexts, where its taxonomy of TTPs provides a foundation for parsing and organizing cyber threat data.

Risk & Critical Infrastructure Security (Red Cluster): This cluster includes terms like "industrial control systems (ICS), risk assessment, threat modelling". It denotes research adapting ATT&CK for safety-critical and industrial domains, such as power grids or manufacturing systems. Studies in this group often integrate ATT&CK with risk management frameworks to evaluate vulnerabilities in operational technology. The presence of ICS here reflects the extension of ATT&CK into industrial control system security (via the ATT&CK for ICS matrix) and efforts to quantify risk in those environments. These projects illustrate ATT&CK's use in cyber risk assessment and sector-specific threat modelling, extending its applicability beyond enterprise IT into critical infrastructure.

Machine Learning Analytics (Blue Cluster): Centered on terms like "machine learning, deep learning, classification, attack graph", this theme covers research that pairs ATT&CK with data-driven detection and analytics. This includes efforts to apply ML/AI techniques to detect attacks or to map events to ATT&CK techniques. For instance, some studies use deep learning models (transformers, neural networks) to classify security events (from logs, IDS alerts, etc.) into ATT&CK tactic/technique categories. The attack graph keyword suggests linking ATT&CK techniques in sequence to model attack paths. Overall, this cluster signifies a strong focus on analytics and automation, where MITRE ATT&CK serves as a schema for training models and correlating complex attack data.

Malware and Evaluation (Yellow Cluster): Keywords like "malware, intrusion detection, penetration testing" appear here, highlighting experimental research that evaluates defenses against known ATT&CK techniques. This includes studies on malware analysis mapped to ATT&CK techniques, intrusion detection systems tested using ATT&CK-defined scenarios, and red-team penetration tests guided by the ATT&CK matrix. The emphasis is on empirical evaluation and benchmarking,

e.g., using ATT&CK as a yardstick to measure how well a security tool or method covers known adversary techniques. This theme indicates an applied strand of research where ATT&CK is used to systematically test and validate security controls (aligning with industry use in adversary emulation exercises and ATT&CK evaluations).

AI-Driven Adversary Emulation (Cyan Cluster): This emerging cluster connects terms such as “adversary emulation, automation, natural language processing, " and " large language models”. The new capabilities reflect advanced research in automating red teaming and threat emulation. For instance, recent studies investigate the use of large language models (LLMs) and AI planning techniques to generate attack plans and simulate adversarial behavior within the ATT&CK framework. The presence of NLP suggests efforts to parse textual threat intel and directly produce ATT&CK-informed attack scenarios. This cluster highlights a growing interest in integrating the ATT&CK framework with AI, mainly large language models (LLMs), to develop advanced tools for cyber defense training and automated threat hunting.

Importantly, these clusters are tightly interconnected, and nearly every secondary keyword is linked via short paths to “MITRE ATT&CK” in Figure 3. This indicates that, while there are distinct subtopics, they all revolve around applying the same framework, and knowledge flows readily between them. The keyword analysis addresses RQ3 (popular themes) by clearly identifying these five thematic areas, which together encompass most of the MITRE ATT&CK research to date.

3.2.3 Frequent Keywords

Table 5 provides a complementary view by listing the most frequent author keywords and their occurrence percentages. The results reinforce that this literature is firmly rooted in cybersecurity, the term “Cybersecurity” (and its variant “Cyber Security”) appears in 42.46% and 36.81% of the papers, respectively, often alongside ATT&CK. “Network Security” (27.62%) is another common context. Notably, “MITRE ATT&CK” itself is explicitly used as a keyword in 27.11% of publications (with another 7.16% using the phrase “MITRE ATT&CK Framework”), highlighting how central the framework is to these studies. Traditional threat-centric terms such as “cyber threats” (19.44%), “cyber-attacks/attacks” (17.14%), and “malware” (13.04%) populate the middle tier of frequency, emphasizing that much ATT&CK research focuses on understanding and countering adversarial actions. Meanwhile, methodological catchphrases also appear “machine learning” (9.72% when counting both hyphenated and non-hyphenated forms) and “risk assessment” (9.21%) reflect popular approaches (AI-driven analysis and risk modelling) used alongside ATT&CK. The keyword “industrial control systems” (8.18%) further confirms the significant interest in applying ATT&CK to critical infrastructure. The keyword frequency analysis shows a blend of general cybersecurity concepts, the ATT&CK framework itself, threat types, and analytic techniques, painting a picture of a research field that is threat-informed, ATT&CK-centric, and methodologically inclined toward AI and risk models.

TABLE V. KEYORDS IN MITRE ATT&CK RESEARCH AND THEIR FREQUENCIES

Author Keywords:	Total Publications (TP)	Percentage (%)
Cybersecurity	166	42.46%
Cyber Security	140	35.81%
Network Security	108	27.62%
MITRE ATT&CK	106	27.11%
Cyber Threats	76	19.44%
Cyber-attacks	67	17.14%
Cyber Attacks	65	16.62%
Malware	51	13.04%
Machine Learning	38	9.72%
Risk Assessment	36	9.21%
Computer Crime	34	8.70%
Cyber Threat Intelligence	33	8.44%
Cyber Threat Intelligence	33	8.44%
Industrial Control Systems	32	8.18%
Knowledge-Based Systems	32	8.18%
Machine-learning	30	7.67%
MITRE ATT&CK Framework	28	7.16%
Crime	27	6.91%
Intrusion Detection	26	6.65%
Malware	26	6.65%

3.2.4 Title Term Analysis

Figure 4 visualizes co-occurring terms in paper titles, offering another lens on the intellectual structure (RQ6). The network of title terms also centers on “ATT&CK framework” as the hub, with several clusters that echo the themes identified in the

keywords. For example, a "techniques & analytics" cluster (green) in the title map links terms like "techniques," "mapping," "dataset," and "deep learning," indicating many titles focus on using datasets and ML to map or detect ATT&CK techniques. The "security & risk management" cluster (red) includes words like "security," "risk," and "mitigation," suggesting titles that integrate ATT&CK into broader security architecture or standards discussions. The "procedures & adversary behavior" cluster (blue) has words such as "procedure," "group," and "matrix," reflecting work that discusses adversary procedure mapping and the use of the ATT&CK matrix to track attacker behavior (e.g., across campaigns or groups). Finally, a smaller "industrial/OT" cluster (yellow) centered on "ICS" and "operational technology" confirms a subset of titles dedicated to industry-specific applications. The cross-links among these clusters are dense, signifying that papers often span multiple topics (e.g., a title might mention both "detection" and "ICS" or both "machine learning" and "threat modelling"). In summary, the term co-occurrence (Fig. 4) corroborates the convergent themes in ATT&CK research analytics, risk, adversary behavior, and domain-specific security, all unified by the common vocabulary of the ATT&CK framework. This provides further evidence supporting RQ6, indicating that the field's intellectual structure is centered on the application of a shared framework (ATT&CK) to diverse cybersecurity challenges.

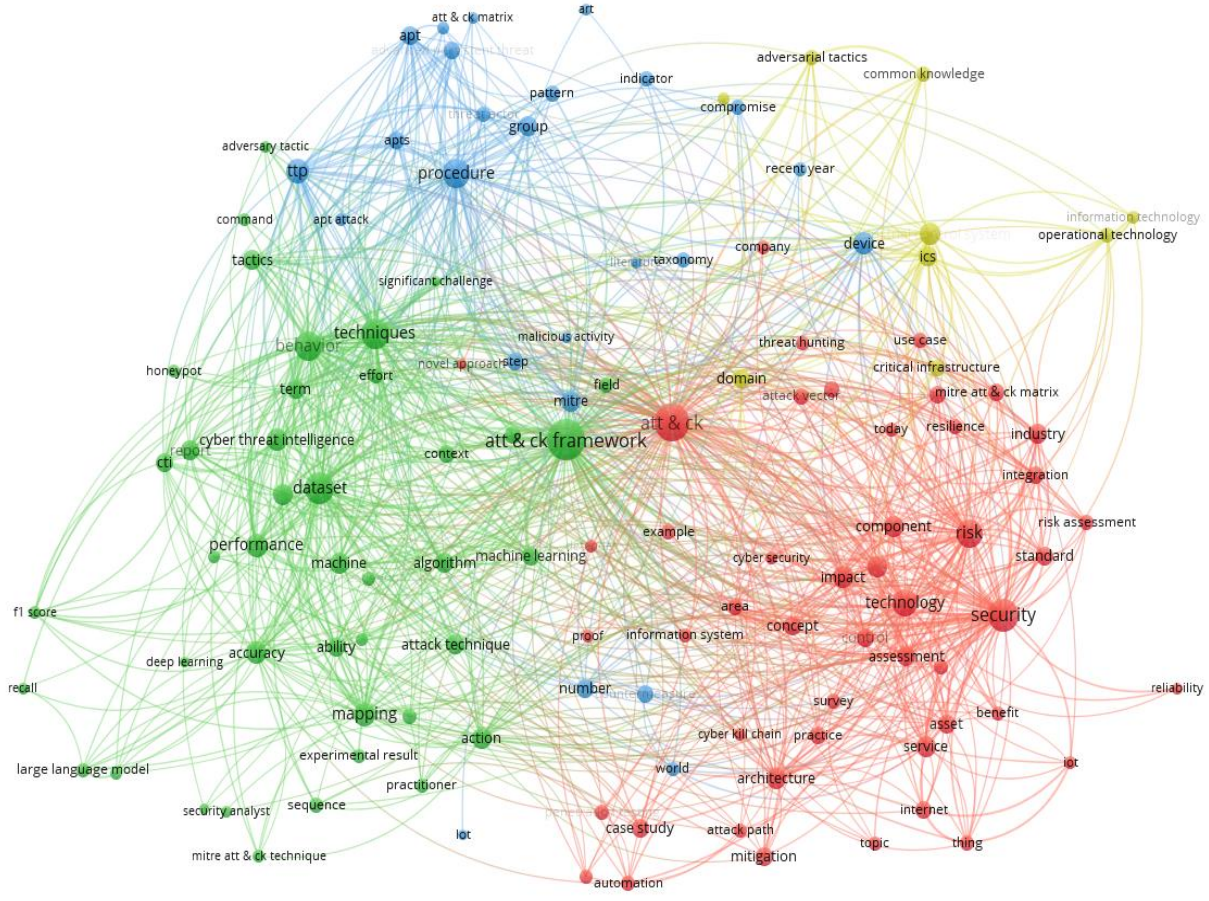

Fig. 4. VOSviewer visualization of term co-occurrence network based on title (Binary Counting)

3.3 Key Contributors and Collaboration Patterns (RQ4, RQ5):

3.3.1 Geographic Distribution of Research:

MITRE ATT&CK research has a global scope, although contributions vary in prominence across countries. Table 6 ranks countries by publication count and impact. The United States leads with 83 publications and the highest overall influence (h-index 11), reflecting its role as the birthplace of ATT&CK and a continued hub of related research. The data further suggest that the quantity of output is not a reliable predictor of per-paper impact. For instance, Greece has produced only 8 papers but demonstrates a disproportionately high citation rate (approximately 20 citations per paper) and an h-index comparable to larger contributors such as India, largely due to one highly cited risk assessment study. Similarly, Pakistan, with 8

publications, averages over 12 citations per paper, indicating high impact relative to its modest output. Mid-sized contributors such as South Korea (28 papers) and the United Kingdom (27 papers) demonstrate consistent academic impact, with approximately 7 to 8 citations per paper and an h-index of around 9 to 10, reflecting sustained influence in the field. In contrast, high-output countries India (26 papers) and China (19 papers) have lower average citations (<5), suggesting that while these countries have many researchers working on ATT&CK, their work collectively garners fewer citations per item (possibly due to many recent or niche conference papers). This uneven landscape suggests two complementary "geographies" of influence, on one hand, established cybersecurity centers (US, UK, South Korea) drive the conversation through volume and broad collaboration networks, and on the other hand, smaller or emerging players (Greece, Pakistan, Norway) achieve impact with a few pivotal contributions. In summary, RQ4's focus on influential contributors finds that no single country monopolizes ATT&CK research; instead, there is a distributed set of active regions, each contributing important pieces to the literature.

TABLE VI. GEOGRAPHIC ORIGIN OF MITRE ATT&CK RESEARCH

Country	TP	NCP	TC	C/P	C/CP	h	g
United States	83	53	389	4.69	7.34	11	17
South Korea	28	19	210	7.50	11.05	9	14
United Kingdom	27	21	210	7.78	10.00	10	16
India	26	16	70	2.69	4.38	4	7
China	19	7	58	3.05	8.29	4	7
Taiwan	17	10	70	4.12	7.00	5	8
Japan	15	10	35	2.33	3.50	3	5
Spain	15	7	76	5.07	10.86	4	7
Germany	14	10	23	1.64	2.30	3	3
Indonesia	13	9	65	5.00	7.22	5	8
Italy	13	9	37	2.85	4.11	3	5
Norway	13	9	79	6.08	8.78	5	8
Russian Federation	13	8	22	1.69	2.75	2	4
Canada	12	7	69	5.75	9.86	3	7
Australia	11	6	52	4.73	8.67	2	6
France	11	7	34	3.09	4.86	3	5
Austria	10	9	40	4.00	4.44	4	6
Greece	8	8	159	19.88	19.88	5	8
Pakistan	8	7	100	12.50	14.29	5	7
Czech Republic	6	5	38	6.33	7.60	3	5
Malaysia	6	4	29	4.83	7.25	3	4
Romania	6	5	59	9.83	11.80	4	5
Saudi Arabia	6	4	23	3.83	5.75	2	4
Singapore	6	5	27	4.50	5.40	3	5
Sweden	6	5	21	3.50	4.20	3	4
Switzerland	4	3	21	5.25	7.00	3	3

Notes: TP=total number of publications; NCP=number of cited publications; TC=total citations; C/P=average citations per publication; C/CP=average citations per cited publication; h=h-index; and g=g-index.

3.3.2 Leading Institutions

The institutional analysis (Table 7) further supports the idea of a diverse contributor base. Unlike some fields where a few elite universities or labs dominate, ATT&CK research output is spread across many organizations. The top contributor, National Taiwan Univ. of Science and Technology (Taiwan), leads with 10 papers but only modest citations per paper (2.9, h-index 3), indicating steady productivity with more than one breakthrough impact. However, several institutions punch above their weight in influence; for instance, the University of North Carolina at Charlotte (USA) has only 6 papers but boasts the highest citations per paper (17) and a high g-index (indicating one or two very highly cited works in that mix). Korea University (South Korea) also shows a strong impact (6 papers with 13.83 citations per paper). Notably, institutions from outside the traditional "big name" sphere appear throughout the top ranks e.g., Swiss German University (Indonesia), Norges Teknisk-Naturvitenskapelige Universitet (Norway), University of West Florida (USA), and even government/industry labs like NIST (National Institute of Standards and Technology) and PNNL (Pacific Northwest National Laboratory) in the US. The presence of U.S. federal laboratories alongside Asian and European universities indicates strong involvement of both academic and government research sectors. Collectively, these patterns suggest that meaningful MITRE ATT&CK research can emerge from a wide range of institutions globally, from mid-tier universities to national labs, underscoring a globally networked and democratized research landscape. This finding is encouraging for RQ4, implying that the advancement of ATT&CK knowledge is not limited to a few centers but is the product of many groups contributing different strengths (tool development, case studies, theoretical integration, etc.).

TABLE VII. INSTITUTION CONTRIBUTING MITRE ATT&CK RESEARCH PUBLICATIONS

Affiliation	Country	TP	NCP	TC	C/P	C/CP	h	g
National Taiwan University of Science and Technology	Taiwan	10	7	29	2.90	4.14	3	5
Norges Teknisk-Naturvitenskapelige Universitet	Norway	8	6	69	8.63	11.50	4	8
Swiss German University	Indonesia	8	8	60	7.50	7.50	5	7
University of West Florida	United States	7	5	34	4.86	6.80	2	5
Korea University	South Korea	6	6	83	13.83	13.83	5	6
University of North Carolina at Charlotte	United States	6	5	102	17.00	20.40	4	6
National Yang Ming Chiao Tung University	Taiwan	6	4	21	3.50	5.25	2	4
The University of Texas at Dallas	United States	5	4	29	5.80	7.25	3	5
Toyo University	Japan	5	5	10	2.00	2.00	2	2
National Institute of Standards and Technology	United States	5	5	19	3.80	3.80	3	4
Pacific Northwest National Laboratory	United States	5	3	28	5.60	9.33	3	5

Notes: TP=total number of publications; NCP=number of cited publications; TC=total citations; C/P=average citations per publication; C/CP=average citations per cited publication; h=h-index; and g=g-index

3.3.3 Prolific Authors

At the individual level, the authorship analysis (Table 8) reveals a geographically dispersed cadre of productive scholar. The most prolific author is Lim (Swiss German University, Indonesia). Lim leads in productivity (TP=8) and aggregate impact (TC=60), with all publications cited (NCP=8) and solid h/g indices (h=5, g=7), signaling both consistency and visibility. In contrast, Huang (National Taiwan University of Science and Technology) exhibits the strongest per-article influence (C/P=8.75; TC=35 over TP=4; NCP=4) with balanced h/g (3/4), highlighting a high-quality, lower-volume strategy. A U.S. node centered at the University of West Florida, D.Mink (TP=7; C/P=4.86; h/g=2/5), S.C. Bagui, and S.S. Bagui (each TP=6; C/P=3.50; h/g=2/4)—shows collaborative productivity but lower citation density, while Khan (Erik Jonsson School, Richardson) combines moderate output (TP=5) with higher efficiency (C/CP=7.25; h/g=3/5). Japanese contributors exhibit steadier yet modest influence: Mitsunaga and Okada (each TP=5; TC=10; C/P=2.00; h/g=2/2; NCP=5) contrast with Beuran (JAIST; TP=4; TC=15; C/P=3.75; h/g=2/3). Notably, several authors (Lim, Huang, Mitsunaga, Okada) have NCP equal to TP, indicating universal uptake of their outputs, whereas others show a mix of cited and uncited work—together mapping a landscape where Southeast Asian institutions increasingly pair visibility with efficiency while U.S. clusters emphasize volume and collaboration.

Overall, the author list underscores that influential voices in ATT&CK research arise from multiple continents, Asia (Southeast and East Asia) hosts the top authors, North America has strong clusters, and Europe/Australia are present in the extended list. This distributed authorship reflects the collaborative nature of the field and addresses RQ4 by identifying key contributors and highlighting the shared nature of thought leadership across regions and institutions.

TABLE VIII. MOST PRODUCTIVE AUTHORS

Author's Name	Affiliation	Country	TP	NCP	TC	C/P	C/CP	h	g
Lim, C.	Swiss German University, Tangerang	Indonesia	8	8	60	7.50	7.50	5	7
Mink, D.	University of West Florida, Pensacola	United States	7	5	34	4.86	6.80	2	5
Bagui, S.C.	University of West Florida, Pensacola	United States	6	4	21	3.50	5.25	2	4
Bagui, S.S.	University of West Florida, Pensacola	United States	6	4	21	3.50	5.25	2	4
Khan, L.	Erik Jonsson School of Engineering and Computer Science, Richardson	United States	5	4	29	5.80	7.25	3	5
Mitsunaga, T.	Toyo University, Tokyo	Japan	5	5	10	2.00	2.00	2	2
Okada, S.	Tokyo University, Tokyo	Japan	5	5	10	2.00	2.00	2	2
Beuran, R.	Japan Advanced Institute of Science and Technology, Nomi	Japan	4	3	15	3.75	5.00	2	3

Chen, J.L.	National Taiwan University of Science and Technology, Taipei	Taiwan	4	3	16	4.00	5.33	1	4
Huang, Y.T.	National Taiwan University of Science and Technology, Taipei	Taiwan	4	4	35	8.75	8.75	3	4

Notes: TP=total number of publications; NCP=number of cited publications; TC=total citations; C/P=average citations per publication; C/CP=average citations per cited publication; h=h-index; and g=g-index.

3.3.4 Author Collaboration Network

Figure 5 provides a network view of co-authorship relationships among authors (using VOSviewer with fractional counting). The visualization uncovers a notable pattern: a single, cohesive collaboration cluster dominates, rather than many small, disconnected groups. In this network, virtually all the prominent authors are part of one giant component – with a dense core centered on a tight-knit team. Specifically, two authors, Lin, Ying-Dar, and Lai, Yuan-Cheng (both associated with National Yang Ming Chiao Tung University, Taiwan), sit at the center of this network, connected by thick co-authorship links to each other and several others. Frequent collaborators such as Wu, Eric Hsiao-Kuang, Huang, Yi-Ting, Hwang, Ren-Hung, and Lin, Po-Ching cluster around them, suggesting a prolific lab or research group that publishes extensively on ATT&CK. The thickness of the connecting lines and the shared color in Figure 5 indicate that VOSviewer did not detect separate sub-groups within this cluster – it is effectively one large "family" of co-authors. This suggests that many of the papers in the dataset are the products of this extended team working in collaboration (likely on related projects or a series of ATT&CK applications). The presence of a name like Vaitheeshwari, R., on the periphery of the same cluster (linked to the core group) hints at an external collaborator who connects this core team to outside researchers. Aside from this main cluster, few other strong co-authorship groups are evident – meaning that, beyond the Taiwan-centric group, most other authors either collaborate within smaller two- or three-person teams or are single-paper contributors. This finding suggests a certain centralization of collaboration in the ATT&CK research community: a highly productive core group exists (likely responsible for multiple benchmark papers), while other authorships are more dispersed. From the standpoint of RQ5 (collaboration patterns), this indicates that while many researchers worldwide study ATT&CK, a significant portion of them are indirectly connected through a single prominent collaboration network. Such a nucleus can act as a knowledge hub, but also underscores the need for broader collaboration across independent groups to avoid insularity.

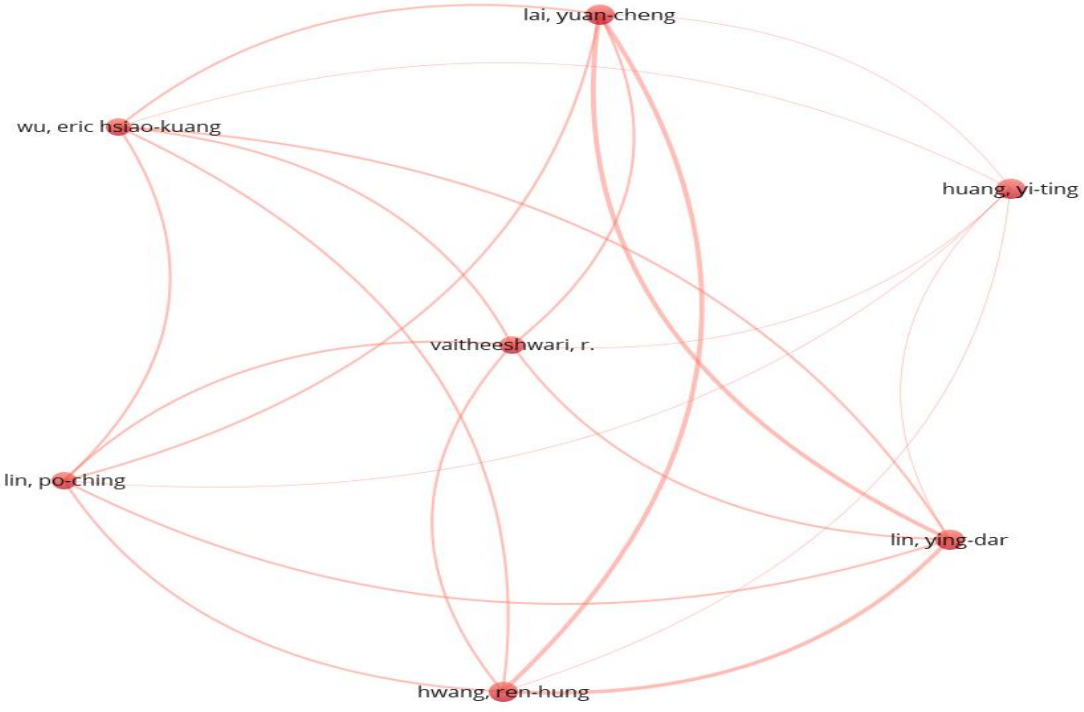

Fig. 5. Network virtualization map by MITRE ATT&CKS research co-authors

3.3.5 International Collaboration Network

Figure 6 maps collaboration at the country level, revealing how nations cooperate on ATT&CK research. The network (constructed with a minimum threshold of 5 documents per country) shows the United States as the central hub of international collaboration – its node is the largest, and it has co-authorship links with almost every other major country. This reflects the U.S.'s pivotal role in the field, often partnering with researchers from Europe, Asia, and elsewhere to produce joint work. Around this hub, several regional clusters emerge, illustrating secondary collaboration circuits. For example, one cluster links South Korea, the United Kingdom, China, and Spain (colored green in Fig. 6), indicating these countries frequently co-author together, perhaps on analytic and experimental cybersecurity topics spanning Asia and Europe. Another cluster centers on India (red cluster), which has collaborative ties to Greece, Malaysia, Australia, Sweden, and Finland. A somewhat eclectic mix, possibly facilitated by diaspora networks or international projects that funnel expertise from India outward. A blue cluster finds Norway connected with France, the Czech Republic, and Singapore, suggesting joint efforts perhaps in critical infrastructure or maritime cybersecurity (domains of interest in those countries). Additionally, Italy, Germany, and Canada form a "transatlantic bridge" cluster (turquoise) linking European and North American research circles. Smaller nodes, such as Japan, Israel, Austria, and Switzerland, appear on the edge (yellow/purple clusters), indicating niche partnerships that occasionally connect the larger network. The main structure is a globally distributed collaboration network anchored by U.S. regional groups that innovate within their localities but tend to connect to the U.S. (and to a lesser extent, through a few key European intermediaries, such as Germany and Italy) to integrate their findings into the broader ATT&CK research discourse. In practical terms, this highlights that the flow of knowledge is facilitated by a few central hubs and bridge countries. For RQ5, it demonstrates an international research network where the U.S. serves as a primary collaboration broker. At the same time, other countries cluster into cooperative sub-networks reflecting geographic or cultural ties (e.g., Commonwealth countries around India, East-West academic partnerships around South Korea and the UK, etc.). This pattern suggests that expanding collaborations (for instance, increasing direct Europe-Asia or Asia-Asia partnerships) could further enrich the global ATT&CK research community beyond the current hub-and-spoke model.

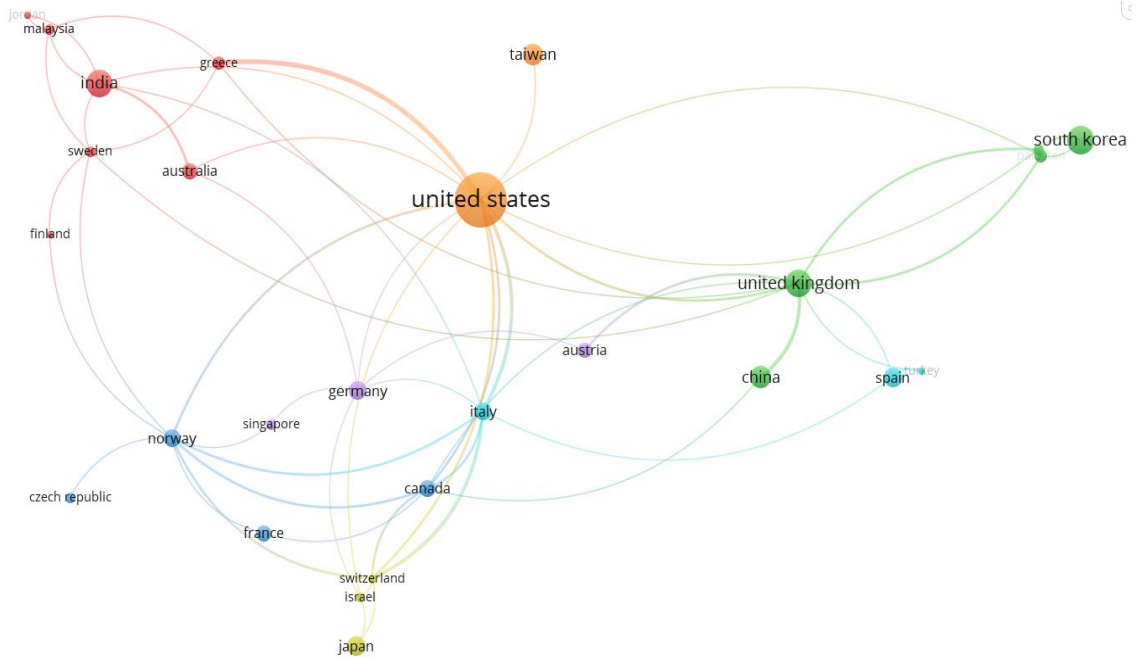

Fig. 6. Network virtualization map of Mitre Att&cks research co-authors by country

3.3.6 Citation Metrics and Influential Works:

The impact of the ATT&CK literature can be further understood through citation analysis. Table 9 summarizes key metrics across 391 documents, comprising a total of 1,878 citations as of early 2025. This equates to approximately 235 citations per year since 2017, or about 4.8 citations per paper. An h-index of 22 indicates that 22 papers each received at least 22 citations, a respectable figure for a field that has only recently gained momentum. A g-index of 30 suggests that there are some highly cited works lifting the citation count (since a g-index of 30 means that the top papers together have at least 30 citations on average, pointing to a subset of publications with tens of citations each). Indeed, a few anchor papers have emerged as particularly influential.

TABLE IX RESEARCH CITATION METRIC ON MITRE ATT&CK

Metrics	**Data**
Total Papers	391
Total Citations	1878
Number of Years	8
Citations/year	234.75
Citations/papers	4.8
Citation/Author	561.09
Papers/Authors	123.78
Authors/Paper	3.8
h_index	22
g_index	30

Figure 7 provides a citation network (citation link map) of ATT&CK documents, which traces how certain papers cite one another and form clusters of influence. Three main clusters can be identified, each centered on a highly cited reference (the nodes with the largest size in Fig. 7):

Fig. 7. Network visualization map of citations of Mitre Att&ck documents

- One cluster is anchored by Ajmal et al. (2021) (IEEE Access), an adversary emulation/threat hunting framework paper. This work was heavily cited by follow-up papers from the same team (e.g., Ajmal et al. 2023) and by others (e.g., Young 2022), indicating that it laid a foundational concept of proactive threat hunting using ATT&CK. The cluster around Ajmal (2021) shows a lineage, where the conceptual groundwork for threat hunting based on ATT&CK was established and then extended by subsequent research from the original authors and early adopters.
- A second cluster centers on Jadidi & Lu (2021), this is the ICS Threat Hunting Framework (ICS-THF) study that integrated ATT&CK with the Diamond Model and kill chain for industrial systems. Jadidi (2021) both cites earlier work like Ajmal (2021) and is in turn cited by a series of methodological papers (e.g., Al Sadi 2024a, 2024b; Fairbanks 2021) that build on its approach. This cluster illustrates how methodological innovations (like combining ATT&CK with risk models) spurred a wave of research refining evaluation metrics and automation tools for ATT&CK in specialized contexts. Jadidi's work effectively connects earlier foundational ideas to later practical implementations, acting as a bridge in the citation network.
- A third cluster is organized around Huang et al. (2022), an influential paper (by Huang Y.T. and colleagues) that appears to broaden ATT&CK's application to operational contexts (possibly an application in security operations or another domain). Huang (2022) is cited by works such as Wong (2024), Lee (2023), and Irfan (2022), forming a cluster that extends the discourse into diverse applied domains. For instance, many citing papers appear to explore ATT&CK in domains such as cloud security or employ it in the evaluation of enterprise defense tools, thereby extending the framework into new areas of practice

Figure 8 shows that the main hub is the United States, where co-authors come mostly from South Korea and the United Kingdom. There are also distinct regional clusters emerging: India with Canada/Indonesia, Australia with Singapore/Austria/Israel, Germany with Italy/Spain, and smaller East Asian links (China, Japan, Taiwan, Malaysia). Italy and Germany act as bridges between these groups. The pattern highlights the dominance of the U.S. role alongside growing region-specific research alliances.

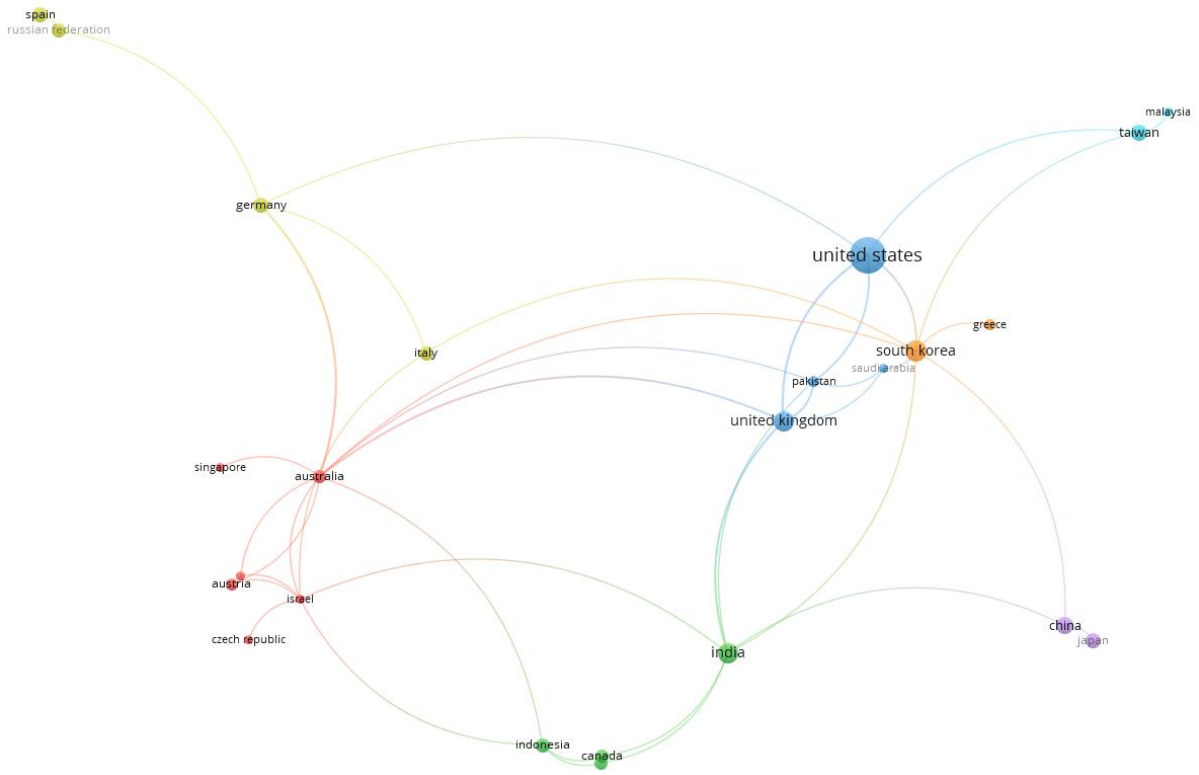

Fig. 8. Network visualization map of Citation of Mitre Att&ck research by country, with a minimum of five documents per country and a minimum of 5 citations per country.

4. DISCUSSION

The bibliometric review presented herein systematically synthesizes the current global research landscape surrounding the MITRE ATT&CK framework, highlighting significant trends, intellectual developments, and notable gaps within the literature.

Research output associated with MITRE ATT&CK has exhibited significant growth since its emergence in academic circles around 2017 [7], with publications doubling approximately every 18 months (see Fig. 2). The framework's expansion into specialized domains closely aligns with this substantial expansion, especially in industrial control systems (ICS) after 2019 [2]. This development has significantly broadened scholarly and industrial engagement. While initial publications predominantly originated from researchers based in the United States, recent bibliometric analyses have demonstrated a pronounced geographic diversification, with increased contributions from European and Asian scholars, particularly those located in the United Kingdom, Germany, Greece, South Korea, India, and Taiwan (table 6, Fig.8). Concurrently, the diversity of publication venues has expanded, and conference proceedings continue to play a pivotal role due to their rapid dissemination capabilities. The proportion of peer-reviewed journal articles has risen remarkably, indicating increased maturity and scholarly validation of the ATT&CK research domain (Tables 1 and 2). These developments highlight the transformation of ATT&CK from a primarily North American initiative into an internationally recognized framework.

The thematic analysis conducted in this review, grounded in keyword co-occurrence and subject area classifications (Fig. 3, Table 5), underlines the depth and diversity of ATT&CK research. Publications remain primarily centered within the disciplines of computer science and engineering (Table 4). The increasing inclusion of mathematics, decision sciences, and social sciences highlights the framework’s interdisciplinary applicability. Particularly, five key thematic clusters emerged from this analysis: Threat Intelligence and Hunting, Intrusion Detection and Machine Learning, Adversary Emulation and Evaluation, Framework Integration and Risk Assessment, and AI-driven Automation. Each of the clusters encapsulates distinct but interrelated research areas, such as Threat Intelligence and Hunting research, extensively employs natural language processing (NLP) and machine learning (ML) methods to leverage ATT&CK’s structured classification, which facilitates the extraction and interpretation of unstructured cyber threat data [9], [10]. Intrusion detection research has seen significant improvement through the integration of transformer-based models and the correlation of system telemetry with ATT&CK techniques, enhancing detection efficacy. Meanwhile, the Adversary Emulation cluster highlights increasing usage of ATT&CK in proactive security practices, such as red and purple teaming [11]. In the Framework Integration and

Risk Assessment cluster, researchers often integrate ATT&CK with complementary models (e.g., Cyber Kill Chain, Diamond Model) to develop quantifiable metrics that are crucial for managing risks, particularly within critical infrastructure [12]. Lastly, AI-driven automation is emerging as a prominent research area, using generative AI techniques and automated planning to enhance scalability and effectively operationalize ATT&CK [9]. Together, these thematic insights highlight ATT&CK's dual role in promoting analytical precision and operational innovation within cybersecurity research and practice [5].

Network visualizations and co-authorship analyses (see Figs. 5 and 6, Tables 6 & 8) reveal a strong pattern of international and interdisciplinary collaboration. The United States remains a central hub of scholarly activity, driving significant exchanges, especially with South Korea and the United Kingdom (Table 6). There are no impactful contributions limited to any specific region. Researchers and institutions around the world have made significant strides, with key contributions from places such as Greece, Indonesia, Norway, and Taiwan. For instance, the research group led by C. Lim in Southeast Asia, the team at the University of West Florida, and international collaborations such as those between UT Dallas and Korea University showcase the global and collaborative spirit of the ATT&CK research community (Table 8). These networks not only accelerated knowledge sharing but also broadened the application of the ATT&CK framework across various fields and methodologies.

Our citation analysis (as illustrated in Table 9 and Figure 7) highlights foundational studies that have significantly shaped the direction of subsequent research. For instance, the work by Ajmal et al. on adversary emulation [11], Jadidi and Lu on threat hunting in industrial control systems (ICS) [12], and Georgiadou et al. on risk assessment methodologies [13] stands out as particularly influential. That said, the way research has been cited also shows a tendency to split into distinct themes, especially when comparing detection methods and risk assessment approaches. This gap could offer a real opportunity for future research that bridges these areas.

While the field has made remarkable progress, several key gaps in the literature surrounding ATT&CK remain. One of the major issues is a lack of attention to ATT&CK techniques that are relevant to emerging areas, such as cloud environments, the Internet of Things (IoT), and more complex ICS scenarios [16][17]. Real-world validation of ATT&CK-based controls is also still missing [18]. Hands-on testing in industrial environments remains rare, despite projects such as [19] examining controls via ATT&CK in ICS settings. Furthermore, Rahman & Williams (2022) highlight that dozens of ATT&CK techniques remain unsupported by existing security controls [20]. The lack of standardized benchmarks and publicly available datasets is another challenge that makes it difficult to ensure reproducibility and carry out in-depth evaluations. On top of that, automating and scaling the process of mapping real-world incidents to the ATT&CK techniques remains a tough challenge [9],[10]. To address these gaps, a more collaborative approach is needed between academia and industry [21]. We need a stronger emphasis on things such as open data sharing, developing new tools, and fostering cross-disciplinary partnerships [22].

Lastly, our analysis highlights the growing role of MITRE ATT&CK as a foundational tool in cybersecurity, which bridges the gap between academic research and practical application. Due to its standardized design, it has made it easier to conduct rigorous, reproducible analyses and support for diverse cybersecurity applications. Future research should focus on validating ATT&CK in real-world settings, creating deeper connections between research areas, and developing open shared resources. By doing so, we can strengthen ATT&CK's role as a cornerstone in both cybersecurity research and practice.

5. CONCLUSION

This bibliometric and network analysis systematically examined 391 Scopus-indexed publications on the MITRE ATT&CK framework from 2017 to 2025, employing quantitative techniques and advanced visualization tools. By analyzing publication trends, citation metrics, thematic clusters, and collaboration networks, this study provides a comprehensive overview of the evolving intellectual landscape surrounding ATT&CK in cybersecurity.

Our results highlight the exponential growth in ATT&CK-related research, particularly in recent years, reflecting the framework's increasing global adoption. Thematic analysis identified five principal clusters: threat intelligence and ontology, adversary emulation and evaluation, machine learning analytics, risk assessment for critical infrastructure, and malware/intrusion detection, demonstrating the diversity and maturity of current research directions. The mapping of co-authorship and institutional networks underscores not only the central role of the United States but also the growing significance of contributions from Asia and Europe, revealing a complex web of regional and interdisciplinary cooperation.

The significance of these findings is twofold. First, they affirm MITRE ATT&CK's role as a foundational tool for both research and practical defense strategies in cybersecurity, standardizing the way adversarial behavior is studied and countered. Second, they highlighted important gaps such as the need for more empirical validation in operational environments and a deeper investigation into cloud-native and ICS domains that can guide future inquiry.

Looking ahead, researchers are encouraged to focus on real-world validation of ATT&CK-informed controls, expand studies into emerging and under-explored areas, such as cloud and IoT security, and leverage international and cross-sector

collaboration to accelerate innovation. By quantifying trends, identifying key contributors and themes, and outlining actionable research priorities, this study not only clarifies the current state of MITRE ATT&CK research but also provides a roadmap for advancing knowledge and practice in global cybersecurity.

Acknowledgement

This work is funded by the collaboration matching grant between Universiti Malaysia Pahang Al-Sultan Abdullah (RDU242745) and Telkom University (UIC241547) and funded by Faculty of Computing UMPSA.

Conflicts of interest

The author's paper explicitly states that there are no conflicts of interest to be disclosed.

References

[1] "MITRE ATT&CK®." Accessed: May 23, 2025. [Online]. Available at: https://attack.mitre.org/

[2] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy," in Technical report, The MITRE Corporation, 2018. Accessed: May 22, 2025. [Online]. Available: https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-andphilosophy.pdf I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] B. Strom, "2020 ATT&CK Roadmap," MITRE ATT&CK®. Accessed: May 29, 2025. [Online]. Available: https://medium.com/mitre-attack/2020-attack-roadmap-4820d30b38ba R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] Y. Jiang et al., "MITRE ATT&CK Applications in Cybersecurity and the Way Forward," Feb. 15, 2025, arXiv: arXiv:2502.10825. doi: 10.48550/arXiv.2502.10825. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[5] S. Roy, E. Panaousis, C. Noakes, A. Laszka, S. Panda, and G. Loukas, "SoK: The MITRE ATT&CK Framework in Research and Practice," Apr. 14, 2023, arXiv: arXiv:2304.07411. doi: 10.48550/arXiv.2304.07411.

[6] B. Al-Sada, A. Sadighian, and G. Oligeri, "Mitre ATT&CK: State of the art and way forward," ACM Comput. Surv., vol. 57, no. 1, pp. 1–37, 2024, Accessed: May 22, 2025. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3687300?casa_token=zApBLSctg_8AAAAA:jTb1uDFdYpjoKlrePiUjA80vjc6Nd0gZtsVVoeat2YCaM9Dl9x8h7bZmIfG4IxD57zjHY3zM0egf

[7] "Scopus - Document search | Signed in." Accessed: May 29, 2025. [Online]. Available: https://www.scopus.com/search/form.uri?display=basic&zone=header&origin=searchbasic#basic

[8] J. Martí-Parreño, E. Méndez-Ibáñez, and A. Alonso-Arroyo, "The use of gamification in education: a bibliometric and text mining analysis," J. Comput. Assist. Learn., vol. 32, no. 6, pp. 663–676, 2016, doi: 10.1111/jcal 12161

[9] L. Wang et al., "From Sands to Mansions: Towards Automated Cyberattack Emulation with Classical Planning and Large Language Models," Apr. 17, 2025, arXiv: arXiv:2407.16928. doi: 10.48550/arXiv.2407.16928

[10] L. Li, C. Huang, and J. Chen, "Automated discovery and mapping ATT&CK tactics and techniques for unstructured Hunting via Adversary Emulation," IEEE Access, vol. 9, pp. 126023–126033, 2021, doi: https://www.vosviewer.com// cyber threat intelligence," Comput. Secur., vol. 140, p. 103815, May 2024, doi: 10.1016/j.cose.2024.103815.

[11] A. B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar, and S. U. Islam, "Offensive Security: Towards Proactive Threat 10.1109/ACCESS.2021.3104260.

[12] Z. Jadidi and Y. Lu, "A Threat Hunting Framework for Industrial Control Systems," IEEE Access, vol. 9, pp. 164118–164130, 2021, doi: 10.1109/ACCESS.2021.3133260.

[13] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," Sensors, vol. 21, no. 9, Art. no. 9, Jan. 2021, doi: 10.3390/s21093267.

[14] "VOSviewer - Visualizing scientific landscapes," VOSviewer. Accessed: May 29, 2025. [Online]. Available: https://www.vosviewer.com//

[15] N. J. van Eck and L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping," Scientometrics, vol. 84, no. 2, pp. 523–538, Feb. 2010.

[16] R. Khan, K. McLaughlin, and S. Sezer, “Security analysis of IoT protocols using formal verification: Current state and future directions,” International Journal of Information Security, vol. 18, pp. 1–18, 2019. [Online]. Available: https://link.springer.com/article/10.1007/s10207-019-00445-y

[17] J. Zhao et al., “A Platform to Evaluate ATT&CK Techniques in IoT Context Sharing,” arXiv preprint arXiv:2407.05290, Jul. 2024. [Online]. Available: https://arxiv.org/abs/2407.05290

[18] OnDefend, “Coverage Isn’t Protection: Why MITRE ATT&CK alignment alone isn’t enough,” OnDefend Blog, Apr. 2025. https://ondefend.com/validate-mitre-attck-coverage-simulations-tabletop/

[19] Divine S. Afenu, Mohammed Asiri, and Neetesh Saxena, “Industrial Control Systems Security Validation Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework,” Electronics, vol. 13, no. 5, art. 917, Feb. 2024. - Demonstrates hands-on ATT&CK-based validation in real ICS scenarios

[20] M. R. Rahman and L. Williams, “An Investigation of Security Controls and MITRE ATT&CK Techniques,” arXiv preprint arXiv:2211.06500, Nov. 2022. [Online]. Available: https://arxiv.org/abs/2211.06500

[21] E. Smyth et al., “The Role of Industry Academia Partnerships Can Play in Cybersecurity: Exploring Collaborative Approaches to Address Cybercrime,” in Proc. ICCWS, 2023. [Online]. Available: (ResearchGate)

[22] Kouper and S. Stone, “Data Sharing and Use in Cybersecurity Research,” Data Sci. J., vol. 23, art. 3, Jan. 2024. [Online]. Available: doi:10.5334/dsj-2024-003

[23] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," Journal of Business Research, vol. 133, pp. 285–296, 2021, doi: 10.1016/j.jbusres.2021.04.070.

[24] A. W. Harzing, Publish or Perish, available at: https://harzing.com/resources/publish-or-perish, 2007

[25] M. Aljanabi, M. A. Ismail, R. A. Hasan, and J. Sulaiman, “Intrusion Detection: A Review,” *Mesopotamian Journal of CyberSecurity*, vol. 2021, pp. 1–4, Jan. 2021. doi: 10.58496/MJCS/2021/001.

[26] W. K. Mohammed, M. A. Taha, and S. M. Mohammed, “A Novel Hybrid Fusion Model for Intrusion Detection Systems Using Benchmark Checklist Comparisons,” Mesopotamian Journal of CyberSecurity, vol. 4, no. 3, pp. 216–232, 2024