Bibliometric analysis of scientific publications on Artificial Intelligence in cybersecurity

Alin ZAMFIROIU[1,2,3,*], Natalia Sierra TOLEDO[1], Daniel-Marian DĂNILĂ[2], Joe FRANCOM[1]

[1] Utah Tech University, Department of Computing, Saint George, Utah, USA
alin.zamfiroiu@utahtech.edu, natalia.sierra.toledo@utahtech.edu, joe.francom@utahtech.edu

[2] Bucharest University of Economic Studies, Department of Economic Informatics and Cybernetics, Bucharest, Romania
alin.zamfiroiu@csie.ase.ro, daniladaniel20@stud.ase.ro

[3] National Institute for Research & Development in Informatics - ICI Bucharest, Bucharest, Romania
alin.zamfiroiu@ici.ro (*Corresponding author)

Abstract: This paper presents a bibliometric review of scientific publications indexed in the Web of Science databases that investigate the use of Artificial Intelligence (AI) in cybersecurity. The study aims to identify the most active authors in the field, the institutions funding research on AI applications in cybersecurity and their main subdomains, as well as the level of documentation of published studies. The study focuses on three major pillars: biometric security, the detection and defense against social engineering, and ethical and privacy implications. The data were extracted and analyzed using a Python script, assessing the total number of published articles, the most influential authors, their affiliated institutions, as well as editorial characteristics such as the average number of pages and the average number of references used annually. The results highlight the continued growth of academic interest in the application of AI in cybersecurity, emphasizing the areas where the greatest research investments are being made and where the most significant challenges arise, including issues related to bias, data privacy, and the robustness of AI models. This analysis provides a coherent picture of current and future research directions, highlighting both the potential of AI and the limits and risks associated with its use.

Keywords: Artificial Intelligence, Cybersecurity, Systematic literature analysis, Bibliometric analysis, Web of Science.

Analiza bibliometrică a publicațiilor științifice despre Inteligența Artificială în securitatea cibernetică

Rezumat: Lucrarea prezintă o analiză bibliometrică a publicațiilor științifice indexate în baza de date Web of Science care investighează utilizarea Inteligenței Artificiale (AI) în securitatea cibernetică. Studiul urmărește identificarea celor mai activi autori în domeniu, a instituțiilor care finanțează cercetarea aplicării AI în securitatea cibernetică și a principalelor lor subdomenii, precum și evaluarea gradului de documentare al studiilor publicate. Studiul se concentrează pe trei piloni majori: securitatea biometrică, detectarea și apărarea împotriva ingineriei sociale, precum și implicațiile etice și de confidențialitate. Datele au fost extrase și analizate utilizând un script Python, fiind evaluate numărul total de articole publicate, cei mai vizibili autori și instituțiile lor afiliate, precum și caracteristici editoriale, cum ar fi numărul mediu de pagini și numărul mediu de referințe utilizate anual. Rezultatele evidențiază creșterea continuă a interesului academic pentru aplicarea inteligenței artificiale în securitatea cibernetică, subliniind domeniile în care se fac cele mai mari investiții în cercetare și în care apar cele mai semnificative provocări, inclusiv în ceea ce privește prejudecățile, confidențialitatea datelor și robustețea modelelor de AI. Această analiză oferă o imagine coerentă a direcțiilor de cercetare actuale și viitoare, evidențiind potențialul AI, dar și limitele și riscurile asociate cu utilizarea acesteia.

Cuvinte-cheie: Inteligență Artificială, securitate cibernetică, analiză sistematică a literaturii, analiză bibliometrică, Web of Science.

1. Introduction

Artificial Intelligence (AI) represents a technological instrument that has been widely implemented across numerous domains of activity. AI especially stands out for its capacity to process and identify threats and it has helped cybersecurity groups accelerate their response to sophisticated and adaptive cyber threats by utilizing machine learning, deep learning and big data analytics (Ovabor et al., 2024). The addition of AI techniques allows for real-time threat detection,

https://doi.org/10.33436/v36i1y202608

an analysis prediction of different risks that could potentially arise and even automated defensive mechanisms (Ejeofobiri et al., 2024).

The use of artificial intelligence has enhanced inconsistency detection for identifying common behaviours in network activity, which makes it more adaptable to unknown or emerging attacks. Traditional signature-based systems are not always accurate in detecting zero-day exploits due to static or unavailable threat signatures. Furthermore, it is also very useful in enhancing Intrusion Detection Systems (IDS). Using supervised learning, models such as Support Vector Machines (SVMs) can be trained on labelled datasets to distinguish between normal and malicious traffic with high accuracy. When labelled data is rare, unsupervised learning techniques, such as clustering and Principal Component Analysis (PCA), help identify anomalies that might signal potential breaches. Moreover, deep learning approaches, including Convolutional Neural Networks (CNNs), allow IDS to detect complex, previously unseen attack patterns in real-time (Ejeofobiri et al., 2024).

While Artificial Intelligence has advanced and has been useful for many cybersecurity tasks, it comes with some limitations and downsides that affect trustworthiness and operational effectiveness. Goswami (2024) talks about issues related to data quality, false positives and vulnerability of AI models to opposing attacks. The effectiveness of AI models is heavily dependent on the quality and volume of data used for training. Incomplete or irrelevant data can lead to poor model performance and inaccurate detection of irregularities. Additionally, learning algorithms require very large volumes of data to accurately represent normal and abnormal behaviour. Some studies have also found that some models are trained on outdated datasets such as KDD99, DARPA98 and NSL-KDD, failing to detect the complexity of modern cyber-attacks and threats (Goswami, 2024).

One of the most urgent issues in AI-driven cybersecurity is to ensure reliable alerts (Dumitrache, et al., 2025). A high rate of false positives can overwhelm security teams with alerts and lead to fatigue. Conversely, there are also false negatives, meaning that there have been missed anomalies. Some attacks are subtle and sophisticated, making them difficult for these tools to detect (Goswami, 2024).

The study aims to answer three research questions. RQ1: Which authors are the most active in this domain. RQ2: Which institutions fund research on the application of AI in cybersecurity and in which subdomains. RQ: How well documented the published studies are, including the number of references used.

This paper is organized as follows. Section 2 presents the methodology. Section 3 describes the related work. Section 4 discusses the obtained results. Section 5 concludes the work.

2. Methodology

Recently, numerous papers have been published on the use of Artificial Intelligence in Cybersecurity. Therefore, it is important to conduct a systematic analysis of the scientific literature addressing these two domains. For this research, we collected bibliographic data on publications indexed in Web of Science.

Three important pillars of Artificial Intelligence in Cybersecurity are considered for our analysis:

- Biometric cybersecurity;
- Social engineering and defense;
- Ethics and privacy.

For each paper indexed in the Web of Science, we have data regarding several aspects. Using a Python script, we generate different reports that highlight the most frequently published papers across various categories, authors with numerous published papers, as well as institutions where these authors are affiliated (see Figure 1).

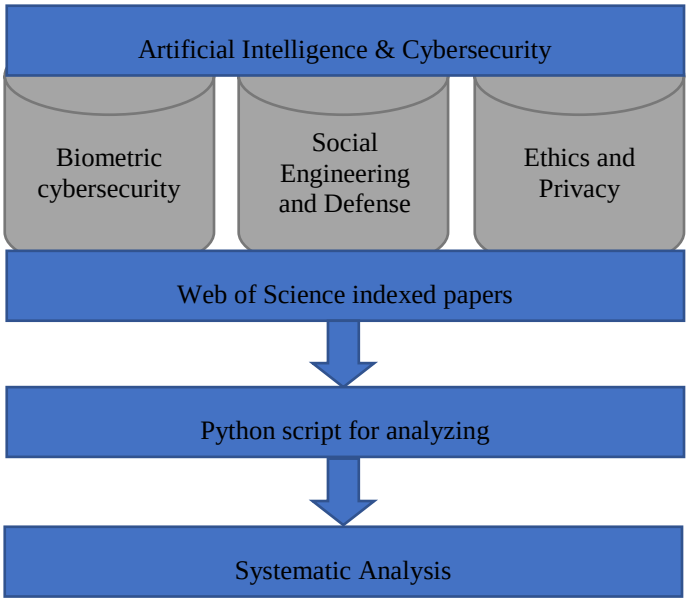

Figure 1. Methodology process (Author's own research)

To create this analysis, we exported data from the Web of Science platform for all papers containing the following keywords:

- "*artificial intelligence*" and "*biometric cybersecurity*"; query used was: "*TS=(artificial intelligence) AND TS=(biometric cybersecurity)*"
- "*artificial intelligence*" and "*social engineering and defense cybersecurity*"; query used was: "TS=(artificial intelligence) AND TS=(social engineering) AND TS=(defense cybersecurity)"
- "*artificial intelligence*" and "*ethics and privacy cybersecurity*"; query used was: "TS=(artificial intelligence) AND TS=(ethics and privacy cybersecurity)"

Information on articles published up to 2026 was gathered, the search being performed in January 2026. Articles published since 2003 were identified, indicating interest in these fields began with that year. All identified papers have been used for the analysis.

Our aim is to find the response for the following questions:

- Which authors are most involved within these domains based on publications?
- Which institutions are funding research on the application of artificial intelligence in cybersecurity, and in which areas of cybersecurity are they focusing?
- Are the published papers in cybersecurity well-researched and do they provide a significant number of references?

The affiliation is important because it allows the analysis to highlight the institutions that invest in this area and have conducted research focused on applying Artificial Intelligence in Cybersecurity. Other aspects examined in our research include the average number of pages per paper every year, as well as the average number of the references.

3. Related work

Similar research is presented in (Albahri & AlAmoodi, 2023). Their analysis is based on a Scopus database covering the period 2012-2023, also examining the annual evolution of publication trends on Cybersecurity and AI applications. Our paper analyses data from the Web of Science database and extends the timeframe to include more recent publications previously not covered. Moreover, we focus on three different pillars of cybersecurity. Through this approach, we aim to highlight the evolving directions of AI in the field of cybersecurity.

Collaboration models, as well as the most common keywords in the domain of AI applications in cybersecurity are identified through research trends (Albahri & AlAmoodi, 2023). Similarly, our paper analyses trends in AI-driven cybersecurity research and identifies institutions and authors that publish in this field.

Another relevant study similar to our research is (Razzaq & Shah, 2025), which analyses published papers from 2016 to 2025. Unlike our research, which is based on the Web of Science database, their analysis relies on the Scopus database, with a number of 3712 analysed papers. The large number is due to a broad search strategy that selects articles containing the terms "machine learning", "deep learning" or "cybersecurity" in their titles, abstracts or keywords. Thus, their study covers the full range of machine learning and deep learning approaches in cybersecurity, whereas our paper focuses on artificial intelligence.

3.1. AI for biometric security (Facial Recognition)

As cyber threats grow more advanced, some organizations are switching to artificial intelligence for biometric cybersecurity. Applications and software make use of various techniques for verifying user identity and regulating access, such as facial recognition, fingerprints, voice, passwords and more.

Facial Recognition is a critical factor in this topic because it uses physical biometrics for AI-supported user authentication. It has become one of the most popular and most used physical biometrics since the aim of this system is to provide a user-friendly security verification system.

Facial Recognition is defined as a system that uses mathematical models of facial features for real-time verification. These features are deeply integrated in cybersecurity, such as unlocking smartphones or securing facilities. The integration of Artificial Intelligence (AI) has significantly advanced facial recognition systems, pushing them beyond the limitations of traditional identification technologies. These systems now make use of machine learning algorithms that help detect and analyse facial characteristics more accurately, Convolutional Neural Networks (CNNs) serving as an example. These systems can process a large number of variations in facial structure, allowing the system to differentiate between expressions and lighting conditions. Ultimately, these systems try to minimize both false positives and false negatives. Furthermore, these AI models can recognize and adapt to changes in a person's appearance over time. This is a significant improvement since aging can affect a person's facial characteristics, such as developing wrinkles or loosening skin, changes in hairstyles or even medical conditions.

Although facial recognition systems are a powerful security enhancement, they are still vulnerable to spoofing attacks. A spoofing attack is digital impersonation, although it can also use physical factors. While AI has improved and is better at detecting spoofing attempts, these attacks are using more sophisticated techniques or tools, such as photos, videos or even 3D masks to avoid security measures. Therefore, AI plays an important role in developing anti-spoofing mechanisms. Certain machine learning models delve deeper into facial recognition, used by more advanced and security-conscious organizations to determine more accurate analyses, beyond simple imitations (Santoso, Safitri & Samidi, 2024).

3.2. AI-powered social engineering detection and defense

Social Engineering attacks have become increasingly complex, rendering traditional security systems insufficient for ensuring safety. Consequently, AI has also been integrated to help against defensive social engineering attacks. Threats such as phishing, pretexting and baiting are social engineering attacks that AI counters through machine learning and behavioural analysis. Artificial intelligence is trained to detect the characteristics of social engineering attacks, which allows systems to identify threats to users regardless of the specific attack (Fakhouri et al., 2024).

Some machine learning models are also trained to detect anomalies and social engineering threats, though they are trained differently using customized featured datasets. Instead of trusting logical rules, the machine learning models learn from statistical patterns of different attacks

(Wang et al., 2022). These may include attacker characteristics, such as technical capabilities or methods employed, as well as victim vulnerabilities, such as their behavioural response, and how specific attack methods exploit these victim weaknesses and what platforms are being used to carry out these attacks (Wang et al., 2022). Some of these models are Decision Tree, Random Forest, Support Vector Machine (SVM), Multilayer Perceptron (MLP) and Adaptive Boosting (AdaBoost). This approach has demonstrated effectiveness (Wang et al., 2022). Moreover, some attacks can be created by using Artificial Intelligence. Grbic and Dujlovic (2023) presented a method for using ChatGPT to design an entire a social engineering attack and process.

Within a network, advanced machine learning algorithms incorporate anomaly detection techniques to identify variations from established patterns of normal behaviour. This is important for detecting more complicated and elaborate attacks that traditional security systems may not succeed in. AI-driven analytics monitor user interactions to detect manipulative signs or irregularities, such as accessing certain data or file transfers during odd hours. Additionally, behaviour-based detection is used to counter targeted scams, such as CEO fraud, by analysing writing styles or communication patterns over time (Fakhouri et al., 2024).

Natural Language Processing (NLP), is a branch of artificial intelligence that enables computers to understand, interpret and generate human language. It is particularly effective in detecting text-based threats, such as phishing. NLP algorithms are trained to identify the differences in language structure, style and tone of a text (Vevera, Vasiloiu & Stoica, 2025). These can be used to protect against malicious spam emails and suspicious domains by analysing characteristics such as URL structures or website layouts. Furthermore, such tools support real-time threat mitigation through predictive analytics based on both historical and live data to anticipate potential attack vectors. This allows cybersecurity systems to reduce overall risk exposure (Fakhouri et al., 2024).

3.3. Ethical and privacy implications of AI in cybersecurity

According to (Narwal, Saraswat & Singh, 2025), ethical challenges arise when organizations prioritize data accessibly over data privacy, which can lead to excessive surveillance or the unregulated collection of personal information. These concerns are intensified by AI tools capable of extracting vast amounts of personal information without explicit consent, raising doubts about individuals' ability to maintain their privacy rights when technologies have the capability to gather data without consent. Such automated systems not only analyse behaviour at scale but may also be used for targeted profiling on social media platforms, advertising manipulation and behavioural surveillance, under the appearance of enhanced security. The shift toward data-driven cybersecurity practices has blurred ethical boundaries, especially when individuals are unaware of how their digital footprints are being used to train and operate these models (Narwal, Saraswat & Singh, 2025).

In addition to surveillance, another pressing concern is the potential for bias and the mishandling of sensitive data by AI systems. Large language models, such as ChatGPT, can perpetuate gender, racial and other social biases, which are inherited from the datasets they are trained on (Dlamini, 2024). These biases often emerge because, while training data is large, it is not always representative, making it challenging for models to answer queries for every topic in the world from different perspectives. This ultimately fails to reflect diverse viewpoints or progressive values. As an example of this, Samsung employees unintentionally leaked sensitive internal code by pasting it into ChatGPT for debugging, inadvertently leading to inputting confidential company information into the AI model, which then became part of its retained memory. These examples highlight the danger of tools intended to secure information when privacy and bias are not central to their design (Gupta et al., 2023).

4. Obtained results and discussions

We gathered the records across three paper categories from the Web of Science platform, as outlined in Table 1.

Table 1. Number of records for each category of papers

Category	Artificial Intelligence Biometric Cybersecurity	Artificial Intelligence Social Engineering and Defense in Cybersecurity	Artificial Intelligence Ethics and Privacy for Cybersecurity
Number of records/papers	124	154	198

After saving all records fields, we begin their analysis. We compiled a list of the top 15 authors by domain, as shown in Figure 2.

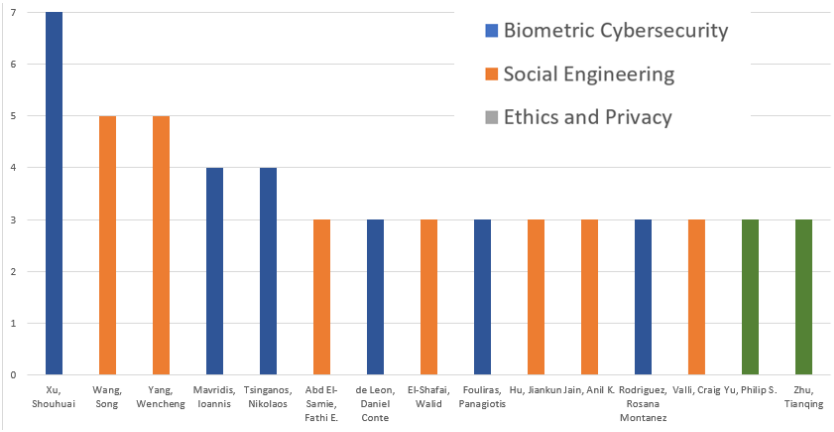

Figure 2. Top 15 authors by domain (Author's own research)

Figure 2 displays the distribution of the 15 most prolific authors across the three analysed fields: Biometric Security, Social Engineering and Ethics and Privacy within the context of Artificial Intelligence applied to cybernetics. The graph highlights significant differences in the level of scientific activity between these fields.

It is observed that the Ethics and Privacy field has the fewest authors, with a low volume of publications. This suggests that academic concern for the ethical implications of AI is a recent development, authors only recently beginning to publishing on this topic. The Social Engineering and Defense field has a significantly larger number of authors, reflecting the increasing importance of studying methods for detecting and preventing attacks based on psychological manipulation. In contrast, the Biometric Cybersecurity field has fewer authors than the Social Engineering field but presents a high thematic coherence, indicating a specialized and ongoing focus in research. The chart allows the identification of scientific leaders in each field and highlights publication trends, emphasizing the areas in which the academic community is investing most intensely. The analysis continues with the top 21 affiliation institutions with researchers who have published papers in these fields, as shown in Figure 3.

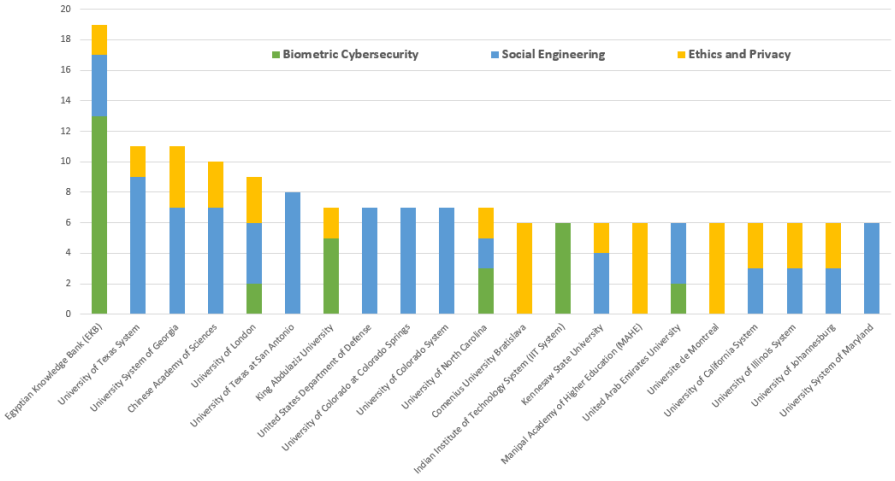

Figure 3. Top 21 institutions with published papers by domain (Author's own research)

Figure 3 illustrates the distribution of the 21 institutions with the highest contribution to the publication of articles in the fields of AI & Biometric Security, AI in Social Engineering and AI in Ethics and Privacy. The graph highlights that scientific production is primarily concentrated in large research institutions or universities with specialized cybersecurity centres.

Some institutions have a higher volume of articles in the field of Ethics and Privacy, which confirms the focus of academic efforts on understanding the social and moral implications of AI. Others excel in Social Engineering and Defense, highlighting the emphasis on researching emerging cyber-attacks and developing automated defense systems. Although numerically smaller, the field of Biometric Cybersecurity shows increased interest from technical institutions, emphasizing the role of AI in authentication and identification. The Figure 3 provides a broader perspective on the academic landscape, indicating where resources, funding and expertise are concentrated in relation to the application of AI in security.

Figure 4 illustrates the average number of pages per published paper each year across all three domains.

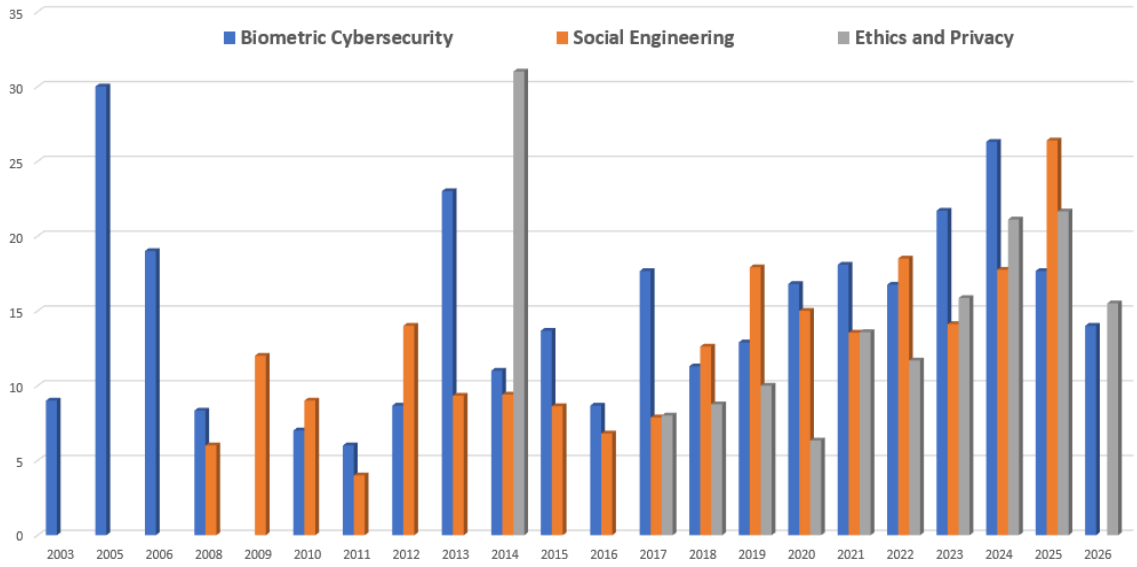

Figure 4. The average number of pages of for each domain (Author's own research)

The evolution of the average number of pages for articles published annually in the three areas of interest, as shown in Figure 4, highlights the complexity of the research conducted and the maturity of the scientific field. Analysis of the graph indicates that articles in the Ethics and Privacy field tend to be longer, particularly in the beginning, such as 2014. This reflects extensive debates, case studies, ethical discussions and conceptual analyses that require detailed exposition. In the Social Engineering and Defense field, the page count is relatively stable, which may indicate a methodological maturity and a standardized approach to experimental studies.

The Biometric Cybersecurity field shows moderate variations, likely due to differences between applied works (focused on algorithms, experiments and implementations) and theoretical studies. These differences provide insights into the dynamics of each field and how research evolves over time.

The last factor we analysed in our study was the average number of references used per year, as shown in Figure 5.

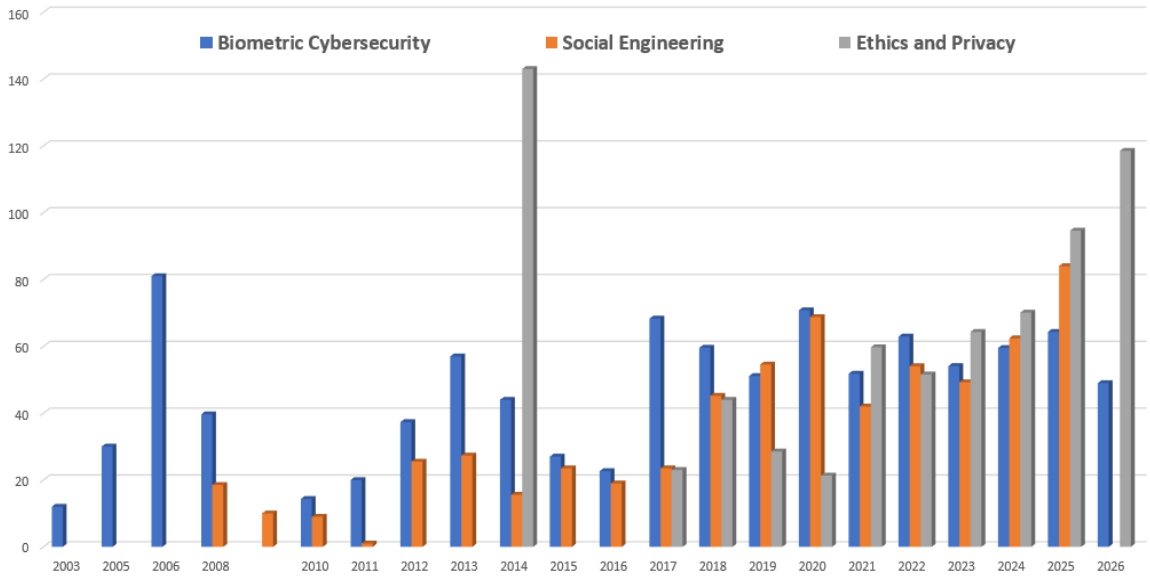

Figure 5. The average number of references used (Author's own research)

Figure 5 illustrates the evolution of the average number of bibliographic references included annually in articles published in the three analysed fields: Biometric Cybersecurity, Social Engineering and Defense, and Ethics and Privacy. This measure provides an important insight into the depth and academic rigor of the works, as a higher number of references usually indicates a stronger theoretical foundation and a broader integration into the specialized literature.

Analysis of the graph suggests that the field of Ethics and Privacy has the highest average number of references, reflecting the multidisciplinary and often complex nature of studies in this sector, with theoretical discussions and ethical arguments requiring extensive citation. This trend highlights the rapid maturation of the field and the increasing focus on understanding the social, legal and moral implications of AI in cybersecurity.

The field of Social Engineering and Defense shows a moderate to high average number of references, indicating that the articles frequently rely on empirical studies, behavioural analyses and mathematical models. The variety of attack techniques, as well as the dynamics of human interactions, require authors to integrate a wide spectrum of studies to support their conclusions.

In Biometric Cybersecurity, the average number of references is slightly lower, but constant, compared to other fields, suggesting a methodologically well-defined field where research emphasizes technical experiments, algorithmic models and performance evaluations over extensive conceptual discussions.

Overall, Figure 5 shows that all three fields are growing, and the diversity and organization of the used references reflect both the maturity of each research area and the rate at which interdisciplinary literature around the application of Artificial Intelligence in cybersecurity is developing.

Based on our analysis, we conclude that during the first period (2003-2015), the field of "Biometric Cybersecurity" received the highest attention. In the subsequent period (2015-2026), the interest shifted to an increased interest in the field of Social Engineering and even higher for the field of Ethics and Privacy. We estimate that in the coming years, Ethics and Privacy will attract the highest level of interest, as the number of publications in this field has greatly increased in recent years. It notable that there are very few institutions in the top 21 without publications in Ethics and Privacy or Social Engineering. This suggests that researchers at these institutions are likely to contribute more articles to these fields, further supporting the expectation of a significant rise in focus on Ethics and Privacy.

5. Conclusions

The systematic analysis of publications indexed in the Web of Science shows a significant increase in academic interest in applying Artificial Intelligence to cybersecurity. Each of the three areas examined represents an essential direction in the evolution of digital security. Additionally, there are other areas that could explored in our future work.

Biometric security continues to evolve in response to the growing need for secure and automated authentication. AI is crucial in improving the accuracy of facial recognition systems and combating spoofing attacks.

Social engineering and automated defense, powered by AI models, are becoming priority areas due to the rise of phishing attacks, fraud and psychological manipulation. Research findings confirm that machine learning and natural language processing techniques can detect subtle patterns that traditional systems cannot detect.

Data ethics and privacy represent the area with the greatest development and scientific concern. Challenges such as algorithmic bias, excessive surveillance, data leakage risks and lack of transparency in AI models are becoming central themes in the academic debate.

The statistical analysis of publications – including top authors, institutions, average page views and references – provide a clear picture of the maturity and research directions in the field. Overall, the study confirms that AI is an essential tool in security, but requires a balanced and responsible approach to maximize benefits while minimizing risks.

Author contributions

Conceptualization: A.Z. and N-S.T.; Data Curation: A.Z., N-S.T. and D-M.D.; Project administration: A.Z.; Supervision: A.Z.; Validation: A.Z., D-M.D. and J.F.; Writing - original draft: A.Z. and N-S.T.; Writing – review and editing: D-M.D. and J.F.; All authors have read and agreed to be published version of the manuscript.

Submitted: 13 January 2026; Revised: 03 February 2026; Accepted: 09 February 2026; Published: 31 March 2026.

REFERENCES

Albahri, O. S. & AlAmoodi, A. H. (2023) Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database. *Mesopotamian Journal of CyberSecurity*. 2023, 158-169. https://doi.org/10.58496/MJCSC/2023/018.

Dlamini, P. (2024) ChatGPT: Racial and Gender Discrimination and Bias Artificial Intelligence. *Master's thesis, University of Johannesburg, South Africa*. 2024. https://ujcontent.uj.ac.za/esploro/outputs/graduate/ChatGPT--racial-and-gender-discrimination/9955394407691#file-0. [Accessed: 20 March 2026].

Dumitrache, M., Sacala, I. S., Rotuna, C. I. et al. (2025) Developing an Intelligent Security Monitoring Platform for Internet Domains. A Practical Implementation Approach. *Studies in Informatics and Control*. 34(1), 75-84. https://doi.org/10.24846/v34i1y202506.

Ejeofobiri, C., Fadare, A. A., Fagbo, O. O. et al. (2024) The role of Artificial Intelligence in enhancing cybersecurity: A comprehensive review of threat detection, response, and prevention techniques. *International Journal of Science and Research Archive*. 13(02), 310-316. https://doi.org/10.30574/ijsra.2024.13.2.2161.

Fakhouri, H. N., Alhadidi, B., Omar, K. et al. (2024) Ai-Driven Solutions for Social Engineering Attacks: Detection, Prevention, and Response. In *2024 2nd International Conference on Cyber Resilience* (ICCR), *26-28 February 2024, Dubai, United Arab Emirates*. IEEE. pp. 1-8. https://doi.org/10.1109/ICCR61006.2024.10533010.

Goswami, M. (2024) AI-Based Anomaly Detection for Real-Time Cybersecurity. *International Journal of Research and Review Techniques*. 3(1), 45-53. https://ijrrt.com/index.php/ijrrt/article/view/174/51 [Accessed: 20 March 2026]

Grbić, D. V. & Dujlović, I. (2023) Social engineering with ChatGPT. In *2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH), 15-17 March 2023, East Sarajevo, Bosnia and Herzegovina*. IEEE. pp. 1-5. https://doi.org/10.1109/INFOTEH57020.2023.10094141.

Gupta, M., Akiri, C., Aryal, K. et al. (2023) From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*. 11, 80218-80245. https://doi.org/10.1109/ACCESS.2023.3300381.

Narwal, N., Saraswat, A. & Singh, M. (2025) Ethics in Cybersecurity and Data Privacy. *International Journal of Recent Research and Review*. Special Issues 2025. 133-149. https://www.ijrrr.com/specialissues2025/ijrrr-Special-Issue-2025-paper13.pdf. [Accessed: 20 March 2026]

Ovabor, K., Sule-Odu, I. O., Atkison, T., et al. (2024) AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools, and future directions. *Open Access Research Journal of Science and Technology*. 12, 40-48. https://doi.org/10.53022/oarjst.2024.12.2.0135.

Razzaq, K. & Shah, M. (2025) Advancing Cybersecurity Through Machine Learning: A Scientometric Analysis of Global Research Trends and Influential Contributions. *Journal of Cybersecurity and Privacy*. 5(2), 12. https://doi.org/10.3390/jcp5020012.

Santoso, W., Safitri, R. & Samidi, S. (2024) Integration of Artificial Intelligence in Facial Recognition Systems for Software Security. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*. 8(2), 1208-1214. https://doi.org/10.33395/sinkron.v8i2.13612.

Vevera, A. V., Vasiloiu, I. C. & Stoica, M. (2025) An AI-based OSINT framework for fake news detection and economic impact assessment in cyber diplomacy. *Romanian Journal of Information Technology and Automatic Control [Revista Română de Informatică și Automatică]*. 35(4), 63-77. https://doi.org/10.33436/v35i4y202505.

Wang, Z., Ren, Y., Zhu, H. & Sun, L. (2022) Threat detection for general social engineering attack using machine learning techniques. To be published in *Cryptography and Security*. [Preprint] https://arxiv.org/pdf/2203.07933 [Accessed: 10 January 2026].

Alin ZAMFIROIU graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2009. In 2011 completed a Master's degree in Economic Informatics at the Bucharest University of Economic Studies, and in 2014, he completed his doctoral research in Economic Informatics. He currently works as a Senior Researcher at the National Institute for Research & Development in Informatics, Bucharest, and as an associate professor at the Department of Economic Informatics and Cybernetics of the Bucharest University of Economic Studies, Bucharest. In 2025, he was a visiting teacher at Utah Tech University, where he conducted teaching and research activities. He has published articles in journals as an author and co-author, as well as scientific presentations at conferences.

Alin ZAMFIROIU a absolvit Facultatea de Cibernetică, Statistică și Informatică Economică în anul 2009. În 2011 a absolvit programul de Master în Informatică Economică, organizat de Universitatea de Studii Economice București, iar în 2014 și-a terminat cercetarea doctorală în

Informatică Economică. În prezent lucrează ca cercetător principal la Institutul Național de Cercetare-Dezvoltare în Informatică - ICI București, și conferențiar universitar la Departamentul de Informatică Economică și Cibernetică a Academiei de Studii Economice, București. În anul 2025 a avut calitatea de profesor invitat la Utah Tech University, unde a realizat activități de predare și cercetare. A publicat în calitate de autor și co-autor articole în jurnale, precum și prezentări științifice la conferințe.

Natalia Sierra TOLEDO is an undergraduate student at Utah Tech University, majoring in Information Technology with an emphasis in Cybersecurity. She completed this paper as part of the SET International Fellowship, a year-long research program supporting undergraduate scholarship. Natalia has been named on the university president's list twice in recognition of academic achievement and maintains a strong interest in cyber defense strategies.

Natalia Sierra TOLEDO este studentă la Universitatea Utah Tech, specializându-se în tehnologia informației, cu accent pe securitatea cibernetică. Ea a realizat această lucrare în cadrul programului internațional SET, un program de cercetare cu durata de un an care sprijină bursele pentru studenți. Natalia a fost inclusă de două ori pe lista președintelui universității ca recunoaștere a realizărilor sale academice și menține un interes puternic pentru strategiile de apărare cibernetică.

Daniel-Marian DĂNILĂ graduated from the Faculty of Cybernetics, Statistics, and Economic Informatics in 2023, and in 2025 he completed a Master's degree in Information Security at the Bucharest University of Economic Studies. His research interests are continuous authentication and behavioral biometrics. He is an associate professor at the faculty from which he graduated.

Daniel-Marian DĂNILĂ a absolvit Facultatea de Cibernetică, Statistică și Informatică Economică în 2023, iar în 2025 a absolvit programul de Master în Securitate Informatică din cadrul Academiei de Studii Economice din București. Interesele sale de cercetare sunt autentificarea continuă și biometria comportamentală. Este cadru didactic asociat în cadrul facultății pe care a absolvit-o.

Joe FRANCOM is a professor and chair of the Department of Computing at Utah Tech University, with a career centered on developing practical, industry-aligned technology programs. His expertise spans software engineering, cloud infrastructure, cybersecurity and systems

automation, emphasizing hands-on learning and real-world problem solving. He earned his PhD in Computer Science from the University of Louisville in 2007, specializing in Identity Management.

Joe FRANCOM este profesor și directorul Departamentului de Informatică la Universitatea Utah Tech, cu o carieră axată pe crearea de programe tehnologice practice, aliniate cerințelor industriei. Expertiza sa acoperă domenii precum ingineria software, infrastructura cloud, securitatea cibernetică și automatizarea sistemelor, cu un accent puternic pe învățarea practică și rezolvarea problemelor din lumea reală. A obținut doctoratul în Informatică la Universitatea din Louisville în 2007, cu specializare în managementul identității.