Fraud Mobile Apps Detection: A Bibliometric Analysis

Parmod[a], Prof. Harish Rohil[b]

[a]Research Scholar, Deptt. of Com Sci & Eng , Chaudhary Devi Lal University(CDLU), Barnala Road, Sirsa (Haryana)-125055, India,
Email:*parmod94843@gmail.com*
[b]Professor, Deptt. of Com Sci & Eng , Chaudhary Devi Lal University(CDLU), Barnala Road, Sirsa (Haryana)-125055, India
Email:*harishrohil@gmail.com*

Abstract:

The growing popularity of mobile apps has led to an increase in fraudulent activity inside the mobile app ecosystem. In response, the investigation and development of detecting techniques has become critical. This study undertakes a comprehensive Bibliometric analysis to delineate the landscape of fraud mobile apps detection. Employing the R-package software for analysis, data sourced from various repositories are scrutinized, resulting in the examination of numerous pertinent documents. Utilizing Microsoft Excel for frequency analysis and R-package for citation metrics, the study offers insights into source titles, document types, publication years, subject areas, languages, keyword analyses, authorship patterns, citation trends and geographical distribution. Employing the Scopus database, the search strategy encompassed keywords such as "counterfeit," "scams," "fake," "fraud," "scam," "detection," "detect," "find," and synonymous terms associated with "mobile application." Through meticulous stages of filtration, including subject, language, and publication stage, the study culled a final corpus of 77 documents for analysis. The information shows an increasing interest in fraud mobile app detection, indicating a rising realization of its importance in the mobile app arena. The findings highlight the critical need for effective detection techniques to protect users and maintain the integrity of the mobile app ecosystem. This paper also reviews the selected papers.

KEYWORDS: Research Trend Analysis, Mobile Apps, Fraud Detection, Bibliometric Analysis.

1. Introduction

The increasing use of mobile applications has raised significant concerns regarding the occurrence of cyber crimes related to these apps (Kaur Bajaj & Chander, 2015). These crimes include various fraudulent activities aimed at deceiving and causing harm to users. In response to this growing problem, machine learning techniques have been employed to analyze the patterns and behaviors exhibited by mobile apps, enabling the detection and mitigation of fraudulent applications (Gupta, 2014). Scientometrics or bibliometrics is a relatively new field that focuses on the quantitative evaluation of scientific publications (Asma & Perna, 2021). It provides an objective and systematic approach for assessing the quality and impact of scientific papers (Trinh Thi Phuong et al., 2022). Bibliometric analysis involves the quantitative examination of extensive databases containing a vast collection of books, articles, and publishers, such as SCOPUS, Web of Science (WOS), ABCD, PubMed, EBSCO, and CrossRef. This analytical approach offers valuable insights into the landscape of scientific publications and their associated citations (Trinh Thi Phuong et al., 2022).. By employing the scientific method and utilizing mathematical equations and statistical tools, bibliometric studies assist researchers, scholars, and practitioners in narrowing down their research focus and initiating their work (Swarnkar, Harikrishnan, & Singh, 2022). As academic knowledge continues to expand rapidly, there has been a noteworthy surge in scientific publications encompassing various forms, including articles, reports, and other relevant materials (França, Dantas, & Araújo-Júnior, 2022). Among the available databases, SCOPUS stands out as the largest repository of abstracts and citations, housing an extensive collection of 1.4 billion citations and information on 16 million authors. SCOPUS is highly regarded for providing comprehensive coverage of the latest literature (Yang & Thoo, 2022). Considering its reputable journals and research documents, SCOPUS was selected as the database for this study (Alviz-Meza, Orozco-Agamez, Quinayá, & Alviz-Amador, 2023). To analyze and visualize publication trends within the field, the study utilized the Biblioshiny. Biblioshiny is a web-based graphical user interface (GUI) tool developed in R for conducting bibliometric analyses This powerful tool facilitated the mapping and graphical representation of bibliometric information. This paper provides a comprehensive and systematic overview of the current landscape of research on fraud detection in mobile apps. This article aims to answer the following research questions:

1. What are the prevalent document types among published articles in fraud mobile apps detection?
2. Is there an increase in the number of publications in fraud mobile apps detection each year?
3. Who are the leading researchers in the field of fraud mobile apps detection?
4. Which articles in fraud mobile apps detection have the most citations?
5. Which scientific journals are widely published in the field of fraud mobile apps detection?
6. What are the most prominently used author keywords in the field of fraud mobile apps detection?
7. Which countries have ranked top in fraud mobile apps detection articles and publications?
8. What are the main contributions, approaches, findings, and key takeaways in the methodologies for fraud detection in mobile applications as discussed in scholarly literature till 2024?

2. Literature Review

Bibliometric analysis and past studies

This section aims to review related research from this field. A bibliography study is a study that demonstrates the present status of a study topic to see what alternatives are available for scholars to further their future research in a certain sector.

The article "Fraud Detection Credit Card: A Bibliometric Analysis Approach" by Risky Mezi Muria offers a comprehensive examination of credit card fraud detection methodologies and trends through a bibliometric analysis. Beginning with an overview of the significance of

credit cards in modern transactions and the escalating need for enhanced security measures, the author delves into the intricacies of different types of credit card fraud and the associated challenges, including data scarcity, feature engineering, scalability, concept drift, performance metrics, and algorithm selection. By analyzing data from reputable sources such as Google Scholar, Science Direct, and Emerald Insight, the author uncovers insights into the distribution of published articles, research methodologies, and fraud detection techniques employed. Notably, quantitative research approaches, particularly those utilizing system-related fraud detection methods, are prevalent. The article also highlights the contributions of various publications and conferences to the field. While providing valuable insights, the article could benefit from further exploration of potential limitations of the bibliometric analysis approach and more detailed recommendations for future research directions (Muria, 2023).

The article "Fraud Detection in Healthcare Organizations: A Bibliometric Analysis Approach" by Yustin Nur Faizah, Siti Musyarofah, and Alexander Anggono presents a meticulous examination of trends and patterns in healthcare fraud detection, drawing insights from an analysis of 51 selected journals and articles sourced from Science Direct, Emerald Insight, and Google Scholar. Through a structured presentation of findings and insightful data visualization, the authors highlight the prevalence of health insurance fraud, the emergence of qualitative research methodologies, and the potential of big data analytics in enhancing fraud detection capabilities. While the article offers valuable contributions to the understanding of healthcare fraud, including identifying future research directions, a more critical discussion of methodological limitations would enhance the study's scholarly rigor. Overall, the article serves as a significant resource for researchers, practitioners, and policymakers in the realm of healthcare governance and forensic accounting (Faizah, Musyarofah, & Anggono, 2021).

3. Methodology

Bibliometric is known as a combination of mathematical and statistical methods to books and other forms of communication that has been widely applied in the field of library and information science studies. The main purpose of conducting Bibliometric analysis is to quantitatively evaluate the productivity of scientific outputs. There are many researchers indicated that statistical tools are needed to conduct Bibliometric analysis to analyze past published academic articles in a specific field of study. Bibliometric includes several descriptive statistics of citation data, and network analysis of authors, journals, universities, countries, and keywords based on citations and frequency analysis techniques. It aids the understanding of research clusters, provides information into current research interests, and reveals patterns for emerging topics in a field. The Bibliometric method of review can be used as a new approach to implicitly evaluate developments in recent years and establish relationship networks between publications (Rajendran, Wahab, Yeap, Kamarulzaman, & Lim, 2023).

There are four main steps applied in the process of analyzing and mapping bibliographic data. Firstly, starting with data collection through systematic literature search, and comprehensive evaluation of the field. The next steps are to conduct Bibliometric citation analysis and network analysis aiming to identify publication trends, the most influential journals, studies, institutions, and authors. Finally, synthesizes findings and discovers potential research direction. The data for this study comes from the Scopus database as of Dec 2024, encompassing a time frame until Dec 2024. This study employs a thorough bibliometric analysis to investigate the evolution and advancement of fraud mobile apps detection over the period.

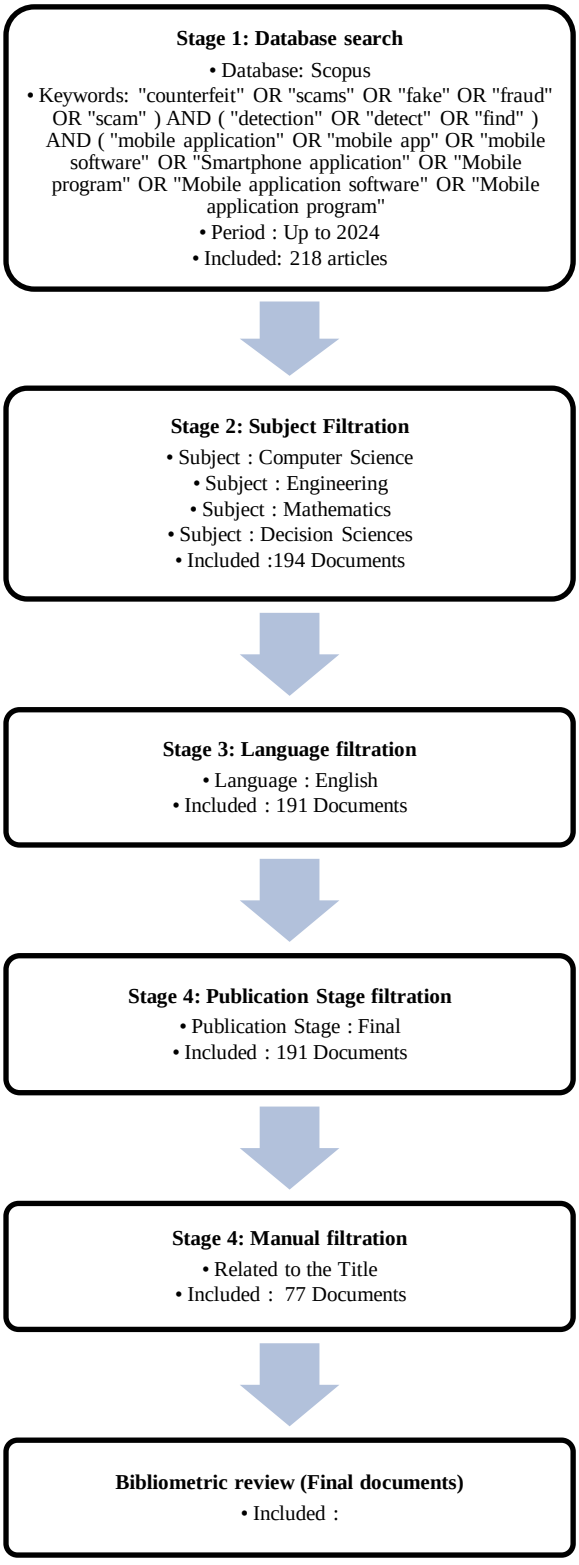


Figure 1: Bibliometric Analysis Stages

Scopus was used as a bibliometric analysis resource in our analysis because it is regarded as the largest citation database and abstracts of peer-reviewed literature by many researchers, compared to Web of Science or PubMed. The keywords "counterfeit" OR "scams" OR "fake" OR "fraud" OR "scam") AND ("detection" OR "detect" OR "find") AND ("mobile application" OR "mobile app" OR "mobile software" OR "Smartphone application" OR "Mobile program" OR "Mobile application software" OR "Mobile application program" were used to find relevant articles about fraud mobile apps detection.

The authors concentrate on the titles of the articles since they represent the specific topic that applies to the field of the study and the scope of the research. Past researchers opined that the title of an article includes information that could be used to capture the interest of readers, as it is the first thing they will notice. A total of 77 documents were acquired for the bibliometric analysis based on a Scopus database search and manual exclusions as shown in Figure 1. In this bibliometric study, all 77 documents in the record were screened and included for further analyses. Tools like Microsoft Excel and R-package were utilized to examine the bibliometric analysis. Microsoft Excel is used to determine the frequencies of published materials and to create the appropriate chart and graph, while R-package software is utilized to generate citation metrics and some of the other frequencies.

4. Result

Bibliometric attributes such as source title, source type, document type, publication year, subject area, languages, keywords analysis, authorship, citation analysis, geographical distribution and active institutions using data from the Scopus database. Most of the results and discussions are described as percentages and frequencies. Biblioshiny is used to map the co-occurrence of the author's keywords, as well as report citation analysis, to identify the top ten most referenced publications in nanotechnology.

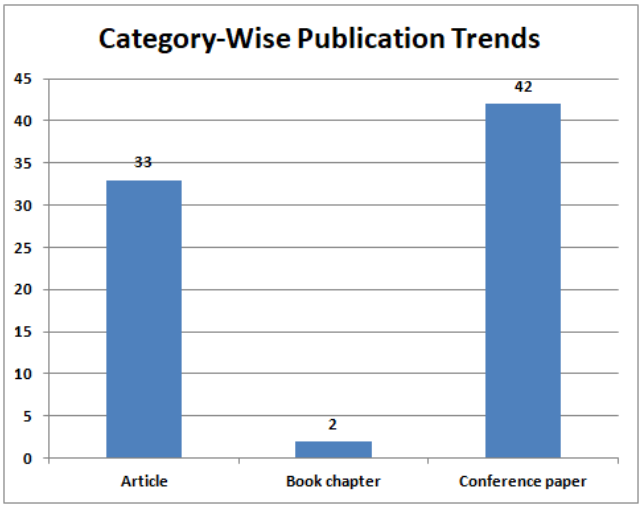
4.1. Main Information

The analysis spans documents published between 2011 and 2024, comprising 68 sources, including journals and books, and a total of 77 documents. The dataset exhibits an average document age of 4.48 years, with 11.22 citations per document on average and 2,349 references in total. In terms of content, the study identifies 544 thematic keywords (Keywords Plus) and 218 authors' keywords. Authorship details reveal contributions from 266 authors, with three single-authored documents, and a collaboration average of 4.43 co-authors per document. International co-authorships account for 29.87% of the total. The documents are categorized as 33 articles, 2 book chapters, and 42 conference papers, reflecting diverse scholarly contributions.

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	2011:2024
Sources (Journals, Books, Etc)	68
Documents	77
Document Average Age	4.48
Average Citations Per Doc	11.22
References	2349
Document Contents	
Keywords Plus (Id)	544
Author's Keywords (De)	218
Authors	
Authors	266
Authors Of Single-Authored Docs	3
Authors Collaboration	
Single-Authored Docs	3
Co-Authors Per Doc	4.43
International Co-Authorships %	29.87
Document Types	
Article	33
Book Chapter	2
Conference Paper	42

4.2. Category-Wise Publication Trends

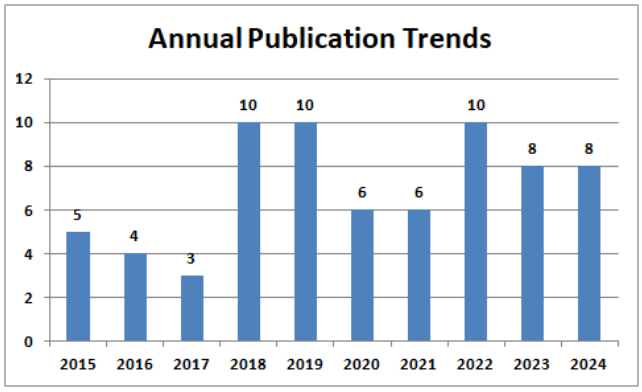
The distribution of document types in the dataset is highlighted below. It reveals that conference papers are the most prevalent document type,



with 42 publications, followed by articles (33) and book chapters (2).

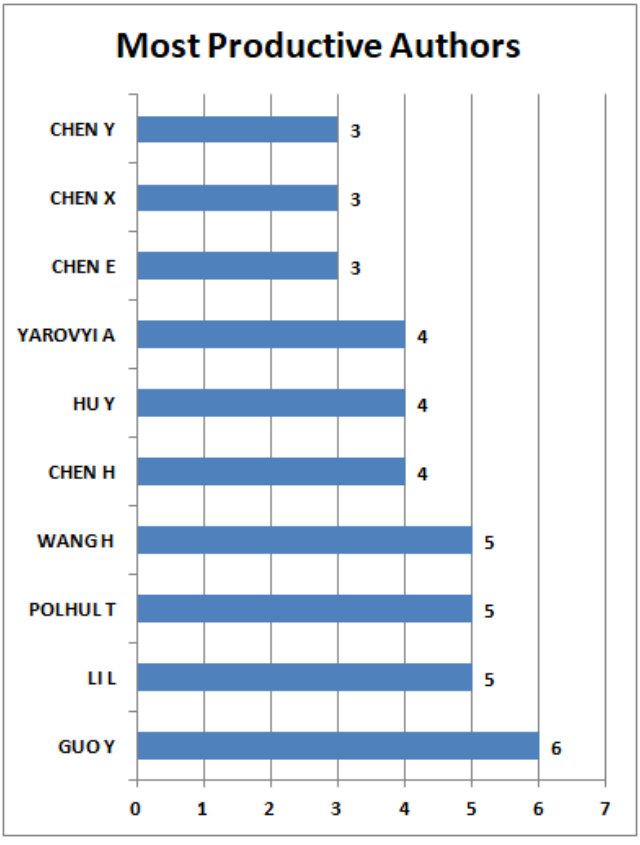
4.3. Annual Publication Trends

The annual publication trends from 2015 to 2024 reveal fluctuating numbers of articles published each year. The trend starts with 5 articles in 2015 and declines to a low of 3 articles in 2017. A sharp increase is observed in 2018 and 2019, each with 10 articles. Following a slight drop in 2020 and 2021, with 6 articles each, the number again peaks at 10 articles in 2022. The years 2023 and 2024 maintain a steady count of 8 articles each, reflecting consistent research contributions in recent years.



4.4. Most Productive Authors

The most productive authors in the dataset are led by GUO Y, who has contributed 6 articles, making them the top contributor. Following closely are LI L, POLHUL T, and WANG H, each with 5 articles. CHEN H, HU Y, and YAROVYI A have each published 4 articles, showcasing their significant contributions. CHEN E, CHEN X, and CHEN Y have each contributed 3 articles, further emphasizing the diversity and collaboration within this research field.



4.5. Most Cited Papers

The most cited papers in mobile app fraud detection include *DeCAF* (2014) with 110 citations, followed by *AdAttester* (2015) with 78 citations, and *FraudDroid* (2018) with 69 citations. Other significant papers include *Discovery of ranking fraud for mobile apps* (2015) with 57 citations and *Identifying spam in the iOS App Store* (2012) with 53 citations. Recent works like *MadDroid* (2020) and *ClickGuard* (2020) have 38 and 28 citations, respectively.

Authors(Year)	Title	Year	Total Citations	TC per Year
Liu, B., Nath, S., Govindan, R., & Liu, J. (2014)	DeCAF: Detecting and characterizing ad fraud in mobile apps	2014	110	10.00
Li, W., Li, H., Chen, H., & Xia, Y. (2015)	AdAttester: Secure online mobile advertisement attestation using trustzone	2015	78	7.80
Dong, Feng, Wang, Haoyu, Li, Li, Guo, Yao, Bissyandé, Tegawendé F., Liu, Tianming, Xu, Guoai, & Klein, Jacques (2018).	FraudDroid: Automated ad fraud detection for android apps.	2018	69	9.86
Y.G. Tamboli & Satarkar, (2015)	Discovery of ranking fraud for mobile apps	2015	57	5.70
Chandy, R., & Gu, H. (2012)	Identifying spam in the iOS App Store.	2012	53	4.08
Zhu, Hengshu, Liu, Chuanren, Ge, Yong, Xiong, Hui, & Chen, Enhong (2015).	Popularity Modeling for Mobile Apps: A Sequential Approach	2015	41	4.10
Liu, Tianming, Wang, Haoyu, Li, Li, Luo, Xiapu, Dong, Feng, Guo, Yao, Wang, Liu, Bissyandé, Tegawendé, & Klein, Jacques (2020).	MadDroid: Characterizing and Detecting Devious Ad Contents for Android Apps	2020	38	7.60
Li, F., Clarke, N., Papadaki, M., & Dowland, P. (2011).	Behaviour profiling for transparent authentication for mobile devices	2011	32	2.29
Shi, Congcong, Song, Rui, Qi,	ClickGuard: Exposing	2020	28	5.60

Xinyu, Song, Yubo, Xiao, Bin, & Lu, Sanglu (2020).	Hidden Click Fraud via Mobile Sensor Side-channel Analysis			
Jiang, N., Jin, Y., Skudlark, A., Hsu, W.-L., Jacobson, G., Prakasam, S., & Zhang, Z. L. (2012)	Isolating and analyzing fraud activities in a large cellular network via voice call graph analysis	2012	28	2.15

4.6. Most Productive Journals

The most productive journals in the field of mobile app fraud detection are led by *IEEE Transactions on Mobile Computing*, which published 4 articles. Following this, *IEEE Transactions on Dependable and Secure Computing* and *Lecture Notes in Computer Science* each contributed 3 articles. Other notable sources include the *ACM International Conference Proceeding Series* and *The Web Conference 2020 - Proceedings of the World Wide Web Conference* (WWW 2020), each with 2 articles.

Source	h index	g index	M _index	Articles
IEEE TRANSACTIONS ON MOBILE COMPUTING	3	3	0.428571	4
IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	1	2	0.25	3
LECTURE NOTES IN COMPUTER SCIENCE (INCLUDING SUBSERIES LECTURE NOTES IN ARTIFICIAL INTELLIGENCE AND LECTURE NOTES IN BIOINFORMATICS)	1	1	0.142857	3
ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES	1	2	0.076923	2
THE WEB CONFERENCE 2020 - PROCEEDINGS OF THE WORLD WIDE WEB CONFERENCE, WWW 2020	2	2	0.4	2

4.7. Most Relevant Affiliations

The most relevant affiliations in the field of mobile app fraud detection include *Nanjing University*, with 20 articles, followed by *Zhejiang University* with 14 articles. Other significant affiliations are *Fudan University* with 8 articles, and *Yeungnam University* with 7. Additional notable institutions include *Southeast University* (6 articles), *AT&T Labs. - Research* (5 articles), *Jiangsu University* (5 articles), *Peking University* (5 articles), *Xiamen University* (5 articles), and *Beijing University of Posts and Telecommunications* (4 articles).

Affiliation	Country	Articles
NANJING UNIVERSITY	China	20
ZHEJIANG UNIVERSITY	China	14
FUDAN UNIVERSITY	China	8
YEUNGNAM UNIVERSITY	South Korea	7
SOUTHEAST UNIVERSITY	China	6
AT AND T LABS. - RESEARCH	United States	5
JIANGSU UNIVERSITY	China	5
PEKING UNIVERSITY	China	5
XIAMEN UNIVERSITY	China	5
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS	China	4

4.8. Average Citations Per Year

The average citations per year for articles in the field of mobile app fraud detection vary across different years. In 2015, the mean total citations per article was 38, with an average of 3.8 citations per year over 10 citable years. This was followed by a decline in 2016, with 6 citations per article and 0.67 citations per year. The trend showed fluctuations, with a peak in 2020 at 16.83 total citations per article and 3.37 citations per year. Recent years, such as 2023 and 2024, show a significant drop, with 0.62 and 0.5 citations per article, respectively.

Year	Mean TC per Art	N	Mean TC per Year	Citable Years
2015	38	5	3.8	10
2016	6	4	0.67	9
2017	10	3	1.25	8
2018	14.2	10	2.03	7
2019	4.5	10	0.75	6
2020	16.83	6	3.37	5
2021	6.5	6	1.62	4
2022	3.7	10	1.23	3
2023	0.62	8	0.31	2
2024	0.5	8	0.5	1

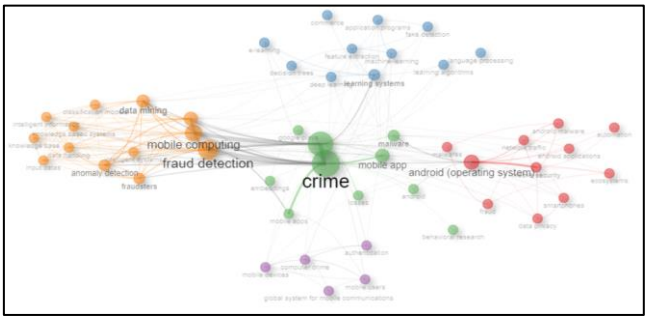
4.9. Most Frequent Keywords

The most frequent keywords in the field of mobile app fraud detection are *Crime* (27 occurrences), *Mobile Applications* (24 occurrences), and *Fraud Detection* (16 occurrences). Other prominent keywords include *Mobile App* (15 occurrences), *Android (Operating System)* (14 occurrences), and *Mobile Computing* (12 occurrences). Additional keywords with notable frequency include *Mobile Apps* (11 occurrences), *Classification (Of Information)* (9 occurrences), *Mobile Security* (9 occurrences), and *Malware* (9 occurrences).

Words	Occurrences
Crime	27
Mobile Applications	24

Fraud Detection	16
Mobile App	15
Android (Operating System)	14
Mobile Computing	12
Mobile Apps	11
Classification (Of Information)	9
Mobile Security	9
Malware	9

Co-occurrence Network



4.10. Country Publication Trend

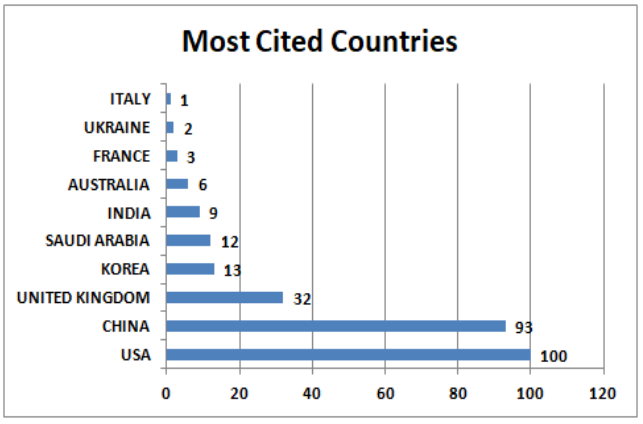
The country publication trend in mobile app fraud detection shows that *China* leads with 122 articles, followed by *India* with 65 articles, and the *USA* with 43 articles. Other notable contributors include *Australia* (15 articles), *South Korea* (14 articles), and *Italy* (12 articles). *Ukraine* follows with 11 articles, while *Japan* and *the UK* contribute 7 and 6 articles, respectively. *Pakistan* rounds out the list with 5 articles.

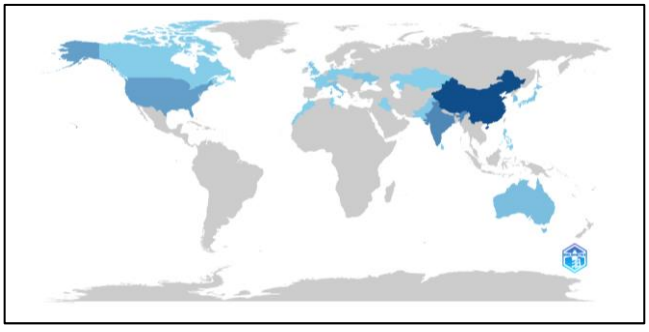
Countries	Number of articles
CHINA	122
INDIA	65
USA	43
AUSTRALIA	15
SOUTH KOREA	14
ITALY	12
UKRAINE	11
JAPAN	7
UK	6
PAKISTAN	5

4.11. Country Citation Trend

The country citation trend in mobile app fraud detection reveals that the *USA* has the highest total citations (100), followed closely by *China* with 93 citations. The *United Kingdom* has 32 citations, and *Korea* has 13. Other countries with notable citations include *Saudi Arabia* (12), *India* (9), *Australia* (6), *France* (3), *Ukraine* (2), and *Italy* (1).

Countries	TC
USA	100
CHINA	93
UNITED KINGDOM	32
KOREA	13
SAUDI ARABIA	12
INDIA	9
AUSTRALIA	6
FRANCE	3
UKRAINE	2
ITALY	1





4.12. Comprehensive Review of selected papers :

Authors(Year)	Main Contribution	Approach/Methodology	Findings/Results	Key Takeaways
Guo, Yao, Ma, Junming, Wu, Wenjun, & Chen, Xiangqun (2018).	Introduces PoWatt, a system for identifying UI states using power consumption analysis.	Analyzes power usage patterns and employs pattern-matching algorithms to pinpoint sensitive UI events.	Demonstrated 71% precision and 70% recall in offline detection, alongside acceptable real-time performance.	PoWatt highlights the risk of exploiting power traces to identify sensitive UI states, posing potential threats such as password exposure.
Joshi, Komal, Kumar, Sidharth, Rawat, Jyoti, Kumari, Ansita, Gupta, Aayush, & Sharma, Neha (2022).	Investigates machine learning models for detecting fraudulent apps.	Applies Decision Tree, Logistic Regression, and Naïve Bayes algorithms, leveraging factors like app ratings, reviews, in-app purchases, and advertisements.	Decision Tree achieved 85% accuracy, with an F1 score of 0.815, demonstrating high precision and recall.	Decision Tree emerges as the most reliable model for identifying fraudulent apps on the Google Play Store.
Dong, Feng, Wang, Haoyu, Li, Li, Guo, Yao, Bissyandé, Tegawendé F., Liu, Tianming, Xu, Guoai, & Klein, Jacques (2018).	Develops FraudDroid to combat dynamic ad fraud that replicates user behavior.	Utilizes a hybrid approach, combining UI state transitions and network traffic analysis.	Achieved 93% precision and 92% recall in detecting fraudulent behavior across various ad platforms.	FraudDroid offers an effective solution for identifying sophisticated dynamic ad fraud in Android applications.
Polhul, T., & Yarovyi, A. (2019).	Introduces a fingerprinting method for identifying fraudulent users.	Implements a fuzzy logic-based model to generate unique fraudster profiles.	Achieved an overall fraud detection accuracy of 99.56%.	Fraudster fingerprinting provides a robust mechanism to enhance the speed and accuracy of fraud detection.
Polhul, T. D., Yarovyi, A. A., Romaniuk, R., Komada, P., & Askarova, N. (2019)	Detects installation anomalies in mobile apps.	Analyzes diverse data streams using a heterogeneous data approach to identify irregularities.	Achieved 99.14% accuracy in detecting installation anomalies in real-world scenarios.	A highly reliable technique for anomaly detection during the installation process of mobile apps.
Sharma, R. M., & Agrawal, C. P. (2022)	Presents a hybrid strategy for optimizing malware detection in Android apps.	Combines Metaheuristic optimization (IWD) with Deep Learning for feature selection and malware classification.	Delivered 93.7% F1-score, 95.35% precision, 99.12% accuracy, and 96.68% recall.	Hybrid feature reduction significantly boosts the accuracy and efficiency of malware detection.
Xu, M., Fu, Y., & Tian, B. (2023)	Proposes an ensemble-based approach to detect fraud in online loan applications.	Employs the GTWE ensemble algorithm integrated with logistic regression, XGBoost, and LSTM to analyze app behavior data.	Achieved 84.19% accuracy in identifying fraudulent activity based on app usage patterns.	The GTWE ensemble method proves effective, highlighting the importance of user behavior analysis in detecting online loan fraud.
Polhul, T., & Yarovyi, A. (2019)	Identifies fraud during app installations by standardizing diverse data types.	Proposes a novel method for transforming heterogeneous data into uniform coefficients to enhance detection accuracy.	Achieved 99.14% fraud detection accuracy through this innovative scaling method.	Standardizing heterogeneous data ensures greater accuracy in detecting fraud during app installations.
Mamidi, K. K., Muppavaram, K., Gotlur, K., Govathoti, S., Vafaeva, K. M., Saxena, A. K., & Shnain, A. H. (2024)	Addresses post-installation threats such as MITD attacks on Android.	Focuses on tracking sensitive data flows and mitigating malicious behavior post-installation.	Achieved 97% detection accuracy for MITD attacks.	Strengthens security against post-installation threats, improving overall Android app safety.
Ndibwile, J. D., Kadobayashi, Y., & Fall, D. (2017)	Introduces UnPhishMe, an application for detecting phishing attempts.	Simulates deceptive login scenarios and monitors URL changes to identify phishing	Achieved 96% accuracy while maintaining low resource requirements.	Offers a lightweight yet highly effective method for protecting Android

		activity.		devices from phishing attacks.
Cheng, Y., Qi, X., Li, Y., & Wang, Y. (2024)	Unveils ReckDroid, a solution for detecting red packet fraud in Android apps.	Employs a heuristic algorithm to identify red packets and analyze associated network traffic.	Achieved 98% precision and 93% recall for red packet detection, alongside 88.6% precision and 92.5% recall for fraud identification.	ReckDroid provides a high-accuracy solution to combat red packet fraud, which is especially prevalent in Chinese markets.

5. Conclusion

In conclusion, this bibliometric analysis of mobile app fraud detection research from 2011 to 2024 reveals growing interest in the field, with a diverse range of documents and increasing publications in recent years. The study highlights key methodologies, including machine learning and secure frameworks, and identifies top-cited papers, productive authors, and leading institutions like Nanjing University and Zhejiang University. The findings show a strong global collaboration, with significant contributions from countries like China, India, and the USA. This analysis underscores the critical need for continued research and innovation to address the evolving challenges in mobile app fraud detection.

6. Societal Impact

The societal impact of research on fraud mobile apps detection through bibliometric analysis is significant, as it highlights critical trends and gaps in addressing mobile app fraud. By identifying influential studies, authors, and regions contributing to this field, such research informs policy-making, enhances app store governance, and promotes ethical development practices. Ultimately, it aids in creating more secure digital environments, protecting user privacy and finances, and fostering trust in mobile technology, benefiting society by ensuring a safer and more reliable app ecosystem.

7. Future Research Directions

Future research in fraud mobile app detection could expand bibliometric analyses by incorporating advanced tools for dynamic citation mapping, co-authorship networks, and thematic evolution studies to uncover emerging research trends and collaborations. Comparative studies across databases like Scopus, Web of Science, and Google Scholar can provide a broader perspective on the field's development. Longitudinal analyses could track the temporal growth of publications, citation impact, and shifts in focus areas, offering insights into the maturation of the domain.

REFERENCES

Alviz-Meza, J., Orozco-Agamez, D. C. P., Quinayá, A., & Alviz-Amador, A. (2023). Bibliometric analysis of fourth industrial revolution applied to material sciences based on Web of Science and Scopus databases from 2017 to 2021. *ChemEngineering*, *7*(1). https://doi.org/10.3390/chemengineering7010002

Asma, L. I., & Perna, S. (2021). Sustainability indicators in agriculture: A review and bibliometric analysis using the Scopus database. *Journal of Agriculture and Environment for International Development*, *115*(2), 5–21. https://doi.org/10.36253/JAEID-12083

Chandy, R., & Gu, H. (2012). Identifying spam in the iOS App Store. *ACM International Conference Proceeding Series*, 56–59. https://doi.org/10.1145/2184305.2184317

Cheng, Y., Qi, X., Li, Y., & Wang, Y. (2024). ReckDroid: Detecting red packet fraud in Android apps. *Computers and Security*, *148*, 104117. https://doi.org/10.1016/j.cose.2024.104117

Dong, F., Wang, H., Li, L., Guo, Y., Bissyandé, T. F., Liu, T., Xu, G., Klein, J. (2018). FraudDroid: Automated ad fraud detection for Android apps. *ESEC/FSE 2018 - Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, 257–268. https://doi.org/10.1145/3236024.3236045

Faizah, Y., Musyarofah, S., & Anggono, A. (2021). Fraud detection in healthcare organization: A bibliometric analysis approach. *International Colloquium on Forensics Accounting and Governance*, *1*(1), 1–8.

França, L. D. M., Dantas, M. A. T., & Araújo-Júnior, H. I. D. (2022). Bibliometric analysis of isotopic studies on Quaternary megafauna available in the Scopus database. *Anais da Academia Brasileira de Ciências*, *94*, 1–24. https://doi.org/10.1590/0001-3765202220211404

Guo, Y., Ma, J., Wu, W., & Chen, X. (2018). Inferring UI states of mobile applications through power side channel exploitation. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *254*, 210–226. https://doi.org/10.1007/978-3-030-01701-9_12

Gupta, N. A. (2014). Mobile cell phones and cyber crimes in India: How safe are we? *Bharati Law Review*, 18–23.

Jiang, N., Jin, Y., Skudlark, A., Hsu, W.-L., Jacobson, G., Prakasam, S., & Zhang, Z. L. (2012). Isolating and analyzing fraud activities in a large cellular network via voice call graph analysis. *MobiSys'12 - Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, 253–266. https://doi.org/10.1145/2307636.2307660

Joshi, K., Kumar, S., Rawat, J., Kumari, A., Gupta, A., & Sharma, N. (2022). Fraud app detection of Google Play Store apps using decision tree. *Proceedings of 2nd International Conference on Innovative Practices in Technology and Management, ICIPTM 2022*, 243–246. https://doi.org/10.1109/ICIPTM54933.2022.9754207

Kaur Bajaj, & Chander, J. (2015). Cyber crime through mobile phone in India and preventive methods. *International Journal of Research and Review,*

2(3), 110. Retrieved from www.ijrrjournal.com

Li, F., Clarke, N., Papadaki, M., & Dowland, P. (2011). Behaviour profiling for transparent authentication for mobile devices. *10th European Conference on Information Warfare and Security 2011, ECIW 2011*, 307–314. ISBN: 978-162276536-2.

Li, W., Li, H., Chen, H., & Xia, Y. (2015). AdAttester: Secure online mobile advertisement attestation using TrustZone. *MobiSys 2015 - Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, 75–88. https://doi.org/10.1145/2742647.2742676

Liu, B., Nath, S., Govindan, R., & Liu, J. (2014). DeCAF: Detecting and characterizing ad fraud in mobile apps. *Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2014*, 57–70. https://doi.org/978-193197109-6

Liu, T., Wang, H., Li, L., Luo, X., Dong, F., Guo, Y., Wang, L., Bissyandé, T., Klein, J. (2020). MadDroid: Characterizing and detecting devious ad contents for Android apps. *The Web Conference 2020 - Proceedings of the World Wide Web Conference, WWW 2020*, 1715–1726. https://doi.org/10.1145/3366423.3380242

Mamidi, K. K., Muppavaram, K., Gotlur, K., Govathoti, S., Vafaeva, K. M., Saxena, A. K., & Shnain, A. H. (2024). Investigation of cyber attacks using post-installation app detection method. *Cogent Engineering, 11*(1). https://doi.org/10.1080/23311916.2024.2411859

Muria, R. M. (2023). Fraud detection credit card: A bibliometric analysis approach. *International Journal of Economics, 5*, 391–398. https://doi.org/10.47353/ijema.v1i5.69

Ndibwile, J. D., Kadobayashi, Y., & Fall, D. (2017). UnPhishMe: Phishing attack detection by deceptive login simulation through an Android mobile app. *Proceedings - 12th Asia Joint Conference on Information Security, AsiaJCIS 2017*, 38–47. https://doi.org/10.1109/AsiaJCIS.2017.19

Polhul, T. D., Yarovyi, A. A., Romaniuk, R., Komada, P., & Askarova, N. (2019). Method of data anomaly detection in the process of mobile applications installation. *Proceedings of SPIE - The International Society for Optical Engineering, 11176*. https://doi.org/10.1117/12.2536855

Polhul, T., & Yarovyi, A. (2019). Development of a method for fraud detection in heterogeneous data during installation of mobile applications. *Eastern-European Journal of Enterprise Technologies, 1*(Feb-97), 65–75. https://doi.org/10.15587/1729-4061.2019.155060

Polhul, T., & Yarovyi, A. (2019). Method of fraudster fingerprint formation during mobile application installations. *Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*, 1099–1103. https://doi.org/10.1109/IDAACS.2019.8924369

Rajendran, S. D., Wahab, S. N., Yeap, S. P., Kamarulzaman, N. H., & Lim, S. A. H. (2023). Nanotechnology in food production: A comprehensive bibliometric analysis using R-package. *Journal of Scientometric Research, 12*(3), 648. https://doi.org/10.5530/jscires.12.3.063

Sharma, R. M., & Agrawal, C. P. (2022). MH-DLdroid: A meta-heuristic and deep learning-based hybrid approach for Android malware detection. *International Journal of Intelligent Engineering and Systems, 15*(4), 425–435. https://doi.org/10.22266/ijies2022.0831.38

Shi, C., Song, R., Qi, X., Song, Y., Xiao, B., & Lu, S. (2020). ClickGuard: Exposing hidden click fraud via mobile sensor side-channel analysis. *IEEE International Conference on Communications*, 10. https://doi.org/10.1109/ICC40277.2020.9149420

Swarnkar, R., Harikrishnan, R., & Singh, M. (2022). Analysis of electric vehicle battery state estimation using Scopus and Web of Science databases from 2000 to 2021: A bibliometric study. *World Electric Vehicle Journal, 13*(8). https://doi.org/10.3390/wevj13080157

Trinh Thi Phuong, T., et al. (2022). Research on the application of ICT in mathematics education: Bibliometric analysis of scientific bibliography from the Scopus database. *Cogent Education, 9*(1). https://doi.org/10.1080/2331186X.2022.2084956

Xu, M., Fu, Y., & Tian, B. (2023). An ensemble fraud detection approach for online loans based on application usage patterns. *Journal of Intelligent and Fuzzy Systems, 44*(5), 7181–7194. https://doi.org/10.3233/JIFS-222405

Y.G. Tamboli, M., & Satarkar, P. P. A. (2015). Discovery of ranking fraud for mobile apps. *IEEE Transactions on Knowledge and Data Engineering, 27*(1), 74–87. https://doi.org/10.1109/TKDE.2014.2320733

Yang, K. H., & Thoo, A. C. (2022). An exploration of trends and future directions in sustainability performance: A bibliometric analysis of the Scopus database. *F1000Research, 11*, 864. https://doi.org/10.12688/f1000research.121838.1

Zhu, H., Liu, C., Ge, Y., Xiong, H., & Chen, E. (2015). Popularity modeling for mobile apps: A sequential approach. *IEEE Transactions on Cybernetics, 45*(7), 1303–1314. https://doi.org/10.1109/TCYB.2014.2349954