DOI: https://doi.org/10.61762/pjstvol8iss2art001

PLATFORM - A Journal of Science & Technology

Received: 22 October 2025, Revised: 20 November 2025, Accepted: 27 November 2025, Published: 31 December 2025, Publisher: UTP Press, Creative Commons: CC BY 4.0

MACHINE LEARNING TECHNIQUES FOR IOT SECURITY: A BIBLIOMETRIC ANALYSIS AND ROAD-MAPPING

Mujaheed Abdullahi[1]*, Hitham Alhussian[1,2], Norshakirah Aziz[1,3], Said Jadid Abdulkadir[1,2]

[1]Department of Computing, Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia
[2]Centre for Research in Data Science (CeRDaS), Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia
[3]Centre for Cyber-Physical Systems (C2PS), Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia

*Corresponding author: abdullahi_18001208@utp.edu.my

ABSTRACT

The integration of the Internet of Things (IoT) across various sectors, including healthcare, smart cities, and industrial automation, has heightened the demand for robust security solutions to counter the threat of cyberattacks. Cyberattacks targeting IoT devices can have significant consequences, including data breaches, operational disruptions, and substantial network compromises. Machine learning (ML) has become an essential approach for addressing these complex security challenges. Therefore, this study conducts a bibliometric analysis to quantitatively map the intellectual structure and thematic development of the ML for the IoT security research domain. An analysis was conducted on 3,744 scientific documents, published from 2015 to 2025, obtained from the Scopus database. Performance analysis and science mapping techniques, including keyword co-occurrence and co-authorship analyses, were employed to identify key contributors, collaboration networks, organisations, and sources. The results indicate that the field is substantially influenced by dominant AI trends, particularly the rise of large language models (LLMs), resulting in a notable "practicality gap" between computationally intensive models and the resource-constrained nature of IoT devices. Additionally, the country collaboration map indicates that the United States, China, the United Kingdom, and India are the largest contributors to publication volume. In contrast, federated learning has become a significant area of research, focusing on data privacy and decentralisation in IoT. Finally, this study identifies potential research gaps by examining current trends, thereby providing insights for future work in developing efficient and resilient IoT security.

***Keywords*:** *Bibliometric, road-mapping, VOSviewer, distributed denial-of-service (DDoS), security, threats*

INTRODUCTION

The rapid growth of the Internet of Things (IoT) has revolutionised various sectors, including healthcare, smart cities, and industrial automation. This expansion has concurrently heightened security vulnerabilities due to the diversity, scale, and resource limitations of IoT devices. Although conventional IoT security measures and rule-based approaches serve as a foundation, they frequently fail to address complex and evolving cyber threats [1]. Machine learning (ML) techniques, including supervised, unsupervised, and deep learning (DL) methods, are capable of intrusion detection, anomaly detection, adaptive threat mitigation, and providing scalability in IoT environments [2]. For example, k-nearest neighbour (KNN) and artificial neural networks (ANNs) have been employed to identify distributed denial-of-service (DDoS) attacks by training classifiers on specialised network traffic datasets [3]. These approaches often require techniques such as the synthetic minority oversampling technique (SMOTE) to mitigate inherent data imbalances, highlighting a broader research effort aimed at safeguarding the vulnerable and rapidly evolving IoT landscape against botnet attacks. Additionally, ML is widely applied to network traffic for detection, and many approaches use generic features, motivating the development of new techniques based on unique IoT-specific network behaviours [4]. Overcoming the exploitation of insecure consumer IoT devices by botnets, such as DDoS attacks, is a critical security challenge.

Bibliometric analysis is a quantitative and statistical approach employed to systematically map the intellectual structure and evolution of a scientific field [5]-[6]. This method uses bibliographic data sourced from academic databases, advancing beyond qualitative literature reviews to provide an objective, reproducible, and transparent summary of the research area. The methodology comprises two primary elements: performance analysis and science mapping [7]-[8]. Performance analysis evaluates the impact and effectiveness of research activities, encompassing authors, institutions, and journals, often employing metrics such as publication and citation numbers. The integration of bibliometric analysis within the assessment of ML techniques for IoT security provides a structured approach to delineate the intellectual, conceptual, and collaborative frameworks in this rapidly advancing field. Advanced tools such as VOSviewer enable researchers to identify key contributors and monitor thematic evolution quantitatively [9]-[10]. It also uncovers the relationship between emerging security challenges and ML innovation. Additionally, by providing a structural and historical summary of the field, these insights reveal untapped research areas that bridge the gap between theoretical frameworks and real-world IoT security implementations.

Despite the growing literature, significant gaps remain in comprehending the intellectual structure, including dominant and advancing research areas, as well as structural shortcomings, particularly misalignment between theoretical ML models and the constraints encountered in real-world IoT deployments [11]-[12]. Bibliometric studies have mapped the landscape of ML in IoT, highlighting increasing publication trends, key authors, and prominent countries that contribute to this domain [13]. Previous bibliometric analyses have explored ML within the larger contexts of cybersecurity or IoT; however, there is a scarcity of studies that concentrate specifically on its application to IoT security, systematically mapping the productivity trends, conceptual frameworks, and practical limitations. Additionally, there is limited synthesis of how geopolitical, institutional, and thematic elements interact to affect the evolution of the study topic [14]. This study addresses a significant gap by using a bibliometric approach to map the comprehensive research landscape of AI applications in IoT security. Additionally, this study combines performance analysis with scientific mapping to provide a comprehensive research roadmap that synthesises current key topics for future exploration. The main aim of this study is to advance from narrative summaries to a data-driven analysis that addresses the following research questions:

1. Which country is leading the research on ML techniques for IoT security?
2. Which journal has published the highest number of studies on ML techniques for IoT security?
3. Which institute plays the most influential role in advancing IoT security research?
4. What are the potential research gaps and challenges in IoT security?

LITERATURE REVIEW

This section presents a review that combines the fundamental and current literature to establish the background for this bibliometric analysis. However, the application of ML to cybersecurity is a well-established domain; its adaptation to the distinct context of the IoT, however, continues to pose both problems and opportunities. The IoT security landscape is characterised by a distinct combination of scale, heterogeneity, and resource constraints. Comprehensive reviews have detailed these challenges, emphasising the vulnerabilities within the perception, network, and application layers of IoT architecture. For example, a survey conducted by Sicari et al. [15] presents a detailed taxonomy of security issues, examining the constraints posed by limited computational power and the current solutions available in the IoT domain. The resource-constrained nature of IoT networks renders them particularly vulnerable to large-scale attacks such as the Mirai botnet. This botnet exploits default credentials to compromise millions of devices and launch massive DDoS attacks [16]. These incidents require intelligent, adaptive, and lightweight security mechanisms to mitigate their impact.

In addition, researchers have increasingly adopted ML and DL techniques to address the security challenges associated with IoT [17]-[18]. Similarly, researchers have utilised algorithms such as support vector machines (SVMs) to identify abnormal network traffic, often testing them with benchmark datasets such as SL-KDD or the more contemporary IoT-specific Bot-IoT dataset [19]. This study demonstrated the capability of employing ML techniques to enhance IoT security.

A recent survey revealed that DL models, such as convolutional neural networks (CNNs), have been employed for malware analysis in IoT binaries, and recurrent neural networks (RNNs) have been employed to analyse sequential network traffic data. These DL-based approaches often outperform traditional ML methods in terms of accuracy in the IoT context [20].

The current literature is extensive, comprising qualitative surveys and systematic reviews that encapsulate advancements in ML techniques for IoT security. These studies provide important technical summaries but are inherently limited in scope. They are proficient in elucidating the techniques employed; however, they are less adept at articulating the overarching quantitative trends, structural dynamics, and intellectual currents within the field. For instance, they may be unable to account for the significant impact of recent AI developments, such as large language models (LLMs), on the research field or illustrate collaborative and non-collaborative relationships between prominent research institutions. This study employs a bibliometric approach to address this gap, complementing existing qualitative reviews with data-driven field analysis.

METHODS

This study used a quantitative bibliometric analysis framework to systematically examine the research landscape of ML applications in IoT security. The search focused on the Scopus database, provided by Elsevier (https://www.scopus.com), due to its comprehensive coverage of peer-reviewed literature. The database offers source-neutral abstracts and citations, which are thoroughly curated by independent subject matter experts recognised as leaders in their respective fields. A search query was formulated using the keywords 'Artificial Intelligence' OR 'AI' AND 'Large Language Models' AND 'Cybersecurity' OR 'Threats' AND 'Internet of Things' OR 'IoT' AND 'IoT Security' AND 'Bibliometric Analysis.' Approximately 26,000 items were obtained from this initial search, which were then narrowed down to a 10-year period, from 2015 to 2025. The final dataset, following a thorough screening process, consisted of 3,744 documents, including 1,842 articles and 1,025 conference papers.

Bibliographic data were exported in comma-separated value (CSV) format and processed using Microsoft Excel for analysis preparation. The curated dataset was then incorporated into the bibliometric analysis step, which aimed to extract key insights into the research landscape of this field. Analysis was conducted using VOSviewer software (version 1.6.20) to ensure improved transparency of the bibliometric research [21]. According to the flowchart, the key goals were to identify the most effective countries with strong research interests, the most important organisations, the most active sources, such as journals, and the primary publication fields. To achieve these objectives, scientific output was quantified using performance analysis, and conceptual and social networks within the field were visualised through science mapping techniques, including keyword co-occurrence and co-authorship analyses.

Figure 1 presents a flowchart of the sequential data processing for the bibliometric analysis using VOSviewer. The procedure comprises four stages: First, publication areas are used to understand the distribution of research across various academic disciplines and publication categories. Countries with a strong research focus aim to map the geographic distribution of research production and identify the leading nations. The most notable organisations are universities, research centres, and institutions that lead in this domain. Finally, the most active sources were utilised to identify the major journals and conference proceedings that have published the majority of research in this field.

RESULT AND DISCUSSION

This section presents the results and discussion of the bibliometric analysis conducted on literature from 2015 to 2025. Table 1 presents a detailed description of the document types incorporated in the bibliometric analysis, indicating their frequency and distribution percentages. According to this data, the most common publication formats for ML approaches to IoT security are conference papers and research articles. Articles constituted the predominant segment, with 1,842 publications, representing 49.2% of the dataset. This high percentage highlights the significance of peer-reviewed journal publications in disseminating foundational research and novel

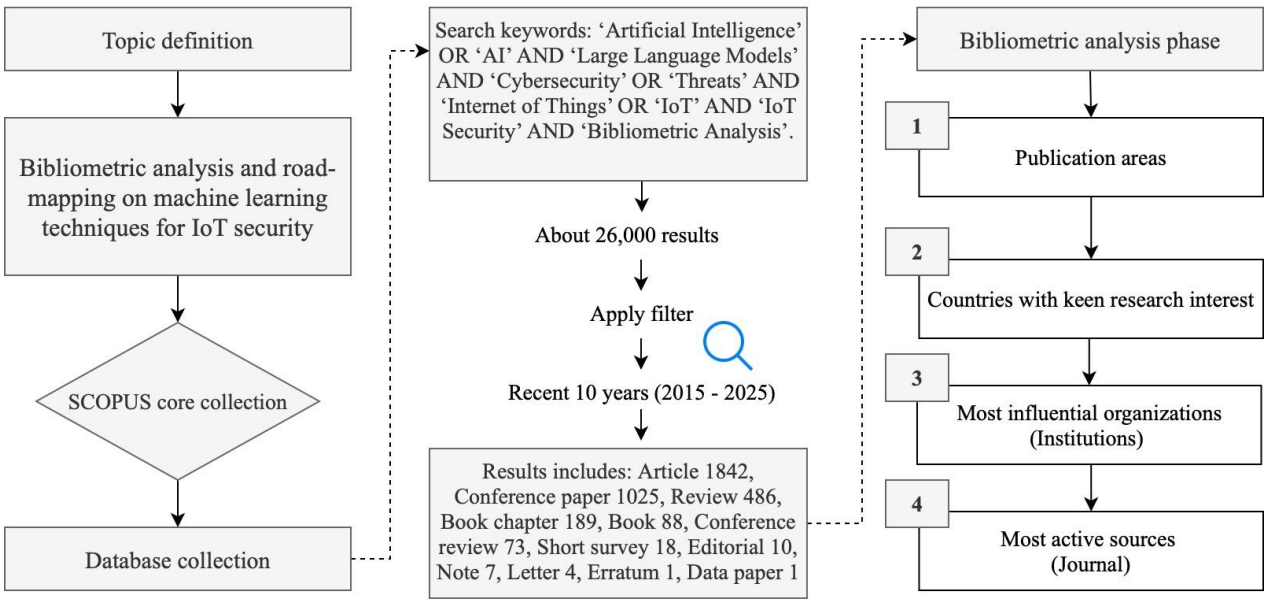

Figure 1 Step-by-step flowchart of VOSviewer bibliometric analysis

field findings. Conference papers represented the second most prevalent document type, totalling 1,025 publications, which accounted for 27.4% of the overall total. Academic conferences serve as essential venues for researchers to showcase innovative methodologies and initial findings, underscoring a dynamic and rapidly evolving research environment that is constantly advancing.

Additionally, the remaining document types, including reviews (13.0%), book chapters (5.0%), books (2.4%), and conference reviews (1.9%), represent smaller, yet important, segments of the literature. A significant volume of reviews suggests an evolving discipline in which researchers are engaged in synthesising the current knowledge. The infrequent occurrence of document types such as short surveys, editorials, notes, letters, errata, and data papers, each comprising less than 1%, underscores the dataset's emphasis on primary research output over administrative or short-form communication.

Table 1 Document types

Types	Frequency	Percentage
Article	1842	49.2%
Conference paper	1025	27.4%
Review	486	13.0%
Book chapter	189	5.0%
Book	88	2.4%
Conference review	73	1.9%
Short survey	18	0.48%
Editorial	10	0.27%
Note	7	0.19%
Letter	4	0.11%
Erratum	1	0.03%
Data paper	1	0.03%

Figure 2 illustrates a VOSviewer representation of the keyword co-occurrence network, which visualises the conceptual framework of the research domain. This study identifies several significant thematic clusters based on 8,621 keywords, 373 of which meet a minimum occurrence requirement of five keywords. The most noticeable and central cluster, which is green in colour and situated at the centre of the network, is centred on 'artificial intelligence' and 'natural language processing.' This prominence underscores their fundamental relevance in broader research. The network also recognises other notable research areas. A concentrated cluster on the left, depicted in red, is characterised by terms such as 'federated learning,' 'anomaly detection,' and 'convolutional neural networks,' signifying a pronounced emphasis on particular ML methodologies and their applications. A separate cluster, represented in blue, encompasses 'IoT security,' 'cyberattack,' and 'malware,' specifically focusing on the security-related applications of these technologies. This image accurately delineates the interrelations of fundamental concepts, uncovering

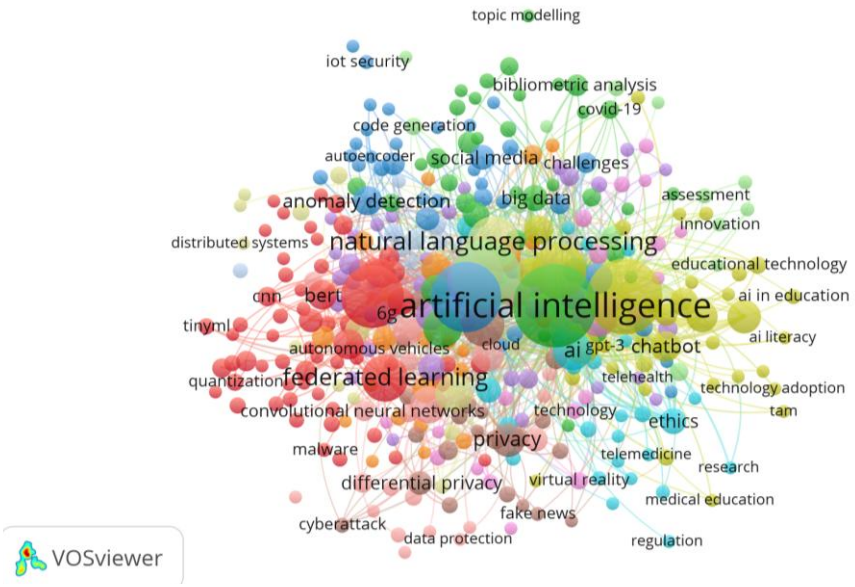

Figure 2 Network visualisation map of co-occurrence keywords

the principal study domains and nascent trends in the ML for IoT security field.

The co-authorship network between nations is depicted in Figure 3, which also shows the main contributors and patterns of collaboration in the field of ML for IoT security. The analysis encompassed 152 countries, of which 83 met the criterion of a minimum of five publications. This depiction emphasises the existence of multiple significant research centres. The United States (U.S.) and China appear to be the most central and well-connected nodes, demonstrating their leadership in research output and international collaborations. The network's clustering into discrete groupings reflects both collaborative and regional interactions. A notable cluster, indicated in red, is centred on the U.S. and the United Kingdom (U.K.), as well as European countries such as the Netherlands and Switzerland. This suggests the existence of strong transatlantic and European research networks.

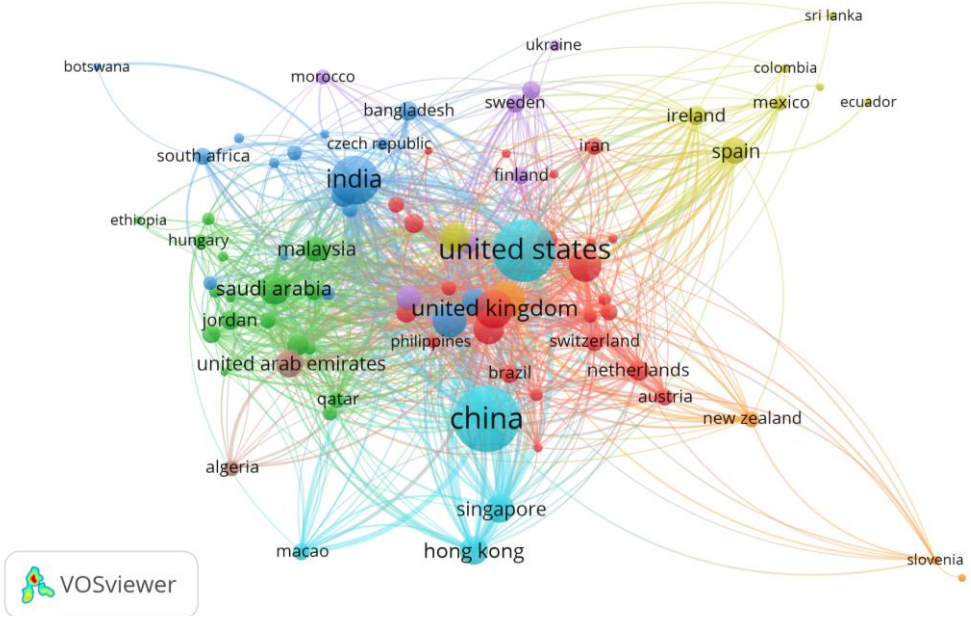

Figure 3 Network visualisation of country clusters

Another significant cluster, shown in blue, was led by China and included collaborators from Singapore and Hong Kong, highlighting a robust East Asian research network. The third significant cluster, depicted in green, is centred around India and encompasses nations from the Middle East and Africa, including Saudi Arabia, the United Arab Emirates, and Ethiopia. These clusters highlight the global yet fragmented nature of research collaboration in this field. Notably, the country collaboration map indicates that the U.S., China, the U.K., and India represent the largest contributors to publication volume.

Figure 4 depicts a network representation of collaborating organisations, highlighting the important institutional players in the field. The analysis encompassed 9,358 organisations, of which 22 met the criterion of having a minimum of five documents, indicating a dispersed and fragmented collaborative landscape. In contrast to the country-level analysis, this network does not exhibit a central, dominant hub. The situation is marked by multiple smaller, isolated clusters, indicating that institutional collaboration tends to be localised or specific to particular projects rather than extensive and inter-institutional. Notable nodes include Nanyang Technological University, Tsinghua University, and the University of Waterloo. Although these firms are quite active, their research networks may not be as connected to those of other significant actors, as indicated by the isolation of nodes from one another. This pattern demonstrates that, while certain institutions have developed a significant presence, the broader research community at the organisational level remains a loosely connected and collaborative network. Additionally, the institutional collaboration map indicates a sparse network with few connections among leading producers, implying that research frequently occurs within institutional silos rather than through robust direct collaborations among the most active universities.

Figure 5 illustrates a network visualisation of the most influential sources in the field, comprising 126 sources that met the criterion of a minimum of five documents from a total of 1,635. The dimensions of each node represent the quantity of published documents, and the connections denote the co-citation and collaborative relationships. The image illustrates several important publication clusters relevant to this research. IEEE Access dominated the largest and most noticeable cluster, highlighted in yellow, demonstrating its important function as a publication venue. This cluster encompasses CEUR Workshop Proceedings, indicating a significant relationship between high-impact journals and conference publications in this field. A significant cluster, indicated in red, is centred on Lecture Notes in Computer Science, a well-established series for publishing conference proceedings and specialised monographs. The central position of this cluster in the network highlights the significance of conference-based research in influencing the field's intellectual landscape. The light blue cluster includes

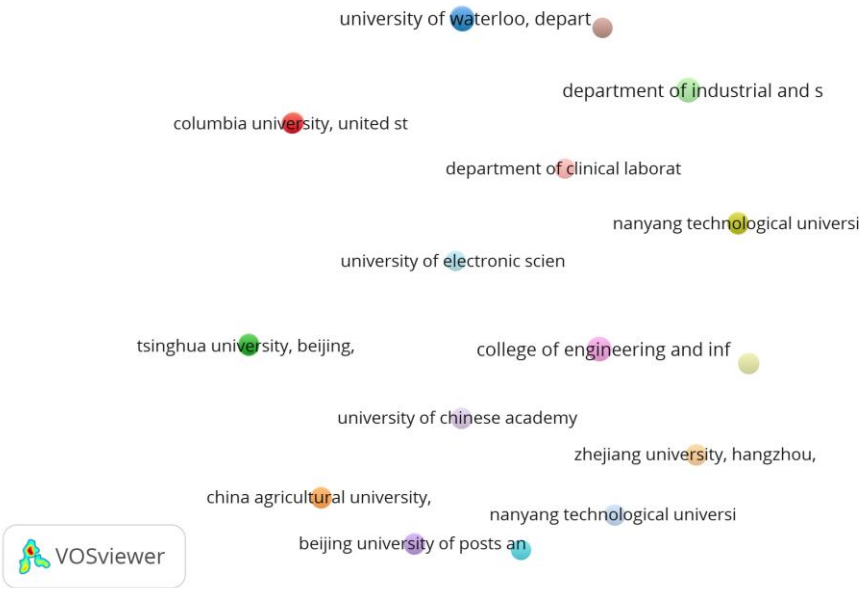

Figure 4 Network visualisation of organisations with keen research interest

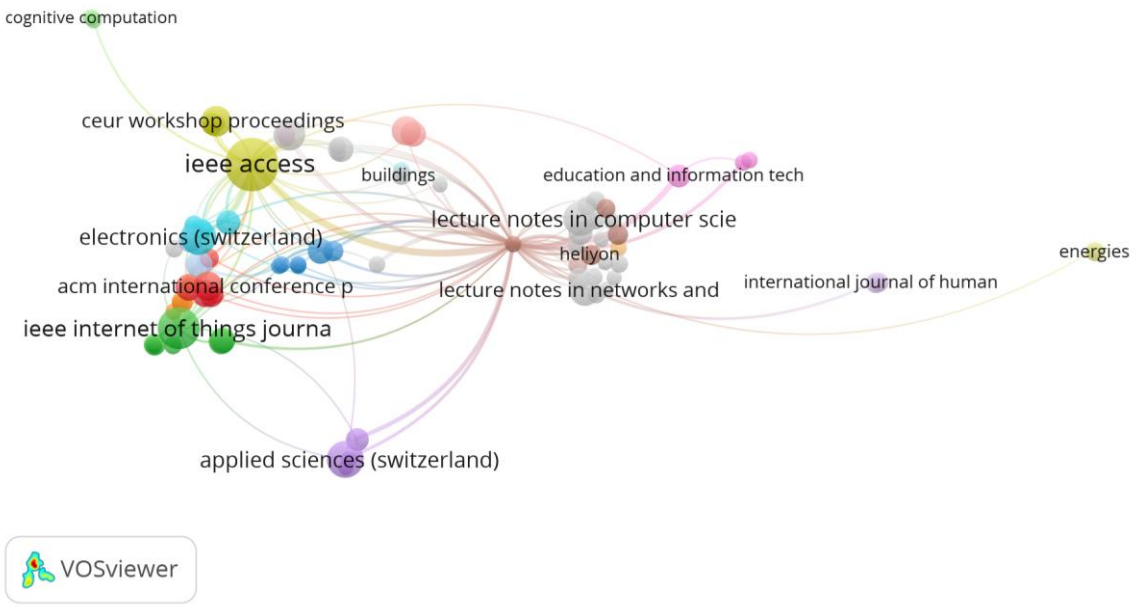

Figure 5 Network visualisation of sources

Electronics (Switzerland) and ACM International Conference Proceedings, specialised publications in electronics and computer science. This network structure reveals the various pathways through which knowledge is transmitted and demonstrates that the discipline is founded upon both major multidisciplinary publications and specialised conference proceedings. The source co-citation map highlights IEEE Access and the IEEE Internet of Things Journal as key hubs for disseminating research.

In addition, the results indicate a rapidly expanding research field that is significantly influenced by breakthroughs in AI and LLMs. The discourse is predominantly scholarly and focused on leading engineering journals, guided by a select number of technologically advanced countries. A significant observation is the substantial impact of mainstream AI trends on the IoT security industry. The occurrence of terms such as ChatGPT (413 instances) and large language models (331 instances) exceeded that of fundamental concepts, such as cybersecurity (100 instances), and was significantly higher than that of niche terms, including IoT security (seven instances). This suggests that the prevailing research approach focuses on applying advanced AI models to address security challenges, rather than creating security solutions tailored to the specific requirements of the IoT. The prevalence of federated learning, which was noted 124 times, represents a significant trend. Beyond centralised cloud-based models, this study demonstrates how the academic community actively addresses the core IoT concerns of data privacy and the requirement for decentralised intelligence. The formation of common best practices and standardised benchmarks may be slowed by the lack of collaboration among top institutions, which could indicate a fragmented research landscape.

POTENTIAL GAPS AND ROADMAP FOR FUTURE DIRECTIONS

This section presents an analysis that identifies several significant gaps warranting further investigation. A three-phase roadmap is proposed to guide future research in this area.

Potential Gaps

The bibliometric analysis revealed three critical gaps in the current research on ML for IoT security:

1. Practicality gap: This is characterised by a disparity between theoretical advancements in large, computationally intensive models, such as LLMs, and the practical requirements of resource-constrained IoT devices. Although keywords such as TinyML, model compression, and quantisation are present, their low frequency (10, 14, and 11 occurrences, respectively) indicates that they are not yet central to discourse. This suggests that a

significant portion of the research does not directly address the challenges of deploying AI on edge devices.

2. Lack of specificity in threat detection: The analysis indicates that although general security terms are widely used, there is less emphasis on particular, detailed IoT threats. This includes adversarial attacks targeting ML models and vulnerabilities associated with specific industrial or medical IoT protocols. This indicates the need for research aimed at moving from broad threat detection to the focused mitigation of highly specialised attacks.
3. From theory to application: The prevalence of academic journal articles and conference papers compared to data papers and practical implementations indicates the necessity of connecting theoretical research with real-world applications. Future research should focus on developing public, high-fidelity datasets and standardised evaluation benchmarks to enable the conversion of theoretical models into practical and deployable solutions.

Roadmap for Future Directions

A three-stage roadmap is proposed to guide future research on the application of machine learning in IoT security, based on the identified gaps.

1. The short-term phase (1-3 years) should focus on efficiency and adaptation. This stage prioritises the adaptation of existing large models for resource-constrained IoT environments by focusing on techniques such as model compression, quantisation, and pruning. The goal of this study was to develop effective TinyML solutions for on-device threat detection.
2. The mid-term phase (3-5 years) focuses on trust and resilience. This phase focuses on developing reliable and resilient security frameworks by enhancing research on federated learning and differential privacy to safeguard user data. The incorporation of explainable AI (XAI) is essential for ensuring that security decisions are transparent and subject to auditability. This phase also encompasses the creation of strong defences to counter adversarial attacks on ML models.
3. The long-term phase, extending beyond five years, is centred on the attainment of Autonomy and Integration. The goal is to develop autonomous and self-repairing IoT security systems. Primary research domains focus on utilising reinforcement learning (RL) to create self-adapting security agents and investigating the amalgamation of AI with blockchain technology to form a decentralised structure for device identity, data provenance, and threat intelligence sharing. This roadmap outlines a systematic strategy for progressing the domain from basic efficiency to completely autonomous and integrated security solutions.

CONCLUSION

This bibliometric analysis provides a quantitative and structural overview of research at the interface of ML and IoT, highlighting significant growth driven by prevailing AI trends, particularly developments in LLMs. However, this has created a notable disparity between computationally intensive models and the resource-limited conditions of IoT deployments. A positive counter-trend is the intense focus on federated learning, addressing critical IoT requirements of data privacy and decentralisation. Key contributors and a fragmented collaboration network among leading institutions were identified, potentially hindering the standardisation of methods and benchmarks. The study is limited by reliance on bibliographic metadata (titles, abstracts, and keywords) rather than full-text analysis, and by search parameters spanning 2015–2025, which may omit some relevant studies. Despite these limitations, the results offer a comprehensive overview of the field. Future research should prioritise the development of efficient and lightweight models, moving beyond mere application to purpose-built ML techniques suited to the constraints of IoT hardware, including TinyML, model quantisation, and pruning. Additionally, enhancing research collaboration is crucial; fostering robust partnerships among leading institutions, creating comprehensive, large-scale, realistic IoT security datasets, and establishing standardised evaluation benchmarks are essential steps toward a more integrated, effective, and impactful research ecosystem.

ACKNOWLEDGMENT

The authors gratefully acknowledge the financial support provided by Universiti Teknologi PETRONAS (UTP) through the YUTP-FRG grant (015LC0-487).

DECLARATION OF INTERESTS

The authors declare that they have no known competing financial interests or personal relationships that could influence the work reported in this study.

REFERENCES

[1] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167–185, 2024, doi: https://doi.org/10.1016/j.iotcps.2023.12.003.

[2] M. Mustafa, M.Z. Hussain, M.Z. Hasan, …, S.H. Chuhan, and A. Belal, "IoT Security Implementation using Machine Learning," *Research Briefs on Information and Communication Technology Evolution*, vol. 9, pp. 116–119, Oct. 2023, doi: 10.56801/rebicte.v9i.161.

[3] S. Pokhrel, R. Abbas, and B. Aryal, "IoT security: botnet detection in IoT using machine learning," *arXiv preprint arXiv:2104.02231*, 2021.

[4] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," in *2018 IEEE Security and Privacy Workshops (SPW)*, 2018, pp. 29–35, doi: 10.1109/SPW.2018.00013.

[5] A.H. Alsharif, N. Salleh, and R. Baharun, "Bibliometric analysis," *J Theor Appl Inf Technol*, vol. 98, no. 15, pp. 2948–2962, 2020.

[6] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W.M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *J Bus Res*, vol. 133, pp. 285–296, 2021.

[7] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W.M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *J Bus Res*, vol. 133, pp. 285–296, 2021.

[8] V.Z. Pessin, L.H. Yamane, and R.R. Siman, "Smart bibliometrics: an integrated method of science mapping and bibliometric analysis," *Scientometrics*, vol. 127, no. 6, pp. 3695–3718, 2022.

[9] H. Arruda, E.R. Silva, M. Lessa, D. Proença Jr, and R. Bartholo, "VOSviewer and bibliometrix," *J Med Libr Assoc*, vol. 110, no. 3, p. 392, 2022.

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

[11] Y. Purnama, A. Asdlori, E. M. S. S. Ciptaningsih, K. Kraugusteeliana, A. Triayudi, and R. Rahim, "Machine Learning for Cybersecurity: A Bibliometric Analysis from 2019 to 2023." *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 15, no. 4, pp. 243–258, 2024.

[12] A. Paleyes, R.-G. Urma, and N.D. Lawrence, "Challenges in deploying machine learning: a survey of case studies," *ACM Comput Surv*, vol. 55, no. 6, pp. 1–29, 2022.

[13] H. Gani, A.D. Damayanti, Nurani, S. Zuhriyah, S.N. Jabir, H. Gani, F. Zhipeng, A.S. Rejeki, "Machine Learning and Internet of Things (IoT): A Bibliometric Analysis of Publications Between 2012 and 2022," *ILKOM Jurnal Ilmiah*, vol. 16, no. 1, pp. 27–37, Apr. 2024, doi: 10.33096/ilkom.v16i1.1700.27-37.

[14] A. Chahal, S.R. Addula, A. Jain, P. Gulia, and N. S. Gill, "Systematic Analysis based on Conflux of Machine Learning and Internet of Things using Bibliometric analysis.," *Journal of Intelligent Systems & Internet of Things*, vol. 13, no. 1, 2024.

[15] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015, doi: https://doi.org/10.1016/j.comnet.2014.11.008.

[16] M. Antonakakis, T. April, M. Bailey, …, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

[17] R.K. Vanakamamidi, L. Ramalingam, N. Abirami, S. Priyanka, C.S. Kumar, and S. Murugan, "IoT security based on machine learning," in *2023 Second International Conference on Smart Technologies for Smart Nation (SmartTechCon)*, IEEE, 2023, pp. 683–687.

[18] W. Abbass, Z. Bakraouy, A. Baïna, and M. Bellafkih, "Classifying IoT security risks using deep learning algorithms," in *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, IEEE, 2018, pp. 1–6.

[19] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-iot dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[20] D.S. Berman, A.L. Buczak, J.S. Chavis, and C.L. Corbett, "A Survey of Deep Learning Methods for Cyber Security," *Information*, vol. 10, no. 4, 2019, doi: 10.3390/info10040122.

[21] J.M. Saiz-Alvarez, "Innovation Management: A Bibliometric Analysis of 50 Years of Research Using VOSviewer® and Scopus," *World*, vol. 5, no. 4, pp. 901–928, 2024.