International Journal on Advanced Science Engineering Information Technology

Vol.15 (2025) No. 3
ISSN: 2088-5334

Trends in IoT Intrusion Detection: A Bibliometric Analysis of Deep Learning Approaches

Amir Muhammad Hafiz Othman [a,b], Mohd Faizal Ab Razak [a,1], Ahmad Firdaus [a], Syazwani Ramli [c,2], Wan Nur Syamilah Wan Ali [d]

[a] Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Pahang, Malaysia
[b] Faculty of Computer Science and Mathematics, Universiti Malaysia Terengganu, Kuala Nerus, Terengganu, Malaysia
[c] Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Parit Raja, Johor, Malaysia
[d] Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia
Corresponding author: [1]faizalrazak@umpsa.edu.my; [2]rsyazwani@uthm.edu.my

***Abstract*—The Internet of Things (IoT) has transformed modern technology by interconnecting devices and systems, improving efficiency and functionality across various domains. However, its rapid expansion has also introduced significant security vulnerabilities, necessitating the development of robust intrusion detection systems (IDS) to counter evolving cyber threats. Despite advancements in IDS research, particularly through deep learning integration, a systematic bibliometric analysis assessing global research trends, key contributors, and collaboration networks remains lacking. This study addresses that gap by conducting a bibliometric analysis of IDS for IoT using deep learning, focusing on articles published between 2016 and 2024 in the Scopus database. It examines global research trends, keyword co-occurrences, publication patterns, citation dynamics, and international collaborations, offering a comprehensive overview of the field. The findings indicate a significant rise in IDS research, with India, China, the United States, and Saudi Arabia emerging as leading contributors and collaborators. The analysis also highlights influential authors and institutions driving advancements in deep learning for IoT security. Keyword analysis reveals the prominence of terms such as "machine learning," "deep learning," and "intrusion detection," underscoring the field's focus on artificial intelligence for IoT security. This bibliometric study enhances the understanding of research dynamics in IDS for IoT, identifies gaps for future exploration, and provides valuable insights to drive innovation and global collaboration in this critical area of cybersecurity.**

***Keywords*— Intrusion detection; bibliometric; internet of things; deep learning; security.**

Manuscript received 5 Nov. 2024; revised 16 Jan. 2025; accepted 18 Apr. 2025. Date of publication 30 Jun. 2025.

I. INTRODUCTION

As technology rapidly evolves, the Internet of Things (IoT) has emerged as a transformative force, offering opportunities to enhance efficiency and reliability across various applications. IoT connects devices and technologies into a seamless, autonomous network, minimizing the need for human intervention [1]. With the global IoT market projected to grow by 64.65% between 2024 and 2029, reaching an impressive $1.6 trillion, this transformative technology continues to expand at an unprecedented rate [2]. However, as IoT adoption grows, so do cybersecurity concerns. The interconnected nature of IoT systems makes them particularly susceptible to cyberattacks, including malware and data breaches. Alarmingly, regions like Asia and Latin America have seen significant increases in IoT-related malware attacks, including a staggering 311% surge in India, while Germany reported a 30% decline [3], [4]. These trends underscore the need for advanced intrusion detection systems (IDS) to safeguard IoT devices against rapidly evolving threats.

The dynamic nature of cyber threats calls for intelligent and adaptive detection systems. Deep learning (DL), a subset of machine learning, has gained traction as a powerful tool for detecting anomalies in IoT by learning patterns from historical data without requiring explicit attack signatures [5]. Consequently, researchers have increasingly adopted deep learning (DL) algorithms to propose more accurate security solutions for the Internet of Things (IoT). Deep Learning (DL) relies on large volumes of raw data to automatically learn complex features through its deep neural networks [6]. With its ability to process large volumes of raw data and automatically identify complex patterns, DL has been applied across diverse fields, including security [7], vehicles [8], and

healthcare [9]. For example, an unmanned aerial vehicle (UAV) detection system represents a security application that leverages deep learning techniques to detect and identify UAVs [10] accurately. Deep learning has also been employed in autonomous vehicles due to its exceptional performance in handling complex, non-linear control problems and its ability to adapt to new scenarios [8]. Article [9] studied the integration of deep learning with healthcare, showing that it provides accurate and reliable results, addresses traditional artificial intelligence challenges, and has been suggested for broader use in healthcare. These advancements highlight the vast potential of deep learning to revolutionize IoT security by addressing its unique challenges.

This study comprehensively uses bibliometric analysis to review IDS research for IoT using deep learning. Bibliometric methods offer valuable insights into research trends, author performance, institutional contributions, and global collaborations [11], [12].

However, these studies often overlook the use of bibliometric analysis in the context of intrusion detection systems (IDS) for the Internet of Things (IoT) using deep learning. Although many articles explore this area, they mainly focus on the impacts and trends of IoT research rather than its applications in IDS using deep learning in IoT. While previous studies have explored bibliometric analyses in cybersecurity and the Internet of Things (IoT), there is a noticeable gap in research specifically focusing on Intrusion Detection Systems (IDS) for IoT through the lens of deep learning. Existing studies often examine broader trends without delving into the specific intersection of IDS, IoT, and DL.

Bibliometrics is a research methodology implemented in library and information science that applies statistical and quantitative analysis to examine the distribution patterns of articles across various topics, fields, institutions, and countries [12]. It is a thorough technique commonly used to evaluate and understand vast quantities of scientific data [13]. It offers informative insights regarding its emerging areas and helps assess the evolutionary dynamics of a specific field [14]. This method has been employed in various studies across multiple research fields. Table I provides a list of studies that have employed the bibliometric method, highlighting similar approaches in this paper**.**

TABLE I
LIST OF STUDIES THAT UTILIZED A BIBLIOMETRIC METHOD

References	Fields	Year
[15]	Operations research and management science	2017
[11]	Safety culture	2018
[16]	Cyber security	2021
[17]	Internet of Things	2023
[18]	Sports	2023
[19]	Cyber security	2024
[20]	Machine learning and blockchain	2024
[21]	Cyber security	2024
This paper	Cyber security	2024

Intrusion detection systems (IDS) for IoT networks have become increasingly important in addressing the unique security challenges posed by the diversity of devices, resource limitations, and the growing complexity of cyberattacks. Traditional IDS approaches, such as signature-based and anomaly-based techniques, often face difficulties in the dynamic and resource-constrained IoT environment [52]. Research by Nguyen et al. [22] highlights the effectiveness of hybrid methods that integrate anomaly detection with machine learning to improve scalability and accuracy. Similarly, deep learning architectures, such as convolutional neural networks (CNNs) and long short-term memory (LSTM) networks, have revolutionized IDS by automating feature extraction and adapting to diverse datasets [23]. For instance, CNN-based models have demonstrated a notable reduction in false positives when detecting malicious traffic [24]. In contrast, LSTM models have proven highly effective in real-time anomaly detection, leveraging the temporal patterns in IoT traffic [25].

Recent advancements have introduced hybrid and transfer learning techniques to overcome challenges such as limited labeled data and varying attack patterns. Zhang et al. [26] proposed a hybrid CNN-LSTM model that effectively combines spatial and temporal feature extraction, resulting in improved cyberattack classification. Additionally, transfer learning approaches, like those by Al-Garadi et al. [27], utilize pre-trained models on large datasets to reduce training time and enhance the accuracy of IDS for IoT-specific threats. Despite these technological advancements, there remains a gap in bibliometric studies that focus specifically on IDS for IoT using deep learning. While prior bibliometric analyses, such as those by Ferrag et al. [24] and Sarker et al. [23], have explored trends in IoT security, they have not delved into the role of deep learning in IDS research. Table II highlights the differences between previous bibliometric analysis studies and this paper.

TABLE II
COMPARISON WITH PREVIOUS STUDIES

Aspect	This paper	Bibliometric Review of Intrusion Detection Research in IoT [28]
Year	2024	2024
Database	Scopus	Web of Science
Timespan	9 years (2016-2024)	7 years
Author analysis	Yes	Yes
Subject analysis	Yes	Yes
Documents type	Included	Included
Citation analysis	Included	Included
Countries coverage	Included	Included
Network analysis		
Country Collaboration	Yes	Yes
Keyword co-occurrences	Yes	Yes
Affiliation collaboration	Yes	Yes

This bibliometric study distinguishes itself from previous bibliometric reviews by focusing specifically on the application of deep learning in IDS for IoT, unlike earlier works that encompassed a broader range of methods, including traditional machine learning, signature-based techniques, and hybrid approaches. By narrowing the focus to deep learning, this paper offers a more in-depth examination

of recent advancements and their role in tackling IoT security challenges. Moreover, the extended timespan and the use of Scopus as the primary database enable a more thorough analysis of research trends, collaboration networks, and the thematic evolution within this specialized area.

This study presents an in-depth bibliometric analysis of intrusion detection systems (IDSs) for the Internet of Things (IoT) using deep learning, addressing a significant gap in the current body of research. Examining 7176 articles published between 2016 and 2024 identifies key trends, influential researchers, and the thematic evolution of this specialized field. Unlike prior studies focusing on IoT security or general applications of deep learning, this research zeroes in on the intersection of IDS and IoT, providing a unique perspective. It explores publication patterns, keyword relationships, and global collaboration networks to reveal how deep learning techniques advance IoT security. The findings not only map the field's current state but also highlight future opportunities, paving the way for innovation and collaboration in this crucial area of cybersecurity.

This study analyzes 7176 research articles published between 2016 and 2024 from the Scopus database to address this gap. It explores global trends, keyword co-occurrences, and collaboration networks to uncover insights into the development of IDS for IoT using deep learning. The key questions driving this research are as follows:

- What are the global trends in IDS research for IoT using deep learning?
- What insights can be gained from these trends, and what future directions can be identified?

The scope of this study includes:

- An assessment of IDS research for IoT using deep learning, based on 7176 studies from Scopus.
- An evaluation of IDS research using deep learning methodologies documented across various sources.
- Identify leading authors and their contributions and analyze publication trends, keywords, and citations.
- An exploration of global IDS research, examining the number of articles, publications, and citations by country.

The remainder of this paper is organized as follows: Section 2 reviews related bibliometric studies, Section 3 describes the methodology and presents the findings, and Section 4 concludes the paper.

II. Materials and Method/Algorithm

This section outlines the method used for this bibliometric study, from the search process to the analysis phase. Additionally, this study examines four main aspects in the specific bibliometric categories: type of document, subject area, authors, and country. The proposed methodology consists of four distinct phases: (1) Search, (2) Results, (3) Findings, and (4) Analysis.

Fig. 1 illustrates the methodological framework, including the flow and progression through each phase. The process of this paper begins with searching the Scopus database using the following keywords: "Internet of Things" or "IoT", "intrusion", "artificial intelligence", "AI", and "deep learning". Using these keywords, all relevant documents related to intrusion detection systems in IoT leveraging deep learning in this database was gathered for further analysis. Scopus was selected as the chosen database for this paper because it contains high-quality and reliable publications [29]. It is a comprehensive citation database offering wide coverage, high citation numbers, and reliable scholarly impact tracking [30]. From the keywords, 7176 relevant documents, published between 2016 and 2024, were retrieved from the database using the specified keywords.

The analysis in this paper begins with 2016, as that year marks the rise of interest in applying deep learning to intrusion detection systems (IDS) for IoT using deep learning. In the next phase of this paper, the focus is on exploring various aspects, including different document types, subject areas, authors, and countries relevant to the paper's topic. After reviewing all relevant aspects of the document, the raw data from Scopus were exported for further analysis. A bibliometric analysis was then conducted to analyze the data and generate visualizations, yielding the results. The final phase involves documenting the entire process and findings for this paper.

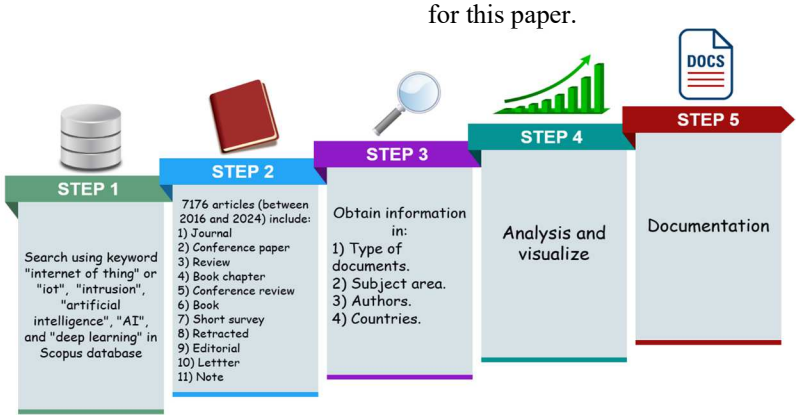

Fig. 1 Methodology phases

This study utilizes RStudio, an open-source statistical software [31], to implement an Intrusion Detection System (IDS) within the Internet of Things (IoT) network using deep learning. The software supports R and Python, making it a reliable tool for data scientists and analysts. In this study, the R language was used in conjunction with the bibliometric [32] package to perform bibliometric analysis and visualization, both of which are accessible through the RStudio environment. Multiple studies have used the bibliometric tool to conduct bibliometric analyses in their respective research fields [26], [33]. The tool enables the exploration of the evolution and trends of this topic, presenting visualizations of the findings for further analyzed in the following section.

The bibliometric analysis in this study is separated into four categories, each with multiple sub-categories. The main categories are: (1) Types of documents, (2) Subject area, (3) Authors, and (4) Countries. The types of documents provide detailed information on the collected article, including the main information, the sources of the document, and the progression of these sources over time. The subject area category outlines the subject area related to IDS within IoT through deep learning. The author category presents the top 20 authors based on each author's total number of publications. The final category, Countries, outlines the countries participating in this research study, including the total number of articles by country and the total number of single- and multiple-country publications. The findings from these categories are essential, as they generate bibliometric data that support the discovery of high-impact research, contributing to new knowledge in this study. Table IV shows the main information exported from the Scopus database, consisting of 7176 articles published from 2016 to 2024.

TABLE IV
MAIN INFORMATION

Main information	Explanation	Results
Timespan	Years of the article	2016:2024
Language	The language used in the articles	English
Sources (Journals, Books, etc)	The frequency distribution of sources	1954
Articles	Total number of articles	7176
Keywords	Total number of all keywords	17708
Author's Keywords	Total number of author's keywords	10963
Authors		
Authors	The number of unique authors	16779
Author Appearance	The number of author appearances	29199
Authors of single-authored article	The number of single authors per article	282
Authors of multi-authored article	The number of multi-authors per article	16497
Single-authored articles	The number of single-authored articles	318
Multi-authored articles	The number of multi-authored articles	6856
Other		
Author per Article	Average number of authors for each article	2.34
Co-Authors per Article	Average number of co-authors for each article	4.07
Average citations per article	Average number of citations for each article	19.01
Collaboration Index	Index collaboration between researchers, institutions, or countries' publications.	2.30
YEAR		
2016	Number of articles in each year	3
2017		17
2018		52
2019		169
2020		432
2021		816
2022		1397
2023		2115
2024		2175

The reviewed articles were published across 1954 sources, including journals, books, and other types of publications. The number of keywords found in the articles is 17708, while the keywords used by the authors are 10963. The keyword is larger than the author's keywords due to the specific search string formulated in the Scopus database advanced search, conducted in early November 2024. In addition, the exported article only includes English. 16779 unique authors were identified across these articles, with 282 being responsible for single-authored publications, while the rest contributed to multi-authored works. The data from 2016 to 2024 shows a dramatic increase in article publications, with the trend expected to continue at the end of 2024, surpassing the number of publications from prior years. To provide better insight, the data in Table IV presents a graph in Figs. 2, 3, 4, and 5. The following section delves into the source of these articles and their respective details.

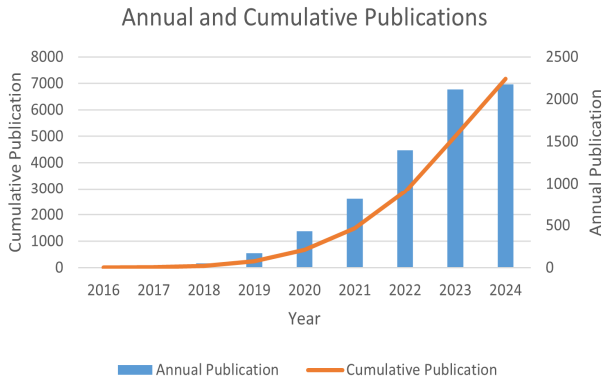

Fig. 2 Cumulative and annual publications from 2016 to 2024

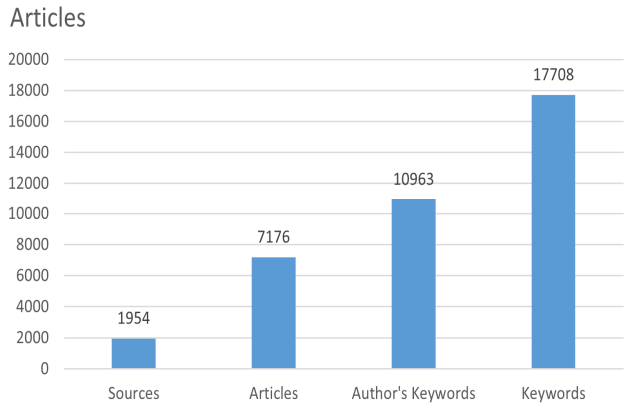

Fig. 3: The article's main information

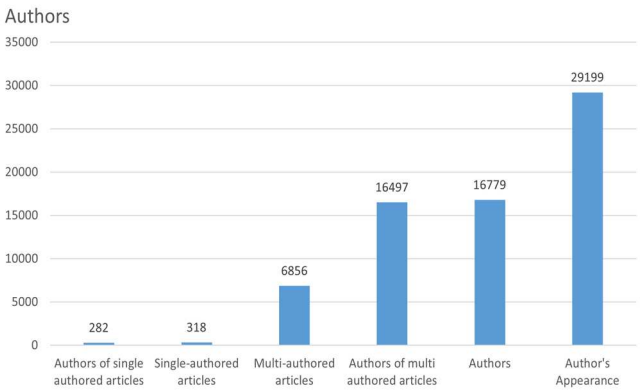

Fig. 4 Authors' main information

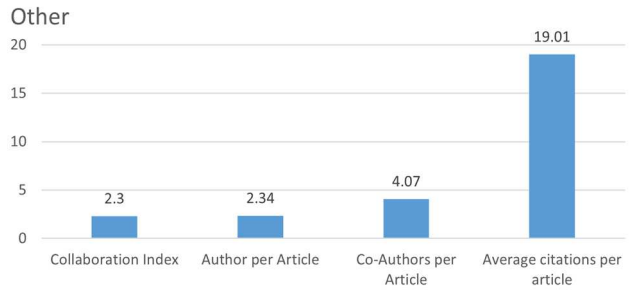

Fig. 5 Other main information

III. Results and Discussion

This section presents the findings and results of the bibliometric analysis, focusing on four key categories: type of document, authors, subject area, and country. It provides insights into the contributions of authors, the distribution of document types, the geographic origins of the research, and the subject areas most explored within the field. These findings offer a comprehensive overview of the trends and patterns identified in the articles.

A. Type of Document

Fig. 6 illustrates the distribution of publications with different types of documents. The analysis and details focus on the ranking of these document types. According to the results, journal articles represent the highest number of publications, with 4038 documents, nearly double the number of conference papers, totaling 1968.

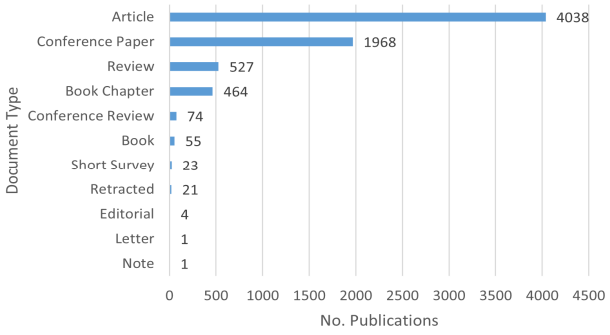

Fig. 6 Type of documents

Fig. 6 demonstrates that journal articles have the highest number of publications, followed by conference papers. These results indicate a strong interest in this topic, with a tendency toward publishing articles. Researchers often aim to publish in journals to reach a wider audience and gain recognition. Established journals, with a history of publishing high-quality research, tend to attract more submissions. These journals are also known for their rigorous peer review process, which enhances their reliability, as experts review articles before being accepted and published. Additionally, open-access journals contribute to the accessibility of research, allowing free access to articles and encouraging wider readership. Given the importance of time, researchers seeking to publish their work quickly prefer journals with faster review and publication processes. These advantages demonstrate that journal articles are considered more reliable and novel than other publications, serving as valuable resources for researchers in finding high-quality references.

Table V shows that IEE Access is the preferred journal chosen by researchers to publish their articles that relate to this topic.

TABLE V
Top 20 Sources

Top 20 sources	No.
IEEE Access	379
IEEE internet of things journal	284
Sensors	199
Electronics (Switzerland)	147
Lecture notes in networks and systems	142
Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)	122
Applied Sciences (Switzerland)	104
Internet of Things (Netherlands)	99
ACM International Conference proceeding series	71
Computers, materials, and continua	69
Cluster computing	64
Computers and Security	63
IEEE transactions on industrial informatics	60
Computer networks	52
Lecture notes in electrical engineering	48
Wireless communications and mobile computing	48
Communications in computer and information science	47
Journal of supercomputing	46
Sustainability (Switzerland)	46
Wireless personal communications	46

Table V represents the top 20 sources related to this topic, with IEEE Access emerging as the journal with the highest publication. IEEE Access leads with 379 publications, making it the most frequently published source. It indicates its popularity among researchers for publishing in journals where many researchers publish their journal articles. IEEE Access is an open-access journal that covers a broad range of topics in science and engineering. Its appeal comes from a fast and thorough peer review process, a reputation for quality research, and unrestricted access to all published articles. This open accessibility allows more people to read the research, making the findings easier to discover and share widely. To maintain the high standards of IEEE publications, every article is carefully reviewed by experts to ensure its originality and technical correctness [34]. This journal's combination of quality, accessibility, and review process makes it the preferred choice for researchers seeking to publish cutting-edge work in science and engineering.

In addition to IEEE Access, the other top four sources have also seen a significant increase in the number of publications on intrusion detection in IoT using deep learning. The following section focus on the subject areas the researchers are exploring in adapting intrusion detection in IoT using deep learning.

B. Subject Area

This section highlights publications related to the research topic. The subject area refers to the academic discipline under which the research is categorized. It serves as a guide for identifying the research's content, target audience, and relevance to existing knowledge. By doing so, it enables academics and professionals to find studies that align with their field of interest. Subject areas are also essential components used by others to evaluate the impact of research, as they are often assessed based on publication and citation

rates. Such evaluation provides insights into the research's influence and reveals the publication trend over time. Examples of subject areas in the Scopus database are Computer Science, Engineering, Mathematics, Decision Sciences, Physics and Astronomy, and Materials Science. Table VI shows an overview of these subject areas for publication from 2016 to 2024.

TABLE VI
TOP 20 SUBJECT AREAS

Subject Areas	Publications	Publications (%)
Computer Science	6274	39.17
Engineering	3762	23.48
Mathematics	1303	8.13
Decision Sciences	762	4.76
Physics and Astronomy	714	4.46
Materials Science	651	4.06
Energy	409	2.55
Social Sciences	373	2.33
Business, Management, and Accounting	299	1.87
Biochemistry, Genetics, and Molecular Biology	280	1.75
Medicine	275	1.72
Chemistry	269	1.68
Environmental Science	166	1.04
Chemical Engineering	148	0.92
Multidisciplinary	105	0.66
Economics, Econometrics, and Finance	64	0.4
Agricultural and Biological Sciences	54	0.34
Neuroscience	37	0.23
Earth and Planetary Sciences	21	0.13
Arts and Humanities	18	0.11

Table VI shows that Computer Science leads this research topic on Scopus, with 6274 documents, while Engineering ranks second with 3762 documents, constituting nearly a quarter of the total publications. This trend indicates a strong preference among researchers to publish their work under these two subject areas, reflecting their important role in advancing this field. The synergy between Computer Science and Engineering is evident, as both fields collaborate to drive innovation and develop advanced technology that benefits academics and society. Software engineering, IoT, robotics, AI-driven control systems, digital twin technology, cyber-physical systems, and autonomous vehicles are the sub-areas under Computer Science and Engineering.

Additionally, other subject areas contribute significantly to research on intrusion detection in IoT networks using deep learning. Mathematics ranks third with 1303 publications (8.13%), emphasizing the importance of mathematical equations in developing effective IDS solutions. Decision Science follows this with 762 publications (4.76%), where research focuses on improving decision-making processes for intrusion detection, enhancing efficiency, and reducing false positives.

Areas such as Physics and Astronomy with 714 publications (4.46%) and Materials Science with 651 publications (4.06%) also play roles, likely due to the development of hardware and sensor technology in IoT devices. The presence of Energy (409 publications, 2.55%) and Social Sciences (373 publications, 2.33%) reflects the growing need to secure smart energy grids and address the societal impacts of IoT security breaches. Moreover, disciplines like biochemistry should be included. Genetics and Molecular Biology (280 publications, 1.75%), Medicine (275 publications, 1.72%), and Environmental Science (166 publications, 1.04%) highlight how IDS research is expanding to secure IoT applications in healthcare, biological research, and environmental monitoring. Even areas like Business, Management, and Accounting (299 publications, 1.87%) demonstrate engagement, underscoring the importance of securing business-critical IoT infrastructure.

This distribution of research across diverse subject areas highlights the multidisciplinary nature of IDS research in the context of the Internet of Things (IoT). Addressing IoT security challenges requires collaboration across domains, providing a broader perspective and fostering innovation that benefits academia and industry. The following section discusses the contributions of authors with advanced knowledge in IDS for IoT using deep learning research.

C. Authors

This section highlights the authors with the most publications, including their highest-cited works. Fig. 7 presents the ranking of the top 20 authors and their respective number of published documents.

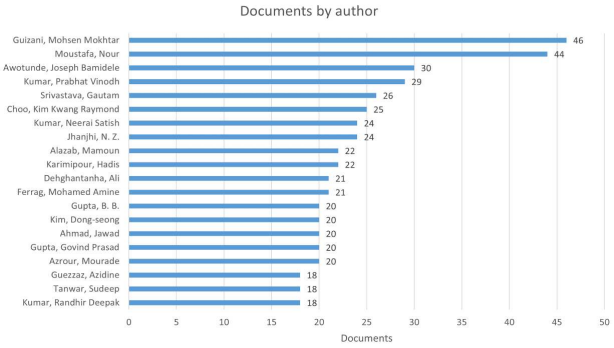

Fig. 7 Top 20 authors based on the number of documents

Among the top 20 authors, Guizani, Mohsen Mokhtar emerges as the most active with 46 publications, representing approximately 0.64% of the total publications. His research primarily focuses on IoT security, wireless communication, and the application of deep learning for intrusion detection systems, with a high citation impact that reflects the significance of his contributions. His most cited works focus on enhancing network security and optimizing intrusion detection mechanisms for Internet of Things (IoT) environments. With 44 publications (0.61% of the total), Moustafa, Nour follows closely, focusing on cybersecurity and applying deep learning models for intrusion detection in IoT environments, particularly in industrial applications. Nour's consistent output highlights his expertise in cybersecurity, particularly in applying deep learning models for intrusion detection in IoT environments. His contributions enhance the reliability and adaptability of IDS models, addressing critical challenges in industrial IoT security. Awotunde, Joseph Bamidele ranks third with 30 publications, followed by Kumar, Prabhat Vinodh with 39 publications. Both have significantly advanced IoT security and machine

learning, particularly in intrusion detection systems, addressing the evolving security challenges in IoT networks. The authors ranked fifth to twelfth, including Srivastava, Choo, Kumar, Jhanjhi, Alazab, Karimipour, Dehghantanha, and Ferrag have publications ranging from 21 to 26, contributing diverse perspectives and advancing intrusion detection, IoT security, and machine learning. Gupta, Govind Prasad, and Azrour, Mourade follow with 20 publications each. At the same time, Guezzaz, Azidine, Tanwar, Sudeep, and Kumar, Randhir Deepak occupy the lower ranks with 18 publications, showcasing the wide range of research addressing the complex challenges of IoT security. Their collective work significantly enriches the field, offering diverse approaches and innovative solutions that address the evolving and complex challenges of IoT security.

Table VII presents the top 20 authors based on their total publications, highlighting their respective top-cited documents. The table includes the author's rank, name, country, document title, and number of citations. Notably, a significant portion of the top authors hail from India. Leading the list is Guizani, Mohsen Mokhtar from the United Arab Emirates, with his most-cited work — a survey on IoT big data streaming analytics — accumulating 1019 citations [35]. Moustafa, Nour from Australia follows, with 274 citations for his study on identifying malicious activities in industrial IoT using deep learning models [36]. Awotunde, Joseph Bamidele from Nigeria has 121 citations for his research on intrusion detection in industrial IoT networks using deep learning with rule-based feature selection [37]. Kumar, Prabhat Vinodh from Finland also stands out, with 198 citations for his work on ensemble learning and fog-cloud architecture for cyber-attack detection in IoMT networks [38]. Some authors share highly cited works, such as Kumar, Prabhat Vinodh (Finland), and Gupta, Govind Prasad (India), whose collaborative paper on ensemble learning for IoMT networks received 198 citations [38]. Similarly, Kumar, Neerai Satish, and Tanwar, Sudeep (India) co-authored a 173-citation study on multimedia big data and IoT applications [41]. These contributions, spanning countries like the UAE, Canada, Algeria, Australia, and India, reflect the global effort and collaboration advancing IoT network security through deep learning innovations.

TABLE VII
LIST OF TOP 20 AUTHORS BASED ON NUMBER OF PUBLICATIONS

	Authors	Country	Documents	Highest cited by
1	Guizani, Mohsen Mokhtar	United Arab Emirates	Deep learning for IoT big data streaming analytics: A survey [35]	1019
2	Moustafa, Nour	Australia	Identification of malicious activities in the industrial Internet of Things based on deep learning models [36]	274
3	Awotunde, Joseph Bamidele	Nigeria	Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection [37]	121
4	Kumar, Prabhat Vinodh	Finland	An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks [38]	198
5	Srivastava, Gautam	Canada	Analysis of Dimensionality Reduction Techniques on Big Data [39]	593
6	Choo, Kim Kwang Raymond	United States	Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning [40]	278
7	Jhanjhi, N. Z.	Malaysia	Internet of things and ransomware: Evolution, mitigation and prevention [40]	120
8	Kumar, Neerai Satish	India	Multimedia big data computing and Internet of Things applications: A taxonomy and process model [41]	173
9	Karimipour, Hadis	Canada	Machine learning based solutions for security of Internet of Things (IoT): A survey [42]	336
10	Alazab, Mamoun	Australia	An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture [43]	365
11	Ferrag, Mohamed Amine	Algeria	Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study [24]	711
12	Dehghantanha, Ali	Canada	Federated-Learning-Based Anomaly Detection for IoT Security Attacks [44]	350
13	Azrour, Mourade	Morocco	An improved anomaly detection model for IoT security using decision tree and gradient boosting [45]	80
14	Gupta, Govind Prasad	India	An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks [38]	198
15	Ahmad, Jawad	Saudi Arabia	An experimental analysis of attack classification using machine learning in IoT networks [46]	150
16	Kim, Dong-Seong	South Korea	Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review [47]	79
17	Gupta, B. B.	Taiwan	An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols [48]	318
18	Kumar, Randhir Deepak	India	SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles [49]	137
19	Tanwar, Sudeep	India	Multimedia big data computing and Internet of Things applications: A taxonomy and process model [41]	173
20	Guezzaz, Azidine	Morocco	An improved anomaly detection model for IoT security using decision tree and gradient boosting [45]	80

To conclude, the prominence of key contributors such as Mohsen Mokhtar Guizani, Nour Moustafa, Joseph Bamidele Awotunde, and Prabhat Vinodh Kumar underscores their significant impact on advancing research in deep learning-based intrusion detection for IoT networks, as evidenced by their prolific publications and highly cited works. Their collective contributions reflect a globally collaborative research environment, with expertise spanning multiple countries, including the UAE, Australia, Nigeria, and Finland. This diversity in perspectives and methodologies highlights ongoing innovation and promises future advancements in enhancing IoT security. The breadth of research from these leading authors contributes to a comprehensive understanding of how deep learning can be leveraged to develop robust, efficient, and adaptive intrusion detection systems for increasingly complex IoT environments [50], [51]. The following section focuses on the countries actively contributing to IDS for IoT research using deep learning.

D. Country Contributes to IDS for IoT Research

This section examines the countries actively contributing to IDS for IoT research using deep learning. It highlights the countries associated with the authors of the publications, detailing the total number of articles, citations, and collaborative networks. The subsection begins by discussing the total number of articles each country publishes.

TABLE VIII
TOP 20 COUNTRIES WITH THEIR RESPECTIVE NUMBER OF ARTICLES

Country	Articles	Articles %	SCP (single country publications)	MCP (multiple country publications)
India	1302	18.1	1048	254
China	1003	14	641	362
Saudi Arabia	333	4.6	165	168
USA	240	3.3	166	74
Korea	195	2.7	86	109
United Kingdom	156	2.2	66	90
Australia	149	2.1	85	64
Malaysia	140	2	40	100
Canada	137	1.9	79	58
Italy	96	1.3	68	28
Pakistan	89	1.2	17	72
United Arab Emirates	87	1.2	30	57
Spain	84	1.2	55	29
Iran	82	1.1	55	27
Egypt	80	1.1	48	32
Morocco	80	1.1	66	14
Turkey	78	1.1	63	15
Iraq	65	0.9	53	12
Jordan	61	0.9	26	35
Tunisia	49	0.7	24	25

E. Publication by Country

This section analyzes the distribution of articles related to intrusion detection in IoT networks using deep learning across single and multiple-country publications. It also examines the collaboration networks among countries publishing in this domain. The data reveals a clear preference pattern for single-country publications (SCP) over multiple-country publications (MCP) across most countries, highlighting individual contributions and collaborative efforts in this research area.

Table VIII shows that India leads the research in this field, with an impressive 1302 articles. Of these, 1048 are SCP, demonstrating India's focus on independent research. China follows closely with 1003 articles, splitting its efforts between 641 SCP and 362 MCP, highlighting a balanced approach to national and international collaborations. Saudi Arabia emerges as a key player, contributing 333 articles with nearly equal emphasis on SCP (165) and MCP (168). This balanced participation underscores the country's commitment to local research and global collaboration. Some countries, like Canada and Iraq, strongly prefer SCP over MCP. For example, Canada's 137 articles include 79 SCP and only 58 MCP, while Iraq's 65 articles are dominated by 53 SCP, with minimal international collaboration. On the other hand, Malaysia stands out with its MCP (100) surpassing SCP (40), showcasing a robust engagement in international partnerships. Similarly, Pakistan, the United Kingdom, and Korea show significant MCP contributions, underlining their collaborative approach to advancing IoT security research.

Fig. 8 visualizes the distribution of SCP and MCP across countries. India and China dominate the research output, with SCP accounting for most of their publications. However, countries like Saudi Arabia and Malaysia exhibit a more balanced SCP-MCP ratio, reflecting their collaborative strategies. Meanwhile, smaller contributors like Tunisia and Jordan have modest publication counts, with nearly equal SCP and MCP values. These trends highlight varying degrees of collaboration and individual research efforts among nations.

The analysis underscores the importance of collaborative research in driving advancements in IoT intrusion detection. Countries with higher MCP contributions, such as Malaysia and Saudi Arabia, benefit from shared knowledge and resources, paving the way for innovative and robust security solutions. At the same time, the dominance of SCP in

countries like India and China highlights the substantial role of localized research in shaping this critical field.

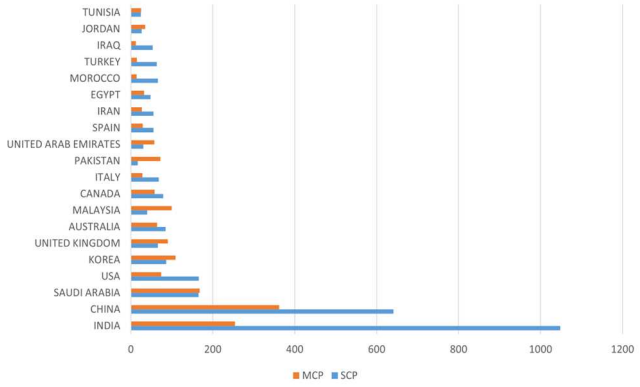

Fig. 8 Country with single and multiple country publications

IV. Conclusion

This study highlights the rapid growth of research on intrusion detection systems (IDS) for IoT using deep learning over the past decade. Journal articles are the leading platform for sharing findings, focusing on rigorous, peer-reviewed research. The field is highly interdisciplinary, with input from computer science, engineering, and mathematics, showing the importance of addressing IoT security issues. Leading contributions come from countries like India, China, the United States, and Saudi Arabia, with key topics including “Internet of Things,” “machine learning,” “deep learning,” and “intrusion detection.” The strong international collaboration emphasizes the global nature of this research community.

What sets this study apart is its focus on deep learning applications in IDS for IoT, offering a detailed look at recent advancements and their implications for the field. This research provides a comprehensive view of global trends, thematic developments, and collaborations by filling gaps in previous bibliometric studies. The findings pave the way for future exploration, encouraging researchers and institutions to build on these insights and address emerging IoT security challenges.

This study deepens our understanding of IDS for IoT and serves as a valuable resource for guiding future research and fostering global partnerships. As the Internet of Things (IoT) continues to expand, such efforts can play a crucial role in strengthening security and ensuring the safe adoption of this transformative technology.

Acknowledgment

Communication of this research is made possible through monetary assistance by Universiti Tun Hussein Onn Malaysia and the UTHM Publisher’s Office via Publication Fund E15216

References

[1] E. H. Houssein, M. A. Othman, W. M. Mohamed, and M. Younan, "Internet of Things in smart cities: Comprehensive review, open issues and challenges," *IEEE Internet Things J.*, 2024, doi:10.1109/JIOT.2024.3449753.

[2] H. Edquist, P. Goodridge, and J. Haskel, "The Internet of Things and economic growth in a panel of countries," *Econ. Innov. New Technol.*, vol. 30, no. 3, pp. 262-283, 2021, doi:10.1080/10438599.2019.1695941.

[3] M. Shahin, M. Maghanaki, A. Hosseinzadeh, and F. F. Chen, "Advancing network security in Industrial IoT: A deep dive into AI-enabled intrusion detection systems," *Adv. Eng. Inform.*, vol. 60, Oct. 2024, doi: 10.1016/j.aei.2024.102685.

[4] M. F. A. Razak, N. B. Anuar, R. Salleh, and A. Firdaus, "The rise of 'malware': Bibliometric analysis of malware study," *J. Netw. Comput. Appl.*, vol. 75, pp. 58-76, 2016, doi: 10.1016/j.jnca.2016.08.022.

[5] R. Saadouni et al., "Intrusion detection systems for IoT based on bio-inspired and machine learning techniques: A systematic review of the literature," *Cluster Comput.*, vol. 27, no. 7, pp. 8655-8681, Oct. 2024, doi: 10.1007/s10586-024-04388-5.

[6] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in *Proc. IEEE Int. Conf. Commun. Softw. Netw. (ICCSN)*, 2016, pp. 1-6, doi:10.1109/iccsn.2016.7586590.

[7] A. Aldhaheri et al., "Deep learning for cyber threat detection in IoT networks: A review," *Internet Things Cyber-Phys. Syst.*, vol. 4, pp. 1-15, 2024, doi: 10.1016/j.iotcps.2023.09.003.

[8] S. Kuutti et al., "A survey of deep learning applications to autonomous vehicle control," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 2, pp. 712-733, Feb. 2021, doi: 10.1109/tits.2019.2962338.

[9] H. A. Helaly, M. Badawy, and A. Y. Haikal, "A review of deep learning approaches in clinical and healthcare systems based on medical image analysis," *Multimedia Tools Appl.*, vol. 83, no. 12, pp. 36039-36080, Apr. 2024, doi: 10.1007/s11042-023-16605-1.

[10] N. Al-lQubaydhi et al., "Deep learning for unmanned aerial vehicles detection: A review," *Comput. Sci. Rev.*, vol. 51, Feb. 2024, doi:10.1016/j.cosrev.2023.100614.

[11] K. V. Nunen, J. Li, G. Reniers, and K. Ponnet, "Bibliometric analysis of safety culture research," *Saf. Sci.*, vol. 108, pp. 248-258, Oct. 2018, doi: 10.1016/j.ssci.2017.08.011.

[12] W. Li and Y. Zhao, "Bibliometric analysis of global environmental assessment research in a 20-year period," *Environ. Impact Assess. Rev.*, vol. 50, pp. 158-166, Jan. 2015, doi: 10.1016/j.eiar.2014.09.012.

[13] N. Donthu et al., "How to conduct a bibliometric analysis: An overview and guidelines," *J. Bus. Res.*, vol. 133, pp. 285-296, Sep. 2021, doi: 10.1016/j.jbusres.2021.04.070.

[14] R. Ullah, I. Asghar, and M. G. Griffiths, "An integrated methodology for bibliometric analysis: A case study of Internet of Things in healthcare applications," *Sensors*, vol. 23, no. 1, Jan. 2023, doi:10.3390/s23010067.

[15] J. M. Merigó and J. B. Yang, "A bibliometric analysis of operations research and management science," *Omega*, vol. 73, pp. 37-48, Dec. 2017, doi: 10.1016/j.omega.2016.12.004.

[16] P. Arora and A. Jain, "Cyber security threats and their solutions through deep learning: A bibliometric analysis," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICAC3N)*, 2021, pp. 1944-1949, doi: 10.1109/icac3n53548.2021.9725480.

[17] A. Sadeghi-Niaraki, "Internet of Thing (IoT) review of review: Bibliometric overview since its foundation," *Future Gener. Comput. Syst.*, vol. 143, pp. 361-377, Jun. 2023, doi:10.1016/j.future.2023.01.016.

[18] C. Dindorf et al., "Conceptual structure and current trends in artificial intelligence, machine learning, and deep learning research in sports: A bibliometric review," *Int. J. Environ. Res. Public Health*, vol. 20, no. 1, Jan. 2023, doi: 10.3390/ijerph20010173.

[19] F. Jahoor, M. K. Joseph, and N. Madhav, "Bibliometric analysis of cybersecurity in e-learning systems and big data," in *Proc. Conf. Inf. Commun. Technol. Soc. (ICTAS)*, 2024, pp. 57-62, doi:10.1109/ICTAS59620.2024.10507133.

[20] A. Valencia-Arias et al., "Machine learning and blockchain: A bibliometric study on security and privacy," *Information*, vol. 15, no. 1, Jan. 2024, doi: 10.3390/info15010065.

[21] K. Ganji and N. Afshan, "A bibliometric review of Internet of Things (IoT) on cybersecurity issues," *J. Sci. Technol. Policy Manage.*, early access, 2024, doi: 10.1108/JSTPM-05-2023-0071.

[22] D. C. Nguyen et al., "Federated learning for Internet of Things: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 3, pp. 1622-1658, Jul. 2021, doi: 10.1109/COMST.2021.3075439.

[23] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *SN Comput. Sci.*, vol. 2, no. 3, May 2021, doi:10.20944/preprints202103.0216.v1.

[24] M. A. Ferrag et al., "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, doi:10.1016/j.jisa.2019.102419.

[25] Y. Meidan et al., "N-BaIoT - Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12-22, Jul.-Sep. 2018, doi: 10.1109/MPRV.2018.03367731.

[26] J. Wang and S. Zhang, "Cross-cultural learning: A visualized bibliometric analysis based on Bibliometrix from 2002 to 2021," *Mobile Inf. Syst.*, vol. 2022, Jan. 2022, doi:10.1155/2022/7478223.

[27] M. A. Al-Garadi et al., "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1646-1685, Jul. 2020, doi:10.1109/COMST.2020.2988293.

[28] N. Goranin, S. K. Hora, and H. A. Čenys, "A bibliometric review of intrusion detection research in IoT: Evolution, collaboration, and emerging trends," *Electronics*, vol. 13, no. 16, Aug. 2024, doi:10.3390/electronics13163210.

[29] F. G. Montoya et al., "A fast method for identifying worldwide scientific collaborations using the Scopus database," *Telemat. Inform.*, vol. 35, no. 1, pp. 168-185, Apr. 2018, doi: 10.1016/j.tele.2017.10.010.

[30] E. M. Lasda Bergman, "Finding citations to social work literature: The relative benefits of using Web of Science, Scopus, or Google Scholar," *J. Acad. Librariansh.*, vol. 38, no. 6, pp. 370-379, 2012, doi:10.1016/j.acalib.2012.08.002.

[31] S. O. Kingsley and S. Hosseini, "Introduction to R programming and RStudio integrated development environment (IDE)," in *R Programming: Statistical Data Analysis in Research*, Singapore: Springer, 2024, pp. 3-24, doi: 10.1007/978-981-97-3385-9_1.

[32] M. Aria and C. Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis," *J. Informetr.*, vol. 11, no. 4, pp. 959-975, Nov. 2017, doi: 10.1016/j.joi.2017.08.007.

[33] R. Rodríguez-Soler, J. Uribe-Toril, and J. De Pablo Valenciano, "Worldwide trends in the scientific production on rural depopulation, a bibliometric analysis using bibliometrix R-tool," *Land Use Policy*, vol. 97, Sep. 2020, doi: 10.1016/j.landusepol.2020.104787.

[34] K. S. Nikita, "Engaging in scientific publishing: Benefits and norms to follow as authors and reviewers," *IEEE Antennas Propag. Mag.*, vol. 64, no. 3, pp. 156-160, Jun. 2022, doi: 10.1109/MAP.2022.3163359.

[35] M. Mohammadi et al., "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 2923-2960, Oct. 2018, doi: 10.1109/COMST.2018.2844341.

[36] M. AL-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," *J. Inf. Secur. Appl.*, vol. 41, pp. 1-11, Aug. 2018, doi: 10.1016/j.jisa.2018.05.002.

[37] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion detection in Industrial Internet of Things network-based on deep learning model with rule-based feature selection," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/7154587.

[38] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110-124, Jan. 2021, doi: 10.1016/j.comcom.2020.12.003.

[39] G. T. Reddy et al., "Analysis of dimensionality reduction techniques on big data," *IEEE Access*, vol. 8, pp. 54776-54788, 2020, doi:10.1109/access.2020.2980942.

[40] A. Azmoodeh, A. Dehghantanha, and K. K. R. Choo, "Robust malware detection for Internet of (Battlefield) Things devices using deep eigenspace learning," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 88-95, Jan.-Mar. 2019, doi: 10.1109/TSUSC.2018.2809665.

[41] A. Kumari et al., "Multimedia big data computing and Internet of Things applications: A taxonomy and process model," *J. Netw. Comput. Appl.*, vol. 131, pp. 28-55, Dec. 2018, doi:10.1016/j.jnca.2018.09.014.

[42] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, doi:10.1016/j.jnca.2020.102630.

[43] R. M. Swarna Priya et al., "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139-149, Jul. 2020, doi: 10.1016/j.comcom.2020.05.048.

[44] V. Mothukuri et al., "Federated-learning-based anomaly detection for IoT security attacks," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2545-2554, Feb. 2022, doi: 10.1109/jiot.2021.3077803.

[45] M. Douiba et al., "An improved anomaly detection model for IoT security using decision tree and gradient boosting," *J. Supercomput.*, vol. 79, no. 3, pp. 3392-3411, Feb. 2023, doi: 10.1007/s11227-022-04783-y.

[46] A. Churcher et al., "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, Jan. 2021, doi: 10.3390/s21020446.

[47] C. I. Nwakanma et al., "Explainable artificial intelligence (XAI) for intrusion detection and mitigation in intelligent connected vehicles: A review," *Appl. Sci.*, vol. 13, no. 3, Feb. 2023, doi:10.3390/app13031252.

[48] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 21, 2020, doi:10.1002/cpe.4946.

[49] R. Kumar et al., "SP2F: A secured privacy-preserving framework for smart agricultural unmanned aerial vehicles," *Comput. Netw.*, vol. 187, Mar. 2021, doi: 10.1016/j.comnet.2021.107819.

[50] E. H. Tusher et al., "Email spam: A comprehensive review of optimize detection methods, challenges, and open research problems," *IEEE Access*, vol. 12, pp. 1-1, 2024, doi: 10.1109/access.2024.3467996.

[51] N. S. Nordin and M. A. Ismail, "A hybridization of butterfly optimization algorithm and harmony search for fuzzy modelling in phishing attack detection," *Neural Comput. Appl.*, vol. 35, no. 7, pp. 5501-5512, Mar. 2023, doi: 10.1007/s00521-022-07957-0.

[52] H. Hanif et al., "The rise of software vulnerability: Taxonomy of software vulnerabilities detection and machine learning approaches," *J. Netw. Comput. Appl.*, vol. 179, 2021, doi:10.1016/j.jnca.2021.103009.