INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY: APPLIED BUSINESS AND EDUCATION RESEARCH
2025, Vol. 6, No. 6, 2822 – 2835
http://dx.doi.org/10.11594/ijmaber.06.06.14

Research Article

Identifying Research Trends and Gaps in the Context of Linux and Unix Security

Raquel C. Adriano[1]*, Jahleine Marielle M. Calayag[1], Marian Minelli S. Cruz[1], Anthony U. Concepcion[2]

[1]College of Information and Communications Technology, Bulacan State University, 3000 City of Malolos, Bulacan, Philippines
[2]Bulacan State University – Bustos Campus, 3000 City of Malolos, Bulacan, Philippines

Article history:
Submission 03 May 2025
Revised 31 May 2025
Accepted 23 June 2025

**Corresponding author:*
E-mail:
raqueladriano143@gmail.com

ABSTRACT

Linux and Unix operating systems are fundamental to modern computing infrastructures, including cloud platforms, mobile devices, and supercomputers. With their increasing adoption, security has remained a persistent and evolving concern over the past two decades. This study conducts a systematic bibliometric analysis of 50 peer-reviewed journal articles and conference papers published between 2001 and 2020, segmented into four time periods: 2001–2005, 2006–2010, 2011–2015, and 2016–2020. Using citation analysis and co-word mapping via Mendeley and VOSviewer, the study identifies four main thematic clusters: (1) access control and authentication, (2) kernel-level vulnerabilities, (3) cloud and container security, and (4) mobile and Android-related threats. Early research focused on foundational topics such as system architecture and access control mechanisms, while more recent studies emphasized cloud-native security, virtualization, and mobile platform vulnerabilities. The analysis also reveals a significant disparity in research volume, with Linux-related studies dominating the field and Unix security receiving less than 20% of the total focus. This underrepresentation of Unix indicates a critical gap in the literature. These findings highlight not only the shifting priorities in open-source operating system security but also the need for renewed attention to Unix-specific threats and cross-platform security strategies in future research.

Keywords*: Linux security, Unix security, Operating system security, Cybersecurity trends, Bibliometric analysis, Access control, Authentication, Cloud security, Open-source security, Kernel vulnerabilities*

How to cite:
Adriano, R. C., Calayag, J. M. M., Cruz, M. M S., & Concepcion, A. U. (2025). Identifying Research Trends and Gaps in the Context of Linux and Unix Security. *International Journal of Multidisciplinary: Applied Business and Education Research*. *6*(6), 2822 – 2835. doi: 10.11594/ijmaber.06.06.14

Introduction

Over the past three decades, Linux has transitioned from a modest personal project into a foundational component of modern computing. As an open-source operating system, Linux has gained substantial traction across a broad spectrum of technological domains. It now underpins mission-critical infrastructures such as cloud platforms, data centers, high-performance computing environments, and embedded systems. Its influence extends to mobile devices, industrial control systems, consumer electronics, and even national security and defense platforms. According to Guo et al. (2004), Linux's appeal lies in its openness, adaptability, and cost-effectiveness, making it a preferred choice for developers and enterprises alike.

Recent industry reports further underscore its dominance. The Linux Foundation's *2017 State of Linux Kernel Development Report* revealed that Linux powered 90% of public cloud workloads and was the operating system of choice for nine out of the top ten public cloud providers. It also ran on approximately 82% of smartphones globally and accounted for a staggering 99% of the operating systems used in supercomputers. Moreover, Linux adoption has even outpaced Windows on Microsoft's Azure cloud platform, highlighting its growing significance in enterprise environments.

However, this widespread deployment has also made Linux an increasingly attractive target for cybercriminals and malicious actors. As more organizations transition their workloads to the cloud—often relying on Linux as the underlying operating system—the associated attack surface expands significantly. Threat vectors such as kernel vulnerabilities, privilege escalation, misconfigured containers, insecure authentication mechanisms, and malware targeting Linux-based systems have become more frequent and sophisticated. Unix-based systems, though less prominently featured in current discussions, continue to support critical legacy applications and infrastructure, making their security just as vital but often less studied.

Despite the escalating importance of securing Linux and Unix systems, the scholarly landscape remains fragmented and uneven. While Linux security has garnered considerable attention, Unix-related security research has not kept pace, resulting in critical blind spots within the broader cybersecurity discourse. Existing studies often concentrate on specific technical implementations or isolated security mechanisms, lacking a comprehensive, long-term perspective on how research in this area has evolved over time.

This study addresses that gap by conducting a systematic bibliometric analysis of Linux and Unix security research published from 2001 to 2020. Through the use of Mendeley and VOSviewer for citation analysis and co-word mapping, this work evaluates scholarly output across four distinct time periods: 2001–2005, 2006–2010, 2011–2015, and 2016–2020. The purpose is to uncover dominant research themes, identify leading contributors and publication venues, and detect underexplored areas in the literature.

By visualizing the intellectual structure and thematic development of this research field, the study offers a nuanced understanding of how academic focus has shifted—from early concerns about foundational security frameworks and access controls to more recent discussions on cloud-native security, mobile threats, and containerization. In doing so, it highlights not only what has been studied but also what remains to be explored, particularly in the context of Unix system vulnerabilities and emerging cross-platform threats.

Ultimately, this research contributes to the growing body of literature on cybersecurity by offering a historical and thematic overview of Linux and Unix security studies. It provides valuable insights for researchers, practitioners, and policymakers aiming to enhance the resilience of open-source operating systems in an increasingly complex and interconnected digital environment.

Related Literature and studies

The following related literature and studies were reviewed to guide and use as references for additional information in the conduct of our research.

Recent years have witnessed an increase in bibliometric analyses as a means of understanding the development of research fields. For instance, (Bao et al., 2025) conducted a bibliometric analysis of blockchain-related literature, identifying key publication trends, prolific authors, and thematic evolution. This study demonstrated the utility of bibliometric tools such as VOSviewer and Scopus for evaluating large volumes of scientific output in a structured manner, a methodology applicable to the domain of Linux and Unix security.

Similarly, (Ilić et al., 2024) applied bibliometric methods to examine the intersection of artificial intelligence and cybersecurity. Their findings revealed rapid growth in interdisciplinary research, with significant implications for Linux security, especially as AI becomes increasingly integral to intrusion detection systems and anomaly detection in Unix-like environments.

The study of Alqurashi & Ahmad (2024) provided another example of a scientometric study focused on cybersecurity literature. Through keyword co-occurrence mapping and citation analysis, they identified the main clusters of cybersecurity research and emphasized the need for deeper exploration of underrepresented subtopics. This approach provides a foundation for identifying neglected areas in Linux and Unix security scholarship.

Beyond bibliometric studies, a number of technical analyses offer insights into specific aspects of Linux security. (Brimhall et al., 2023) performed a comparative evaluation of mandatory access control mechanisms, such as SELinux and AppArmor, which are central to Linux's internal security architecture. Their findings highlight both the strengths and limitations of existing policy enforcement frameworks, underscoring areas where further research and improvement are needed.

The study of Lin et al. (2018) conducted a measurement study on the security of Linux containers, documenting prevalent attack methods and corresponding countermeasures. Given the increasing use of containers in cloud-native applications, their work is especially relevant to identifying new research directions focused on virtualization and isolation in Unix-based environments.

Moreover, Ren et al. (2019) examined the performance evolution of Linux core operations, revealing how optimization decisions can introduce security trade-offs. Their work reinforces the importance of considering both functionality and security in kernel development—a key consideration for Linux security researchers.

Other researchers have focused on broader trends in authentication, threat modeling, and adversarial testing. (Bezerra et al., 2022) carried out a 28-year bibliometric study of authentication systems and threat models, providing a longitudinal view of the development of foundational cybersecurity concepts. Such long-term analyses serve as a benchmark for this study's time frame, which spans two decades of Linux and Unix security literature.

The study of Staves et al. (2023) explored adversary-centric security testing in both information and operational technology contexts. Their findings are particularly relevant to the security of Unix-based systems used in industrial and critical infrastructure environments.

Baldwin et al. (2018) also conducted a bibliometric study in the area of cloud forensics, highlighting the growing reliance on Linux systems in virtualized platforms and the importance of forensic readiness. Their work suggests potential gaps in Linux-specific forensic tools and techniques, which can be addressed through targeted research.

The reviewed literature demonstrates a strong and growing interest in the application of bibliometric techniques to cybersecurity and related domains. While blockchain, AI security, and threat modeling have been thoroughly examined through scientometric lenses, a dedicated bibliometric analysis of Linux and Unix security remains notably scarce. Moreover, technical studies, although rich in detail, are often narrow in scope and do not provide a macroscopic view of the research landscape.

This gap justifies the current study, which aims to fill this void by systematically analyzing the corpus of Linux and Unix security research from 2001 to 2020. Through bibliometric mapping, the study seeks to identify leading contributors, dominant research themes, underexplored areas, and the evolution of security priorities within Unix-like operating systems.

Objectives

This study identifies research trends and gaps in Linux and Unix Security over 20 years, from 2001 to 2020. It seeks to analyze peer-reviewed journals, conference papers, and research articles in order to determine major producers, primary research themes, and notable publication outlets related to the subject of study. The following specific objectives guide the research:

- **Timeframe**: The study covers a 20-year period from **2001 to 2020**.
- **Research Focus**: It aims to identify **research trends** and **gaps** in the field of **Linux and Unix security**.
- **Sources Analyzed**: The analysis includes **peer-reviewed journal articles**, **conference papers**, and **research publications** relevant to the topic.
- **Objectives**:
  - Identify **major contributors** (authors, institutions, countries) to Linux and Unix security research.
  - Determine the **primary research themes** and **thematic trends** over time.
  - Highlight **notable publication outlets** in the field.
- **Temporal Segmentation**:
  To observe shifts in research priorities, the study divides the literature into **four temporal scales**:
  - 2001–2005
  - 2006–2010
  - 2011–2015
  - 2016–2020
- **Analytical Tools Used**:
  - **Mendeley**: for reference management and citation analysis.
  - **VOSviewer**: for co-word mapping, keyword clustering, and visualizing bibliometric networks.
- **Expected Contribution**:
  The study aims to uncover **gaps in the existing literature** and provide **evidence-based direction** for future research in Linux and Unix security.

Methods

I. Research Design

This study employs a descriptive research design to analyze research trends and gaps in the field. A bibliometric analysis approach was utilized to systematically review and categorize relevant literature. This design is appropriate as it enables a structured examination of publication trends over a defined period, facilitating an understanding of the evolution of research topics.

II. Participants/Respondents/Subjects

This study is not human-subject based and focuses on an extensive secondary data review of peer-reviewed literature. The inclusion criteria for literature selection were:

- Publication Type: Peer-reviewed journal articles, conference papers, and technical reports
- Publication Date: January 2001 to December 2020
- Language: English
- Relevance: The title, abstract, and keywords must focus on Linux and/or Unix security
- Database Indexing: Indexed in reputable scholarly databases such as:
  - Google Scholar
  - ScienceDirect
  - IEEE Xplore
  - ResearchGate
  - SpringerLink

Search Strategy:
Keyword combinations used for the initial search included:

- “Linux security”
- “Unix security”

Boolean operators (AND/OR) were applied where supported by the database.

III. Instruments (Materials/Measures)

The primary tools utilized for data collection and analysis included:
Citation Matrix: Used for organizing and evaluating 50 selected studies, with columns for Title, Author(s), Abstract, Link, Publication, and Keywords.

Mendeley Desktop & Mendeley Reference Manager: Reference management tools used for organizing sources and exporting .ris files for further analysis.

VOSviewer: It refers to software that enables bibliometric mapping and visualization of research activities, trends, and networks, including co-authorship.

Procedures

A thorough search of peer-reviewed literature was conducted across multiple databases, including Google Scholar, Science Direct, IEEE, ResearchGate, and SpringerLink. The selection criteria focused on studies published between 2001 and 2020. The review process involved the following steps:

a. Identification of relevant research papers using keyword searches.
b. Screening of articles based on relevance, citations, and journal impact.
c. Extraction of key details using the Citation Matrix.
d. Organization and management of references using Mendeley.
e. Exporting references in .ris format for bibliometric analysis using VOSviewer.

Data Analysis

Research trends were analyzed across the four standardized 5-year intervals (2001–2005, 2006–2010, 2011–2015, and 2016–2020). VOSviewer generated bibliometric maps highlighting:

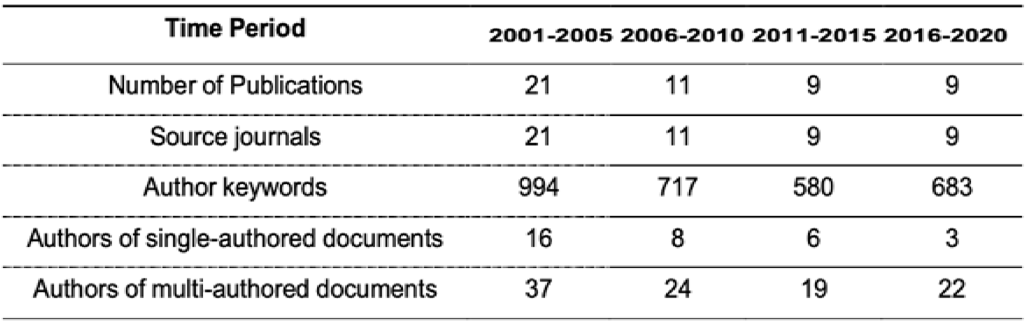
- Keyword clusters (frequent terms and themes)
- Temporal shifts in thematic focus
- Co-authorship and collaboration patterns
- Gaps in Unix-specific research topics

Publication volume and keyword frequency across time periods were tabulated and summarized in Table 1.

Ethical Considerations

This study uses secondary data, ethical issues are limited to the attribution of the sources. No confidential/personal data is included. The study keeps to the ethical principles of literature reviews, in particular, honesty about the information presented. No conflicts of interest or funding sources influenced the research outcomes.

Table 1. Main information of the relevant Linux and Unix security publications between the year of 2001 and 2020



Time Period	2001-2005	2006-2010	2011-2015	2016-2020
Number of Publications	21	11	9	9
Source journals	21	11	9	9
Author keywords	994	717	580	683
Authors of single-authored documents	16	8	6	3
Authors of multi-authored documents	37	24	19	22

A word cloud was used to analyze the Linux and Unix security research topics over time and reflect the dominant topics during each period. A 'word cloud' is a visual representation of word frequency. The more commonly a term appears within the analyzed text, the larger the word appears in the generated image. Word clouds are increasingly being employed as a simple tool to identify the focus of written material (Atenstaedt, 2012). Also, co-word analysis (Chen et al., 2016) was used to construct a cooccurrence map to reveal the research hotspots and evolution of each time slice. Co-word analysis is used in a longitudinal framework, allowing us to analyze the research field over consecutive periods. It also develops a performance analysis of specific themes using fundamental bibliometric indicators.

Author keywords are a list of terms that authors believe best represent the content of their papers. In the following study, the hot topics of each time slice are visualized by building the word cloud of author keywords. Since titles and abstracts can interpret the contents of a paper more comprehensively than keywords, terms extracted from titles and abstracts are used to construct the co-word map by VOSviewer, and the topic clusters of each time slice are analyzed based on the co-word map.

Results and Discussions

Research Trends Until 2020

I. Time Period: 2001 – 2005

From 2001 to 2005, the frequency of security occurrences was 82, which appeared to occur most often in over 50 articles. Several studies on security security have been conducted throughout this period (Figure 1). In addition, the frequency of research on systems during this period was also significant, with 63 occurrences. From the statistical results, the hot topics in 2001–2005 are shown in Table 2.

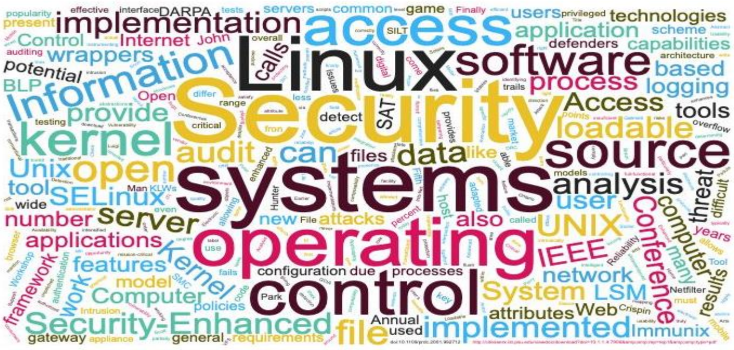


Figure 1: Keywords Cloud Map of 2001–2005

Table 2. Items and frequency of hot keywords between 2001–2005

Item	Frequency
Security	82
Systems	63
Linux	49
Control	16
Operating	16
Access	13
Source	13
Kernel	11
Software	10
Information	9

Table 3. Top cited paper over 50 articles during 2001–2005

Author Name	Year	Publication Journal	Title
Guo, Jinhong et al	*2004*	*IEEE Consumer Communications and Networking Conference, 2004*	*Applicability of low water-mark mandatory access control security in linux-based advanced networked consumer electronics*

During 2001–2005, the most cited work was written by (Guo et al. 2004) and published in IEEE Consumer Communications and Networking Conference, titled "Applicability of low water-mark mandatory access control security in Linux-based advanced networked consumer electronics."

VOSViewer is adopted to construct the terms cooccurrence map. Terms are extracted from the title and abstract fields, the minimum number of occurrences of a term is set as 10, and a relevance score is calculated for each term. Based on the score, 60% of the most relevant terms are selected to build the cooccurrence map (Figure 1). Purple clusters are studies of Linux, and the Green clusters are studies of access control. The red clusters are studies of Intelligent networks and Data Analysis. The yellow clusters are studies of Hash Functions and DNS, and the blue clusters are Control Systems studies. The analysis shows a strong presence of Purple clusters (Linux).

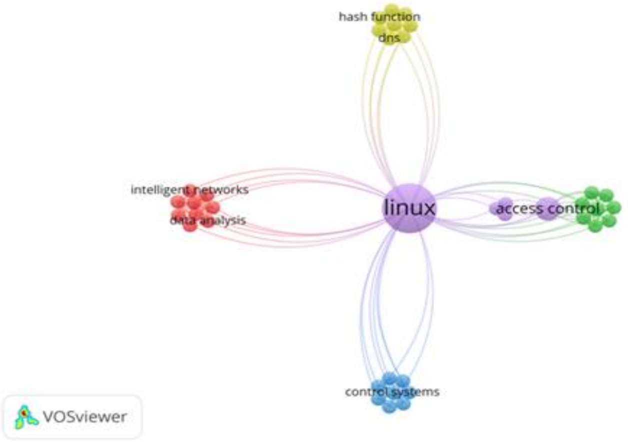


Figure 2: 2001–2005 term co-occurrence map.

II. Time Period: 2006 – 2010

From 2006 to 20010, Security declined but still has become a research focus, with 40 occurrences over the 50 articles. (Figure 3)

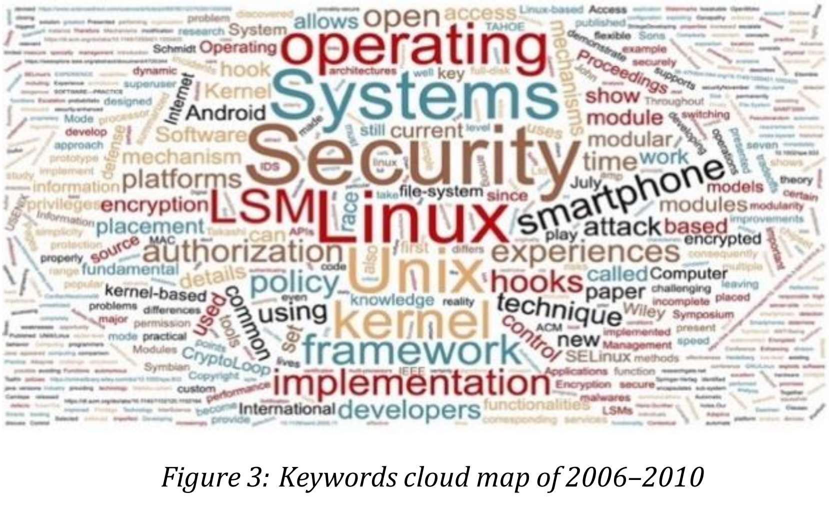


Figure 3: Keywords cloud map of 2006–2010

The 15 hot topics in 2006–2010 extracted from the statistical results are shown in Table 4. It is noted that two articles were cited between 2005 and 2009. This information is shown in Table 4 (Schmidt et al., 2008)(Cai, Gui, and Johnson 2009).

Table 3. Items and frequency of hot keywords during 2006–2010

Item	Frequency
Security	40
Linux	29
Systems	28
Unix	13
Kernel	12
Operating	12
LSM	11
Framework	9
Implementation	7
Smartphone	7
Authorization	6
Experiences	6
Hooks	6
Open	6
Policy	6

Table 4. Top cited papers over 50 articles during 2006–2010

Author Name	Year	Publication Journal	Title
Albayrak, Sahin et al	*2008*	*International Linux 2008*	*Enhancing Security of Linux-based Android Devices*
Cia X et al	*2009*	*Proceedings - IEEE Symposium on Security and Privacy*	*Exploiting Unix File-System Races via Algorithmic Complexity Attacks*

The term cooccurrence map are shown in Figure 4. Red clusters are researches on opengl, directx, windows, Linux, Mac OS x, and cyc window toolkit. There was just one distinct high concentration of clusters that occurred.

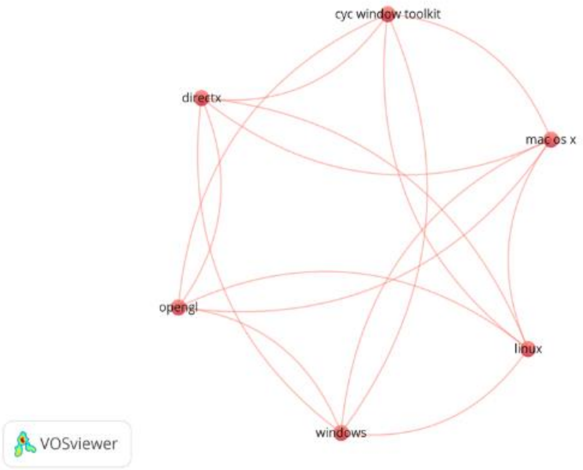


Figure 4. 2006–2010 Term Cooccurrence Map

III. Time Period: 2011 – 2015

From 2011 to 2015, research on Security increased, with 44 occurrences remaining at the hotspot. Furthermore, Systems occurred 26 times, and other popular keywords are shown in (Figure 5). The topic trends of 2011–2015 are illustrated in Table 5. One paper appeared to be the most cited between 2011 and 2015; the information is shown in Table 6 (Salah et al., 2013).

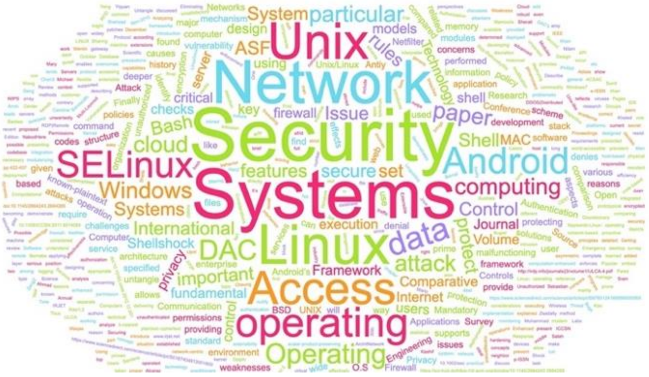


Figure 5. Keywords cloud map of 2010–2015

Table 5. Items and frequency of hot keywords during 2011–2015

Item	Frequency
Security	44
Systems	26
Linux	20
Network	20
Unix	16
Access	13
Operating	11
Android	8
SELinux	8
Data	7
DAC	6
Operating	6
Attack	5
Cloud	5
Computing	5

Table 6. Top cited papers over 50 articles during 2011–2015

Author Name	Year	Publication Journal	Title
Khaled Salah et al	*2013*	*Computers & Security*	*Analyzing the security of Windows 7 and Linux for cloud computing*

The term co-occurrence map of 2011–2015 publications is generated in Figure 6. The Green cluster is the study of Linux, Kernel, File System, and Groups, and the blue cluster is an Authorization, Security, Authentication, Protocol, Design, and Analysis. The red cluster is the study of Accounts, which requires Linux, Different Users, and integration. Here, an intense concentration is found in the blue cluster (Authorization, Security, Authentication, Protocol, Design, and Analysis), followed by the red cluster (Account which is required, Linux, Different User, and integrate to into).

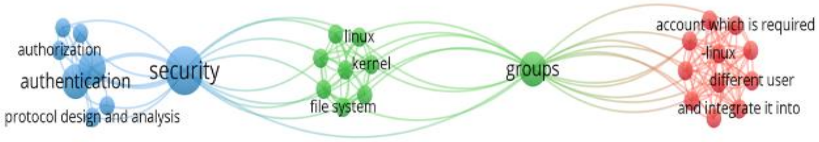


Figure 6: 2011–2015 term co-occurrence map

IV. Time Period: 2016 – 2020

From 2016 to 2020, Security is the most prevalent topic, with 36 occurrences. (Figure 7). The trending topics of each year during 2016–2020 are shown in Table 7. During the years 2016–2020, one paper appeared to be the most cited. (Table 8).

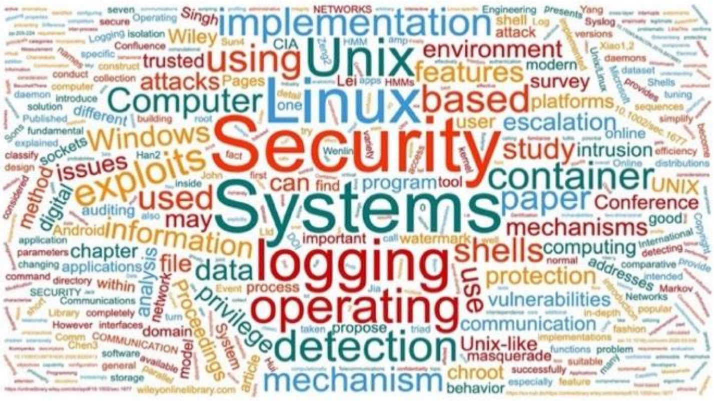


Figure 7. Keywords cloud map of 2016–2020

Table 7. Items and frequency of hot keywords during 2016–2020

Item	Frequency
Security	36
Systems	27
Linux	26
Logging	16
Unix	12
Operating	11
Detection	9
Based	8
Container	8
Exploits	8
Implementation	8
Using	8
Computer	7
Mechanism	7

Table 8. Top cited papers over 50 articles during 2016–2020

Author Name	Year	Publication Journal	Title
Abdullah Kidwai et al	*2008*	*Materials Today: Proceeding Volume 37, Part 2, 2020*	*A comparative study on shells in Linux: A review*

The terms extracted from the title and abstracts of 2016–2020 publications on Linux and Unix are used to build the cooccurrence map shown in Figure 4. Red clusters are studies on GNU, Foss, Scripting, Linux, Shells, and Zshell. It was interesting to note that the red cluster is more concentrated in studies.

During 2016–2020, the most cited work was written by (Kidwai et al., 2020) and published in Materials Today: Proceeding Volume 37, Part 2, 2020, titled "A comparative study on shells in Linux: A review."

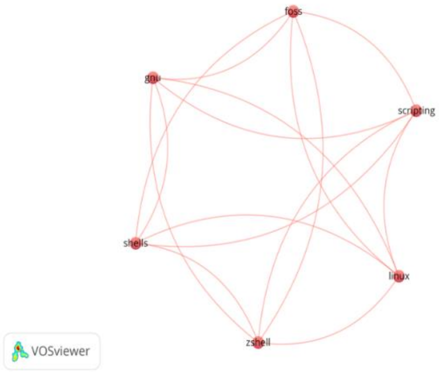


Figure 8. 2016–2020 term co-occurrence map

V. Summary of Research Trends: 2001 – 2020

From 2001 to 2020, appeared Linux as the main research hotspots as shown in (Figure 9 and Figure 10). Studies on Linux, security, Unix, authentication, access control, kernel, data analysis, operating systems, groups, DNS, Foss, and control systems were terms occurred.

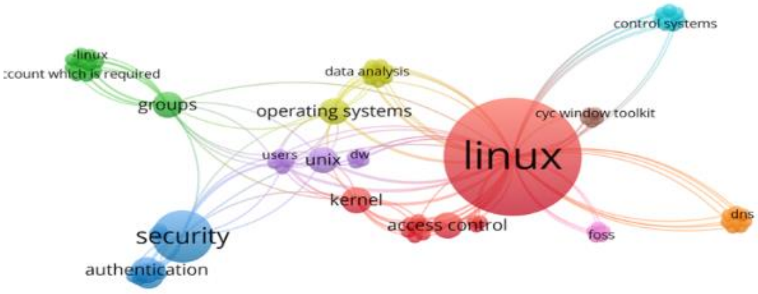


Figure 9. 2001–2020 term co-occurrence map

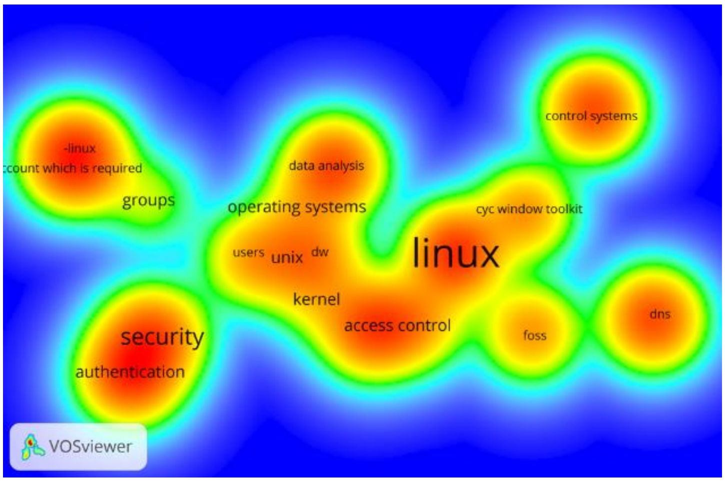
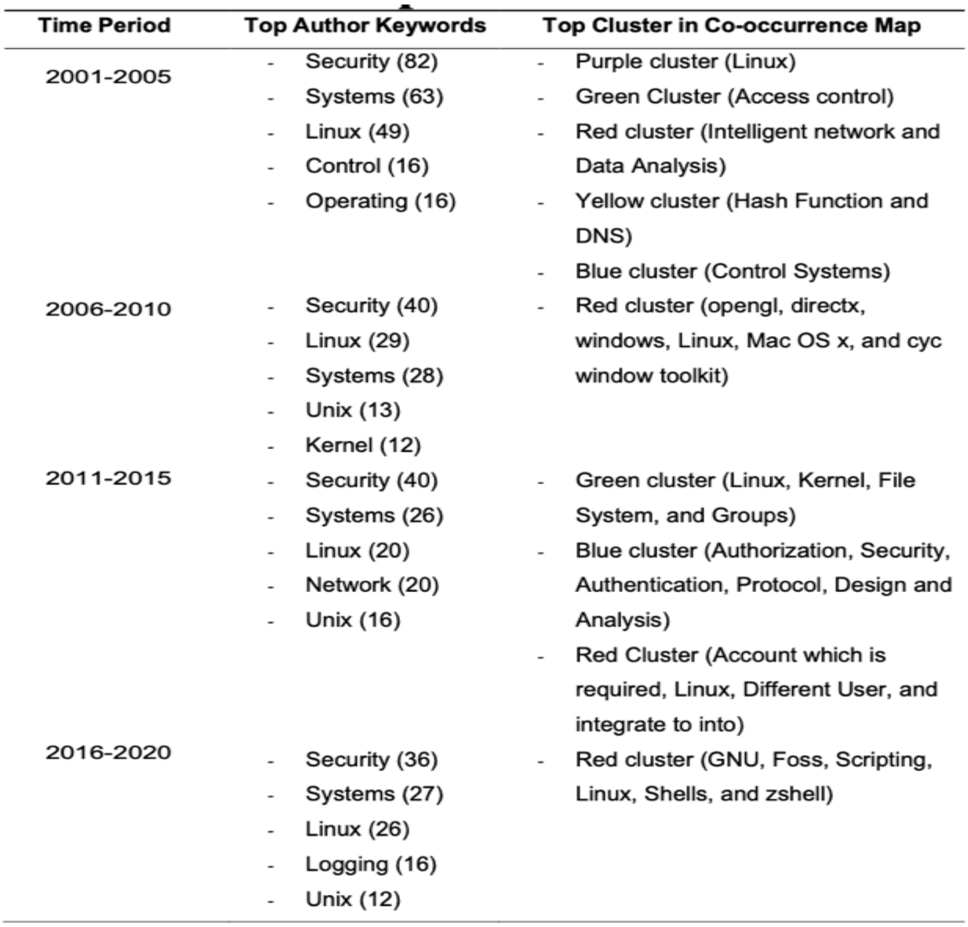


Figure 10. 2001–2020 term co-occurrence density map

Table 9 shows that in the four time periods, research on Security has been a hot spot, and many scholars have conducted research on Linux and Systems related to Linux, as well as access control, operating Kernel, Unix, and Networks. Logging is also counted in the top 5 hot topics after 2005. It is worth noting that the study of Cloud, Android, and SELinux (Security-enhanced Linux) in 2011–2015. From 2016 to 2020, many scholars have also studied GNU, Foss, Scripting, Linux, Shells, and zshell.

Table 9. Summary of word cloud and co-occurrence maps for four time series



Time Period	Top Author Keywords	Top Cluster in Co-occurrence Map
2001-2005	- Security (82) - Systems (63) - Linux (49) - Control (16) - Operating (16)	- Purple cluster (Linux) - Green Cluster (Access control) - Red cluster (Intelligent network and Data Analysis) - Yellow cluster (Hash Function and DNS) - Blue cluster (Control Systems)
2006-2010	- Security (40) - Linux (29) - Systems (28) - Unix (13) - Kernel (12)	- Red cluster (opengl, directx, windows, Linux, Mac OS x, and cyc window toolkit)
2011-2015	- Security (40) - Systems (26) - Linux (20) - Network (20) - Unix (16)	- Green cluster (Linux, Kernel, File System, and Groups) - Blue cluster (Authorization, Security, Authentication, Protocol, Design and Analysis) - Red Cluster (Account which is required, Linux, Different User, and integrate to into)
2016-2020	- Security (36) - Systems (27) - Linux (26) - Logging (16) - Unix (12)	- Red cluster (GNU, Foss, Scripting, Linux, Shells, and zshell)

Conclusions

This bibliometric study examined research trends in Linux and Unix security from 2001 to 2020 across four standardized 5-year intervals. The analysis revealed that Linux has consistently dominated the security discourse, with topics such as access control, authentication, and kernel-level protection emerging as central themes across all periods. While early research focused on foundational system components, more recent studies have shifted toward user-level environments, including scripting languages, shell tools, and FOSS applications—reflecting the evolving role of Linux in modern computing ecosystems.

Despite the extensive focus on Linux, the study found that Unix security has received significantly less attention, suggesting a critical gap in the literature. Given Unix's continued use in enterprise, government, and legacy systems, this underrepresentation warrants deeper investigation.

Limitations:

- The sample was limited to 50 articles, which may have excluded relevant but less-cited work.
- The analysis relied on author keywords and VOSviewer-extracted terms, which may omit nuanced or implicit thematic content.
- Citations and keyword frequency were used as primary metrics; other impact indicators (e.g., altmetrics, collaboration networks) were not included.
- Future Research Directions
- Deepen Unix-Focused Studies: Investigate Unix-specific vulnerabilities, legacy system threats, and security practices.
- Expand Bibliometric Scope: Use complementary tools like CiteSpace or Biblioshiny to explore collaboration patterns, thematic evolution, and citation bursts.
- Contextual Security Trends: Examine Linux/Unix security within specific domains such as cloud infrastructure, IoT, containers, and edge computing.
- Vulnerability Lifecycle Analysis: Study the timeline of known exploits and patching behavior in both Linux and Unix environments.
- Human Factors and Tool Usage: Assess how scripting tools and shell environments affect system security from a user behavior perspective.

Recommendations

The researchers suggests that future researchers should be able to add further emphasis to the trends by providing an analytical framework using various emerging technologies. The system may have LLM capabilities for data analytics and visualizations.

Acknowledgement

The researchers would like to sincerely thank all of the people involved in the research for their invaluable contributions to make the study possible. We are especially grateful to Dr. Teody C. San Andres, our university president, for providing the opportunity to conduct the study. Additionally, thanks to all of the collaborators who helped support the study.

References

Alqurashi, F., & Ahmad, I. (2024). Scientometric Analysis and Knowledge Mapping of Cybersecurity. International Journal of Advanced Computer Science and Applications, 15(3), 1177–1184. https://doi.org/10.14569/IJACSA.2024.01503117

Atenstaedt, Rob. 2012. "Word Cloud Analysis of the BJGP." *British Journal of General Practice* 62(596):148. doi: 10.3399/bjgp12X630142.

Baldwin, J., Alhawi, O. M. K., Shaughnessy, S., Akinbi, A., & Dehghantanha, A. (2018). Emerging from the cloud: A bibliometric analysis of cloud forensics studies. Advances in Information Security, 70, 311–331. https://doi.org/10.1007/978-3-319-73951-9_16

Bao, L., Yang, J., Yang, X., & Rong, C. (2025). Bibliometric Analysis of Scientific Publications on Blockchain Research and Applications. 0921, 0–3. http://arxiv.org/abs/2504.13387

Bezerra, W. dos R., de Souza, C. A., Westphall, C. M., & Westphall, C. B. (2022). A Bibliometrics Analysis on 28 years of Authentication and Threat Model Area. September. https://doi.org/10.48550/arXiv.2209.12985

Brimhall, B., De La Garza, C., Garrard, J., & Coffman, J. (2023). A Comparative Analysis of Linux Mandatory Access Control Policy Enforcement Mechanisms. EUROSEC 2023 - Proceedings of the 2023 European Workshop on System Security, 1–7. https://doi.org/10.1145/3578357.3589454

Cai, Xiang, Yuwei Gui, and Rob Johnson. 2009. "Exploiting Unix File-System Races via Algorithmic Complexity Attacks." *Proceedings - IEEE Symposium on Security and Privacy* 27–41. doi: 10.1109/SP.2009.10.

Chen, Xiuwen, Jianming Chen, Dengsheng Wu, Yongjia Xie, and Jing Li. 2016. "Mapping the Research Trends by Co-Word Analysis Based on Keywords from Funded Project." *Procedia Computer Science* 91(Itqm):547–55. doi: 10.1016/j.procs.2016.07.140.

Guo, Jinhong K., Stephen Johnson, David Braun, and Il Pyung Park. 2004. "Applicability of Low Water-Mark Mandatory Access Control Security in Linux-Based Advanced Networked Consumer Electronics." *IEEE Consumer Communications and Networking Conference, CCNC* 364–69. doi: 10.1109/ccnc.2004.1286889.

Ilić, L., Šijan, A., Predić, B., Viduka, D., & Karabašević, D. (2024). Research Trends in Artificial Intelligence and Security—Bibliometric Analysis. Electronics (Switzerland), 13(12). https://doi.org/10.3390/electronics13122288

Kidwai, Abdullah, Chandrakala Arya, Prabhishek Singh, Manoj Diwakar, Shilpi Singh, Kanika Sharma, and Neeraj Kumar. 2020. "A Comparative Study on Shells in Linux: A Review." *Materials Today: Proceedings* 37(Part 2):2612–16. doi: 10.1016/j.matpr.2020.08.508.

Lin, X., Lei, L., Wang, Y., Jing, J., Sun, K., & Zhou, Q. (2018). A measurement study on linux container security: Attacks and countermeasures. ACM International Conference Proceeding Series, 418–429. https://doi.org/10.1145/3274694.3274720

Ren, X., Rodrigues, K., Chen, L., Vega, C., Stumm, M., & Yuan, D. (2019). An analysis of performance evolution of Linux's core operations. SOSP 2019 - Proceedings of the 27th ACM Symposium on Operating Systems Principles, 20, 554–569. https://doi.org/10.1145/3341301.3359640

Salah, Khaled, Jose M. Alcaraz Calero, Jorge Bernal Bernabé, Juan M. Marín Perez, and Sherali Zeadally. 2013. "Analyzing the Security of Windows 7 and Linux for Cloud Computing." *Computers and Security* 34:113–22. doi: 10.1016/j.cose.2012.12.001.

Schmidt, Aubrey-derrick, Hans-Gunther Schmidt, Jan Clausen, Ahmet Camtepe, Sahin Albayrak, Kamer Ali Yüksel, and Osman Kiraz. 2008. "Enhancing Security of Linux-Based Android Devices." *15th International Linux Kongress* (August 2015).

Staves, A., Gouglidis, A., & Hutchison, D. (2023). An Analysis of Adversary-Centric Security Testing within Information and Operational Technology Environments. Digital Threats: Research and Practice, 4(1). https://doi.org/10.1145/3569958