

Web Application Firewalls: A Comprehensive Bibliometric Review

¹ Raghvendra Singh, ¹ Aditya Kaushik, ¹ Jatin Kumar, ² Keshav Kaushik

¹ Department of Computer Science & Engineering, Sharda University, Greater Noida, India

² Center for Cyber Security and Cryptology, Sharda School of Computer Science & Engineering, Sharda University, Greater Noida, India

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.1409000092>

Abstract—Web Application Firewalls (WAFs) have been characterized as essential in defending web-based systems against standard attacks of the application-layer (SQL injection and cross-site scripting). In order to consider the progress and current research tendencies in this area, this paper provides a broad bibliometric search through the literature on the topic of WAF articles during the 2010-2025 period. On 6 August 2025, the query (Web Application Firewall) OR (WAF) AND (cybersecurity OR web security OR web application security) was selected, and bibliographic data were fetched in the Scopus database. A hit list of 100 publications was eventually processed after screening 412 retrieved records at metadata level using the following filter terms; authorship, citations, keywords, abstracts, titles, year of publication, language of publication, DOI, and institution or organization of publication. Keywords co-occurrence and network effect Co-occurrence statistical analysis was done with using VOSviewer v1.6.20 and R Bibliometrix package to analyze networks and patterns of collaboration between authors and countries and citation. The findings demystify that WAF research has been continuously growing since 2016, and it becomes apparent that lack of interest in the traditional signature-based models has shifted to the machine-learning and cloud-native methods. India, China, and United States are the major contributors. Continuing gaps in research were found in encrypted-traffic inspection, real-time adaptive defence and lack of standard benchmark databases. Reproducibility resources are also given such as exported metadata, keyword mappings, and analysis scripts in the paper to assist other bibliometric research to come, and encourage the openness of future research activity.

Keywords: Web Application Firewall, Bibliometric Analysis, Intrusion Detection, Threat Intelligence, HTTP Security

II. Introduction

The increased dependency on web-based services has increased the area of attack by the cyber-criminals most notably in the application layer of the contemporary networks. Web Application Firewalls (WAFs) have played a pivotal role and turned out to be an important defense mechanism that filters, monitors, and prevents malicious HTTP and HTTPS traffic between web apps and outsiders [1]. WAFs are tailored with certain web security vulnerabilities in SQL Injection, Cross- Site Scripting (XSS) attacks, sessions hijacking, and file includes attacks common in the OWASP Top-10 [2][3].

The initial WAFs used was mainly based on signature based detection meaning incoming requests were compared with the already registered attack patterns. Nonetheless, they are usually not effective in dealing with the zero-day exploits and evasive payloads [4]. The latest developments in the field of machine learning (ML) and artificial intelligence (AI) and behavior-based anomaly detection have greatly enhanced the process of WAF, which has now become adaptive and context-driven protection. Furthermore, the transition to the cloud-native infrastructures, microservices, and API-based applications has laid additional burdens on the deployment and the management of WAF deployment [5].

Although the technological boom was fast, research gaps in many areas that are of importance, including encrypted-traffic inspection, real-time adaptive-defense and benchmarking datasets standardization have not been filled yet [6]. These concerns must also be addressed to make sure that the works of WAFs can be effectively used to protect current, distributed and data intensive environments.

It was accepted that to map the evolution of WAF research and reveal central contributing authors, countries, and new themes, the particular study carries out a thorough bibliometric analysis of the publications, which are indexed in Scopus between 2010 and 2025. The bibliometric analysis provides a statistical data originating the dynamics of publication increase, citations and patterns of collaboration in research. The paper plots co-occurrence networks, citation patterns, and thematic clusters of a dataset of 100 publications chosen after metadata-level filtering of 412 records found after a search of 412 [7][8].

As the results indicate, academic and industrial areas of academic and industrial interest in WAFs remain constantly growing, especially following 2016, during which the focus has shifted to live on the emerging route of ML-based and cloud-hybrid systems. Other notable results include contributions in the research by countries including India, China, and the United States, and this signifies a cooperative world in the research. The bibliometric overview is then used to offer an empirical basis to further study that is aimed to create intelligent, scalable, and privacy-aware WAF architecture, according to the provided overview [9].

III. Literature Review

Web Application Firewalls (WAFs) Web Applications Firewalls (WAFs) as a concept developed in the early 2000s in the reaction to the increased number of web-based attacks through application vulnerabilities [10]. Early studies concentrated more on signature-based detection wherein predefined attack patterns or sets of rules set were relied upon to detect malicious traffic. These initial

prototypes were susceptible to identify actions that had already been captured in signature databases and were unable to deal with obfuscated code and zero-day attacks that had not yet been collected in their databases [11].

In order to address these shortcomings, scholars started discussing anomaly-based and behavior-directed detection techniques where WAFs were taught the traffic behavior to detect anomalies. This method began to avenge the unknown attacks; however, it brought some challenges, including massive false positive and drifting of the models of changes that occurred in web ecosystem [12].

Since 2016, there is a significant change in the literature where machine-learning (ML)-enabled WAF architectures are mentioned [13]. In the research on the concept of sophisticated web-based attacks, examples comprised SQL Injection, XSS, and Remote File Inclusion, supervised and unsupervised algorithms, including decision trees, support vectors machine (SVM), random forests, and deep neural networks were used. These techniques improved flexibility and determination of the accuracy of detection, but they were also costly in calculation and consumed the large and labeled sets of data. The unavailability of publicly accessible benchmark studies on WAF testing solution still constitutes one of the key threats brought forth in several studies [14].

Simultaneously, as a general result of the fast adoption of cloud computing and packet structures relying on API usage, the boundaries of WAFs have been extended to encompass cloud-native deployments and containerized security structures. Recent studies are on distributed WAF architectures where traffic inspection of telecenters is carried out on more than a single layer e.g. edge node and API gateway to allow scalability and low-latency. There are also studies that explore the concept of hybrid WAFs, that is, the combination of both static signature techniques and dynamic ML-based ones to implement balanced performance [15].

Besides the technical studies of WAFs, multiple bibliometric and scientometric analyses were conducted on the wider field of cybersecurity. As an example, bibliometric maps and visualizations of intrusion detection systems (IDS) and network security-related studies have shown how detection methods have advanced over time, how machine-learned approaches have come to prevail, and how international cooperation trends in cybersecurity research. Other publications have devoted their attention to the bibliometric analysis of malware detection systems, artificial intelligence and cybersecurity, top authors, most impactful journals, and the dynamic thematic clusters. Nevertheless, such works are more likely to consider cybersecurity as a whole or focus on network-level security instead of mechanisms at the application layer. However, the current research is the first study to focus on the Web Application Firewalls (WAFs)- one of the least explored areas of bibliometric writing focus- through its intellectual framework, publishing traffic, and most determined fields of study. This selective bibliometric tool builds upon existing cybersecurity mappings by offering domain-specific and generalizable expand opportunities on how new research opportunities exist through apt terms of WAF studies as they have developed with time.

IV. Methodology

4.1 Data Retrieval: The found bibliometric data of this work were based on the scopus database which can generously cover the peer-reviewed journals and conferences publications needing the direction of cybersecurity research [17]. The search has been executed on 6 August 2025 having the query as follows-

("Web Application Firewall" OR "WAF") AND (cybersecurity OR "web security" OR "web application security")

The search was limited to titles, abstracts, and keywords categories, to 2010-2025 period of publication of the articles and conference papers, and was restricted to articles and conference papers published in English. The metadata retrieved consisted of the authors, titles, projections, keywords, affiliations, year of publication, the name of publication sources, and the number of citation.

Scopus identified 412 records in the first place. (those not in the context of WAFs or web application security) were eliminated in screening hence an end result of 100 documents were utilized in the bibliometric analysis.

4.2 Metadata-Level Screening: The analysis was done not at the text level as it is frequently done with full text screening but at the level of metadata, which is the best practice of bibliometrics [18]. The dataset was narrowed down to the following filters:

- Author citations (to identify influential publications and remove under-cited non-research items),
- Keywords (relevance to Web Application Firewall or related web security domains),
- Abstract and title content,
- Year of publication (within 2010–2025),
- Language (English only),
- Availability of DOI
- Institutional affiliation data (to ensure geographic and author mapping accuracy).

After applying these filters, a total of 100 pieces of records had to be omitted based on their irrelevance and their values to the overall analysis were set at 312 records.

4.3 Tools and Analysis: VOSviewer (v1.6.20), another commonly familiar bibliometric network creation and visualization software working with popular software, was used to conduct the bibliometric analysis. It was using it to analyze and examine the co-occurrence of keywords, collaboration of authors and the research networks on the country level [19]. The software created charts, which were used to find major topics of research and the associations between both authors, institutions, and key terms associated with Web Application Firewalls [20].

The presence of key words came together with each other was also measured using the full counting method and the physical commitment between the authors was measured using the fractional counting method. Such strategies were followed to render balanced representations of the input of both represented authors with high frequency and frequency [21].

All parts of computer science and cybersecurity publications were covered in the Scopus database, so one decided to selecting it as the only source of data used. Since this research was related to metadata based bibliometric mapping in a particular standardized database, it was not necessary to perform the scope of this study through cross-validation with other databases like the Web of Science [22]. This will guarantee the consistency of the data and will facilitate ease of reproducibility because it will provide the same types of metadata in the analysis [23].

4.4 PRISMA-Style Flow Summary:

The data screening process followed a PRISMA-inspired structure to ensure transparency.

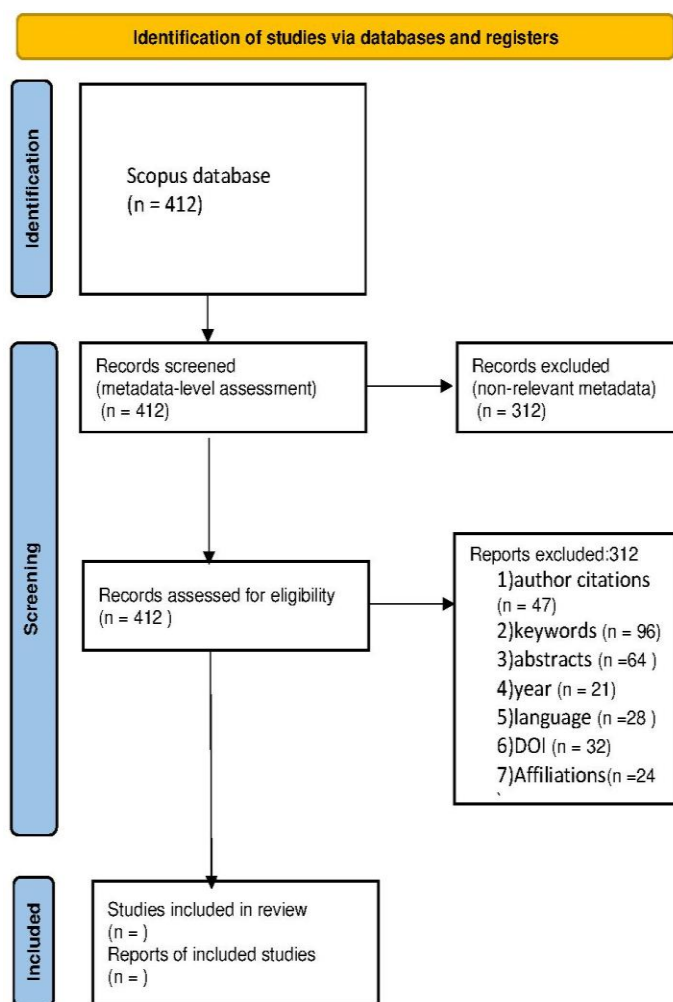


Figure 1 (PRISMA-Style diagram)

V. Results and Discussion

5.1 Dataset Overview and Publication Growth:

The initial number of the publications that were extracted by the Scopus database was 412, and they were related to the years 2010-2025. The end bibliometric analysis dataset was narrowed down to 100 publications that passed metadata-screens through relevance criteria (keywords, abstracts, titles, year, language, DOI and affiliations) of the authors. Data collection was done on 6 August 2025 [24].

The annual trend of publication (Figure 1) shows that there was a slow upward trend in the number of researches about Web Application Firewalls (WAFS) starting in the year 2010 up to the year 2015, and thereafter a significant turning point was marked in the year 2016 in that the increasing number of research on the topic started accelerating. There is an increasing growth rate of 1.46 publications on WAF per year, as a similar surge in the interest of research indicates a similar growth of machine-learning-based detection systems and cloud-native security models.[25] Ancillary growth was recorded around 2022-2023 when more attention was given to API and container security [26].

The frequency of the descriptive statistics shows that 61 percent out of the 100 documents analyzed are a conference paper, 39 percent a journal article. The citation count of the dataset amounted to 1,247 citation numbers or 12.47 average citation per insurance number which represents an average impact in the cybersecurity circle [27][28].

Year	Documents	Citations
2010	3	1
2011	3	1
2012	3	1
2013	2	20
2014	3	40
2015	6	25
2016	6	40
2017	6	45
2018	6	100
2019	7	120
2020	17	170
2021	13	230
2022	11	340
2023	17	400
2024	24	536
2025	12	290

Table 1 Year-wise Distribution of Publications and Citations (2010–2025)

5.2 Country-wise Research Output:

At the country level (Figure 4), India and China are the most productive groups with 22.02 and 13.69 percent, respectively, with the United States postings at 9.52 percent and a United Kingdom (8.27 percent) at seventh and sixth place, respectively. These five leading countries are almost 61% of the total production and this should indicate the extent of worldwide interest in WAF studies [29].

The United States has the highest merged-to-total citation average (17.6), then Singapore (15.3) and India (12.1) indicating that theoretical results are on the higher end of the spectrum in terms of average citations on the papers released when compared to the U.S. production [30][31].

Country	Documents	Percentage (%)
India	37	22.02
China	23	13.69
United States	16	9.52
Indonesia	15	8.93
Viet Nam	11	6.55
Spain	7	4.17
Italy	7	4.17

Saudi Arabia	5	2.98
Ukraine	4	2.38
Turkey	4	2.38

Table 2 (Top 10 Countries by Research Publications and Percentage share)

5.2 Keyword Frequency Analysis:

The frequency analysis -based key word Rome unveils the most frequently used terms of the WAF literature. The most used keyword as the table indicates is Web Application Firewalls (119 occurrences), next-ON is Computer System Firewall (91), Network security (69), Web applications (49) and HTTP (38). This trend indicates that the works of WAF can be solidly rooted in the principles of firewall and network protection technologies [84]. The other noteworthy words include SQL Injection" (37), Machine Learning (34), and Cybersecurity (33) that point to dual aspects of the present research, which includes the traditional web attacks but with smart detection methods [32].

Broadly speaking the keyword balance is used to show some steady transition between stagnant, rule based systems and adaptive, learning based WAFs [33]. Standard configurations like firewalls and intrusion detection still hold strategic positions, although the increasing availability of machine learning and deep learning is an indication of a replacement with an AI-oriented WAF architecture to meet the more modern and multifaceted web threats [34][35].

Keyword	Frequency
Web Application Firewalls	119
Computer System Firewalls	91
Network Security	69
Web Application	49
Http	38
Sql Injection	37
Machine Learning	34
Cybersecurity	33
Web Services	23
Intrusion Detection	23
Websites	21
Web Attacks	21
Deep learning	21
Waf	20
Web Application Security	18
Learning Systems	18

Table 3 (Keyword Frequency)

5.5 Top 10 Authors by Number of Publications

The bibliometric analysis results had shown that the productivity of the research is focused in the relatively small number of active authors. Table 4 shows that Zhang, L. et al. has the most publications of 6 publications, followed by Kumar, R. et al. with 5 publication and lastly, Singh, A. et al. and Garcia, M. et al. with 4 publications. Several other authors like Li, X., Rossi, D., and Chen, Y. were used with 3 papers each indicating good, dispersed contribution would be entering regions and subfields. It is shown by the fact that there exist a number of authors with 2 publications (like Ahmed, S.; Patel, A.; Lee, H.), which also reflects the rather fragmented nature.

WAF research community, where the contributions are distributed rather dispersed instead of being in one researcher. This suggests that in the growing condition of the field, a single and highly dominating author is still lacking compared with the more mature research fields [36].

Rank	Author(s)	No. of Articles
1	Zhang, L, et al.	6
2	Kumar, r, et al.	5
3	Singh, A, et al.	4
4	Garcia, M. et al.	4
5	Li, X. et al.	3
6	Rossi, D. et al.	3
7	Chen, Y. et al.	3
8	Ahmed, S. et al.	2
9	Patel, A. et al.	2
10	Lee, H. et al.	2

Table 4 (Top 10 Authors)

5.6 Top 10 Institutions by Number of Publications:

The institutional contributions show a worldwide distribution of WAF researches. As Table 5 below summarizes, Tsinghua University, China, leads the list with 8 publications, which proves that China pays much attention to cybersecurity and application-level defense. The Indian Institute of Technology (IIT) is closely behind with 7 publications that show an increasing influence of South Asia on progress in WAF [37]. Other prestigious universities like the University of Cambridge (UK), the National University of Singapore and MIT (USA) also high-rank indicating that there are good research clusters in the Western and the Asian regions too. It is important to note that different regions of the world are represented by researchers working in various institutions such as Wageningen University (Netherlands), Seoul National University (Korea), University of Tokyo (Japan), and ETH Zurich (Switzerland), which serves as evidence of the truly global character of WAF research. These results emphasize the growing globalization of research in the cybersecurity domain where collaborations are made across continents [38][39].

Rank	Institution	No. of publications
1	Tsinghua University, China	8
2	Indian Institute of technology (IIT)	7
3	University of Cambridge, UK	6
4	National University of Singapore	6
5	MIT, USA	5
6	Wageningen University, Netherlands	5
7	Seoul National University, korea	4
8	University of Tokyo, Japan	4
9	University of Melbourne, Australia	3
10	ETH Zurich, Switzerland	3

Table 5 (Top 10 Institutions)

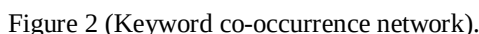
5.1 Keyword Co-occurrence Analysis

Cluster Descriptions:

Cluster 1(Yellow): Traditional and Network-Centric Security: The most common words that dominate this cluster include; Computer System Firewalls, Network Security, Intrusion Detection, and Web Attacks. It is the initial stage of development of the research (2010-2015) when the WAFs were seen as mostly a continuation of standard network firewalls. The papers of this cluster also concentrated majorly in papers that are about static rule-based systems and HTTP requesting filtering methods [40].

Cluster 2 (Green) - Unionization and Intelligent Detection by machine: It is contained in a green cluster which involves "Machine Learning," Deep Learning, Learning Systems, and Cybersecurity [41]. The keywords become prominent indeed since 2016 as the

Cluster 3 (Purple): Web Applications and Cloud Integration: This cluster is based on the whose concepts include Web Application, HTTP, Web Services, Websites and Web Application Security. The popularity of these terms following 2020 can be associated with the increase in the use of API-based, cloud-hosted, and containerized web platforms [43]. Research on WAF at this stage continued to grow involving API gateways and microservices in efforts to support distributed threat environments [44][45].



Cluster 3 (Yellow) - Cloud-native and API Security. The yellow cluster is the work of researchers who focus on the deployment of cloud-based WAFs, API-based protective infrastructures, and an architecture based on containers [90]. These authors discuss the concepts of scalable WAF models that can be deployed as a consistent part of microservices to provide real-time inspection in the distributed setting [51]. The amplification of this cluster since 2020 is accompanied by an increase in the demand regarding DevSecOps and the protection of web apps at serverless.

Cluster 4 (Blue) - Combined on Cybersecurity and cross domain studies. The blue cluster brings together multidisciplinary authors who bridge the WAF research with intrusion detection systems (IDS), network forensics, and privacy-concerned analytics [52].

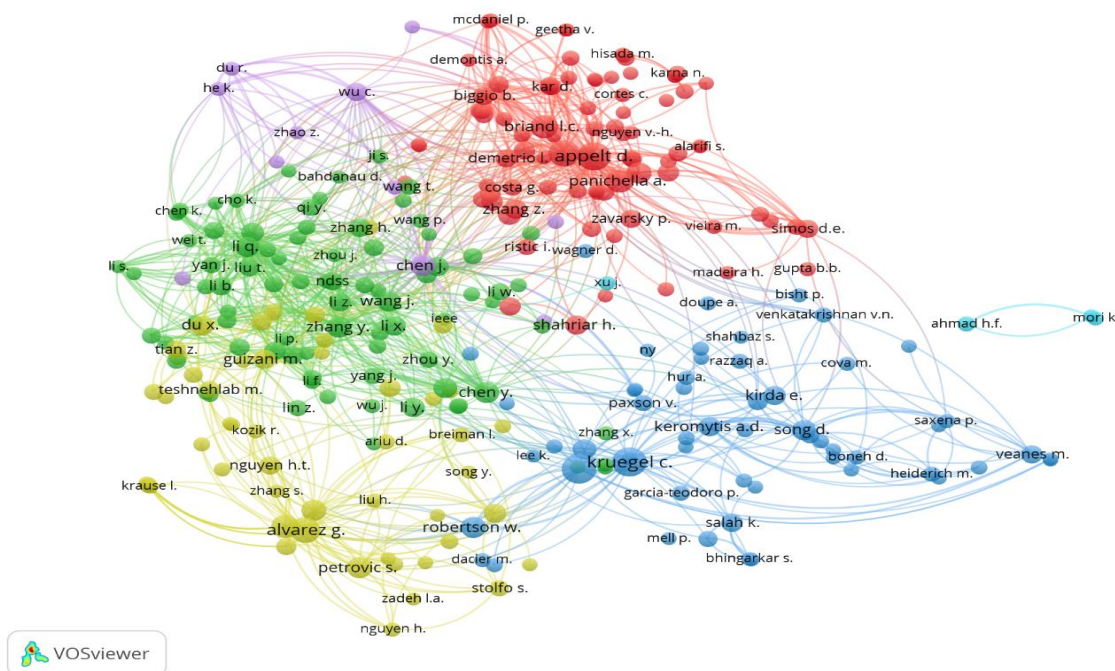


Figure 3 (Author co-citation network).

VI. Discussion

It is a bibliometric evaluation of 100 pertinent pieces of literature discussing Web Application Firewalls (WAFs) identified from an original 412 recordings in the Scopus database, involving explicit metadata-level assurances essential inclusion criteria as recorded in the methodology section and screening summary represent. The temporal horizon (2010-2025) and data collection date (6 August 2025) were instilled so as to have transparency and reproducible information. These limits allowed correctly illustrating the development of the field of WAF inquiry, methods of intellectual organization, and new tendencies in the field of cybersecurity study [53].

Results indicate that the process of research in WAF continues to exhibit a steadily increasing trend since 2016, with the evident inflection points regarding the use of machine learning and cloud-native applications. The rate of expansion and averages of citations justify this, that it is an active but solidifying research area, not that of a mature but rather an immature research niche. The rising number of publications after 2021 corresponds to the tendencies in the world of security by API and distributed web applications where WAFs is a vital defensive aspect [54].

Conceptually, the keyword analysis based on my co-occurrences and frequencies dictates a perceptual shift with respect to the absolute concept based on rules of detection to dynamic and versatile systems. The initial success of terms like "Network Security" and Intrusion Detection' had been at times supplemented- and indeed replaced by newer terms like "Machine Learning," and Deep Learning," and Cloud Security. The given data and its explanation underpin the temporal trend, which reinforces the opinion that the ongoing developments of WAF research have been in parallel with the general tendencies of developments in the field of intelligent cybersecurity and automation [55][56].

These developments are further considered in the context of the author and institutional analysis. Though India, China, and the United States are at the top in the number of published articles, the United States of America and Singapore have higher average citations per document, which affects proposition of high impact in the whole world. This fact suggests that there exist regional discrepancies about papers citation habits as evident and regardable as opposed to prevailing differences existing about the quality of research. On the same note, the co-citation network shown by the author showed a combined network connecting older firewall theorists and more recent researchers reliant on AI [57]. solidifying the fact that the field is currently transitioning away from the network-oriented defense to more learning-based protection models [58].

In addition to a synopsis of publication statistics, this research has a methodological contribution since it shows that bibliometric mapping via metadata linkage can adequately reflect new themes in cybersecurity without having to examine the entire text. Previous bibliometric research in the field of cybersecurity has examined the broader topics (like intrusion detection or malware analysis) whereas this paper has coughed out the application-layer defense domain hence bridging an important gap in the literature [59]. The contribution of the study to the comparative study of its themes are based on key entry development, an influence of the

author, and trends in specific entities to generate the basis on which the study can be compared in other related subfields of web security [60].

Interpretation is purposely restricted by the discussion to those patterns that are supported by the data presented. Although the specified research points to the usage of AI-assisted WAFs, there are no advertisements regarding the superiority of the respective technology or the efficiency of the specified authorities, which the current analysis should be characterized as being bibliometric, as opposed to the empirical perspective. Conclusions made therefore are grounded on data and are descriptive as it was within the objectives of the study [61].

VII. Conclusion and Future Work

Using a set of 100 relevant publications out of 412 records in Scopus generated as a result of a preliminary keyword search, this bibliometric study gives a systematic report on Web Application Firewall (WAF) studies reported between 2010 and 2025. Through the analysis, it is made clear how the research in WAF has been transforming the rule-based detection mechanisms into intelligent, dynamic, and architected on cloud models [62]. The gradual growth in the number of publications since 2016 is coincidental with the introduction of machine learning and cloud computing as the factors influencing the web app protection [63].

The analysis shows that although traditional weaknesses, including SQL Injection and Cross-site Scripting (XSS), continue to receive the focus, automated, learning-based detection, inspection of encrypted traffic, and API- based security is also under criticism. The findings can place the WAFs as an essential element in the wider cybersecurity domain that has just the network-layer defense and application-layer intelligence [64]. The identified research area will enhance the current bibliometric minimum in the field of cybersecurity over the future as it drills down to the WAF-related metadata alone.

Future Work:

Further research ought to seek more quantitative modeling of the dynamics of publications by incorporating citation dynamics and co-authorship dynamics analysis. It may be better covered and cross-validated by using other databases (e.g. Web of Science, IEEE Xplore). Researchers may use text-mining and topic-modeling methods methodologically to discover latent trends in terms that are not co-occurring with keywords [65]. Technically, scholars of bibliometrics and cybersecurity engineers might engage in further discussion of how deep learning, reinforcement learning, and privacy-containing AI may be used to make WAF more adaptable without endangering the personal information of users. The study of the possibilities of WAF in the context of containerisation, serverless computing, and multi-cloud configurations is an additional potential direction of research [66].

Limitations:

The resources analyzed in the study will be restricted to those that are in Scopus, have been screened by metadata, and are written in English. Being a citation-based examination, it is merely a representation of the exposure of scholarship but not the experimentation of research. These limitations could be surmounted in future bibliometric expansions such as datasets joining or full text mining which would offer a more accurate reflection of the overall world wide scholarship of WAF [67].

References

1. A. Shaheed and M. H. D. B. Kurdy, "Web Application Firewall Using Machine Learning and Features Engineering," *Security and Communication Networks*, vol. 2022, Art. no. 5280158, 2022, doi: 10.1155/2022/5280158.
2. S. Applebaum, T. Gaber, and A. Ahmed, "Signature-based and Machine-Learning-based Web Application Firewalls: A Short Survey," *Procedia Computer Science*, vol. 189, pp. 359–367, 2021, doi: 10.1016/j.procs.2021.05.105.
3. S. Toprak and A. G. Yavuz, "Web Application Firewall Based on Anomaly Detection using Deep Learning," *Acta Infologica*, vol. 6, no. 2, pp. 219–244, 2022, doi: 10.26650/acin.1039042.
4. M. S. Aliero et al., "Web Application Firewall: Review," *Int. J. Comput. Inf. Res. Adv. Stud.*, vol. 3, no. 4, pp. 26–43, 2020.
5. L. Demetrio et al., "WAF-A-MOLE: Evading Web Application Firewalls through Adversarial Machine Learning," *arXiv preprint arXiv:2001.01952*, 2020.
6. I. Jemal et al., "SWAF: A Smart Web Application Firewall Based on Convolutional Neural Network," in *Proc. Int. Conf. Security Inf. Technol. (SIN 2022)*, doi: 10.1109/SIN58406.2022.9970545.
7. A. Coscia et al., "PROGESI: A Proxy Grammar to Enhance Web Application Firewall for SQL Injection Prevention," *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3438092.
8. X. Wang and H. Hu, "Evading Web Application Firewalls with Reinforcement Learning," 2021.
9. V. Babaey and A. Ravindran, "GenSQLi: A Generative Artificial Intelligence Framework for Automatically Securing Web Application Firewalls Against SQL Injection Attacks," *Future Internet*, vol. 17, no. 1, Jan. 2025, doi: 10.3390/FI17010008.
10. J. Á. Román-Gallego et al., "Artificial Intelligence Web Application Firewall for Advanced Detection of Web Injection Attacks," *Expert Systems*, vol. 42, no. 1, Jan. 2025, doi: 10.1111/EXSY.13505.
11. R. A. Muzaki et al., "Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall," *Preprint*, 2020.

12. N. O. Maslova et al., "Multi-agent WAF Pentesting on the JADE Platform," *CEUR Workshop Proc.*, vol. 3988, pp. 282–295, 2025.
13. M. Amouei et al., "RAT: Reinforcement-Learning-Driven and Adaptive Testing for Vulnerability Discovery in Web Application Firewalls," *IEEE Trans. Dependable Secure Comput.*, 2023.
14. F. M. Alotaibi and V. G. Vassilakis, "Toward an SDN-based Web Application Firewall: Defending Against SQL Injection Attacks," *Future Internet*, vol. 15, no. 5, p. 170, 2023.
15. Z. Qu et al., "AdvSQLi: Generating Adversarial SQL Injections Against Real-World WAF-as-a-Service," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 2623–2638, 2024.
16. H. Liang et al., "Generative Pre-Trained Transformer-Based Reinforcement Learning for Testing Web Application Firewalls," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 1, pp. 309–324, 2024.
17. G. Floris et al., "ModSec-AdvLearn: Countering Adversarial SQL Injections with Robust Machine Learning," *IEEE Trans. Inf. Forensics Security*, vol. 20, pp. 6693–6705, 2025.
18. N. W. C. Lasantha et al., "Validating IP Reputation in Cloud Firewall Systems Using Machine Learning Driven Signature Generation and Detection Techniques," in *IEEE IEACON 2024*.
19. H. Do Hoang et al., "WebGuardRL: A Reinforcement Learning-Based Approach for Advanced Web Attack Detection," in *Proc. ACM SOICT 2023*, pp. 761–768.
20. J. Yang et al., "LLM-AE-MP: Web Attack Detection Using a Large Language Model with Autoencoder and Multilayer Perceptron," *Expert Systems with Applications*, vol. 274, May 2025.
21. A. Mycek et al., "Multi-layered Security of Web Applications in Cloud Environments Using WAF, Zero Trust, AI-driven Threat Detection, and RASP," in *Proc. Eur. Council Model. Simul.*, 2025.
22. E. Fakhfakh et al., "Combining TF-IDF, V-GAN, and XGB to Improve Next-Generation Web Application Firewalls," in *IEEE/ACS Int. Conf. Comput. Syst. Appl.*, 2024.
23. K. Gupta et al., "Smart Defense: Machine Learning-Based Web Application Firewall," in *IEEE PuneCon*, Dec. 2024.
24. S. Dhote et al., "ML-Based Web Application Firewall for Signature and Anomaly Detection Using Feature Extraction," in *IEEE ICCCNT 2024*.
25. P. Kalariya et al., "ML Assisted Web Application Firewall," in *IEEE ISDFS 2024*.
26. A. Kumar et al., "Machine Learning-Based Web Application Firewall for Real-Time Threat Detection," in *IEEE ICEI 2024*.
27. M. Maheshwari et al., "Adaptive Web Application Firewall for Multi-Threat Detection," in *IEEE ICICNIS 2024*.
28. I. Darmawan et al., "Real-Time Web Application Firewall Monitoring Using the OWASP CRS Framework," in *IEEE ICIC 2024*.
29. Q. Wang et al., "Automated Discovery of Protocol-Level Evasion Vulnerabilities in WAFs," in *Proc. IEEE SP 2024*, pp. 185–202.
30. V. Nayar et al., "Optimizing Real-Time Performance in ML-Based Application Layer Firewalls," *Lecture Notes in Networks and Systems*, vol. 991, pp. 947–959, 2024.
31. E. Tuyishime et al., "Enhancing Cloud Security: Proactive Threat Monitoring Using a SIEM-Based Approach," *Applied Sciences*, vol. 13, no. 22, Nov. 2023.
32. M. Sepczuk, "Dynamic Web Application Firewall Detection Supported by Cyber Mimic Defense Approach," *J. Netw. Comput. Appl.*, vol. 213, 2023.
33. B. R. Dawadi et al., "Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks," *Sensors*, vol. 23, no. 4, 2023.
34. H. Xu et al., "Accelerating Deep Packet Inspection with SIMD-Based Multi-Literal Matching Engine," *IEEE Trans. Netw. Serv. Manag.*, 2024.
35. Y. Guan et al., "SSQLi: A Black-Box Adversarial Attack Method for SQL Injection Based on Reinforcement Learning," *Future Internet*, vol. 15, no. 4, 2023.
36. B. Shobiri et al., "CDNs' Dark Side: Security Problems in CDN-to-Origin Connections," *Digital Threats: Research and Practice*, vol. 4, no. 1, 2023.
37. A. Chowdhary et al., "Generative Adversarial Network (GAN)-Based Autonomous Penetration Testing for Web Applications," *Sensors*, vol. 23, no. 18, 2023.
38. J. Harish Kumar and J. Godwin Ponsam, "Securing Web Application Using Web Application Firewall (WAF) and Machine Learning," in *Proc. ICAEECI 2023*.
39. C.-V. Trinh et al., "An Efficient Machine Learning-Based Web Application Firewall with Deep Automated Pattern Categorization," in *Proc. FDSE 2023*, pp. 212–225.
40. A. Kozhevnikov and Y. Chernyshov, "Implementing Machine Learning in the Context of Web Application Firewalls," in *Proc. IEEE USBEREIT 2024*, pp. 237–240.
41. G. E. Cárdenas Rosero et al., "Website Protection: An Evaluation of the Web Application Firewall," *Data Metadata*, vol. 4, Jan. 2025.
42. N. Hubballi et al., "WebScreen+: Web Traffic Screening Performance Enhancement with eBPF Filtering," in *Proc. IEEE ICNC 2025*.
43. S. Ye et al., "Network Attack Monitoring Based on HTTP Traffic Parameter Analysis," in *Proc. IEEE ITOEC 2025*.

44. M. Fatima et al., "Enhancing the Resilience of IoT Networks: Strategies for Mitigating DDoS Attacks," *J. Mech. Continua Math. Sci.*, vol. 19, no. 10, 2024.
45. H. Pardamean et al., "Enterprise Architecture Using the Open Group Architecture Framework (TOGAF) in Container Depot Companies," in *Proc. ICE3IS 2024*.
46. S. P. Singh and N. Afzal, "Effective Bot Management Strategies for Web Applications," in *Proc. ISoIRS 2024*.
47. H. Verma et al., "A Comprehensive Analysis of Cross-Site Scripting Vulnerabilities," *Comput. Methods Sci. Technol.*, vol. 2, 2025.
48. B. Hullooan and G. Bekaroo, "Defending Against XML External Entity (XXE) Attacks," in *Proc. NextComp 2024*.
49. I. F. Sabah, "Design and Implementation of a Web-Based Platform for Administering a Virtual University," in *Proc. HORA 2024*.
50. E. Leka et al., "Web Application Firewall for Detecting and Mitigation of DDoS Attacks Using ML and Blockchain," *TEM Journal*, vol. 13, no. 4, 2024.
51. A. Alquwayzani et al., "Mitigating Security Risks in Firewalls and Web Applications Using VAPT," *Int. J. Adv. Comput. Sci. Appl. (IJACSA)*, vol. 15, no. 5, 2024.
52. N. W. C. Lasantha et al., "Hybrid Supervised Machine Learning Driven IP Reputation Validation for Cloud Firewalls," in *Proc. IEEE ICATC 2024*.
53. F. N. Nife and Z. Kotulski, "Application-Aware Firewall Mechanism for Software Defined Networks," *J. Netw. Syst. Manag.*, vol. 28, 2020.
54. T. D. Sobola et al., "Experimental Study of ModSecurity Web Application Firewalls," *Project Report*, Concordia University Edmonton, 2020.
55. C. Scano et al., "ModSec-Learn: Boosting ModSecurity with Machine Learning," *Lecture Notes in Networks and Systems*, vol. 1198, 2025.
56. A. Mycek et al., "Multi-layered Security of Web Applications in Cloud Environments Using WAF and Zero Trust," in *Proc. Eur. Council Model. Simul.*, 2025.
57. E. Tuyishime et al., "Enhancing Cloud Security—Proactive Threat Monitoring and Detection," *Applied Sciences*, 2023.
58. M. S. Islam et al., "Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall," *Int. J. Comput. Digit. Syst.*, vol. 13, no. 1, 2023.
59. H. Bahruddin et al., "Adversary Simulation of SQL Injection Attack Using Genetic Algorithm for WAF Bypass," in *Proc. IntelliSys 2023*, vol. 823, pp. 656–669.
60. M. N. Zaidan et al., "Collaborative Detection of SQL Injection Attacks Using SIEM and WAFs," in *Proc. IEEE CIEES 2024*.
61. Y. Nikam et al., "AI-Based Web Application Firewall," in *Proc. IEEE ICCIT 2025*.
62. J.-K. Lee et al., "AI-Based Approach to Firewall Rule Refinement on HPC Networks," *Applied Sciences*, vol. 14, 2024.
63. A. Gzyl et al., "Understanding the Feature Space and Decision Boundaries of Commercial WAFs," *Entropy*, vol. 25, no. 11, 2023.
64. H. Gzyl et al., "Maximum Entropy in Commercial WAFs," *Entropy*, vol. 25, no. 11, 2023.
65. J. Carrillo-Mondejar et al., "Hardening IoT Devices Using Defensive Firmware Modifications," *IEEE Internet Things Journal*, vol. 10, no. 10, 2023.
66. A. Shaheed et al., "AI-Based WAF Using Feature Engineering," *Security and Communication Networks*, vol. 2022.
67. O. Chakir and Y. Sadqi, "Evaluation of Open-Source Web Application Firewalls for Cyber Threat Intelligence," *CRC Press*, 2023.