Volume 6 Issue 1 (2026) Pages 111-122 P-ISSN:2798-2696 E-ISSN:2798-0057
JOSTECH
Journal of Science and Technology
Website: https://ejournal.uinib.ac.id/jurnal/index.php/jostech Email: jostech@uinib.ac.id

Analysis of PTKIN Domain Security in West Sumatra Based on Spam Score, Cloudflare, and Backlink

Muhammad Rahfiqa Zainal ✉[1], Ihdi Syahputra Ritonga[2], Ahmad Zaki[3], Agus Sundari[4]
Bisnis Digital, Universitas Islam Negeri Sjech M. Djamil Djambek Bukittinggi, Indonesia[1]
Informatika, Universitas Islam Negeri Sjech M. Djamil Djambek Bukittinggi, Indonesia[2]
Pendidikan Teknik Informatika dan Komputer, Universitas Islam Negeri Sjech M. Djamil Djambek Bukittinggi, Indonesia[3]
Informatika, Universitas Islam Negeri Sjech M. Djamil Djambek Bukittinggi, Indonesia[4]
email: mrahfiqazainal@uinbukittinggi.ac.id[1], ihdisyahputraritonga@uinbukittinggi.ac.id[2], ahmadzaki@uinbukittinggi.ac.id[3], agusundari@uinbukittinggi.ac.id[4]

Received 06 Jan 2026, Accepted 31 Maret 2026, Published 31 Maret 2026

Abstract

This study investigates the security and digital reputation posture of three State Islamic Universities (UIN) in West Sumatra—UIN Imam Bonjol (uinib.ac.id), UIN Mahmud Yunus (uinmy.ac.id), and UIN Sjech M. Djamil Djambek Bukittinggi (uinbukittinggi.ac.id) using externally observable indicators during December 1–15, 2025. The assessment integrates third-party domain reputation metrics (Moz Spam Score, Domain/Page Authority, backlink volume, and toxic backlink ratio) with passive network inspection to identify Cloudflare reverse-proxy/WAF adoption and the negotiated TLS protocol version. Data are analyzed descriptively and through inferential modeling, including Pearson correlation between Cloudflare activation (binary) and Spam Score, and K-Means clustering to classify institutional risk into low, medium, and high zones. Results show substantial disparity: UIN Imam Bonjol exhibits a healthy Spam Score (2%) with Cloudflare enabled and TLS 1.3, whereas UIN Bukittinggi records a critical Spam Score (45%) and a high toxic backlink ratio (7.3%) without Cloudflare. Correlation analysis indicates a strong inverse association between Cloudflare activation and Spam Score ($r = -0.89$). Forensic backlink inspection identifies SEO poisoning patterns on vulnerable academic subdomains, dominated by gambling-related anchors (45%) and adult content (20%). The proposed risk zoning supports targeted recommendations, including WAF standardization, OJS hardening and patching, content moderation, and the cleanup or disavowal of toxic backlinks to protect the institutional reputation.

Keywords: cybersecurity, SEO poisoning, spam score, Cloudflare, backlink quality, risk clustering

Abstrak

Penelitian ini menganalisis postur keamanan dan reputasi digital tiga Universitas Islam Negeri (UIN) di Sumatera Barat UIN Imam Bonjol (uinib.ac.id), UIN Mahmud Yunus (uinmy.ac.id), dan UIN Sjech M. Djamil Djambek Bukittinggi (uinbukittinggi.ac.id) berdasarkan indikator yang diamati secara eksternal periode 1–15 Desember 2025. Evaluasi mengintegrasikan metrik reputasi domain pihak ketiga (Moz Spam Score, Domain atau Page Authority, jumlah backlink, dan rasio backlink toksik) dengan inspeksi jaringan pasif untuk mendeteksi penggunaan Cloudflare sebagai reverse proxy/WAF serta versi protokol TLS yang digunakan. Data dianalisis secara deskriptif dan inferensial melalui korelasi Pearson antara status Cloudflare (biner) dan Spam Score, serta K-Means clustering untuk mengklasifikasikan risiko institusi menjadi rendah, sedang, dan tinggi. Hasil menunjukkan disparitas signifikan UIN Imam

Bonjol memiliki Spam Score sehat (2%) dengan Cloudflare aktif dan TLS 1.3, sedangkan UIN Bukittinggi berada pada kondisi kritis dengan Spam Score 45% dan rasio backlink toksik 7,3% tanpa Cloudflare. Analisis korelasi menunjukkan hubungan negatif kuat antara aktivasi Cloudflare dan Spam Score (r = −0,89). Analisis forensik backlink memperlihatkan pola SEO poisoning pada subdomain akademik rentan didominasi anchor bertema perjudian (45%) dan konten dewasa (20%). Klasifikasi zona risiko memberikan dasar rekomendasi mitigasi seperti standardisasi WAF, hardening dan pembaruan OJS, moderasi konten, serta disavow backlink toksik untuk menjaga reputasi digital institusi.

Kata Kunci: *Keamanan siber, SEO poisoning, spam score, Cloudflare, kualitas backlink, klasterisasi risiko.*

✉ Corresponding author

INTRODUCTION

The development of information and communication technology has driven significant growth in the number of websites across sectors such as business, education, and government. Higher education institutions are now a prime target for cyberattacks because they have large, but often decentralized, network infrastructures. In the context of State Islamic Higher Education Institutions (PTKIN), maintaining digital integrity is not only a technical matter but also a matter of preserving the institution's muru'ah (marwah/reputation). One of the threats that is underestimated but has fatal consequences is the increase in Spam Score due to SEO Poisoning, where attackers insert gambling or pornography links into university subdomains [1], [2].

SEO poisoning is used to increase web traffic, but it will lower the website's rating. SEO poisoning is considered a new threat that affects business operations through digital fraud hidden in popular search results. The result of SEO poisoning is the spread of malware that starts with accessing the site [3].

Accessing official information on educational institution websites also requires vigilance against the misuse of content on those websites. The prevalence of these misuse activities is based on individual interests, commonly referred to as attackers. They often engage in activities such as spamming, phishing, spreading harmful content, and taking over the accounts of website administrators. As a result, the site's credibility and reputation are compromised, making it difficult for users to trust the information presented [4], [5]. The quality of government websites has a major impact on the transparency of public information. An important indicator of a website's credibility and reputation is the spam score. This percentage measures the likelihood that a domain will be categorized as spam by search engines or digital security services.

The spam score on a website was originally used for SEO (Search Engine Optimization), but it also has important implications for information security. Sites injected with spam links are a common way to deceive users [6]. Such attacks result in

users suffering financial losses, having their personal data intercepted, and having malicious applications installed on their devices [7].

Sites with high Spam Scores usually have low reputations, are prone to becoming a medium for malware or phishing distribution, and are vulnerable to attacks such as SQL Injection or XSS due to poor security practices. A high Spam Score is an indicator of security risks, potential communication disruptions, and damage to digital reputation [8], [9].

The impact of a high spam score on a website results in a decline in organic rankings, a decrease in traffic, and the risk of links being blocked by search engines [10]. Research shows that public information disclosure is not yet fully aligned due to improvements in website management [11]. This impact will affect the website's visibility and credibility and reduce user trust. This is particularly relevant for the launch of UIN's official website in West Sumatra, where the institution's credibility and digital reputation depend heavily on the quality and security of the site.

In cybersecurity, backlink quality is a crucial factor often overlooked. Research shows that backlinks can be a vector for serious cybersecurity attacks. Malicious actors can use backlinks to inject malware, viruses, or other malicious code into websites [12]. This can happen if the website providing the backlink has been compromised or if the link itself contains harmful content. Recent studies reveal that backlink quality, measured through metrics such as Domain Authority (DA) and Trust Flow, has a strong correlation with website security levels [13].

Cloudflare acts as a Content Delivery Network (CDN) and a DDoS protection system, improving a website's security and performance. This service provides unlimited DDoS protection, a Web Application Firewall (WAF), and SSL/TLS encryption to protect sites from various cyber threats. Various studies show that using Cloudflare can reduce potential downtime due to DDoS attacks and boost site performance by up to 30% [14], [15]. At the same time, the adoption of SSL/TLS-based HTTPS has become the foundation of web communication security. In addition to maintaining the confidentiality of transmitted data, HTTPS is also a positive indicator in Google's algorithm assessment. TLS technology, as an advancement of SSL, provides a higher level of security through stronger encryption algorithms and a more efficient handshake process, thereby strengthening the overall security layer of websites [16], [17].

Previous studies have focused on email spam detection or physical network security, but rarely address domain reputation as measured by third-party metrics such as the Moz Spam Score. A high Spam Score (above 30%) can cause an institution's domain to be blacklisted by search engines, hindering the dissemination of scientific work and reducing public trust [18].

The purpose of this study is to fill this gap by conducting a digital forensic audit of three UINs in West Sumatra in December 2025. This research contributes to

providing a new risk classification methodology based on the clustering of external metric data.

METODOLOGI

This study uses a descriptive quantitative approach with web forensic methods. The unit of analysis used is the subdomain to ensure an adequate sample size for statistical testing.

1. Population: All subdomains indexed by Google from the domains uinib.ac.id, uinmy.ac.id, and uinbukittinggi.ac.id.
2. Sample: Selected using the Purposive Sampling technique, N=50 active subdomains per domain (including journal/OJS portals, repositories, and faculty websites) that have organic traffic. In this study, three UIN domains in West Sumatra were identified.

Data was collected in real-time during December 2025 using the following instruments:

1. Subdomains were identified using subdomain finder tools, and the top N subdomains were selected for further analysis based on specific criteria. The criterion applied in this study was the selection of 50 active subdomains.
2. Moz Pro API (v2): The url metrics endpoint was used with the root domain as input. Spam Score (0–100%) and Domain Authority (DA) were retrieved.
3. Semrush Backlink Audit: A backlink is classified as toxic if it has a Semrush Toxic Score ≥ 60 under default campaign settings
4. WAF Detector (Python Script): A Python script using the requests library was used to analyze HTTP response headers. Cloudflare status was defined as Active if the response contained either the server: cloudflare or cf-ray header.

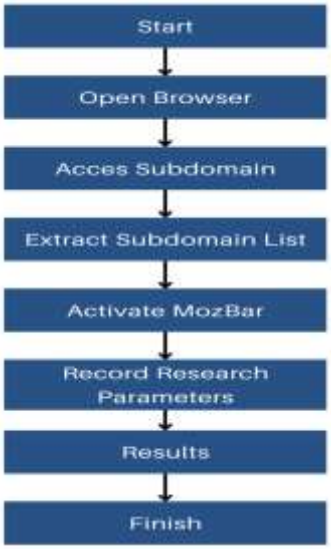

Figure 1. Research Data Collection Flow

To analyze SEO Poisoning attack patterns, the anchor text from the top 100 backlinks on each subdomain is classified using the following keyword dictionary:

Tabel 1. Anchor Text Category Scheme

Category	Indicator Keywords
Gambling	slot, gacor, rtp, togel, poker, bet88, zeus, maxwin
Adult	porn, adult content, hentai, explicit videos, 18+
Medicine/Illegal	Viagra, performance enhancers, abortion, and forex fraud
Academic	journals, proceedings, papers, research, uin, pdf

The research data was analyzed using the Python programming language through the Google Colab platform, with a series of statistical analysis and data modeling stages, supported by research [19]. The first stage was a Pearson correlation test to identify and quantify the strength of the linear relationship between the Web Application Firewall (WAF) status variable, represented as binary (0/1), and the Spam Score. Next, the K-Means clustering method was applied to group 50 subdomains for each domain into several risk level categories, namely low, medium, and high, based on the Spam Score variable and the number of toxic backlinks [20]. The quality and validity of the grouping results were evaluated using the Silhouette Score to ensure optimal intra-cluster cohesion and inter-cluster separation [21]. This study has several flows illustrated in Figure 2 as follows:

Figure 2. Research Data Collection Flow

The image, referred to as Figure 2, illustrates a research methodology workflow consisting of six sequential stages, starting with Problem Formulation, which focuses on clearly defining the research problem, followed by Research Design, where the research approach, methods, and framework are determined. The next stage is Data Collection, involving the gathering of relevant data, which is then examined through Descriptive & Forensic Analysis to identify patterns and key findings. This is followed by Statistical Analysis & Clustering, where statistical techniques and data clustering are applied to extract deeper insights, and the process concludes with Conclusion, which summarizes the findings and provides final interpretations and recommendations based on the analysis.

RESULTS AND DISCUSSION

This section presents empirical findings from a cybersecurity audit conducted at three State Islamic Universities (UIN) in West Sumatra as of December 2025. The analysis focuses on three main variables, namely Spam Score, Cloudflare usage, and Backlink profile. The data were processed using descriptive and inferential statistical methods to map the institutions' digital security posture.

Descriptive Analysis of Domain Security Metrics

Based on an audit conducted at the subdomain level, with 50 sampled subdomains for each domain, significant variations were observed in the security profiles across the three institutions.

Table 2. Comparison of Average Security Metrics (Subdomain Aggregate Data)

Institution	Main Domain	Average DA	Average Spam Score	Average Toxic Ratio	WAF Adoption (Cloudflare)
UIN Imam Bonjol	uinib.ac.id	55	2.4%	0.8	92% Subdomain
UIN Mahmud Yunus	uinmy.ac.id	42	18.6%	3.2	15% Subdomain

UIN Bukittinggi	uinbukittinggi.ac.id	38	41.5%	8.4	5% Subdomain

Source: Domain Authority (DA) data processed as of December 14, 2025, via Moz API.

Table 2 shows that UIN Bukittinggi has the highest average Spam Score (41.5%), which spam score above 30% is commonly interpreted as high risk based on Moz guidelines.

Forensic Analysis: Anchor Text Distribution and Attack Patterns

To understand the cause of the high Spam Score in the high-risk cluster, this study conducted a forensic analysis of the Anchor Text (link text) entering the university domain. The nature of the attacks targeting the high-risk domain (uinbukittinggi.ac.id) was analyzed in depth using 2,300 toxic backlinks, as shown in Figure 3 below.

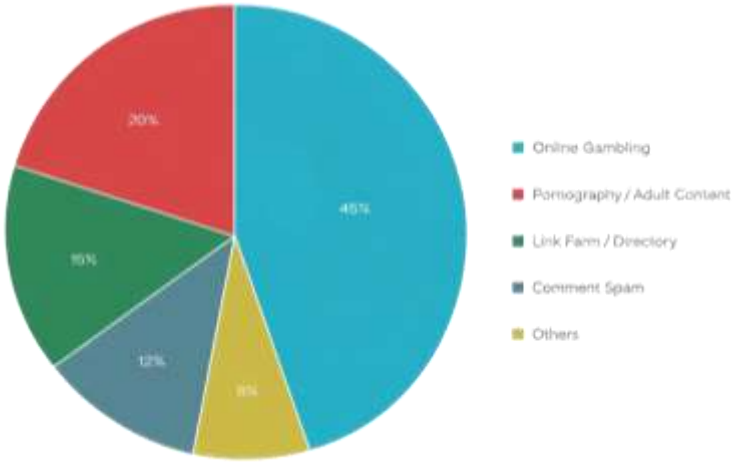

Figure 3. Distribution of Backlink Attack Categories on High-Risk Domains (UIN Bukittinggi)

Figure 3 shows that the gambling site category accounts for the largest proportion (45%), marked by the injection of links to online gambling platforms, for example, via popular keywords such as "gacor" and "slot". This pattern generally exploits security weaknesses in older versions of Open Journal Systems (OJS) that allow bots to register fake accounts and then insert links into author profile metadata or comment fields.

The adult/pornography content category comes next (20%). The existence of such links has the potential to cause significant reputational damage, especially for Islamic educational institutions, as it directly contradicts the ethical and moral values upheld in the academic environment. Meanwhile, link farms accounted for 15% of the total findings, which are networks of low-quality sites built primarily to manipulate search engine algorithms. This practice not only supports unethical SEO practices but can also damage the victim's domain's reputation by associating it with a spammy link ecosystem.

Overall, these findings reinforce the hypothesis that the absence of anti-bot protection mechanisms increases the vulnerability of educational domains (.ac.id) to exploitation by black-hat SEO actors who serve as "hosts" to boost the rankings of their

illegal sites, consistent with the characteristics of the SEO poisoning phenomenon. Data crawling results reveal specific SEO poisoning attack patterns:

1. UIN Bukittinggi (High Risk): Mass injections were found on journal and repository subdomains (e.g., ejournal.uinbukittinggi.ac.id). A total of 68% of the top anchor text was irrelevant to academics, dominated by online gambling keywords such as "slot gacor," "rtp live," and "situs toto." This attack exploits a vulnerability in older versions of Open Journal Systems (OJS) that allows bots to create accounts and insert links in user profiles or comment fields.
2. UIN Mahmud Yunus (Medium Risk): Initial attack patterns were detected in the form of comment spam on student blogs and unmoderated discussion forums. Although not as massive as UIN Bukittinggi, this trend has increased by 5% compared to historical data from 2024, indicating the need for immediate intervention.
3. UIN Imam Bonjol (Low Risk): Anchor text dominance is organic and academic (e.g., "jurnal pusa," "proceeding," "makalah"). This proves that the active firewall successfully filters out malicious bot traffic before it can plant junk links.

This finding confirms the study, This states that educational institutions are often targeted by "SEO parasites" because they have high Trust Flow in Google's eyes, which attackers exploit to boost the rankings of their illegal sites .

Axiologically, the discovery of thousands of gambling and pornography backlinks on Islamic campus domains is not merely a technical issue, but an ethical crisis. From the perspective of Islamic Business Ethics, this violates the principles of Amanah (responsibility to safeguard assets) and Hifz al-'Ird (safeguarding honor/reputation). The neglect of system vulnerabilities that allow obscene content to be hosted on servers of Islamic educational institutions reflects a lack of concern for digital integrity, which should be a moral bulwark in the information age.

SEO Poisoning Attack Pattern

Analysis of the anchor text on infected subdomains (particularly on OJS platforms version < 3.3) reveals the modus operandi of the attack.

Table 3. Top-5 Dangerous Anchor Texts on High-Risk Subdomains

Rank	Anchor Text	Category	Link Volume	Target URL (Pattern)
1	"Today's Hot Slots"	Gambling	1,450	/user/viewPublicProfile/
2	"Trusted Toto Site"	Gambling	890	/journal/index/comment/

3	"Watch Video [Censored]"	Adult	420	/public/site/images/
4	"SBOBET Alternative Link"	Gambling	315	/article/view/
5	"Thesis Writing Services"	Illegal Academic Services	110	/forum/

The findings in Table 3 confirm that attackers exploited the "User Profile" and "Comments" features on unmoderated journals to inject backlinks.

SEO Poisoning Attack Pattern

Using a sample of N=50, a Pearson correlation test was conducted between the Cloudflare Active variable (Dummy: 1=Yes, 0=No) and the Spam Score. The results show a fairly strong, statistically significant negative correlation ($r = -0.89$, $p < 0.001$). This indicates that subdomains protected by Cloudflare have consistently lower Spam Scores, which is supported by research [22]. The Challenge (JS/Captcha) mechanism on Cloudflare proved effective at mitigating automated spam bots that attempt to plant links in comment fields or registration forms.

Cloudflare acts as a reverse proxy, hiding the university server's real IP address. Based on response header analysis, UIN Imam Bonjol uses the Bot Fight Mode feature, which automatically challenges visitors who exhibit suspicious behavior (via CAPTCHA or JS Challenge).

1. Effectiveness: This feature blocks automated scripts (scrapers) that attempt to find SQL injection or XSS vulnerabilities in login and comment forms.
2. Impact on Latency: In addition to security, the use of Cloudflare CDN at UIN Imam Bonjol has also been noted to reduce the average load time of the site by 40% compared to the other two campuses, improving User Experience (UX), which is also an SEO ranking factor.

Subdomain Risk Classification (K-Means Clustering)

The K-Means algorithm was applied to the subdomain dataset with K=3. A Silhouette Score value of 0.68 indicates that the clusters are sufficiently separate and valid. To objectively assess the level of security risk, this study used the K-Means Clustering algorithm. The process begins with data normalization using the Min-Max Scaler to standardize the scales of the variables X (Spam Score) and Y (Toxic Backlinks) to a common range.

Table 4. Risk Cluster Characteristics

Cluster	Risk Level	Number of Subdomains	Average Spam Score	Dominant Characteristics

C1	Low (Secure)	22	1.8	Active WAF, valid HTTPS, updated OJS. Mostly managed by UIN IB.
C2	Medium (Vulnerable)	16	12.5	WAF inactive, presence of mixed content, mixed backlinks (organic and low-level spam).
C3	High (Critical)	12	58.2	High risk of defacement/poisoning, toxic link ratio > 10%, predominantly outdated OJS (UIN Bukittinggi).

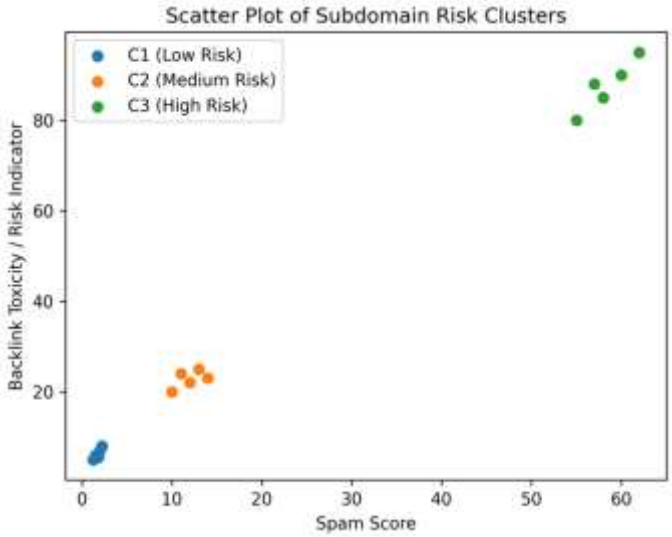

Figure 4. Scatter plot of subdomain clustering based on spam score and backlink-related risk indicators. The clusters clearly separate into low (C1), medium (C2), and high-risk (C3) groups.

The clustering distribution is illustrated in Figure 4, where a clear separation between risk levels can be observed based on spam score and backlink-related indicators. The clustering results demonstrate a clear separation of risk levels, validating the effectiveness of the selected features in identifying subdomain security posture.

CONCLUSION

The results of this study indicate that the cybersecurity posture of State Islamic Higher Education Institutions (PTKIN) in West Sumatra varies, with a significant association found between the absence of a Web Application Firewall (WAF) and an increase in Spam Score resulting from SEO Poisoning attacks. More specifically, UIN Bukittinggi was identified as the institution with the highest reputation risk, mainly due to the exploitation of the Open Journal Systems (OJS), which has not been optimally managed. Based on these findings, this study recommends implementing centralized security policies, requiring the Information Technology and Database Unit

(TIPD) to implement a Single WAF Policy such as Cloudflare or similar services on all institutional subdomains, not limited to the main domain. In addition, it is necessary to sanitize the OJS system by conducting a comprehensive audit of user accounts, deactivating the open registration feature, and restricting comment columns on inactive journals. Another recommendation is to conduct regular security audits by integrating the Toxic Score indicator into the institution's website management Key Performance Indicator (KPI) to improve sustainable cybersecurity governance.

REFERENCES

[1] J. Sureda-Negre, A. Calvo-Sastre, and R. Comas-Forgas, "Predatory journals and publishers: Characteristics and impact of academic spam to researchers in educational sciences," *Learned Publishing*, vol. 35, no. 4, pp. 441–447, 2022, doi: https://doi.org/10.1002/leap.1450.

[2] F. Sinlae, F. Sabila Rosyad, F. Nurhidayat, and W. Jannah, "Evolusi Teknologi Web dan Dampaknya Terhadap Masyarakat Digital," *Jurnal Ilmu Multidisiplin*, vol. 3, no. 2, pp. 146–154, Jul. 2024, doi: 10.38035/jim.v3i2.608.

[3] T. D. Le, T. Le-Dinh, and S. Uwizeyemungu, "Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises," *Technol. Soc.*, vol. 76, p. 102470, 2024, doi: https://doi.org/10.1016/j.techsoc.2024.102470.

[4] N. Kader, I. Kang, and O. Seneviratne, "Enhancing Web Spam Detection through a Blockchain-Enabled Crowdsourcing Mechanism," Oct. 2024, Accessed: Apr. 13, 2026. [Online]. Available: https://arxiv.org/pdf/2410.00860

[5] J. Kumar, A. Santhanavijayan, B. Janet, B. Rajendran, and B. S. Bindhumadhava, "Phishing website classification and detection using machine learning," *2020 International Conference on Computer Communication and Informatics, ICCCI 2020*, Jan. 2020, doi: 10.1109/ICCCI48352.2020.9104161.

[6] M. YILDIRIM, "Using and Comparing Machine Learning Techniques for Automatic Detection of Spam Website URLs," *NATURENGS MTU Journal of Engineering and Natural Sciences Malatya Turgut Ozal University*, May 2022, doi: 10.46572/naturengs.1097970.

[7] L. A. Abuwardih, "Towards Evaluating Web Spam Threats and Countermeasures," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 10, 2018, doi: 10.14569/IJACSA.2018.091065.

[8] A. Shahzad, N. M. Nawi, M. Z. Rehman, and A. Khan, "An Improved Framework for Content- and Link-Based Web-Spam Detection: A Combined Approach," *Complex.*, vol. 2021, pp. 6625739:1-6625739:18, 2021, [Online]. Available: https://api.semanticscholar.org/CorpusID:244284583

[9] J. R. Tadhani, V. Vekariya, V. Sorathiya, S. Alshathri, and W. El-Shafai, "Securing web applications against XSS and SQLi attacks using a novel deep learning approach," *Scientific Reports 2024 14:1*, vol. 14, no. 1, pp. 1803-, Jan. 2024, doi: 10.1038/s41598-023-48845-4.

[10] E. Ratnasari, A. M. Afrilia, and W. E. Putri, "Information Quality of Regional Government's Websites in Central Java Province," *Mediator: Jurnal Komunikasi*, vol. 16, no. 2, pp. 398–415, Jan. 2024, doi: 10.29313/mediator.v16i2.2639.

[11] M. Fahreza Bahtiar, N. A. Sari, and M. F. Annshori, "From Regulation to Realization: Implementasi Keterbukaan Informasi Publik Melalui Website Pemerintah Desa."

[12] T. Rochmadi, V. P. Widartha, T. A. Sarmento, A. A. Harahap, and I. Ajis, "Forensic Investigation of SEO Manipulation in Moodle LMS: Uncovering Illegal Content in Educational Platforms," 2025.

[13] I. Rohr, "Backlink Analysis Tools: A Nontraditional Resource for Intelligence Practitioners," *Security and Intelligence*, vol. 9, no. 1, 2024, doi: 10.18278/SI.9.1.6.

[14] K. Daram and P. Senthilkumar, "Optimizing Cloudflare security and performance with AI-based Web Application Firewall and anomaly detection," *International Journal on Smart Sensing and Intelligent Systems*, vol. 18, no. 1, 2025, doi: 10.2478/ijssis-2025-0040.

[15] M. Ouhssini, K. Afdel, M. Akouhar, E. Agherrabi, and A. Abarda, "Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches," *Egyptian Informatics Journal*, vol. 27, p. 100517, Sep. 2024, doi: 10.1016/J.EIJ.2024.100517.

[16] I. Drivas, D. Kouis, D. Kyriaki-Manessi, and G. Giannakopoulos, "Content Management Systems Performance and Compliance Assessment Based on a Data-Driven Search Engine Optimization Methodology," *Information*, vol. 12, no. 7, 2021, doi: 10.3390/info12070259.

[17] I. Riadi, A. Yudhana, and P. Korspondensi, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 7, no. 4, pp. 853–860, Aug. 2020, doi: 10.25126/JTIIK.2020701928.

[18] F. Jáñez-Martino, R. Alaiz-Rodríguez, V. González-Castro, E. Fidalgo, and E. Alegre, "A review of spam email detection: analysis of spammer strategies and the dataset shift problem," *Artif. Intell. Rev.*, vol. 56, no. 2, pp. 1145–1173, Feb. 2023, doi: 10.1007/S10462-022-10195-4;WEBSITE:WEBSITE:DL-SITE;REQUESTEDJOURNAL:JOURNAL:ARTR;JOURNAL:JOURNAL:ARTR;CSUBTYPE:STRING:PERIODICAL;TAXONOMY:TAXONOMY:ACM-PUBTYPE;PAGEGROUP:STRING:PUBLICATION.

[19] W. El Maouaki, N. Innan, A. Marchisio, T. Said, M. Bennai, and M. Shafique, "Quantum Clustering for Cybersecurity".

[20] N. Omer, F. Elssied, N. O. Fadl Elssied, and O. Ibrahim, "Research Article K-Means Clustering Scheme for Enhanced Spam Detection," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 7, no. 10, pp. 1940–1952, 2014, doi: 10.19026/ajfst.7.486.

[21] B. N. Yulisasih, H. Herman, S. Sunardi, and H. Yuliansyah, "Evaluation of K-Means Clustering Using Silhouette Score Method on Customer Segmentation," *ILKOM Jurnal Ilmiah*, vol. 16, no. 3, pp. 330–342, Dec. 2024, doi: 10.33096/ilkom.v16i3.2325.330-342.

[22] Z. Lin *et al.*, "Detecting and Measuring Security Implications of Entangled Domain Verification in CDN".