

Research Article

Mapping the Evolving Landscape of Ransomware Research: A Bibliometric Analysis for Cybersecurity Advancements

Fauzi Adi Rafrastara^{1,*}, , Pulung Nurtantio Andono^{1,*}, , Purwanto¹, , Pujiono², , Deshinta Arrova Dewi², , Mohd. Faizal Abdollah³, 

¹ Faculty of Computer Science, Universitas Dian Nuswantoro, 50231, Indonesia

² Faculty of Data Science and Information Technology, INTI International University, 71800, Malaysia

³ Faculty of Artificial Intelligence and Cyber Security, Universiti Teknikal Malaysia Melaka, Malaysia

ARTICLE INFO

Article History

Received 13 Jul 2026

Revised 22 Aug 2026

Accepted 19 Sep 2026

Published 23 Oct 2026

Keywords

Ransomware,
Bibliometric Analysis,
Cybercrime,
Research Trends,
Artificial Intelligence.



ABSTRACT

Ransomware is a critical cybersecurity threat that disrupts healthcare, finance, and government by encrypting data and demanding ransom. Although narrative and systematic reviews have examined ransomware from technical, sector-specific, and legal perspectives, quantitative bibliometric mapping remains scarce, and existing studies cover shorter periods and fewer analytical techniques. This study addresses that gap through a bibliometric analysis of 1,386 ransomware-related publications indexed in Scopus from 2007 to 2024, using Scopus, BiblioMagika, VOSviewer, Publish or Perish, and Bibliometrix. It examines publication trends, leading authors, institutions, countries, thematic clusters, and collaboration patterns. Results show a sharp rise in output since 2017, though only seven researchers have published ten or more papers on the topic. Keyword and thematic-map patterns point to early detection techniques, deep learning, data breach analysis, convolutional neural networks, feature selection, machine learning, and artificial intelligence as areas of growing activity, consistent with a shift toward proactive and intelligent defense mechanisms. By mapping the intellectual structure and evolution of ransomware research, this study offers insights for cybersecurity professionals, academics, and policymakers seeking to understand current trends, anticipate future challenges, and design more effective mitigation strategies.

1. INTRODUCTION

In today's digital era, we are immersed in a continuous stream of data, created, stored, and shared every second [1]. While these technological advancements offer tremendous opportunities for progress, they also open the door to increasingly complex cyber threats. These dangers extend far beyond personal devices, reaching critical infrastructures such as public utilities, corporate networks, and consumer-integrated healthcare devices, where a successful intrusion can disrupt operations and directly jeopardize patient safety [2]. Prevalent threats in this landscape include denial-of-service (DoS), distributed denial-of-service (DDoS), and man-in-the-middle (MitM) attacks, but ransomware stands out as the most alarming [2], [3]. Reported increases of over 50% in ransomware assaults on consumer-integrated healthcare devices illustrate how quickly this threat has escalated [4]. Its ability to inflict severe financial losses and paralyze operations in an instant makes it a persistent and destructive force in the cybersecurity landscape.

Ransomware is a malicious program that has recently become very popular due to its devastating power. This software can cripple various vital facilities, stop businesses, and even uncover private data. Several cases, such as the Colonial Pipeline ransomware attack, show just how severe the damage and losses incurred by ransomware can be [5], [6]. Given that we are currently highly dependent on data, it's crucial for us to understand how ransomware works and its impact, so we can be more careful and prepare better protection [7].

Ransomware, a malicious software designed to lock files or systems for ransom, has surged dramatically, not just in its sophistication but also in the frequency of its attacks [8], [9], [10]. The facts show that the impact of ransomware incidents like the WannaCry attack in 2017 crippled over 200,000 computers across more than 150 countries [11]. More recently, the Colonial Pipeline incident in 2021 caused widespread fuel shortages in the United States [12], exposing the vulnerability of critical infrastructure to cyberattacks.

*Corresponding author. Email: pulung@dsn.dinus.ac.id

The 2021 ransomware attack on the Irish Health Service Executive (HSE) caused chaos, severely disrupting healthcare services and sparking a nationwide public sector crisis [13]. The attack on the HSE server permeated every aspect of healthcare service from outpatient appointments, radiological and laboratory investigations, and result reporting to electronic patient records and personal data including contact information and online communication methods, even compromising secure and confidential HSE email servers. More strikingly, in late 2023, the Xfinity data breach, linked to a widespread vulnerability (CVE-2023-4966) in Citrix technology, exposed the data of nearly 36 million people [2]. These incidents vividly illustrate ransomware's disruptive potential and the dire consequences it imposes on both individuals and organizations.

Fortunately, the battle against ransomware is also evolving right alongside the threat. Technological innovation has paved the way for far more robust and sophisticated ransomware detection and prevention mechanisms. A significant amount of research has focused on artificial intelligence-based solutions, particularly machine and deep learning algorithms, to predict and identify ransomware activities in real-time [2], [14], [15], [16]. Additionally, extensive research has explored the use of blockchain technology to secure data transactions and prevent unauthorized access. As we move forward, ongoing research and innovation are essential to staying ahead of this persistent and ever-evolving threat.

While technical efforts have advanced significantly including detection systems, mitigation strategies, and encryption mechanisms, non-technical studies tend to rely heavily on Systematic Literature Reviews (SLRs) to explore conceptual developments. However, relatively few have utilized bibliometric methods to systematically map the intellectual structure, influential contributions, and thematic evolution within the ransomware research domain—a gap this study seeks to address. The lack of bibliometric exploration leaves critical questions unanswered: How has the field evolved? Who are the central contributors shaping it? What are the dominant clusters of knowledge, and where are the underexplored areas? Unlike conventional reviews, bibliometric analysis provides quantitative insights into citation patterns, author collaboration, and conceptual trends at scale.

Leveraging these strengths, this study presents a comprehensive bibliometric and network analysis of ransomware research indexed in Scopus, from its inception to 2024. It identifies key research trends and emerging themes, leading contributors, high-impact publication venues, and foundational works that have shaped the field—while simultaneously uncovering literature gaps that point to new directions in ransomware research.

Specifically, this study seeks to answer the following research questions:

1. What is the current landscape of research on ransomware?
2. What new trends are appearing in ransomware research?
3. Who are the key contributors driving progress in ransomware research?
4. What are the main publications that serve as leading platform for disseminating high-impact ransomware research?
5. What seminal works have shaped the trajectory and key discussions within ransomware research?
6. What are the main research themes that characterize the development and expansion of ransomware studies, and how do these themes suggest future research directions in this field?

The importance of this analysis extends beyond documenting the historical progression of ransomware studies; it also reveals key influences and future research paths, thereby supporting future scholarly work and industry advancements in our data-driven world.

The key contributions of this study are fourfold. First, it provides the most temporally extensive bibliometric mapping of ransomware research to date, spanning the entire period available in Scopus at the time of retrieval (2007–2024), compared with the narrower 2013–2023 window covered by the only prior ransomware-specific bibliometric study [17]. Second, it extends the analytical scope beyond conventional performance metrics (publication trends, key authors, institutions, countries, and publishers) to include an overall publication-landscape overview, an author-keyword co-occurrence network, and a thematic map, none of which were reported in [17]. Third, it cross-validates the reported indicators across five complementary tools (Scopus, BiblioMagika, Publish or Perish, VOSviewer, and Bibliometrix) to improve reliability. Fourth, by explicitly linking the identified thematic clusters (e.g., early detection, deep learning, and feature selection) to concrete future research directions, this study offers actionable guidance for researchers, practitioners, and policymakers seeking to anticipate the next phase of ransomware research.

2. LITERATURE REVIEW

As discussed previously, this form of malicious software, known as ransomware, prevents users from accessing their computer system or data unless a payment is made. [8], [9]. The victim must adhere to the instructions provided in the ransom note to make a Bitcoin payment in order to decrypt and regain access to the original files. Attackers use Bitcoin because transactions are pseudonymous, making it difficult to trace the recipient [2].

Ransomware attacks typically begin with the distribution of malicious files through various methods [18]. These files are often spread via drive-by downloads, where users inadvertently download malware by visiting compromised websites, as well as through phishing emails that trick recipients into clicking malicious links or attachments [15], [16]. Additionally, attackers exploit vulnerabilities in internet-accessible systems and strategically compromise web servers to distribute ransomware [6], [18].

Ransomware can be categorized into three main types, as shown in Figure 1 as adapted from [11]: Scareware, Locker, and Crypto. Scareware is designed to intimidate users into paying a ransom by displaying fake warnings or alerts. Locker is a more aggressive form that locks victims out of their entire device or screen, denying access until a ransom is paid, but unlike crypto ransomware, it does not encrypt files. Crypto ransomware focuses on encrypting valuable data, making it inaccessible until a ransom is paid [19]. Additionally, Crypto ransomware can be further categorized into Symmetrical, Asymmetrical, and Hybrid encryption methods. Symmetrical encryption uses the same key for both encryption and decryption, while Asymmetrical encryption employs a pair of public and private keys. Hybrid encryption combines both methods to enhance security.

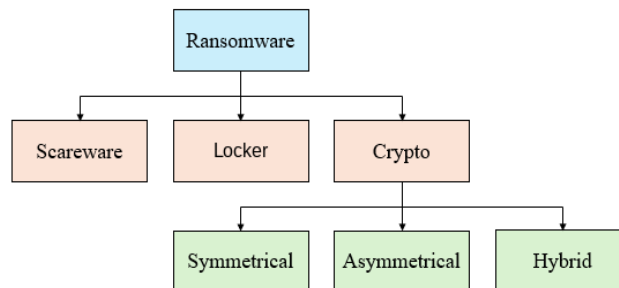


Fig. 1. Types of ransomware [11]

Regarding the ransomware life cycle, researchers in [3] explained that it consists of six phases as illustrated in Figure 2. It begins with distribution, where ransomware files are spread through vectors like phishing emails and drive-by downloads. This is followed by the infection phase, where the malicious payload is executed. The ransomware then enters the communication phase, establishing a connection with a command-and-control server. Next is the file search phase, where the ransomware scans the system for valuable files to encrypt. In the encryption phase, it uses algorithms to encrypt these files, rendering them inaccessible. Finally, the ransom demand phase involves presenting the victim with instructions to pay a ransom, typically in cryptocurrency, to regain access to their files. This organized process shows the clear steps ransomware takes to compromise target systems.

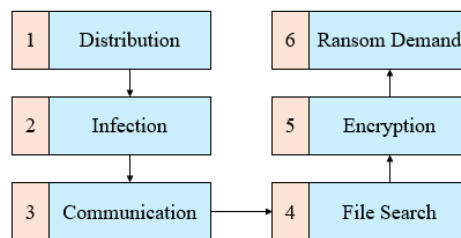


Fig. 2. Ransomware life cycle [3]

A deeper understanding of ransomware attack complexities emerges with the help of a detailed taxonomy provided in [7]. This work breaks down different elements into four main categories: Target, Infection, Communication, and Harmful Action, illustrated in Figure 3. This structure genuinely helps us make sense of how ransomware functions and the different tactics it uses to infect and harm computer systems.

The Target category is the target of ransomware attacks, which is divided into 2 subcategories. The first, Platforms, covers devices and systems like PCs, workstations, mobile devices, and IoT/CPS. The second, Victims, refers to the specific entities targeted, such as end-users or particular organizations. The Infection category, which comes next, describes the various tactics used to get ransomware onto systems, including common ones like phishing emails, malicious applications, and even drive-by downloads. Whereas vulnerabilities are security gaps in the system that can be exploited by hackers to infect devices with ransomware.

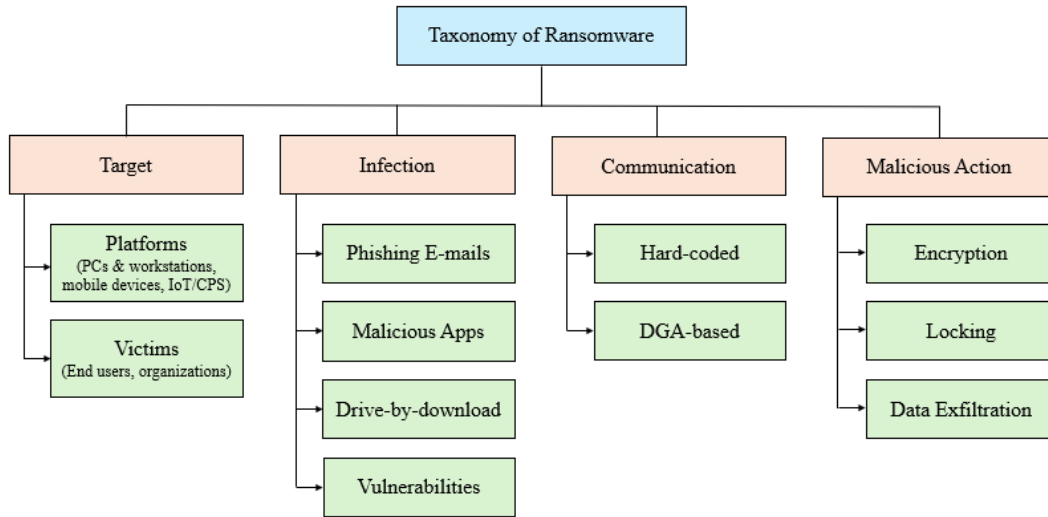


Fig. 3. Taxonomy of ransomware [7]

The third category, Communication, explains how ransomware interacts with command-and-control servers, either using hard-coded domains or Domain Generation Algorithms (DGA) to evade detection. Finally, the Malicious Action category outlines the harmful activities carried out by ransomware after infection, such as data encryption, system locking, and data exfiltration—tactics designed to pressure victims into paying a ransom. This taxonomy provides a structured approach to understanding ransomware operations, aiding cybersecurity professionals in developing effective prevention and response strategies [7].

Research on ransomware identified in the Scopus database began in 2007 with the study titled ‘Awareness Education as the Key to Ransomware Prevention’ [20]. In this study, Luo and Liao proposed a framework comprising four steps to proactively prevent ransomware threats. The steps include policy/ procedure/regulation, access control & management, exposure analysis & reporting, and finally, awareness education & training. This awareness needs to be comprehended by management, IT staff, and end-users alike.

Subsequent publications on ransomware detection began to emerge in 2014 and 2015, where expert system-based detection, dynamic analysis, and static analysis started to be developed [21], [22]. Authors in [21] discussed an expert system that authorizes processes based on administrator approval using hash codes generated by the MD5 algorithm. This system enhances data and information security by detecting and preventing ransomware attacks and other malware, while also improving operating system performance by limiting CPU usage and resource utilization. Whereas the researchers in [22] discussed the detection of ransomware on mobile devices using a combined approach of static and dynamic analysis. This method enhances mobile security by detecting and analyzing ransomware behavior to understand its attack principles comprehensively. Since then, the number of studies on ransomware has significantly increased, peaking in 2024 with 284 publications on Scopus.

Over the past five years, numerous studies examining ransomware trends and developments have been released in various publications. These studies extensively cover a wide array of critical areas and platforms, as detailed in Table I. These reviews also strive to equip researchers and practitioners with meaningful insights that can inform the development of more resilient and adaptive defense strategies. Ideally, the recommendations offered will help guide future efforts in tackling the increasingly complex landscape of ransomware threats.

TABLE I. OVERVIEW OF RANSOMWARE SURVEY PUBLICATIONS BY RESEARCH AREA

No.	Research Area	Referenced Publications
1.	Healthcare	[23], [24], [25]
2.	Food Supply Chains	[26]
3.	Internet of Things (IoT)	[3], [27], [28], [29]
4.	Prevention and Detection Methods	[2], [14], [15], [16], [28], [30], [31], [32], [33], [34], [35], [36]
5.	Android Operating Systems	[5]

Recent studies have drawn attention to the increasing threat of ransomware attacks targeting healthcare institutions, with serious consequences for patient care, data integrity, and operational continuity. For instance, researchers in [23] examine how ransomware tactics have evolved over time, calling for more customized detection approaches and the use of

frameworks like MITRE ATT&CK to better anticipate attacker behavior. Meanwhile, study [24] analyzes ransomware incidents in U.S. hospitals between 2016 and 2022, highlighting recurring vulnerabilities such as compromised patient records and service disruptions. The findings point to an urgent need for stronger security protocols and sustainable mitigation efforts. Similarly, [25] reports a notable rise in ransomware activity from 2016 to 2021, emphasizing not only the growing sophistication of these attacks but also their tangible impact, ranging from system outages to canceled medical procedures. Taken together, these studies underscore the pressing need for more effective detection, real-time monitoring, and transparent reporting systems to help healthcare organizations stay ahead of this evolving threat.

Ransomware has become an increasingly pressing issue in the food supply chain sector, particularly during the COVID-19 pandemic [26]. One study highlights how the industry's digital vulnerabilities were exposed during this period, calling attention to the urgent need for more resilient food defense strategies. The research also points to the critical role of collaboration between government agencies and private companies in shaping effective cybersecurity governance. These findings offer practical guidance not only for policymakers and industry leaders but also for researchers seeking to better understand the intersection of food security and cyber threats.

Several studies have explored how ransomware can be detected more effectively. For example, researchers in [2] and [33] reviewed methods that use deep learning to spot ransomware activity. These techniques are especially useful because they can recognize complex patterns in large amounts of data. Other researchers, such as those in [11], [16], [28], have focused on detecting ransomware early before it starts encrypting files. Catching it at this stage is important because it gives systems a chance to stop the attack before serious damage is done. This kind of early warning can help prevent data loss, reduce downtime, and limit financial impact. It also gives security teams time to respond and block further threats. Overall, these studies highlight the need for smarter, real-time monitoring tools that can keep up with how ransomware is changing.

Moreover, there is a review paper that discusses the interdisciplinary aspects between technology and law [6]. This study emphasizes the need for an integrated approach to develop effective defense, mitigation, and sanction strategies, proposing guidelines such as defining ransomware as an autonomous offense to address this global cybersecurity challenge.

Most recently, several 2026 studies have continued to advance the technical frontier that this bibliometric analysis independently identifies as an emerging thematic cluster. Barnes and Ghafarian [37] evaluated static, PE-header-based machine learning classifiers for ransomware detection, finding that tree-based ensembles such as XGBoost perform strongly when ransomware and other malware families are structurally distinct, while recommending hybrid static–dynamic pipelines for harder cases. Maghanaki et al. [38] benchmarked a broad set of machine learning and deep learning models for IoT malware detection across eight malware categories including ransomware, reinforcing the centrality of ML/DL techniques already highlighted in our keyword co-occurrence network. These 2026 contributions confirm that the field continues to move quickly, further motivating the need for an up-to-date bibliometric account such as the one presented here.

Table II summarizes the methodology, advantages, and limitations of the literature discussed above, grouped by methodological family (domain-specific narrative reviews, ransomware/malware detection surveys, prior bibliometric/scientometric studies, recent 2026 empirical studies, and the present study), to make explicit how this study's scope and methodology relate to, and extend beyond, the existing literature.

Despite numerous review papers available on ransomware, bibliometric analysis specifically focusing on this threat has been scarce until very recently. Bibliometric analysis and traditional surveys or reviews differ significantly: bibliometric analysis involves a quantitative evaluation of academic literature to identify key research trends, influential authors, and knowledge gaps, while surveys or reviews are typically qualitative, summarizing findings and offering critical assessments.

A recent and notable exception is the work by [17]. Their study delves into 1,200 publications from the WoS Core Collection, covering articles from 2013 to 2023. Mohanty et al. examined crucial aspects like publication trends, key authors, institutions, countries, publishers, highly cited documents, and research themes.

Beyond this, broader bibliometric studies have been conducted on malware in general [39], [40]. For instance, one study [40] analyzed over 4,000 articles from the ISI Web of Science between 2005 and 2015. It focused on the geographical spread of research activities, highlighting significant contributions from Asia. This research broke down articles, citations, research areas, keywords, institutions, and authors, even classifying terms for malware detection systems. Another project [39] specifically tackled Android malware, reviewing 5,622 Web of Science articles from 2010 to 2019. After filtering, 1,278 articles were analyzed. This study mapped the academic scene, assessing productivity, research areas, Web of Science categories, authors, most-cited articles, institutions, and impactful journals. Both of these broader studies consistently showed the dominant role of Asian researchers and institutions in malware research.

TABLE II. SUMMARY OF METHODOLOGY, ADVANTAGES, AND LIMITATIONS OF REVIEWED RANSOMWARE LITERATURE, GROUPED BY METHODOLOGICAL APPROACH.

Ref.	Study Focus (Year)	Methodology	Advantages	Limitations
[13],[23],[24],[25]	Healthcare-sector ransomware (2022–2024)	Narrative / thematic review	Sector-specific empirical detail; links attacker behavior to frameworks such as MITRE ATT&CK	Qualitative only; single sector; no citation-impact or authorship mapping
[26]	Food-supply-chain ransomware (2023)	Qualitative case discussion	Novel sector angle; highlights public–private governance gaps	Single-sector scope; no systematic search protocol reported
[3],[27],[28],[29]	IoT / IIoT / cyber-physical-systems ransomware	Narrative technical review / taxonomy	Deep technical taxonomy of IoT-specific attack surfaces and mitigations	No bibliometric mapping of the literature itself; taxonomies not cross-validated across tools
[2], [14], [15], [16], [28], [30], [31], [32], [33], [34], [35], [36]	Ransomware/malware detection methods (ML, DL, dynamic/static analysis)	Narrative review / SLR	Deep technical synthesis of detection techniques and datasets	Narrow technical scope; do not map authorship, collaboration, or thematic structure at field scale
[6]	Legal–technical interdisciplinary analysis (2022)	Conceptual / legal analysis	Rare integration of legal and technical perspectives; proposes policy guidelines	Non-quantitative; single-perspective; not literature-wide
[17]	Ransomware scientometric analysis, WoS 2013–2023 (2024)	Bibliometric / scientometric	First ransomware-specific bibliometric study; covers authors, institutions, countries, and themes	Shorter window (2013–2023); WoS only; no co-occurrence network, thematic map, or publication-landscape overview
[39]	Android-malware bibliometric analysis, WoS 2010–2019 (2021)	Bibliometric	Rigorous productivity/citation mapping; broad WoS coverage	Malware-general (Android), not ransomware-specific
[40]	Malware bibliometric analysis, WoS 2005–2015 (2016)	Bibliometric	Early, broad geographic and keyword mapping	Predates the post-2016 ransomware surge; malware-general, not ransomware-specific
[37],[38]	Ransomware ML/DL detection, empirical studies (2026)	Empirical ML/DL evaluation	Reflect the latest (2026) technical advances within the emerging AI-based detection cluster identified in this study (Section 4.8.2)	Technique-specific empirical studies, not literature-mapping studies; reinforce rather than replace the need for bibliometric synthesis
Proposed	Ransomware bibliometric analysis, Scopus 2007–2024	Bibliometric + science mapping (citation, co-citation, co-authorship, co-occurrence, thematic map)	Widest time window to date; multi-tool cross-validation; adds publication-landscape, co-occurrence network, and thematic map absent from [17]	Restricted to Scopus and English-language records; citation-based indicators may undervalue very recent work (Section 4.2)

Building on earlier efforts in malware bibliometric analysis, particularly updating and expanding upon the scope of publication [17], our current study takes an even wider and more current look at ransomware data. This research applies bibliometric analysis to comprehensively explore the ransomware research landscape, encompassing traditional aspects like publication trends, key authors, institutions, countries, publishers, highly cited documents, and research themes. Crucially, we enhance this by including the overall publication landscape, showing how keywords connect in a co-occurrence network, and creating a thematic map. The specific differences between our study and publication [17] are detailed in Table III. This approach, which incorporates citation analysis, will highlight influential works, key contributors, and emerging themes that have shaped the field, not only mapping the current state of research but also pointing to potential directions for future inquiry and offering a clearer understanding of how ransomware studies have evolved over time.

3. METHODS

In recent years, bibliometric methods have gained traction as a way to explore research trends using quantitative techniques like citation analysis. This approach has been especially popular in fields such as business, social sciences, engineering, and computer science, as shown by keyword searches on Scopus. Researchers use bibliometric tools to track keyword patterns,

identify collaborative author networks, and map research activity across countries [41]. These studies help build a clearer picture of how a field is developing, revealing gaps in knowledge and pointing to new research opportunities [42].

TABLE III. SCOPE COMPARISON OF BIBLIOMETRIC ANALYSES ON RANSOMWARE

Studies	[17]	Proposed
Published Year	2024	2026
Covered Year	2013-2023	2007-2024
Publication Landscape	-	✓
Publication Trends	✓	✓
Key Authors	✓	✓
Key Institutions	✓	✓
Key Countries	✓	✓
Key Publishers	✓	✓
Highly Cited Documents	✓	✓
Research Themes	✓	✓
Co-occurrence Network	-	✓
Thematic Map	-	✓

This chapter outlines the methodology used to conduct a bibliometric analysis of ransomware-related literature. Drawing on approaches from [42] and [43], the method was adapted to suit the specific context of ransomware research. It includes a structured search strategy designed to capture a broad range of academic and industry publications. The discussion is divided into two parts: the first explains how the data were collected (Search Strategy), and the second describes the bibliometric techniques and tools used to analyze the dataset (Techniques and Tools).

3.1 Search Strategy

The data for analysis were obtained from the Scopus database, which is recognized for its reliable and comprehensive citation information. The search string employed was “ransomware*”, where the asterisk * was utilized as a wildcard to ensure broad coverage of variations, including “ransomware” and “ransomwares.” This string was applied to document titles and keywords. The time span for the data was before February 2025, and the source types selected included conference proceedings, journal articles, reviews, and books. This search focused on documents written in English only. This query returned a total of 1,424 records retrieved on 1 February 2025. Before analysis, all 1,424 records were screened against explicit eligibility criteria: a record was excluded if it (i) was an exact duplicate across export batches, (ii) had an inaccessible or un retrievable abstract/full metadata entry in Scopus, (iii) was missing bibliographic fields essential for bibliometric processing (e.g., author, year, or source title), or (iv) was not written in English despite matching the search string. Applying these criteria removed 38 records, leaving 1,386 documents that constitute the bibliometric corpus analyzed in this study and exported in RIS and CSV formats. The four criteria were applied together in a single screening pass rather than logged separately, so a per-criterion breakdown of the 38 exclusions is not available; Figure 4 reports them as a single aggregate count. The 1,386-document corpus (processed via BiblioMagika, VOSviewer, Publish or Perish, and Bibliometrix to generate the statistics, networks, and maps in Section 4) is distinct from this manuscript’s own numbered references [1]–[70], which were consulted to write the Introduction and Literature Review and are not a sample of the corpus, though some overlap is expected. This study is classified as a bibliometric analysis rather than a systematic literature review, so Figure 4’s screening constructs the quantitative corpus rather than following a full PRISMA protocol. The corpus is bounded at 2024 because, at the February 2025 retrieval date, that year’s Scopus indexing was still incomplete; early-2025 records were therefore excluded so that every included year (2007–2024) reflects a complete annual count.

These articles served as the foundation to evaluate the existing state of ransomware research. Analyzing these foundational articles allowed us to pinpoint key advancements, existing hurdles, and promising directions in ransomware research. This meticulous process guaranteed our insights were derived directly from cutting-edge primary literature, thus reflecting the most current and crucial findings. The overall process is depicted in Figure 4, with the methodology adapted from [42].

3.2 Techniques and Tools

According to [43], bibliometric analysis consists of two techniques: main techniques and enrichment techniques. The main techniques include performance analysis and science mapping. This research employed both by performing various metrics for performance analysis, including publication-related metrics, citation-related metrics, and a combination of citation-and-publication-related metrics. For science mapping, the research utilized citation analysis, co-citation analysis and co-authorship analysis.

Publication-related metrics include total publications, number of contributing authors, sole-authored publications, co-authored publications, and more. Citation-related metrics encompass total citations and average citations. Citation-and-publication-related metrics cover the number of cited publications, citations per cited publication, h-index, and more.

In science mapping, citation analysis explores the relationships among publications and identifies the most influential publications. Co-citation analysis examines the relationships among cited publications and foundational themes. Co-authorship analysis investigates social interactions and relationships among authors, including their affiliations. Additionally, the research involved enrichment techniques focused on visualizations to facilitate the interpretation of the analyzed data. These visualizations help in presenting complex data in a more accessible and understandable manner.

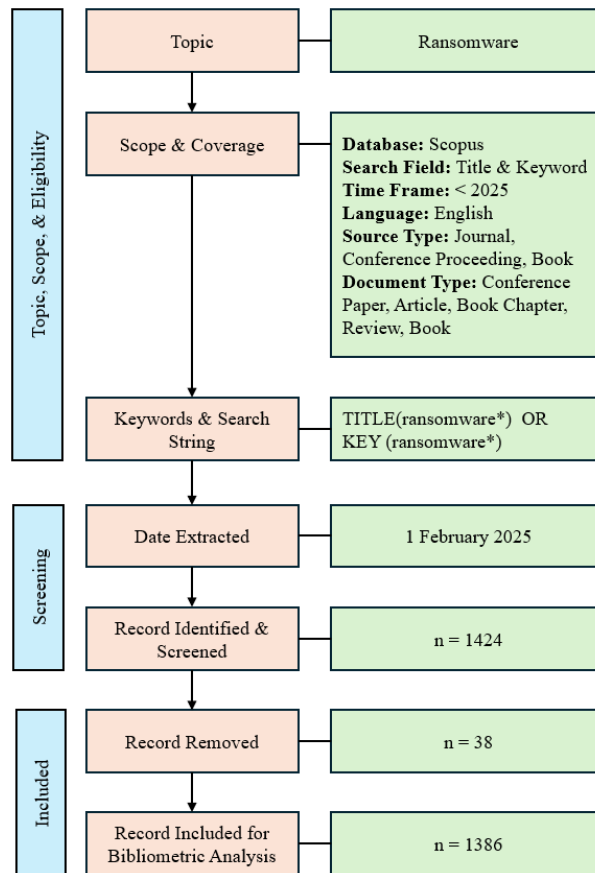


Fig. 4. Flow diagram of the search strategy

To achieve all those metrics and analysis, several tools were used, such as Scopus Website, BiblioMagika, Harzing's Publish or Perish, VOSviewer, iipmaps, and Bibliometrix. Figure 5 illustrates the key tools used in bibliometric analysis and their roles in achieving essential metrics.

The Scopus website [44] was utilized to download the dataset for this bibliometric analysis. By using the "Analyze Results" feature on Scopus Website, we could obtain various visual and tabular information related to the searched publications, such as documents by year, documents per year by source, documents by author, documents by affiliation, and documents by country. Some statistical results, like documents by subject area, documents by type, and documents per year by source, could be directly used. However, for other results, we needed to perform refinement and harmonization processes to ensure more accurate data, particularly regarding author names and affiliations. Therefore, the Scopus website served as a crucial tool for addressing RQ1, RQ2, and RQ3 in this research.

Another tool used in this study is BiblioMagika, developed by Aidi Ahmi from Universiti Utara Malaysia [45]. Built on Microsoft Excel, BiblioMagika is designed to support bibliometric analysis, particularly in tracking publication output and measuring research impact. It also helps streamline the process of cleaning and organizing bibliographic data, which is essential for accurate analysis. In this study, we used BiblioMagika to process raw data retrieved from Scopus, including data cleaning and refinement. This step was crucial to ensure the validity of the results. Without it, inconsistencies such as author name variations due to typos, or institutional names being treated as different entities because of abbreviations (e.g., "University" vs. "Univ."), could lead to misleading conclusions. Given its features and flexibility, BiblioMagika was well-suited for addressing all six research questions (RQ1–RQ6) in this study.

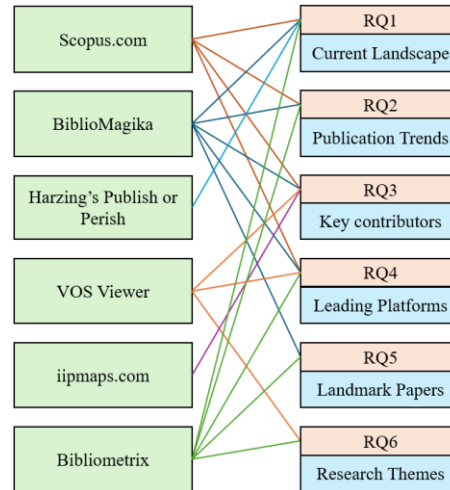


Fig. 5. Tools and Their Contributions to Bibliometric Analysis Metrics

Harzing's Publish or Perish is a widely used software tool for analyzing citation data in academic publications [46]. It supports a variety of data sources and can extract raw bibliographic data, which it then processes into several citation metrics, including the number of publications, total citations, and the h-index. In this study, we used Publish or Perish to gather detailed citation information such as the h-index, g-index, and other author- and paper-level metrics. It also served as a benchmark to compare results from other tools used in this research. Combined with data from Scopus, BiblioMagika, and Bibliometrix, this software was particularly helpful in addressing RQ1, which focuses on mapping the current landscape of ransomware research.

VOSviewer is a software tool commonly used to create and visualize bibliometric networks [47]. These networks help illustrate how journals, authors, or publications are connected through citations, co-authorships, or co-citations. The tool also includes text mining features, which allow it to generate visual maps of key terms found in scientific literature. In this study, we used VOSviewer to produce visualizations that support our analysis for RQ3, RQ4, and RQ6, particularly in identifying research clusters and keyword patterns.

We also used iipmaps.com [48] to support our analysis of global research contributions. This online tool provides country-level visualizations that show how publications and authors are distributed around the world. For our study, it was particularly helpful in answering RQ3, as it allowed us to quickly identify which countries are most active in ransomware research. By using this tool, we gained a clearer picture of regional trends and academic engagement across different parts of the world. The final tool used in this study is Bibliometrix, an R-based package designed for conducting detailed bibliometric analysis [49]. It offers a wide range of features for exploring research trends, identifying influential publications, and mapping collaboration networks. In our research, we used Bibliometrix to help answer RQ1, RQ2, RQ4, RQ5, and RQ6. However, we chose not to use it for RQ3 due to inconsistencies in how some author names were recognized in our dataset. These issues led to discrepancies when compared with results from other tools, particularly in identifying contributors by country.

4. RESULTS

The results section will analyze the ransomware research landscape, addressing the RQs from the introduction. By shedding light on the current status and future outlook of the field, this analysis seeks to benefit scholars, practitioners, and policymakers alike.

4.1 Current Research Landscape

To address RQ1, understanding the current ransomware research landscape, we analyze bibliometric statistics: publication numbers, citation metrics, and distribution by document type, source, and subject area. Table IV presents these metrics, generated using BiblioMagika, Publish or Perish, and Bibliometrix, highlighting the growth of ransomware research.

Ransomware research, tracked by Scopus since 2007, shows significant growth: 1,386 publications by 3,762 authors. While there are 109 single-authored publications, the vast majority (1277) are collaborative works, indicating a highly collaborative field.

The degree of collaboration can be calculated using the specific formula [50], as shown in Equation 1.

$$c = \frac{NM}{NM+NS} \quad (1)$$

Where c , the degree of collaboration, NM is multi-authored and NS is single-authored papers, is 0.92. This high score indicates strong collaboration, reflecting common multi-authorship practices and the pooling of diverse expertise, leading to impactful research, signifying a research community that values shared knowledge and joint effort.

TABLE IV. BASIC INFORMATION AND CITATION METRICS.

Main Information	Data
Publication Years	< 2025: 2007-2024
Total Publications	1,386
Single-author Publications	109
Multi-author Publications	1277
Citable Year	18 (2007-2024)
Number of Contributing Authors	3,762
Number of Cited Papers	1,072
Total Citations	20,136
Citation per Paper	14.53
Citation per Cited Paper	18.78
Citation per Year	1,118.67
Citation per Author	5.35
Author per Paper	2.71
Citation sums within h-Core	13,841
h-index	69
g-index	100
m-index	3.83

The bibliometric indicators reported in Table IV are defined as follows. Citations per year is Total Citations divided by the number of citable years ($20,136 / 18 = 1,118.67$). Citations per author is Total Citations divided by the Number of Contributing Authors ($20,136 / 3,762 = 5.35$). The h-index is the largest number h such that h publications in the dataset have each received at least h citations; an overall h-index of 69 means 69 publications in the corpus have each been cited at least 69 times. The g-index is the largest number g such that the top g publications, ranked by citations, have jointly received at least g^2 citations; a g-index of 100 indicates that the 100 most-cited publications in the corpus have jointly accumulated at least 10,000 citations. The citation sum within the h-core is the total number of citations received by the h most-cited publications (here, the 69 publications defining the h-index), reported in Table IV as 13,841. The m-index, originally proposed by Hirsch to evaluate individual researchers, is defined as the h-index divided by the number of years since the first publication ($m = h / n_{\text{years}}$); applied here at the level of an entire research field for illustrative purposes only, $m = 69 / 18 = 3.83$. Because the m-index was formulated to normalize an individual researcher's h-index for career length rather than to characterize an aggregate research field, this field-level value should be interpreted with caution and is reported for completeness rather than as a primary indicator of ransomware research maturity.

Ransomware studies demonstrate significant impact: 20,136 total citations (14.53 per paper), with 1,072 cited papers averaging 18.78 citations. An annual citation rate of 1,118.67 and 5.35 citations per author indicate broad scholarly recognition. The h-index of 69 and g-index of 100 reflect high quality and influence, while the h-core citation total of 13,841 underscores its established and growing presence in scientific inquiry.

Publication distribution by document type (Table V) reveals that conference papers (678 publications, representing 48.92% of the total) and articles (600 publications, representing 43.29% of the total) are the dominant publication forms. Book chapters, reviews, and books contribute smaller portions, specifically: 56 publications (4.04%), 46 publications (3.32%), and 6 publications (0.43%), respectively.

TABLE V. DOCUMENT TYPE.

Document Type	Total Publications	Percentage (%)
Conference Paper	678	48.92
Article	600	43.29
Book Chapter	56	4.04
Review	46	3.32
Book	6	0.43

In terms of source type, conference proceedings account for the highest number of publications, with 672 entries, representing 48.48% of the total. Journals contribute 652 publications, or 47.04%. Books contribute a smaller portion of the total, with 62 publications, accounting for 4.47% (see Table VI).

TABLE VI. SOURCE TYPE.

Source Type	Total Publications	Percentage (%)
Conference Proceeding	672	48.48
Journal	652	47.04
Book	62	4.47

Statistics related to subject areas can illustrate the distribution and focus of ransomware research (see Table VII). Computer Science leads with 1,155 publications, accounting for 83.33% of the total, followed by Engineering with 598 publications (43.15%). Decision Sciences (248 publications, 17.89%) and Social Sciences (226 publications, 16.31%) also contribute significantly.

TABLE VII. SUBJECT AREA.

Subject Area	Total Publications	Percentage (%)
Computer Science	1,155	83.33
Engineering	598	43.15
Decision Sciences	248	17.89
Social Sciences	226	16.31
Mathematics	218	15.73
Medicine	113	8.15
Physics and Astronomy	103	7.43
Business, Management and Accounting	85	6.13
Materials Science	78	5.63
Energy	56	4.04
Economics, Econometrics and Finance	32	2.31
Biochemistry, Genetics and Molecular Biology	30	2.16
Chemistry	26	1.88
Environmental Science	23	1.66
Chemical Engineering	18	1.30
Health Professions	18	1.30
Psychology	16	1.15
Multidisciplinary	10	0.72
Arts and Humanities	6	0.43
Nursing	6	0.43
Earth and Planetary Sciences	5	0.36
Neuroscience	4	0.29
Agricultural and Biological Sciences	3	0.22
Pharmacology, Toxicology and Pharmaceutics	2	0.14
Dentistry	1	0.07
Immunology and Microbiology	1	0.07

Ransomware research spans diverse disciplines, including Mathematics (218 publications, representing 15.73% of the total) and Business (85 publications, representing 6.13%), highlighting its interdisciplinary nature. Its impact extends to Medicine (113, 8.15%), Physics (103, 7.43%), and Environmental Science (23, 1.66%). This diversity shows ransomware impacts multiple sectors.

This analysis (RQ1) reveals a diverse, interdisciplinary ransomware research landscape. Key findings include significant publication in conferences and journals, with contributions from engineering, computer science, decision science, and medicine. It underscores the need for cross-disciplinary collaboration to combat ransomware.

4.2 Publication Trends

This section addresses RQ2, focusing on emerging trends in ransomware publications by examining publication and citation patterns (Figure 6). From 2007 to 2015, ransomware publications indexed in Scopus remained relatively low, with publications not exceeding 6 per year and citations not surpassing 152. However, a notable surge in both publications and citations occurred from 2016 onwards. Within this period, citations peaked in 2018 at 3,576 (a year in which 118 publications were recorded), whereas publication output kept climbing well beyond that point, reaching its own separate peak of 284 publications in 2024. By 2024, annual citations had declined to 317 even as publications continued to rise; as discussed below, this divergence is best explained by a citation-age effect rather than a genuine shift in the field's impact.

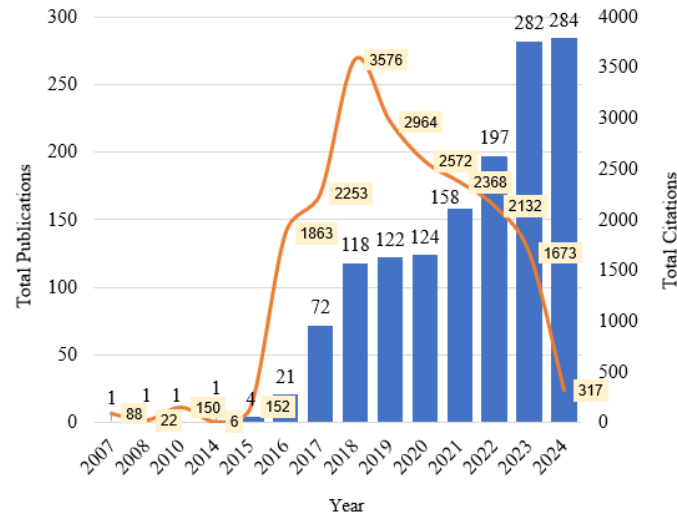


Fig. 6. Total publications and citation by year.

This chart highlights distinct trends in publications and citations over time. While the number of publications has shown a consistent upward trajectory since 2015, reflecting growing interest and investment in ransomware research, the number of citations has been more volatile, peaking in 2018 before declining in raw terms through 2024. However, raw annual citation counts are not directly comparable across publication years, because older papers have simply had more time to accumulate citations; a paper published in 2018 has had up to six additional years to be cited relative to one published in 2024. Consequently, the apparent post-2018 decline in aggregate citations is expected under normal citation accumulation dynamics and should not, by itself, be read as evidence that recent ransomware research is less impactful or that the field has matured with fewer breakthrough contributions.

To test this age-adjustment explanation directly, Table VIII reports citations per year since publication (C/Y) for the corpus's most highly cited individual papers, rather than raw totals alone. Several papers published well after 2018 show C/Y rates comparable to or higher than the earliest landmark works: Gopinath and Sethuraman (2023) [51] average 45.33 citations per year and Oz et al. (2022) [7] average 32.00; the former exceeds, and the latter is comparable to, the 35.40 C/Y of Scaife et al. (2016) [52], the corpus's highest raw-citation paper. This indicates that recent ransomware research continues to be highly influential once publication age is accounted for, and that the raw decline in aggregate annual citations after 2018 is better read as a citation-window (age) artifact of recent publications not yet having had time to accumulate citations, rather than as direct evidence of declining research impact or quality.

Figure 7 presents the graph of the number of single-author and multi-author publications for each year from 2007 to 2024. From the graph, it is evident that the number of single-author publications is always significantly lower than that of multi-author publications each year.

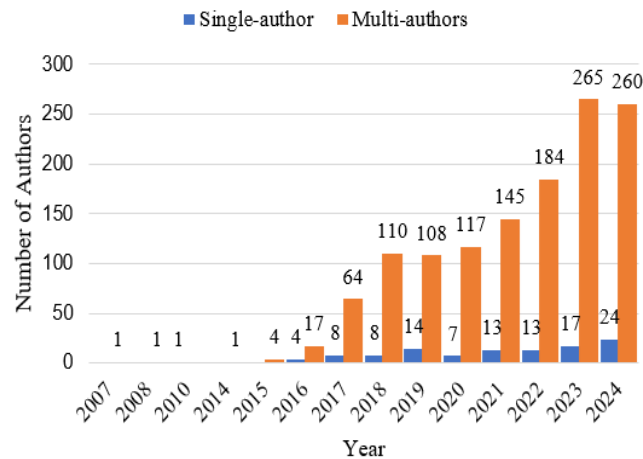


Fig. 7. Single Author vs. Multi Authors.

TABLE VIII. TOP 20 HIGHLY CITED ARTICLES.

No.	Author(s)	Title	TC	C/Y
1	Scaife et al (2016) [52]	CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data	354	35.40
2	Kharraz et al. (2016) [53]	Unveil: A large-scale, automated approach to detecting ransomware	347	34.70
3	Al-Rimy et al. (2018) [54]	Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions	285	35.63
4	Kruse et al. (2017) [55]	Cybersecurity in healthcare: A systematic review of modern threats and trends	254	28.22
5	Continella et al. (2016) [56]	ShieldFS: A self-healing, ransomware-aware file system	226	22.60
6	Zhang et al. (2019) [57]	Classification of ransomware families with machine learning based on N-gram of opcodes	218	31.14
7	Yaqoob et al. (2017) [58]	The rise of ransomware and emerging security challenges in the Internet of Things	217	24.11
8	Azmoodeh and Dehghantanha (2018) [59]	Detecting crypto-ransomware in IoT networks based on energy consumption footprint	203	25.38
9	Kolodinker et al. (2017) [60]	PayBreak : Defense against cryptographic ransomware	183	20.33
10	Singh and Singh J. (2021) [61]	A survey on machine learning-based malware detection in executable files	163	32.60
11	Chen and Bridges (2017) [62]	Automated behavioral analysis of malware: A case study of wannacry ransomware	159	17.67
12	Huang et al. (2018) [63]	Tracking Ransomware End-to-end	155	19.38
13	Gazet A. (2010) [64]	Comparative analysis of various ransomware virii	150	9.38
14	Chen et al. (2018) [65]	Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection	140	17.50
15	Liao et al. (2016) [66]	Behind closed doors: Measurement and analysis of CryptoLocker ransoms in Bitcoin	140	14.00
16	Gopinath and Sethuraman (2023) [51]	A comprehensive survey on deep learning based malware detection techniques	136	45.33
17	Oz et al. (2022) [7]	A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions	128	32.00
18	Paquet-Clouston et al. (2019) [67]	Ransomware payments in the Bitcoin ecosystem	128	18.29
19	Almashhadani et al. (2019) [68]	A Multi-Classifer Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware	128	18.29
20	Cabaj et al. (2018) [69]	Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics	126	15.75

Note: TC=total citations; C/Y=citations per year.

The highest number of single-author publications occurred in 2024, with 24 publications. Conversely, the highest number of multi-author publications occurred in 2023, with 265 publications, surpassing the 2024 count by 5 publications. The degree of collaboration, calculated in the previous section, yielded a score of 0.92, indicating a very high level of collaboration among researchers. Analyzing this data reveals that collaborative efforts in research are increasingly favored and lead to a higher output of publications. This trend highlights the importance of teamwork and shared knowledge in advancing scientific and academic fields.

To observe the distribution of author contributions in ransomware-related research, Lotka's law can be utilized [70]. Lotka's law is a statistical distribution that describes the frequency of publication by authors in a given field. Figure 8 illustrates the proportion of authors (blue line) in relation to Lotka's law, specifically in the context of ransomware-related research, while the details of the statistics regarding the frequency of publication by authors are shown in Table IX.

The majority of authors (83.07%) have written only one document, as shown by the blue line. Author percentage sharply declines with increasing authored documents. This trend closely follows Lotka's law (orange line), where authors with 'n' documents are approximately $1/n^2$ of single-document authors, demonstrating the law's applicability in modeling scientific collaboration.

In summary, the steady rise in publications underscores the increasing importance and attention given to ransomware research, while the fluctuating citation trends reflect the varying impact and relevance of the studies over time. These patterns illustrate the dynamic nature of the field, where the volume of research and its influence do not always align linearly.

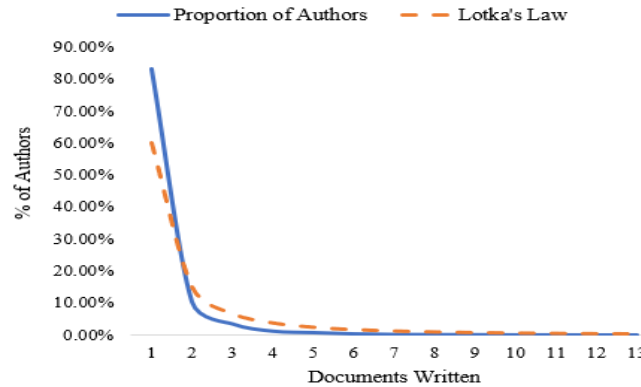


Fig. 8. Proportion of Authors vs. Lotka's Law.

TABLE IX. FREQUENCY OF PUBLICATION BY AUTHORS.

Document Written	N. of Authors	Proportion of Authors
1	3125	83.07%
2	393	10.45%
3	132	3.51%
4	46	1.22%
5	29	0.77%
6	14	0.37%
7	7	0.19%
8	5	0.13%
9	4	0.11%
10	3	0.08%
11	2	0.05%
12	1	0.03%
13	1	0.03%
Grand Total	3762	100.00%

4.3 Key Contributors (Authors)

This section addresses RQ3 by identifying productive and influential researchers in the field of ransomware. Recognizing their contributions helps reveal key collaborators, thought leaders, and emerging trends that are important for guiding future research and innovation. Highlighting these individuals also brings attention to areas of expertise and potential collaboration opportunities within the ransomware research community, contributing to a more connected and impactful scholarly network.

The analysis includes not only Total Publications (TP) but also additional citation-based metrics such as the Number of Cited Publications (NCP), Total Citations (TC), Average Citations per Publication (C/P), Average Citations per Cited Publication (C/CP), as well as the h-index, g-index, and m-index. These indicators collectively provide a comprehensive view of a researcher's academic influence and productivity. All scores were initially retrieved from the Scopus database and subsequently refined using BiblioMagika. The results are presented in Table X and Table XI.

For clarity, TP refers to the total number of publications authored by a researcher. NCP indicates how many of those works have been cited at least once. TC represents the total number of citations received. C/P is calculated by dividing total citations by total publications, while C/CP reflects the average number of citations for only the cited works, offering insight into the impact of a researcher's most recognized contributions.

The h-index measures both the productivity and citation impact of a researcher's publications, where an h-index of 'n' indicates the researcher has 'n' papers each cited at least 'n' times. In contrast, the g-index focuses on the distribution of citations received by a researcher's publications, emphasizing the impact of highly cited papers; a g-index of 'n' signifies the top 'n' articles together have at least 'n²' citations. It considers the cumulative impact of a researcher's publications. Lastly, the m-index is calculated by dividing the h-index by the number of years the researcher has been active, offering an annualized measure of their impact.

Bander Ali Saleh Al-Rimy (Universiti Teknologi Malaysia) leads with 13 publications (h-index 11). Nitin Naik (Aston University) and Paul Jenkins (University of Portsmouth) follow with 12 and 11 publications, respectively, each also having an h-index of 11. An h-index of 11 signifies that each researcher has at least 11 papers that have each been cited at least 11 times, reflecting their significant research impact and quality within the field of ransomware. These researchers are key contributors to ransomware research (Table X).

TABLE X. MOST PRODUCTIVE AUTHORS WITH OVER 7 PUBLICATIONS & MOST INFLUENTIAL AUTHORS WITH G-INDEX ABOVE 7.

Full Name	Affiliation	Country	TP	NCP	TC	C/P	C/CP	h	g	m
Al-Rimy, Bander Ali Saleh	Universiti Teknologi Malaysia	Malaysia	13	12	809	62.23	67.42	11	13	1.375
Naik, Nitin	Aston University	United Kingdom	12	12	181	15.08	15.08	11	12	1.571
Jenkins, Paul	University of Portsmouth	United Kingdom	11	11	179	16.27	16.27	11	11	1.571
Hernandez-Castro, Julio	University of Kent	United Kingdom	11	11	134	12.18	12.18	7	11	0.875
Mercaldo, Francesco	University of Molise	Italy	10	10	561	56.10	56.10	7	10	0.700
Cartwright, Edward	De Montfort University	United Kingdom	10	10	139	13.90	13.90	6	10	0.857
Cartwright, Anna	De Montfort University	United Kingdom	10	10	139	13.90	13.90	6	10	0.857
Savage, Nick	University of Portsmouth	United Kingdom	9	9	147	16.33	16.33	9	9	1.286
Maarof, Mohd Aizaini	Universiti Teknologi Malaysia	Malaysia	9	9	595	66.11	66.11	7	9	0.875
Almomani, Iman	University of Jordan	Jordan	9	9	276	30.67	30.67	9	9	1.286
Sheldon, Frederick T.	University of Idaho	United States	9	9	135	15.00	15.00	6	9	1.000
Yang, Longzhi	Northumbria University	United Kingdom	8	8	128	16.00	16.00	8	8	1.143
Davies, Simon R.	Edinburgh Napier University	United Kingdom	8	6	84	10.50	14.00	5	8	0.833
Bajpai, Pranshu	Michigan State University	United States	8	8	116	14.50	14.50	6	8	0.750
Macfarlane, Richard	Edinburgh Napier University	United Kingdom	8	6	84	10.50	14.00	5	8	0.833
Enbody, Richard	Michigan State University	United States	8	8	116	14.50	14.50	6	8	0.750

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

TABLE XI. MOST INFLUENTIAL AUTHORS WITH OVER 300 CITATION.

Full Name	Affiliation	Country	TP	NCP	TC	C/P	C/CP	h	g	m
Al-Rimy, Bander Ali Saleh	Universiti Teknologi Malaysia	Malaysia	13	12	809	62.23	67.42	11	13	1.375
Maarof, Mohd Aizaini	Universiti Teknologi Malaysia	Malaysia	9	9	595	66.11	66.11	7	9	0.875
Mercaldo, Francesco	University of Molise	Italy	10	10	561	56.10	56.10	7	10	0.700
Shaïd, Syed Zainudeen Mohd	Universiti Teknologi Malaysia	Malaysia	5	5	513	102.60	102.60	5	5	0.625
Dehghantanha, Ali	University of Salford	United Kingdom	4	4	506	126.50	126.50	4	4	0.500
Martinelli, Fabio	Consiglio Nazionale delle Ricerche	Italy	7	7	423	60.43	60.43	5	7	0.556
Jhanjhi, N.Z.	Taylor's University	Malaysia	7	7	389	55.57	55.57	7	7	1.000
Conti, Mauro	University of Padua	Italy	3	3	378	126.00	126.00	3	3	0.375
Kirda, Engin	Northeastern University	United States	2	2	377	188.50	188.50	2	2	0.200
Robertson, William	Northeastern University	United States	2	2	377	188.50	188.50	2	2	0.200
Kharraz, Amin	University of Illinois Urbana-Champaign	United States	2	2	377	188.50	188.50	2	2	0.200
Scaife, Nolen	University of Colorado Boulder	United States	3	3	373	124.33	124.33	3	3	0.300
Traynor, Patrick	University of Florida	United States	2	2	370	185.00	185.00	2	2	0.200
Butler, Kevin	University of Florida	United States	2	2	370	185.00	185.00	2	2	0.200
Carter, Henry	Villanova University	United States	1	1	354	354.00	354.00	1	1	0.100
Arshad, Sajjad	Northeastern University	United States	1	1	347	347.00	347.00	1	1	0.100
Mulliner, Collin	Northeastern University	United States	1	1	347	347.00	347.00	1	1	0.100
Choo, Kim-Kwang Raymond	University of Texas at San Antonio	United States	2	2	324	162.00	162.00	2	2	0.250
Xiao, Xi	Tsinghua University	China	2	2	311	155.50	155.50	2	2	0.286
Sangaiah, Arun Kumar	VIT University	India	2	2	311	155.50	155.50	2	2	0.286

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

Aside from discussing the most productive researchers, this discussion also addresses the most influential researchers, measured by both g-index and total citations. The most influential researchers based on the g-index (particularly those with a g-index of 8 or higher) have the same ranking as the most productive researchers with over 7 publications, as presented in Table X and Table XI. Bander Ali Saleh Al-Rimy ranks first with a g-index score of 13, followed by Nitin Naik with 12, and Paul Jenkins and Julio Hernandez-Castro, each with a g-index of 11.

In terms of total citations, Bander Ali Saleh Al-Rimy has the highest number of citations, totaling 809. The second position is held by Mohd Aizaini Maarof from Universiti Teknologi Malaysia, Malaysia, with a total of 595 citations. Francesco Mercaldo from the University of Molise, Italy, is in the third position with 561 total citations. The most influential authors by total citation can be seen in Table XI.

TABLE XII. CO-AUTHORSHIP NETWORK WITH AUTHORS.

Author Name	TP	TC	TLS
Naik, Nitin	12	181	28
Jenkins, Paul	11	179	28
Savage, Nick	9	147	26
Yang, Longzhi	8	128	24
Cartwright, Anna	10	139	14
Cartwright, Edward	10	139	14
Bajpai, Pranshu	8	116	8
Enbody, Richard	8	116	8
Davies, Simon R.	8	84	8
Macfarlane, Richard	8	84	8
Al-Rimy, Bander Ali Saleh	13	809	7
Maarof, Mohd Aizaini	9	595	7
Hernandez-Castro, Julio	11	134	8
Mercaldo, Francesco	10	561	0
Almomani, Iman	9	276	0
Sheldon, Frederick T.	9	135	0

Note: TP=total number of publications; TC=total citations; TLS=total link strength.

Co-authorship analysis is then used to identify collaborative relationships among authors and to map the structure of research communities within a given field. In this co-authorship analysis, 16 authors with the strongest links were selected from a total of 3762 authors, representing 8 clusters. Table XII provides detailed information about these 16 authors. These authors appeared as nodes if they were involved in 8 or more publications. The total number of links formed was 12, and the total link strength was 94.

The total link strength of 94 among the 16 authors suggests that there is a moderate level of collaborative relationships within the selected group. However, the link strength varies significantly among the authors. For example, Paul Jenkins and Nitin Naik have the highest link strengths of 28, indicating robust collaborative ties, while several authors have a link strength of 0, indicating no co-authorship with others in this subset.

Figure 9 shows a co-authorship network map with 8 author clusters, indicating frequent collaboration. Paul Jenkins and Nitin Naik are central nodes with high collaboration levels. Thicker connecting lines and larger circle size represent stronger co-authorship relationships.

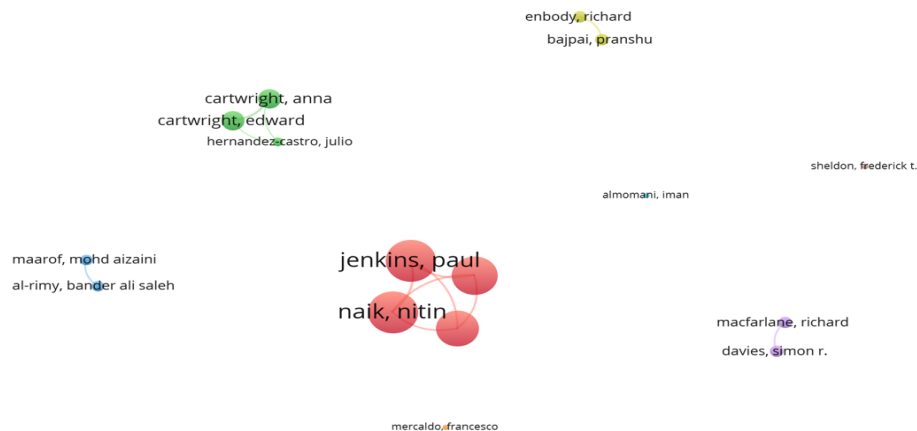


Fig. 9. Co-authorship network map.

The network map analysis reveals that collaboration within this research community is concentrated among a few key authors, while others have lower levels of collaboration. To strengthen the research network, it is recommended to promote cross-cluster collaboration and provide opportunities for authors with low link strength. Initiatives like joint research projects, workshops, and conferences can enhance collaborative relationships and expand the research network.

4.4 Key Contributors (Institutions)

To address Research Question 3 (RQ3) on identifying key contributors to ransomware research, an analysis highlighted the most productive and influential institutions. Table XIII showcases the top 9 institutions with over 25 publications. Leading the list is Amrita Vishwa Vidyapeetham in India with 51 total publications (TP) and 31 contributing authors (NCA), followed by Universiti Teknologi Malaysia with 47 publications and 16 contributing authors. Amity University in India ranks third with 36 publications and 30 contributing authors, while Kennesaw State University in the United States is fourth with 35 publications and 19 contributing authors

TABLE XIII. THE MOST PRODUCTIVE INSTITUTIONS WITH OVER 25 PUBLICATIONS.

Institution Name	Country	TP	NCA	TC
Amrita Vishwa Vidyapeetham	India	51	31	1170
Universiti Teknologi Malaysia	Malaysia	47	16	2249
Amity University	India	36	30	137
Kennesaw State University	United States	35	19	683
University of Kent	United Kingdom	35	11	385
Chitkara University	India	34	21	344
Edinburgh Napier University	United Kingdom	28	8	312
Imam Abdulrahman Bin Faisal University	Saudi Arabia	28	25	243
Universiti Teknikal Malaysia Melaka	Malaysia	26	10	82

Note: TP=total number of publications; NCA=number of contribution authors; TC=total citations.

The analysis measures publication volume, impact, and collaboration, as reflected by the number of contributing authors. The top 9 institutions include Amrita Vishwa Vidyapeetham, Amity University, and Chitkara University from India with 121 publications and 82 contributors; Universiti Teknologi Malaysia and Universiti Teknikal Malaysia Melaka from Malaysia with 73 publications and 26 contributors; University of Kent and Edinburgh Napier University from the United Kingdom with 63 publications and 19 contributors; and one institution each from the United States and Saudi Arabia.

Table XIV highlights the most influential affiliations in ransomware research with over 800 citations. Universiti Teknologi Malaysia leads with 47 total publications, 42 of which are cited, and a remarkable 2249 total citations. Northeastern University in the United States follows with 24 total publications, all of which are cited, accumulating 1897 citations. Politecnico di Milano in Italy, although having only 7 publications, sees all of them cited, resulting in 1582 citations, indicating a high impact per publication.

TABLE XIV. THE MOST INFLUENTIAL INSTITUTIONS WITH OVER 800 CITATIONS.

Institution Name	Country	TP	NCP	TC
Universiti Teknologi Malaysia	Malaysia	47	42	2249
Northeastern University	United States	24	24	1897
Politecnico di Milano	Italy	7	7	1582
Amrita Vishwa Vidyapeetham	India	51	47	1170
University of Florida	United States	7	7	1158
Texas State University	United States	6	6	1037
Consiglio Nazionale delle Ricerche	Italy	15	15	918
Florida International University	United States	17	13	912
Arizona State University	United States	13	13	909
University of Texas at San Antonio	United States	22	19	898
University of Malaya	Malaysia	4	4	868

Note: TP=total number of publications; NCP=number of cited publications; TC=total citations.

Amrita Vishwa Vidyapeetham in India leads with 51 publications, 47 of which have been cited, resulting in a total of 1,170 citations. The University of Florida, although contributing only seven publications, has achieved a comparable citation count of 1,158, indicating a high level of research impact. Other institutions included in the analysis, such as Texas State University, Consiglio Nazionale delle Ricerche, Arizona State University, the University of Texas at San Antonio, and the University of Malaya, also demonstrate strong citation performance despite having fewer publications. These findings reflect the international scope of ransomware research, with institutions from various regions contributing meaningfully to the field.

This review aims to identify leading institutions in terms of both research output and scholarly influence. Institutions such as Amrita Vishwa Vidyapeetham and Universiti Teknologi Malaysia demonstrate significant output in terms of publication volume and author contributions. Conversely, Universiti Teknologi Malaysia and Northeastern University show substantial

research impact through their high citation counts. Recognizing these institutions offers valuable insights for strategic decisions, such as directing research funding or forming new collaborations. Strengthening partnerships with these highly productive and influential institutions can boost knowledge exchange and significantly advance ransomware research.

4.5 Key Contributors (Countries)

Country statistics are essential for Research Question 3 (RQ3), focusing on key contributors to ransomware research. These statistics include the most productive countries by publications and researchers. The United States leads with 363 publications, followed by India with 264. The United Kingdom has 125 publications, Saudi Arabia 86, and China 78. Table XV lists countries with over 30 publications, based on data from BiblioMagika. The global distribution of publications is illustrated on a map in Figure 10, created using *iipmaps.com*.

TABLE XV. THE MOST PRODUCTIVE COUNTRIES WITH OVER 30 PUBLICATIONS

Country	TP	NCA	TC
United States	363	772	6150
India	264	683	2788
United Kingdom	125	169	2829
Saudi Arabia	86	165	1679
China	78	215	1197
Malaysia	62	107	1603
South Korea	61	156	1151
Australia	58	91	1001
Canada	50	91	1089
Pakistan	39	95	641

Note: TP=total number of publications; NCA=number of contributing authors; TC=total citations.

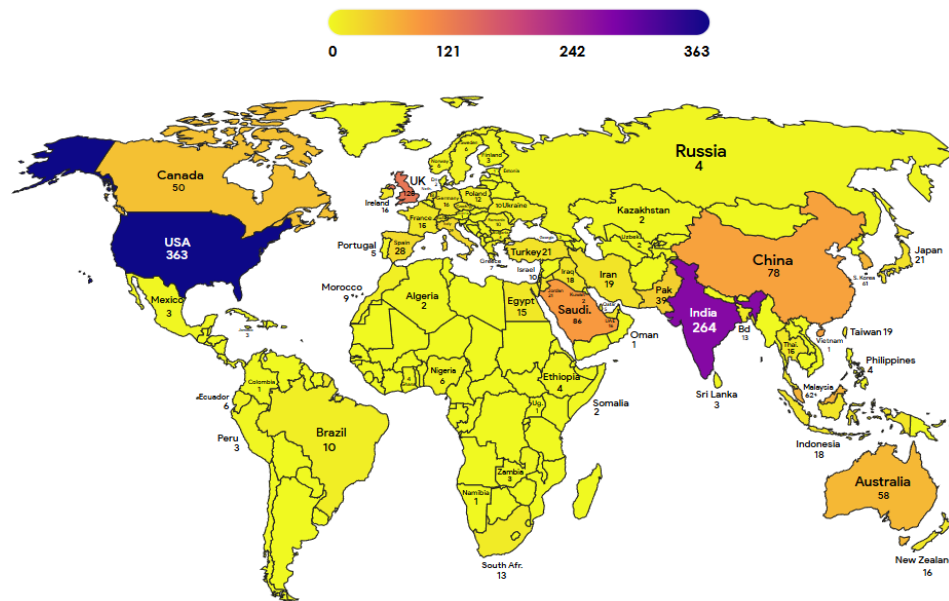


Fig. 10. Distribution of publications by Country.

The United States leads with 772 contributing authors, followed by India with 683, China with 215, the United Kingdom with 169, and Saudi Arabia with 165. Table XV also provides information about contributing authors in countries that produce the most publications on ransomware. The global map in Figure 11 visually represents the distribution of contributing authors by country.

The productivity of each country in ransomware research appears to correlate with its scholarly influence, as reflected in citation counts. The United States leads with 6,150 citations, followed by the United Kingdom (2,829), India (2,788), Saudi Arabia (1,679), and Malaysia (1,603). These figures suggest that the United States not only produces a high volume of research but also exerts considerable impact on the field. India's position as the second most productive country, both in terms of publications and contributing authors, highlights its growing role in cybersecurity scholarship. Similarly, the United Kingdom and Saudi Arabia demonstrate notable influence through relatively high citation counts, despite producing fewer

publications. These findings underscore the global nature of ransomware research and point to the value of international collaboration in advancing knowledge and developing effective responses to this evolving threat.

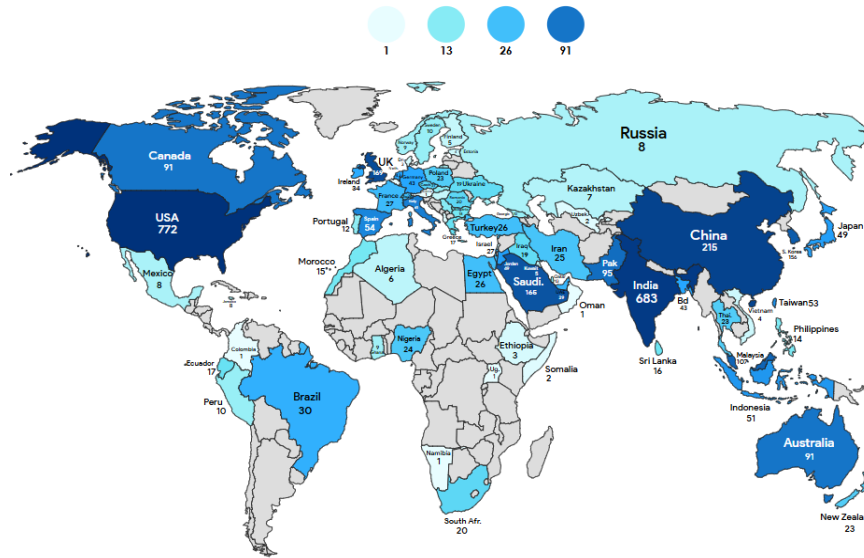


Fig. 11. Distribution of contributing authors by Country.

4.6 Publications by Source Titles

To address the fourth research question (RQ4) on the main publications that serve as leading platforms for disseminating high-impact ransomware research, Table XVI highlights the most active source titles, each featuring a minimum of 10 documents. We'll evaluate their impact factors, the volume of ransomware articles published, number of contributing authors, and the influence these articles have in the field.

TABLE XVI. THE MOST ACTIVE SOURCE TITLES WITH MINIMUM OF 10 DOCUMENTS

Source Title	TP	NCA	NCP	TC	C/P	C/CP	h	g	m
IEEE Access	43	175	40	1111	25.84	27.78	20	33	2.500
ACM International Conference Proceeding Series	38	123	29	494	13.00	17.03	9	21	0.900
Computers and Security	35	140	35	1347	38.49	38.49	19	35	2.375
Sensors	19	68	17	234	12.32	13.76	8	15	2.000
International Journal of Advanced Computer Science and Applications	14	45	11	51	3.64	4.64	5	6	0.833
Applied Sciences (Switzerland)	13	60	10	214	16.46	21.40	8	13	1.333
Electronics (Switzerland)	10	35	8	157	15.70	19.63	5	10	0.714

Note: TP=total number of publications; NCA=number of contributing authors; NCP=number of cited publications; TC=total citations; C/P=average citations per publication; C/CP=average citations per cited publication; h=h-index; g=g-index, m=m-index.

IEEE Access emerges as a dominant publication channel, boasting the highest volume of contributions in this domain, with 43 total publications (TP) involving 175 authors since 2017. This robust output underscores its position as a foremost platform for disseminating research. Its considerable influence is further corroborated by a remarkable 1111 total citations (TC), a notable h-index of 20, and an exceptional g-index of 33, reflecting the extensive reach and profundity of the research it showcases. The ACM International Conference Proceeding Series also shows a significant contribution to this field with 38 publications since 2016. The number of involved authors is quite substantial, reaching 123. However, the influence is much smaller compared to IEEE Access, with an h-index of 9, a g-index of 21, and a total of 494 citations.

Computers and Security, published by Elsevier Ltd, ranks third with 35 publications by 140 authors. Despite having fewer publications than IEEE Access, it excels in total citations (1347), with a g-index of 35, and an average citation per publication (C/P) and per cited publication (C/CP) of 38.49.

This indicates that Computers and Security is the most impactful source for ransomware research. Following this is Sensors by MDPI with 19 publications and 68 contributing authors. This source is relatively new, with its first ransomware-related publication in 2022, making it the youngest among the three sources mentioned. Nonetheless, Sensors has managed to generate a total of 234 citations, a C/P of 12.32, a C/CP of 13.76, an h-index of 8, and a g-index of 15, indicating significant contributions and influence in ransomware research despite its recent start.

In short, Table XVI illuminates the leading platforms for ransomware research. Journals like IEEE Access, along with ACM International Conference Proceeding Series, Computers & Security, and Sensors, stand out as primary conduits for groundbreaking studies. While other publications and conferences also significantly enrich the field's knowledge, identifying these central sources is key for scholars looking to keep up with the latest findings and choose where to publish their own work.

Figure 12 illustrates the yearly publication trends of the top five source titles in the field of ransomware research. These source titles have produced the most publications in this area. The ACM International Conference Proceeding Series (orange) began its publications in 2016 and saw a steady increase until 2019, reaching over 7 publications annually. However, since then, its publication count has declined, ranging between 2 to 5 publications per year. IEEE Access started publishing ransomware studies in 2017 and has shown a consistent upward trend. Since 2019, it has consistently produced 5 or more publications each year.

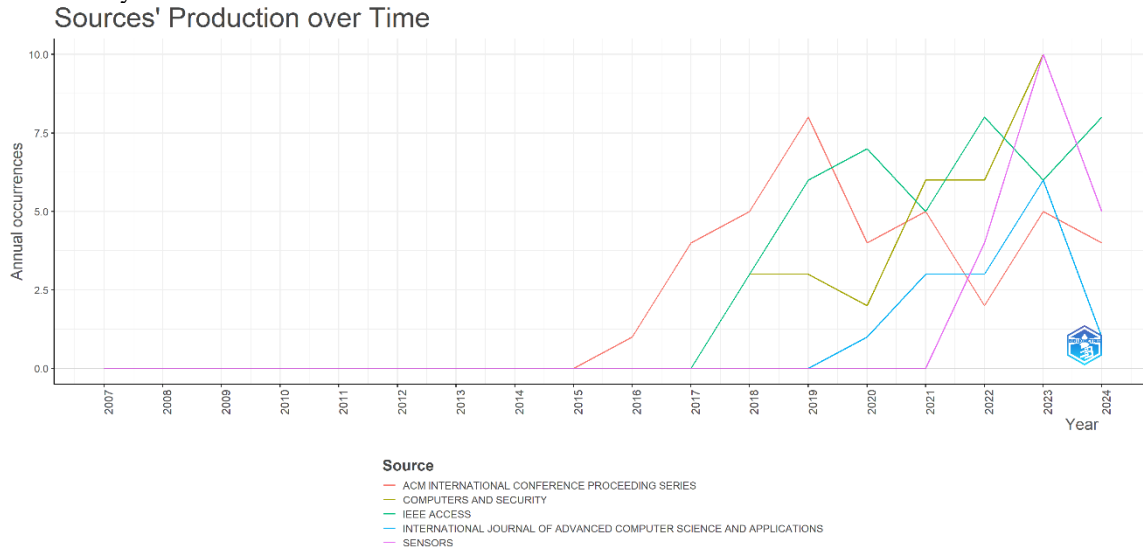


Fig. 12. Source's Production over Time (Annual Occurrences).

Meanwhile, Figure 13 presents the cumulative publication graph, showing IEEE Access's impressive growth, surpassing the ACM International Conference Proceeding Series, which started earlier. Computers and Security ranks third. Despite being relatively new to ransomware research, Sensors from MDPI, which began publishing in this field in 2022, has shown significant growth, surpassing the International Journal of Advanced Computer Science and Applications.

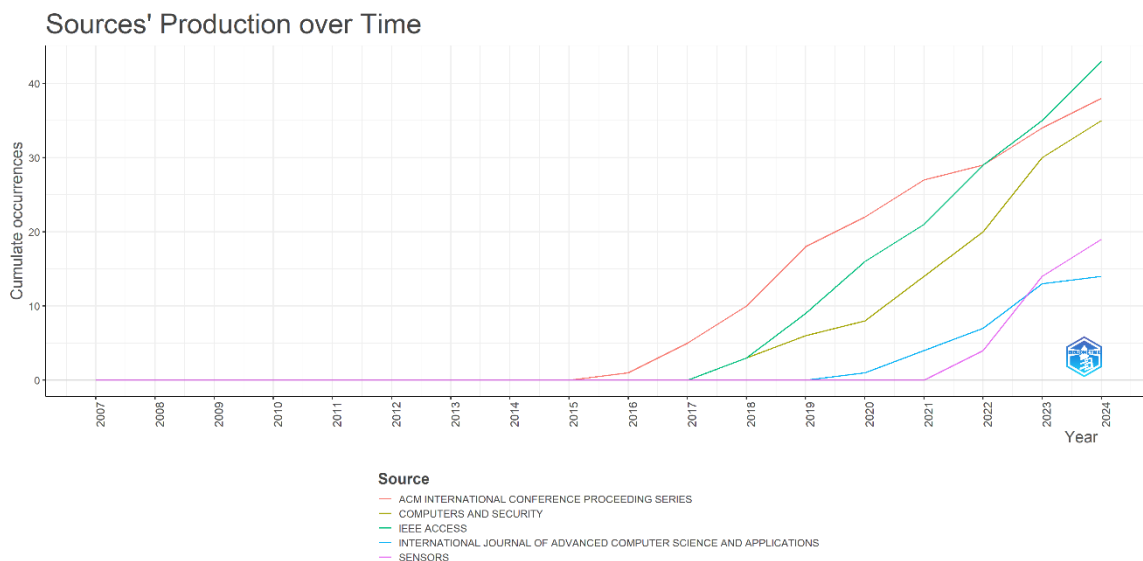


Fig. 13. Source's Production over Time (Cumulate Occurrences).

Bradford's Law, a bibliometric principle, describes the distribution of articles among journals in a field [42]. Bradford's Law describes the distribution of scientific productivity (not citation impact) among the sources that publish on a given topic. It divides sources into three zones of roughly equal total publication output: Zone 1 (the core) contains the smallest number of sources that together produce roughly one-third of all publications on the topic, meaning these are the most prolific rather than necessarily the most-cited sources; Zone 2 contains a larger number of sources producing a similar share of publications at a lower average output per source; and Zone 3 (the tail) contains the largest number of sources, each contributing only a few publications, together producing the remaining third. Bradford's Law predicts that the number of sources in Zones 2 and 3 will be approximately n and n^2 times greater than in Zone 1, respectively, following a $1 : n : n^2$ progression [70].

Applying Bradford's Law with Bibliometrix and BiblioMagika helps identify the most productive publication sources within the ransomware dataset and visually represents how publication output is distributed across sources. In this dataset, Zone 1 (the core) comprises 64 sources, Zone 2 comprises 322 sources, and Zone 3 (the tail) comprises 461 sources. Figure 14, generated using Bibliometrix, shows the core sources identified under Bradford's Law.

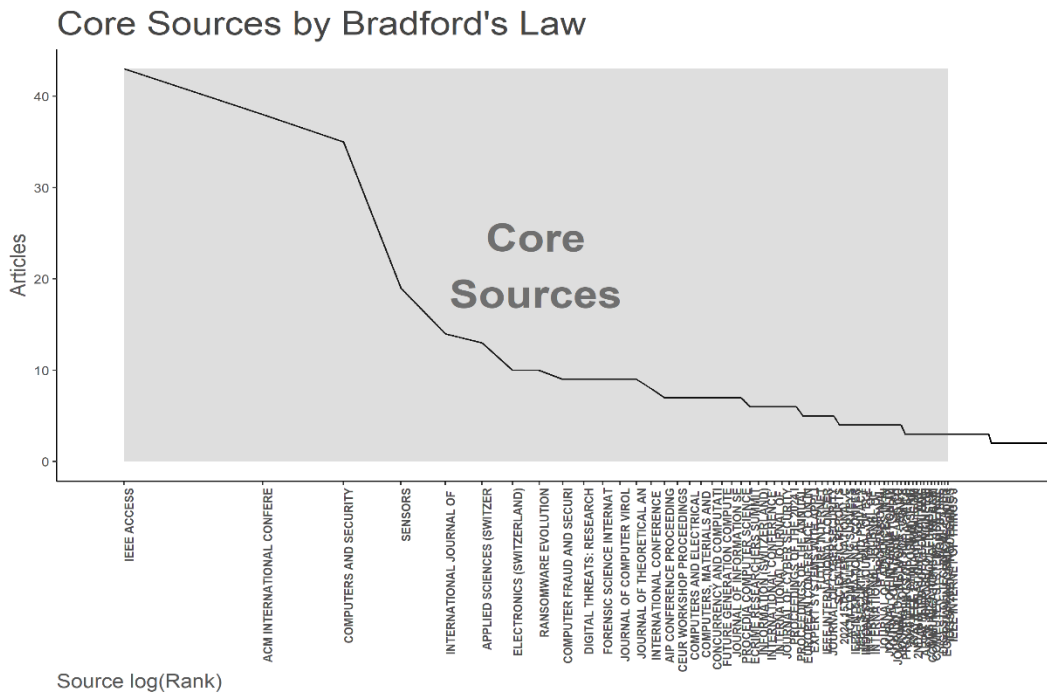


Fig. 14. Core sources by Bradford's Law.

The observed zone distribution (64:322:461) departs noticeably from the theoretical $1:n:n^2$ progression implied by Bradford's Law. Taking Zone 1 as the reference ($n_1 = 64$), the observed multipliers are only about 5.0 ($322/64$) for Zone 2 and 7.2 ($461/64$) for Zone 3, far below the multiplicative (n vs. n^2) growth the law predicts, while the ratio between Zone 3 and Zone 2 ($461/322 \approx 1.4$) is much closer to linear than to the expected n -fold increase over Zone 2. This pattern suggests that the ransomware literature is comparatively concentrated in a small set of core venues relative to its long tail, which is common in emerging, still-consolidating interdisciplinary fields where authors have not yet converged on a stable set of specialized outlets. Restricting the corpus to Scopus-indexed sources may also compress the tail relative to what a multi-database corpus (e.g., including non-Scopus conference proceedings or regional journals) would show, since additional peripheral sources would be expected to inflate Zone 3 disproportionately. Despite this quantitative departure from the classical model, Bradford's Law remains a useful heuristic for identifying the core sources that concentrate ransomware research output, as reflected in Figure 14.

The co-citation network analysis reveals important insights into the research landscape. IEEE Access stands out as the most influential source in the network with the highest TLS of 6362, signifying its strong co-citation links with other publications. This indicates that IEEE Access is highly regarded and frequently referenced in the field of ransomware research. Details of the top sources with the highest co-citation TLS values can be seen in Table XVII.

Computers & Security follows as the second most influential source, with a TLS of 5733. This journal also plays a significant role in the research community, reflecting its substantial contribution and recognition in related studies. Future Generation Computer Systems, with a TLS of 2342, and Sensors with a TLS of 2072, also demonstrate strong co-citation links, highlighting their relevance and impact.

In 2016, Scaife et al. published a paper titled ‘CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data’ [52]. This paper has the highest number of citations compared to other papers, with a total of 354 citations and an average of 35.4 citations per year. Although not the highest, this number sufficiently proves the consistent interest and impact of this paper in ransomware research.

The second most cited publication is ‘Unveil: A large-scale, automated approach to detecting ransomware’ by Kharraz et al., published in 2016 [53]. This paper closely follows the first with 347 total citations and 34.70 citations per year. The slight difference in performance indicates the seminal nature of this paper in the field of ransomware.

The paper ‘Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions,’ by Al-Rimy et al. (2018), ranks third in citations [54]. It has 285 citations with an average of 35.63 per year, higher than the two previously discussed publications. This indicates a greater impact despite its more recent publication date. The comprehensive review of ransomware threats, taxonomy, and countermeasures makes this paper a key reference for researchers.

The paper with the highest citations per year is ‘A comprehensive survey on deep learning-based malware detection techniques’ by Gopinath and Sethuraman, published in *Computer Science Review*, 2023 [51]. Despite its recent publication, this paper has attracted significant interest, with an average of 45.33 citations per year and a total of 136 citations. Its review nature and focus on deep learning (a hot research topic) likely contribute to its high citation count. Figure 16 illustrates the top 20 highly cited documents per year, generated using Bibliometrix.

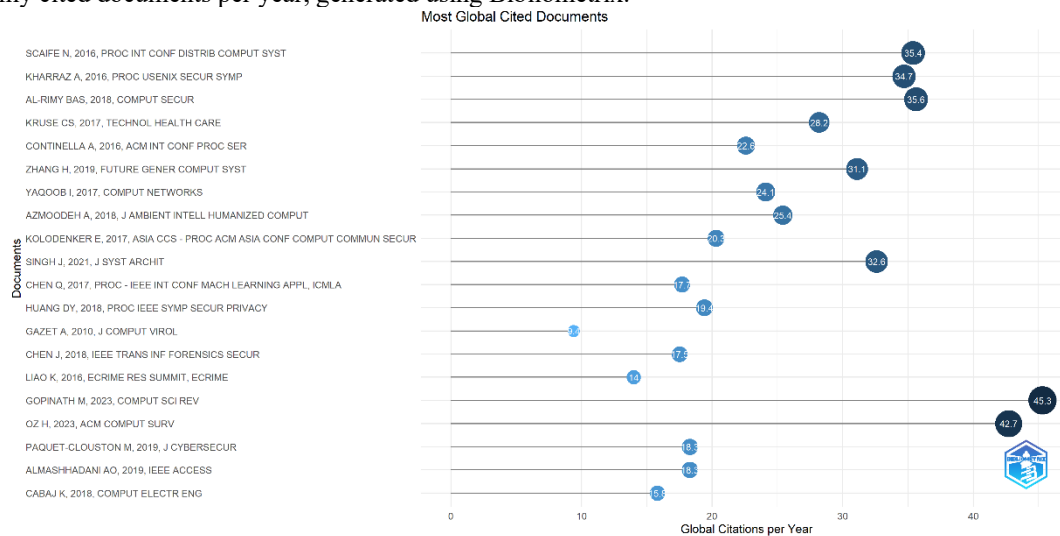


Fig. 16. Most Cited Documents (Citation per Year).

Similarly, Oz et al. achieved significant recognition with their 2022 publication titled ‘A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions’ [7]. This newly published review paper discusses the evolution of ransomware, taxonomy, and defense mechanisms. It has garnered a citation rate of 32.00 citations per year and a total of 128 citations, a respectable rate for a 2022 publication, though lower than the citation-per-year rates of the more recent reviews discussed above.

Taken together, these most highly cited publications point to two complementary patterns of influence: sustained, high-volume citation accumulated over a long window (e.g., Scaife et al. [52] and Kharraz et al. [53], both from 2016) and rapid, high-rate accumulation by more recent comprehensive reviews (e.g., Gopinath and Sethuraman [51] and Oz et al. [7]). Both patterns indicate publications that the field continues to treat as key reference points, underscoring the value of ongoing, high-quality survey and detection work in addressing the evolving ransomware threat.

4.8 Research Themes

To address research question 6 (RQ6), this section explores the main research themes in ransomware studies, highlighting future directions. The discussion is divided into two parts: co-occurrence networks of author keywords, which analyze relationships between frequently co-occurring keywords to identify related topic clusters, and thematic maps of author keywords, which visually represent major themes and subthemes in ransomware research. These approaches help uncover patterns and trends and propose new directions to address gaps in the current literature.

characterized by keywords related to cryptocurrency, including "bitcoin" and "blockchain," underscoring the connection between ransomware operations and blockchain-based financial systems.

Figure 18 presents an overlay visualization of ransomware-related research topics generated using VOSviewer. The visualization employs a color gradient to represent the temporal distribution of topics, with darker shades indicating earlier research and lighter shades (e.g., yellow) representing more recent developments. The term "ransomware" appears prominently at the center of the map, reflecting its central role in the literature. This overlay visualization provides insight into the evolution of research themes over time, enabling the identification of emerging areas and potential gaps in the existing body of knowledge. Notably, recent studies have increasingly focused on topics such as "machine learning," "deep learning," "early detection," "feature selection," "CNN," "artificial intelligence," "ensemble learning," and "data breach."

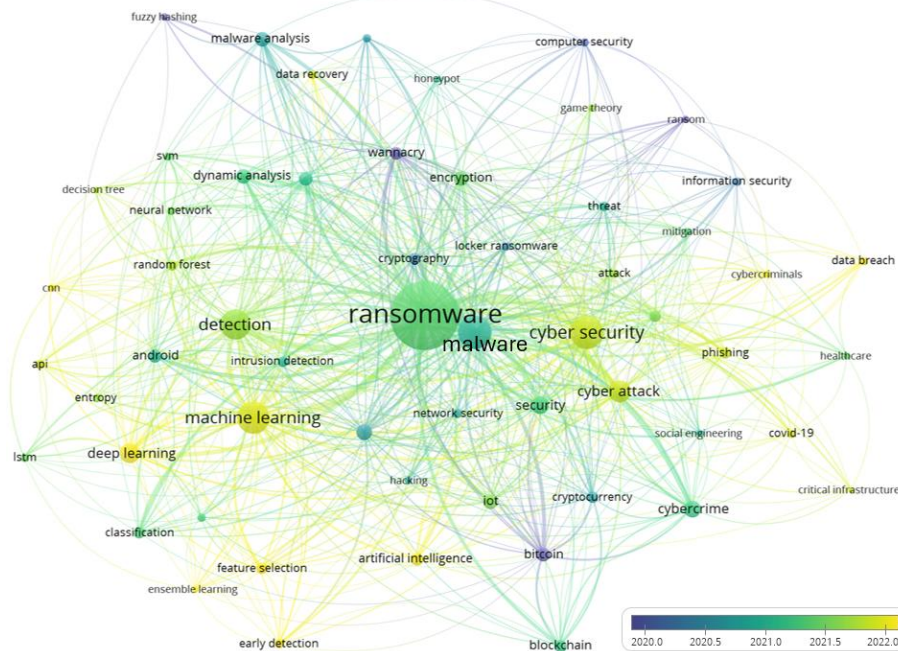


Fig. 18. Co-occurrence overlay visualization of the authors' keywords.

Together, the network and overlay visualizations offer complementary perspectives on the ransomware research landscape. The network visualization reveals the structural relationships among key terms, highlighting thematic clusters and their interconnections. In contrast, the overlay visualization adds a temporal dimension, illustrating how research interests have shifted over time. These visual tools contribute to a more nuanced understanding of the field and may inform future research directions and strategic planning in cybersecurity.

4.8.2 Thematic Map

Figure 19 provides a thematic map visualization of research topics related to ransomware, using author keywords from co-occurrence networks. The visualization was generated using the Bibliometrix tool. The map categorizes themes into four quadrants, each representing their development degree and relevance. The top-left quadrant, Niche Themes, includes topics like ‘android malware’, ‘behavioral analysis’, and ‘adware’, indicating these are well-developed but not central to the main topic. The top-right quadrant, Motor Themes, features highly relevant and developed topics such as ‘ransomware’, ‘cyber security’, and ‘malware’, emphasizing their importance in the context of ransomware research.

The bottom-left quadrant, labeled Emerging or Declining Themes in Bibliometrix’s thematic-map convention, contains themes such as ‘machine learning’, ‘detection’, ‘deep learning’, ‘early detection’, and ‘feature selection’; this label alone cannot distinguish a theme gaining momentum from one that is fading, so we read it alongside each keyword’s band in the co-occurrence overlay (Figure 18, where yellow denotes the most recent average publication year) and its overall occurrence count (Section 4.8.1). All five keywords fall in the yellow band and rank among the highest-occurrence keywords overall (‘machine learning’, ‘detection’, and ‘deep learning’ at 211, 195, and 79 occurrences, respectively), a pattern more consistent with continued growth than decline. This reading is suggestive rather than confirmed: overlay color is a coarse, visually binned proxy, and the exact mean publication year and year-over-year trajectory for each keyword would require VOSviewer keyword-year data not available for this analysis, which we note as a limitation.

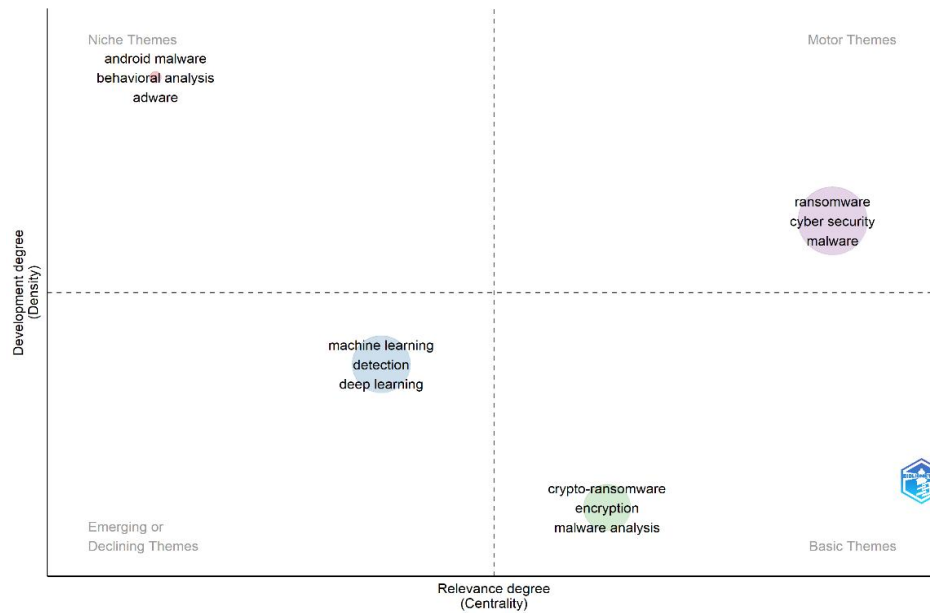


Fig. 19. Thematic map of the authors' keywords.

The bottom-right quadrant, Basic Themes, includes fundamental yet less developed topics such as 'crypto-ransomware', 'encryption', and 'malware analysis'. This quadrant highlights foundational concepts crucial to understanding ransomware but indicates a need for further development in these areas.

5. CONCLUSIONS

This study presents a bibliometric analysis of ransomware-related research published in the Scopus database before the year 2025. Since the first Scopus article on ransomware was published in 2007, this analysis focuses on papers published from 2007 to 2024. A total of 1,424 documents were initially collected. After removing records with issues such as inaccessibility, incomplete data, or duplicates, 1,386 documents remained.

Various tools were used in the analysis process, including the Scopus website, Microsoft Excel, Biblio Magika, Harzing's Publish or Perish, VOSviewer, iipmaps, and Bibliometrix. Using these tools, the analysis aimed to answer six research questions regarding: the current research landscape, publication trends, key contributors (including the most productive and influential authors, institutions, and countries), leading platforms for publications, landmark papers, main research themes, and future research directions.

The key findings of this study are listed as follows:

1. Since 2018, more than 100 papers related to ransomware have been published annually in Scopus. Specifically, in 2023 and 2024, ransomware-related publications reached 282 and 284, respectively.
2. The majority of these publications are research papers, either in the form of conference papers (48.92%) or journal articles (43.29%).
3. The journal IEEE Access has published the most ransomware-related research, with a total of 43 publications.
4. Amrita Vishwa Vidyapeetham (Amrita University) in India is the most productive institution, with 51 publications related to ransomware.
5. Universiti Teknologi Malaysia, Malaysia, is the most influential institution, with a total of 2,249 citations.
6. Only seven authors have published 10 or more papers on ransomware by 2024.
7. Bander Ali Saleh Al-Rimy is the most productive and influential author, with 13 publications, 809 total citations, an h-index of 11, and a g-index of 13.
8. The United States is the most productive and influential country in this field, with the highest number of publications (363), the highest number of contributing authors (772), and the highest total citations (6,150).
9. Computer Science is the most popular research area for ransomware publications, with 1,155 publications, accounting for 83.33% of the total publications.

10. The publication by Scaife et al. in 2016, titled "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," has the highest number of citations, with a total of 354.
11. Keyword and thematic-map patterns (Section 4.8) point to early detection, deep learning, data breach, CNN, feature selection, machine learning, and artificial intelligence as areas of growing research activity, though this reading is qualitative rather than a statistically confirmed classification (Section 4.8.2).

This bibliometric study thus fills a critical void in the existing literature by uncovering structural patterns, scholarly influences, and evolving themes within ransomware research—effectively answering the gap articulated in the introduction. The findings provide valuable insights for researchers, policymakers, and industry practitioners, helping to identify prominent areas, key players, and future research directions essential for effectively combating the ever-evolving threat of ransomware.

6. LIMITATIONS AND DIRECTIONS FOR FUTURE WORK

This study provides a comprehensive overview of ransomware research through bibliometric and network analysis; however, several limitations should be noted. The data were limited to English-language publications indexed in Scopus up to 2024, which may exclude relevant research from other databases or more recent contributions. Differences among bibliometric tools may also influence the interpretation of collaboration patterns and thematic clusters. Additionally, citation-based indicators used in this study may undervalue recently published but potentially impactful works.

Despite these limitations, the findings offer a clear foundation for future work. The keyword and thematic-map patterns associated with early ransomware detection using artificial intelligence, particularly deep learning and Convolutional Neural Networks (CNN), represent promising areas for further exploration, and confirming their emerging status with directly computed temporal indicators (Section 4.8.2) is itself a priority for that future work. Future studies may also benefit from refining feature selection methods to enhance the precision and speed of ransomware detection models. Expanding the scope to include multi-database sources, more languages, or hybrid approaches that combine bibliometric and qualitative analyses could further enrich the understanding of this dynamic research domain.

Acknowledgment

The authors would like to express their sincere gratitude to Universitas Dian Nuswantoro, INTI International University, and Universiti Teknikal Malaysia Melaka for providing the essential research facilities and continuous academic support throughout the completion of this study.

Funding

This research was financially supported by the Directorate General of Higher Education, Science, and Technology, Ministry of Higher Education, Science, and Technology, Republic of Indonesia, through the Doctoral Dissertation Research scheme (Penelitian Disertasi Doktor/PDD) under Master Contract Number: 027/LL6/AL.04.03/PL-BARU/2026 and Derivative Contract Numbers: 131/F.09/UDN-09/III/2026.

CRedit Authorship Contribution Statement

Conceptualization, Fauzi Adi Rafrastara and Pulung Nurtantio Andono; Methodology, Fauzi Adi Rafrastara; Formal Analysis, Fauzi Adi Rafrastara; Investigation, Fauzi Adi Rafrastara; Writing – Original Draft Preparation, Fauzi Adi Rafrastara; Writing – Review and Editing, Pulung Nurtantio Andono, Deshinta Arrova Dewi and Mohd. Faizal Abdollah; Supervision, Pulung Nurtantio Andono, Purwanto and Pujiono; Validation, Purwanto and Pujiono; Resources, Deshinta Arrova Dewi and Mohd. Faizal Abdollah. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Data Availability Statement

The bibliometric data analyzed in this study were retrieved from the Scopus database (Elsevier). Due to licensing restrictions imposed by Scopus, the raw dataset cannot be made publicly available; however, it is available from the corresponding author upon reasonable request.

Ethical Approval

Not applicable.

References

- [1] K. Lee, J. Lee, S.-Y. Lee, and K. Yim, "Effective Ransomware Detection Using Entropy Estimation of Files for Cloud Services," *Sensors*, vol. 23, no. 6, p. 3023, Mar. 2023, doi: 10.3390/s23063023.
- [2] Kritika, "A comprehensive literature review on ransomware detection using deep learning," *Cyber Security and Applications*, vol. 3, p. 100078, Dec. 2025, doi: 10.1016/j.csa.2024.100078.
- [3] M. Al-Hawawreh, M. Alazab, M. A. Ferrag, and M. S. Hossain, "Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms," *Journal of Network and Computer Applications*, vol. 223, p. 103809, Mar. 2024, doi: 10.1016/j.jnca.2023.103809.
- [4] Md. Fahim-Ul-Islam, A. Chakrabarty, Md. G. R. Alam, and S. S. B. Maidin, "A Resource-Efficient Federated Learning Framework for Intrusion Detection in IoMT Networks," *IEEE Trans. Consumer Electron.*, vol. 71, no. 2, pp. 4508–4521, May 2025, doi: 10.1109/TCE.2025.3544885.
- [5] Md. A. Hossain, T. Hasan, F. Ahmed, S. H. Cheragee, M. H. Kanchan, and M. A. Haque, "Towards superior android ransomware detection: An ensemble machine learning perspective," *Cyber Security and Applications*, vol. 3, p. 100076, Dec. 2025, doi: 10.1016/j.csa.2024.100076.
- [6] M. Robles-Carrillo and P. García-Teodoro, "Ransomware: An Interdisciplinary Technical and Legal Approach," *Security and Communication Networks*, vol. 2022, pp. 1–17, Aug. 2022, doi: 10.1155/2022/2806605.
- [7] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions," *ACM Comput. Surv.*, vol. 54, no. 11s, pp. 1–37, Jan. 2022, doi: 10.1145/3514229.
- [8] W. Z. A. Zakaria, M. F. Abdollah, O. Mohd, S. M. W. M. S. M. M. Yassin, and A. Ariffin, "RENTAKA: A Novel Machine Learning Framework for Crypto-Ransomware Pre-encryption Detection," *IJACSA*, vol. 13, no. 5, 2022, doi: 10.14569/IJACSA.2022.0130545.
- [9] S. Sharma, R. Krishna, and R. Kumar, "An Ensemble-based Supervised Machine Learning Framework for Android Ransomware Detection," *IAJIT*, vol. 18, no. 3A, 2021, doi: 10.34028/iajit/18/3A/5.
- [10] W. Y. Leong, Y. Z. Leong, and W. S. Leong, "Strategies for Identifying Online Scams," in *2024 Asian Conference on Communication and Networks (ASIANComNet)*, Bangkok, Thailand: IEEE, Oct. 2024, pp. 1–6. doi: 10.1109/ASIANComNet63184.2024.10811085.
- [11] S. H. Kok, A. Abdullah, and N. Jhanjhi, "Early detection of crypto-ransomware using pre-encryption detection algorithm," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 1984–1999, May 2022, doi: 10.1016/j.jksuci.2020.06.012.
- [12] R. M. A. Molina, S. Torabi, K. Sarriddine, E. Bou-Harb, N. Bouguila, and C. Assi, "On Ransomware Family Attribution Using Pre-Attack Paranoia Activities," *IEEE Trans. Netw. Serv. Manage.*, vol. 19, no. 1, pp. 19–36, Mar. 2022, doi: 10.1109/TNSM.2021.3112056.
- [13] A. Feeley et al., "Under viral attack: An orthopaedic response to challenges faced by regional referral centres during a national cyber-attack," *The Surgeon*, vol. 20, no. 5, pp. 334–338, Oct. 2022, doi: 10.1016/j.surge.2021.09.007.
- [14] S. R. B. Alvee, B. Ahn, T. Kim, Y. Su, Y.-W. Youn, and M.-H. Ryu, "Ransomware Attack Modeling and Artificial Intelligence-Based Ransomware Detection for Digital Substations," in *2021 6th IEEE Workshop on the Electronic Grid (eGRID)*, New Orleans, LA, USA: IEEE, Nov. 2021, pp. 01–05. doi: 10.1109/eGRID52793.2021.9662158.
- [15] A. Kapoor, A. Gupta, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, "Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions," *Sustainability*, vol. 14, no. 1, p. 8, Dec. 2021, doi: 10.3390/su14010008.
- [16] M. Cen, F. Jiang, X. Qin, Q. Jiang, and R. Doss, "Ransomware early detection: A survey," *Computer Networks*, vol. 239, p. 110138, Feb. 2024, doi: 10.1016/j.comnet.2023.110138.
- [17] K. Mohanty, V. Goswami, S. N. Qurashi, and R. K. Barik, "Ransomware and its future trends: A scientometric analysis," *smr*, vol. 9, no. 1, pp. 15–43, Dec. 2024, doi: 10.55284/smr.v9i1.1259.
- [18] U. Urooj, M. A. B. Maarof, and B. A. S. Al-Rimy, "A proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model," in *2021 3rd International Cyber Resilience Conference (CRC)*, Langkawi Island, Malaysia: IEEE, Jan. 2021, pp. 1–6. doi: 10.1109/CRC50527.2021.9392548.

- [19] U. Urooj, B. A. S. Al-Rimy, A. B. Zainal, F. Saeed, A. Abdelmaboud, and W. Nagmeldin, "Addressing Behavioral Drift in Ransomware Early Detection Through Weighted Generative Adversarial Networks," *IEEE Access*, vol. 12, pp. 3910–3925, 2024, doi: 10.1109/ACCESS.2023.3348451.
- [20] X. Luo and Q. Liao, "Awareness Education as the Key to Ransomware Prevention," *Information Systems Security*, vol. 16, no. 4, pp. 195–202, Sep. 2007, doi: 10.1080/10658980701576412.
- [21] C. U. Om Kumar, S. Kishore, and A. Geetha, "Debugging using MD5 process firewall," in *2014 International Conference on Contemporary Computing and Informatics (IC3I)*, Mysore, India: IEEE, Nov. 2014, pp. 1279–1284. doi: 10.1109/IC3I.2014.7019657.
- [22] T. Yang, Y. Yang, K. Qian, D. C.-T. Lo, Y. Qian, and L. Tao, "Automated Detection and Analysis for Android Ransomware," in *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, New York, NY: IEEE, Aug. 2015, pp. 1338–1343. doi: 10.1109/HPCC-CSS-ICSS.2015.39.
- [23] G. Kirubavathi, W. Regis Anne, and U. K. Sridevi, "A recent review of ransomware attacks on healthcare industries," *Int J Syst Assur Eng Manag*, vol. 15, no. 11, pp. 5078–5096, Nov. 2024, doi: 10.1007/s13198-024-02496-4.
- [24] G. Munoz Cornejo, J. Lee, and B. A. Russell, "A thematic analysis of ransomware incidents among United States hospitals, 2016–2022," *Health Technol.*, vol. 14, no. 6, pp. 1059–1070, Nov. 2024, doi: 10.1007/s12553-024-00890-3.
- [25] H. T. Neprash et al., "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016–2021," *JAMA Health Forum*, vol. 3, no. 12, p. e224873, Dec. 2022, doi: 10.1001/jamahealthforum.2022.4873.
- [26] L. Manning and A. Kowalska, "The threat of ransomware in the food supply chain: a challenge for food defence," *Trends Organ Crim*, Nov. 2023, doi: 10.1007/s12117-023-09516-y.
- [27] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 186–202, 2024, doi: 10.1016/j.iotcps.2023.12.001.
- [28] M. Gazzan and F. T. Sheldon, "Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems," *Future Internet*, vol. 15, no. 4, p. 144, Apr. 2023, doi: 10.3390/fi15040144.
- [29] M. Humayun, N. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egyptian Informatics Journal*, vol. 22, no. 1, pp. 105–117, Mar. 2021, doi: 10.1016/j.eij.2020.05.003.
- [30] L. Albshaier, S. Almarri, and M. M. H. Rahman, "Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review," *Information*, vol. 15, no. 8, p. 484, Aug. 2024, doi: 10.3390/info15080484.
- [31] A. Alqahtani and F. T. Sheldon, "A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook," *Sensors*, vol. 22, no. 5, p. 1837, Feb. 2022, doi: 10.3390/s22051837.
- [32] A. Alraizza and A. Algarni, "Ransomware Detection Using Machine Learning: A Survey," *BDCC*, vol. 7, no. 3, p. 143, Aug. 2023, doi: 10.3390/bdcc7030143.
- [33] M. S. Balamurugan, V. Rajendran, and S. C. MARY, "A Review on Cognitive-based Ransomware Detection using Machine Learning and Deep Learning Techniques," *JATIT*, vol. 102, no. 10, pp. 4572–4581, May 2024.
- [34] S. Jawad and H. M. Ahmed, "Machine Learning Approaches to Ransomware Detection: A Comprehensive Review," *IJSSE*, vol. 14, no. 6, pp. 1963–1973, Dec. 2024, doi: 10.18280/ijssse.140630.
- [35] U. Urooj, B. A. S. Al-Rimy, A. Zainal, F. A. Ghaleb, and M. A. Rassam, "Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions," *Applied Sciences*, vol. 12, no. 1, p. 172, Dec. 2021, doi: 10.3390/app12010172.
- [36] I. A. Chesti, M. Humayun, N. U. Sama, and N. Jhanjhi, "Evolution, Mitigation, and Prevention of Ransomware," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia: IEEE, Oct. 2020, pp. 1–6. doi: 10.1109/ICCIS49240.2020.9257708.
- [37] G. Barnes and A. Ghafarian, "Machine Learning-Based Static Ransomware Detection Using PE Header Features and SHAP Interpretation," *JCP*, vol. 6, no. 2, p. 58, Apr. 2026, doi: 10.3390/jcp6020058.

- [38] M. Maghanaki, S. Keramati, F. F. Chen, and M. Shahin, “Systematic Evaluation of Machine Learning and Deep Learning Models for IoT Malware Detection Across Ransomware, Rootkit, Spyware, Trojan, Botnet, Worm, Virus, and Keylogger,” *Sensors*, vol. 26, no. 6, p. 1750, Mar. 2026, doi: 10.3390/s26061750.
- [39] S. R. T. Mat, M. F. Ab Razak, M. N. M. Kahar, J. M. Arif, S. Mohamad, and A. Firdaus, “Towards a systematic description of the field using bibliometric analysis: malware evolution,” *Scientometrics*, vol. 126, no. 3, pp. 2013–2055, Mar. 2021, doi: 10.1007/s11192-020-03834-6.
- [40] M. F. A. Razak, N. B. Anuar, R. Salleh, and A. Firdaus, “The rise of ‘malware’: Bibliometric analysis of malware study,” *Journal of Network and Computer Applications*, vol. 75, pp. 58–76, Nov. 2016, doi: 10.1016/j.jnca.2016.08.022.
- [41] X.-L. Pham and T. T. Le, “Bibliometric Analysis and Systematic Review of Research on Expert Finding: A PRISMA-guided Approach,” *IAJIT*, vol. 21, no. 4, 2024, doi: 10.34028/iajit/21/4/9.
- [42] T. Hakim, A. Ahmi, and S. Alam, “A Decade in Blockchain: A Bibliometric Reflection on the Growth and Interdisciplinary Reach of a Disruptive Technology,” *JICT*, vol. 23, no. 4, pp. 627–665, Oct. 2024, doi: 10.32890/jict2024.23.4.3.
- [43] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, “How to conduct a bibliometric analysis: An overview and guidelines,” *Journal of Business Research*, vol. 133, pp. 285–296, Sep. 2021, doi: 10.1016/j.jbusres.2021.04.070.
- [44] “Scopus preview - Scopus - Welcome to Scopus.” Accessed: Feb. 17, 2025. [Online]. Available: <https://www.scopus.com/home.uri>
- [45] A. Ahmi, “biblioMagika®,” biblioMagika®. Accessed: Feb. 17, 2025. [Online]. Available: <https://bibliomagika.com/index.php>
- [46] A. W. Harzing, “Publish or Perish,” Harzing.com. Accessed: Feb. 17, 2025. [Online]. Available: <https://harzing.com/resources/publish-or-perish>
- [47] “VOSviewer - Visualizing scientific landscapes.” Accessed: Feb. 17, 2025. [Online]. Available: <https://www.vosviewer.com/>
- [48] “iipmaps map maker.” Accessed: Feb. 17, 2025. [Online]. Available: <https://iipmaps.com/>
- [49] “Bibliometrix - Home.” Accessed: Feb. 17, 2025. [Online]. Available: <https://www.bibliometrix.org/home/>
- [50] S. Thangaraj and J. Ramalingam, “Authorship Pattern on Multiple Disabilities During 2006-2020: A Scientometric Analysis,” *IJISM*, vol. 21, no. 2, Apr. 2023, doi: 10.22034/ijism.2023.1977826.0.
- [51] M. Gopinath and S. C. Sethuraman, “A comprehensive survey on deep learning based malware detection techniques,” *Computer Science Review*, vol. 47, p. 100529, Feb. 2023, doi: 10.1016/j.cosrev.2022.100529.
- [52] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, “CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data,” in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, Nara, Japan: IEEE, Jun. 2016, pp. 303–312. doi: 10.1109/ICDCS.2016.46.
- [53] A. Kharraz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, “UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware,” in *25th USENIX Security Symposium*, Austin, TX, USA: USENIX Association, Aug. 2016, pp. 757–772.
- [54] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, “Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions,” *Computers & Security*, vol. 74, pp. 144–166, May 2018, doi: 10.1016/j.cose.2018.01.001.
- [55] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, “Cybersecurity in healthcare: A systematic review of modern threats and trends,” *THC*, vol. 25, no. 1, pp. 1–10, Feb. 2017, doi: 10.3233/THC-161263.
- [56] A. Continella et al., “ShieldFS: a self-healing, ransomware-aware filesystem,” in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, Los Angeles California USA: ACM, Dec. 2016, pp. 336–347. doi: 10.1145/2991079.2991110.
- [57] H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli, and A. K. Sangaiah, “Classification of ransomware families with machine learning based on N -gram of opcodes,” *Future Generation Computer Systems*, vol. 90, pp. 211–221, Jan. 2019, doi: 10.1016/j.future.2018.07.052.

- [58] I. Yaqoob et al., “The rise of ransomware and emerging security challenges in the Internet of Things,” *Computer Networks*, vol. 129, pp. 444–458, Dec. 2017, doi: 10.1016/j.comnet.2017.09.003.
- [59] A. Azmoodeh, A. Dehghantanha, M. Conti, and K.-K. R. Choo, “Detecting crypto-ransomware in IoT networks based on energy consumption footprint,” *J Ambient Intell Human Comput*, vol. 9, no. 4, pp. 1141–1152, Aug. 2018, doi: 10.1007/s12652-017-0558-5.
- [60] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, “PayBreak: Defense Against Cryptographic Ransomware,” in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi United Arab Emirates: ACM, Apr. 2017, pp. 599–611. doi: 10.1145/3052973.3053035.
- [61] J. Singh and J. Singh, “A survey on machine learning-based malware detection in executable files,” *Journal of Systems Architecture*, vol. 112, p. 101861, Jan. 2021, doi: 10.1016/j.sysarc.2020.101861.
- [62] Q. Chen and R. A. Bridges, “Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware,” in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Cancun, Mexico: IEEE, Dec. 2017, pp. 454–460. doi: 10.1109/ICMLA.2017.0-119.
- [63] D. Y. Huang et al., “Tracking Ransomware End-to-end,” in *2018 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA: IEEE, May 2018, pp. 618–631. doi: 10.1109/SP.2018.00047.
- [64] A. Gazet, “Comparative analysis of various ransomware virii,” *J Comput Virol*, vol. 6, no. 1, pp. 77–90, Feb. 2010, doi: 10.1007/s11416-008-0092-2.
- [65] J. Chen, C. Wang, Z. Zhao, K. Chen, R. Du, and G.-J. Ahn, “Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection,” *IEEE Trans.Inform.Forensic Secur.*, vol. 13, no. 5, pp. 1286–1300, May 2018, doi: 10.1109/TIFS.2017.2787905.
- [66] K. Liao, Z. Zhao, A. Doupe, and G.-J. Ahn, “Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin,” in *2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, ON, Canada: IEEE, Jun. 2016, pp. 1–13. doi: 10.1109/ECRIME.2016.7487938.
- [67] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, “Ransomware payments in the Bitcoin ecosystem,” *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz003, Jan. 2019, doi: 10.1093/cybsec/tyz003.
- [68] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O’Kane, “A Multi-Classifer Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware,” *IEEE Access*, vol. 7, pp. 47053–47067, 2019, doi: 10.1109/ACCESS.2019.2907485.
- [69] K. Cabaj, M. Gregorczyk, and W. Mazurczyk, “Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics,” *Computers & Electrical Engineering*, vol. 66, pp. 353–368, Feb. 2018, doi: 10.1016/j.compeleceng.2017.10.012.
- [70] Z. Sadeqi-Arani and A. Kadkhodaie, “A bibliometric analysis of the application of machine learning methods in the petroleum industry,” *Results in Engineering*, vol. 20, p. 101518, Dec. 2023, doi: 10.1016/j.rineng.2023.101518.