



A Recent Systematic Review of Cloud-Assisted Web Filtering Framework using Software-Defined Networking

Lukmanulhakim Ngah^{1*}, Mohd Nordin Abdul Rahman²

¹Faculty Computer, Media and Technology Management (FKMPT), University College TATI, Jalan Panchor, Telok Kalong, 24000 Kemaman, Malaysia

²Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Kampus Besut, 22200 Besut, Terengganu, Malaysia

*Corresponding author email: hakim@uctati.edu.my

KEYWORDS	ABSTRACT
SDN	The increasing complexity of cloud and network environments has intensified the need for more advanced web filtering mechanisms, particularly those leveraging Software-Defined Networking (SDN). This systematic literature review examines the current state of research on "Cloud-Assisted Web Filtering Framework using SDN" to address existing gaps and emerging challenges. The problem lies in the evolving security threats, resource management inefficiencies, and scalability limitations faced by traditional network architectures. To systematically explore these issues, the PRISMA protocol was applied, with data collection conducted across two leading scientific databases, Web of Science and Scopus. A total of 24 primary studies were identified and analysed. The findings were organized into three thematic categories: (1) Security and Attack Mitigation in SDN and IoT Systems, where advanced frameworks for intrusion detection and DDoS mitigation were prominent; (2) Intelligent Resource Management and Optimization in SDN, Fog, and Edge Systems, focusing on strategies such as reinforcement learning and blockchain-based task offloading to enhance resource utilization; and (3) Network Management, Scalability, and Architectural Innovations, highlighting developments in hierarchical control models, federated authentication systems, and SD-WAN traffic prediction. The results demonstrate significant advancements in applying SDN to support more adaptive, resilient, and efficient cloud-assisted web filtering solutions. However, challenges remain, particularly concerning integration complexity, latency management, and ensuring robust multi-domain coordination. In conclusion, this review provides a comprehensive synthesis of current approaches and identifies critical areas for future research, emphasizing the importance of intelligent, secure, and scalable frameworks in the evolving landscape of cloud and SDN-based web filtering systems.
Cloud Computing	
Web-Filtering	

Received 14 March 2026; Revised 29 June 2026; Accepted 30 July 2026; Published 01 October 2026

1.0 INTRODUCTION

The exponential growth of internet usage and digital content consumption has raised critical concerns about secure and efficient web access management, particularly in educational and enterprise environments. Web filtering, a technique used to restrict access to harmful or non-productive content, has become a vital component of modern network security and content governance (1,2). Traditional web filtering solutions, however, often struggle with scalability, dynamic adaptability, and latency due to their reliance on static and centralized architectures. To address these limitations, the integration of cloud computing and Software Defined Networking (SDN) has emerged as a promising paradigm (3–5). Cloud-assisted frameworks provide elastic computational resources and centralized policy enforcement, while SDN introduces programmability and network-wide visibility (4,6–8). Together, they offer the potential for dynamic, scalable, and intelligent web filtering systems capable of meeting modern digital challenges.

Recent studies have explored the convergence of SDN and cloud technologies in various networking domains, including traffic management, intrusion detection, and access control. (9–11) Despite these advancements, existing frameworks often lack fine-grained policy control, real-time adaptability, and seamless integration of contextual data (e.g., user roles or device types). Moreover, there is limited work addressing how cloud-SDN collaboration can support intelligent filtering based on behavioural analytics and evolving threats. This article aims to bridge these gaps by proposing a Cloud-Assisted Web Filtering Framework using SDN, designed to provide adaptive filtering decisions through centralized control and scalable processing. The central research question explores how the synergy between cloud services and SDN can enhance web filtering mechanisms in terms of efficiency, scalability, and contextual awareness. By introducing a modular, policy-driven architecture, this work contributes to the growing body of knowledge on secure and intelligent network management, offering new insights into the design of next-generation web filtering systems.

2.0 LITERATURE REVIEW

The integration of Software Defined Networking (SDN) into cloud-based and web-oriented systems has demonstrated significant improvements in security, efficiency, and management of modern networks. Notably, this approach has shown relevance in areas such as the Web of Things (WoT), Web of Industrial Things (WoIT), and web application security, offering innovative pathways for enhancing web filtering frameworks. These frameworks benefit from SDN's centralized control and programmable interfaces, which address the limitations found in traditional, rigid networking infrastructures. The study by (12) presented WoT/SDN, an architecture that merges SDN with the Web of Things to manage smart devices through resource-oriented approaches. By leveraging SDN's centralized control, the framework introduced components like the Security and Management Controller (SMC), atomic services, and resource subscription syntax to improve device integration, data access, and security. Their evaluation of three applications—device management, security, and data handling—showed enhanced performance and simplified management compared to traditional WoT systems. This research supports the assertion that SDN can strengthen security and scalability within WoT environments by enabling dynamic configuration and flow-based control mechanisms.

Expanding on the idea of SDN for industrial applications, (13) proposed an integrated SDN and MQTT-based framework aimed at WoIT ecosystems. Their work addressed communication inefficiencies in Industrial Internet of Things (IIoT) systems, which often struggle with latency and energy consumption due to constrained device capabilities and high traffic volumes. By incorporating MQTT-SN—an optimized version of the MQTT protocol for constrained devices—their SDN architecture reduced end-to-end latency while maintaining low system overhead. This solution showed practical effectiveness in real-world IIoT settings by ensuring responsive and reliable data exchange while optimizing system lifetime and resource allocation. (14) took a different angle by

focusing on SDN's potential in network security, particularly in defending against SQL injection attacks. Their proposed SDN-based Web Application Firewall (WAF) used signature and regular expression detection techniques within the SDN controller to inspect and filter web traffic. When compared to the traditional ModSecurity WAF, the SDN-based solution achieved superior performance in TCP ACK latency, although ModSecurity showed slightly better results in controller overhead. This study demonstrated that SDN can function not only as a network traffic manager but also as a core component in real-time security systems, enhancing protection against evolving web threats.

Together, these studies highlight SDN's strengths in programmable control, improved network visibility, and responsiveness. (12) demonstrated SDN's ability to streamline WoT services by enabling real-time application development and resource management. Similarly, Bartoli, (13) et al. (2025) emphasized SDN's importance in industrial settings where latency and communication reliability are critical. (14) illustrated how SDN could support adaptive security mechanisms at the network level. The combined evidence from these studies reinforces the versatility of SDN across different technological contexts from device management to industrial communications and cybersecurity. Despite these contributions, the current body of research presents several gaps. Scalability concerns remain underexplored, particularly in large-scale deployments involving cloud and edge devices across multiple administrative domains. For instance, both (12) and (13), evaluated performance on relatively limited infrastructures, which may not reflect the challenges in real-world, complex environments. Furthermore, the current models focus heavily on latency and data flow efficiency, but lack in-depth analysis of quality of service (QoS) differentiation, policy orchestration across clouds, or handling of diverse traffic types under varying workloads.

In the domain of web security, (14) addressed SQL injection, a single attack vector. However, modern cyber threats are multidimensional, including cross-site scripting, DDoS attacks, and zero-day vulnerabilities. The SDN-WAF approach remains limited unless integrated with advanced machine learning or behavioural analysis tools that can detect and respond to emerging threats dynamically. Furthermore, privacy concerns in SDN-controlled web filtering systems are often overlooked, especially in cloud-assisted environments where multiple tenants may share resources and policies. To address these limitations, future research must explore scalable and intelligent web filtering frameworks that combine SDN with other technologies such as Network Function Virtualization (NFV), cloud-native orchestration, and artificial intelligence. These frameworks should support real-time, distributed filtering capabilities that can adjust to dynamic threat landscapes while maintaining performance and compliance with privacy regulations. Additionally, tighter integration with cloud platforms is necessary to enable policy enforcement across hybrid infrastructures, ensuring a unified and adaptive defence posture.

In summary, the adoption of SDN across web filtering applications ranging from WoT integration to industrial IoT and cybersecurity shows strong potential in addressing performance, flexibility, and security challenges. However, to achieve comprehensive and sustainable solutions, future frameworks must evolve beyond current limitations by embracing multi-domain scalability, intelligent threat detection, and deeper cloud integration.

3.0 RESEARCH QUESTION

Research questions hold a pivotal role within a systematic literature review (SLR) as they establish the foundation and guide the overall direction of the review process. They define the scope and focus of the SLR, enabling precise inclusion and exclusion of studies to ensure the review remains aligned with the topic of interest. Well-formulated research questions support an exhaustive and systematic search strategy, minimizing bias and promoting a comprehensive examination of existing evidence. Furthermore, they provide a coherent framework for the categorization, organization, and synthesis of findings, thereby facilitating meaningful analysis and interpretation. Clear and specific

research questions enhance the transparency and reproducibility of the review process, allowing subsequent researchers to replicate or extend the study. Ultimately, research questions ensure that the review achieves its intended objectives—whether to identify research gaps, assess intervention effectiveness, or explore thematic trends—thus forming the backbone of a rigorous, focused, and relevant SLR.

The specification of Research Questions (RQs) represents the most critical task during the planning phase and is equally crucial throughout the entire SLR process, as it drives the overall review methodology (15). In this study, the PICo framework, a mnemonic model particularly suited for formulating research questions in qualitative research and proposed by (16), is employed. The PICo framework encompasses three elements: Population (P), Interest (I), and Context (Co). The Population refers to the group or subjects of interest; the Interest represents the phenomenon, behaviour, or intervention under investigation; and the Context defines the specific setting or environment relevant to the study. The application of the PICo framework ensures the formulation of research questions that are clear, systematic, and focused, thereby enhancing the precision of literature searches and the overall robustness of the research design. This study achieved three research question as below;

1. How effective are cloud-assisted frameworks in mitigating security attacks within Software-Defined Networks (SDN) and Internet of Things (IoT) systems?
2. What intelligent strategies optimize resource management in cloud-assisted SDN, Fog, and Edge Computing systems?
3. In what ways do cloud-assisted SDN frameworks contribute to enhancing network management, scalability, and architectural innovations?

4.0 METHODOLOGY

When conducting a systematic literature review, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, introduced by Page et al. When conducting a systematic literature review, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, introduced by Page et al. When conducting a systematic literature review, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, introduced by Page et al. (17), is a widely recognised and trusted standard. It helps ensure the review process is transparent, thorough, and consistent. By following PRISMA's guidelines, researchers can enhance the precision and reliability of their analysis, as the framework provides clear steps for identifying, screening, and selecting studies to include in the review. It also emphasises the importance of randomised studies, recognising their role in reducing bias and strengthening the evidence base.

For this review, two major databases—Web of Science and Scopus—were selected due to their comprehensive coverage and strong reputation. The PRISMA process is divided into four main stages: identification, screening, eligibility, and data abstraction. In the identification stage, researchers search databases to gather all potentially relevant studies. During screening, these studies are reviewed against set criteria to filter out those that are irrelevant or of poor quality. In the eligibility stage, the remaining studies undergo a detailed evaluation to ensure they meet the inclusion standards. Finally, during data abstraction, key information from the selected studies is extracted and synthesised to draw meaningful and reliable conclusions. By following this structured approach, researchers can conduct systematic reviews with a high level of rigour, leading to results that are both credible and valuable for guiding future research and practice.

4.1 Identification

In this study, essential steps of the systematic review process were employed to collect a significant amount of relevant literature. The process started with the selection of keywords, followed by identifying related terms using dictionaries, thesauri, encyclopedias, and previous research. All relevant terms were identified, and search strings were formulated for the Web of Science and Scopus databases as shown in Table 1. This initial phase of the systematic review resulted in 996 publications relevant to the study topic from the two databases.

Table 1: The Search String

Scopus	TITLE-ABS-KEY ((cloud OR "cloud based") AND (sdn OR "software define network" OR "network programmability") AND framework)
WoS	(cloud OR "cloud based") AND (sdn OR "software define network" OR "network programmability") AND framework (Topic)

4.2 Screening

Potentially pertinent research items are assessed in the screening step to make sure they support the predetermined research question or questions. During this stage, choosing research topics is frequently done Cloud-Assisted Web Filtering Framework using SDN. At this point, duplicate documents are eliminated. After 924 publications were initially discarded, 72 papers were left for additional analysis in accordance with particular inclusion and exclusion standards (refer to Table 2). The literature was the first criterion because it is the primary source of useful advice. This includes book series, book reviews, meta-syntheses, meta-analyses, conference proceedings, and chapters that were not included in the most recent study. Only English-language publications from 2024 to 2025 were included in the review. Due to duplication, 24 publications in total were rejected.

Table 2: The Selection Criterion in Searching

Criterion	Inclusion	Exclusion
Language	English	Non-English
Time line	2024 – 2025	< 2023
Literature type	Journal (Article)	Conference, Book, Review
Publication Stage	Final	In Press
Subject Area	Computer Science	Besides Computer Science

4.3 Eligibility

In the third step, known as the eligibility phase, 48 articles were prepared for review. During this stage, the titles and key content of all articles were carefully examined to ensure they met the inclusion criteria and aligned with the current research objectives. Consequently, 24 articles were excluded as they did not qualify as due to the out of field, title not significant, abstract not related on the objective of the study, no full text access founded on empirical evidence. As a result, a total of 24 articles remains for the upcoming review.

4.4 Data Abstraction and Analysis

An integrative analysis was used as one of the assessment strategies in this study to examine and synthesis a variety of research designs (quantitative methods). The goal of the competent study was to identify relevant topics and subtopics. The stage of data collection was the first step in the development of the theme. Figure 1 shows how the authors meticulously analyzed a compilation of 24 publications for assertions or material relevant to the topics of the current study. The authors then evaluated the current significant studies related to Cloud-Assisted Web Filtering Framework using SDN. The methodology used in all studies, as well as the research results, are being investigated. Next, the author collaborated with other co-authors to develop themes based on the evidence in this study's context. A log was kept throughout the data analysis process to record any analyses, viewpoints, riddles, or other thoughts relevant to the data interpretation. Finally, the authors compared the results to see if there were any inconsistencies in the theme design process. It is worth noting that, if there are any disagreements between the concepts, the authors discuss them amongst themselves.

Table 3: Number and Details of Primary Studies Database

No	Authors	Title	Year	Source title	Scopus	WoS
1	Risdianto A.C.et al (18)	Transforming Network Management: Intent-Based Flexible Control Empowered by Efficient Flow-Centric Visibility	2024	Future Internet	/	
2	Abou El Houda et al.(19)	Securing IIoT applications in 6G and beyond using adaptive ensemble learning and zero-touch multi-resource provisioning	2024	Computer Communications	/	/
3	Krishnaveni et al.(20)	CyberDefender: an integrated intelligent defense framework for digital-twin-based industrial cyber-physical systems	2024	Cluster Computing	/	/
4	Chen et al. (21)	Human-Aware Dynamic Hierarchical Network Control for Distributed Metaverse Services	2024	IEEE Journal on Selected Areas in Communications	/	
5	Oyucu et al.(22)	Ensemble Learning Framework for DDoS Detection in SDN-Based SCADA Systems	2024	Sensors	/	
6	Gilani et al.(23)	SDN-based multi-level framework for smart home services	2024	Multimedia Tools and Applications	/	

7	Snehi et al.(24)	Foggier skies, clearer clouds: A real-time IoT-DDoS attack mitigation framework in fog-assisted software-defined cyber-physical systems	2024	Computers and Security	/	/
8	Nahar et al.(25)	Clouds on the Road: A Software-Defined Fog Computing Framework for Intelligent Resource Management in Vehicular Ad-Hoc Networks	2024	IEEE Transactions on Mobile Computing	/	/
9	Basu et al.(26)	A study of supervised machine learning algorithms for traffic prediction in SD-WAN	2024	International Journal of Web and Grid Services	/	/
10	T.G. et al.(27)	EFraS: Emulated framework to develop and analyze dynamic Virtual Network Embedding strategies over SDN infrastructure	2024	Simulation Modelling Practice and Theory	/	/
11	Kabdjou et al.(28)	Improving Quality of Service and HTTPS DDoS Detection in MEC Environment with a Cyber Deception-Based Architecture	2024	IEEE Access	/	/
12	Ramalakshmi et al.(29)	DDoS Attack Mitigation using Distributed SDN Multi Controllers for Fog Based IoT Systems	2024	International Journal of Intelligent Systems and Applications in Engineering	/	
13	Kirmizioğlu et al (30)	Distributed virtual selective-forwarding units and SDN-assisted edge computing for optimization of multi-party WebRTC videoconferencing	2025	Signal Processing: Image Communication	/	
14	Anoushee et al.(31)	An intelligent resource management method in SDN based fog computing using reinforcement learning	2024	Computing	/	
15	Li et al.(32)	Blockchain-based reliable task offloading framework for edge-cloud cooperative workflows in IoMT	2024	Information Sciences		/
16	Quadri et al.(33)	Intrusion Detection System for Cyber Security in Smart Agriculture with Abcis Techniques	2024	Journal of Theoretical and Applied Information Technology	/	
17	Sarabia-Jácome et al.(34)	Progressive Adoption of RINA in IoT Networks: Enhancing Scalability and Network Management via SDN Integration	2024	Applied Sciences (Switzerland)	/	
18	Songa A.V.; Karri G.R. (35)	An integrated SDN framework for early detection of DDoS attacks in cloud computing	2024	Journal of Cloud Computing		/

19	Sousa et al.(36)	FedAAA-SDN: Federated Authentication, Authorization and Accounting in SDN controllers	2024	Computer Networks	/	
20	Pei et al.(37)	Multi-resource interleaving for task scheduling in cloud-edge system by deep reinforcement learning	2024	Future Generation Computer Systems		/
21	Christila et al.(38)	A Deep Ensemble Framework for DDoS Attack Recognition and Mitigation in Cloud SDN Environment	2024	Journal of Computer Science	/	
22	Razvan et al (39)	Enhancing network security through integration of game theory in software-defined networking framework	2025	International Journal of Information Security		/
23	Banitalebi Dehkordi A. (40)	EDBLSD-IIoT: a comprehensive hybrid architecture for enhanced data security, reduced latency, and optimized energy in industrial IoT networks	2025	Journal of Supercomputing		/
24	He et al.(41)	Efficient Large-Scale Multiple Migration Planning and Scheduling in SDN-Enabled Edge Computing	2024	IEEE Transactions on Mobile Computing		/

4.5 Quality of Appraisal

According to the guidelines proposed by Kitchenham and Charters (15), once we had selected primary studied, we have to assess the quality of the researches they present and quantitatively compare them. In this study we apply quality assessment from Anas Abouzahra et al. (42) which consist of six QAs for our SLR. The scoring procedure for evaluating each criterion involves three possible ratings: "Yes" (Y) with a score of 1 if the criterion is fully met, "Partly" (P) with a score of 0.5 if the criterion is somewhat met but contains some gaps or shortcomings, and "No" (N) with a score of 0 if the criterion is not met at all.

- QA1. Is the purpose of the study clearly stated?
- QA2. Is the interest and the usefulness of the work clearly presented?
- QA3. Is the study methodology clearly established?
- QA4. Are the concepts of the approach clearly defined?
- QA5. Is the work compared and measured with other similar work?
- QA6. Are the limitations of the work clearly mentioned?

The table outlines a quality assessment (QA) process used to evaluate a study based on specific criteria. Three experts assess the study using the criteria listed, and each criterion is scored as "Yes" (Y), "Partly" (P), or "No" (N). Here's a detailed explanation:

1. Is the purpose of the study clearly stated?

This criterion checks whether the study's objectives are clearly defined and articulated. A clear purpose helps set the direction and scope of the research.

2. Is the interest and usefulness of the work clearly presented?

This criterion evaluates whether the study's significance and potential contributions are well-explained. It measures the relevance and impact of the research.

3. Is the study methodology clearly established?

This assesses whether the research methodology is well-defined and appropriate for achieving the study's objectives. Clarity in methodology is crucial for the study's validity and reproducibility.

4. Are the concepts of the approach clearly defined?

This criterion looks at whether the theoretical framework and key concepts are clearly articulated. Clear definitions are essential for understanding the study's approach.

5. Is the work compared and measured with other similar work?

This evaluates whether the study has been benchmarked against existing research. Comparing with other studies helps position the work within the broader academic context and highlights its contributions.

6. Are the limitations of the work clearly mentioned?

Each expert independently assesses the study according to these criteria, and the scores are then totaled across all experts to determine the overall mark. For a study to be accepted for the next process, the total mark, derived from summing the scores from all three experts, must exceed 3.0. This threshold ensures that only studies meeting a certain quality standard proceed further.

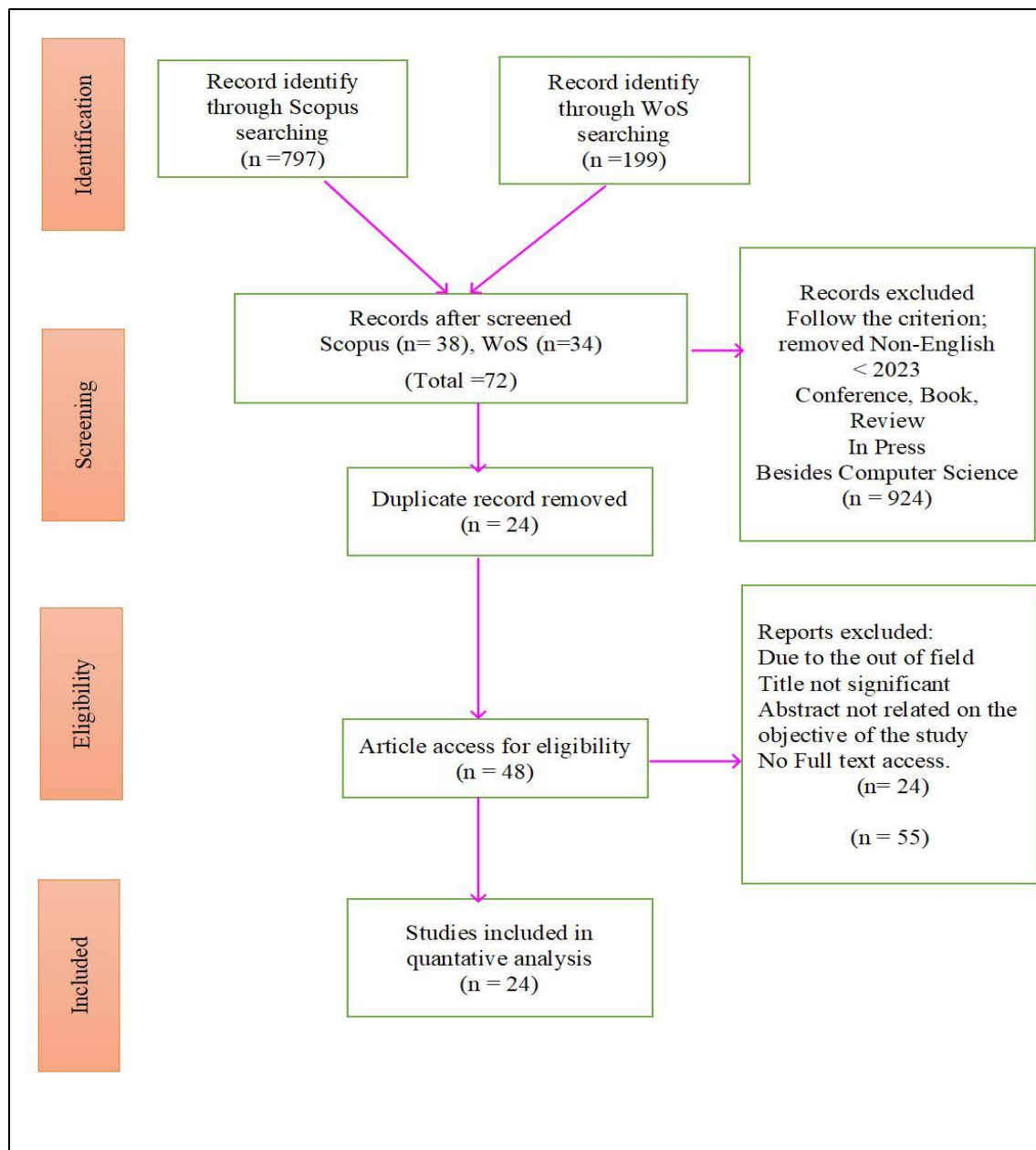


Figure 1: Flow Diagram of the Proposed Searching Study

5.0 RESULTS AND DISCUSSION

Based on quality assessment, Table 4 shown the result of assessment performance for selected primary studies. The quality assessment of 24 selected studies shows that the overall standard is very high, with an average score of 89.58%. Seventeen papers achieved 91.67%, indicating clear objectives, strong relevance, solid methodologies, and well-defined concepts. While most studies excelled in these areas, a common weakness was observed in the discussion of limitations (QA6) and

comparative analysis with other works (QA5). Only one paper (PS16) scored notably lower (58.33%) due to unclear methodology and weak conceptual definitions, requiring cautious use in the review. Overall, the papers selected provide a strong foundation for the systematic literature review, with more than 90% meeting over 75% of the quality criteria. It is important to highlight in the final review that while the majority of studies are robust, the lack of thorough limitation discussions could impact the completeness of findings and recommendations for future research. This critical observation strengthens the credibility of the review by demonstrating a balanced and analytical approach

Table 4 : Performance Quality Assessment for the Primary Studied (PS)

Primary Study	QA1	QA2	QA3	QA4	QA5	QA6	Total Mark	Percentage (%)
PS 1 (Risdianto et al.)	Y	Y	Y	Y	P	N	4.5	75%
PS 2 (Abou El Houda et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 3 (Krishnaveni et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 4 (Chen et al.)	Y	Y	Y	Y	Y	N	5.0	83.33%
PS 5 (Oyucu et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 6 (Gilani et al.)	Y	Y	Y	Y	P	N	4.5	75%
PS 7 (Snehi et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 8 (Nahar et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 9 (Basu et al.)	Y	Y	Y	Y	P	N	4.5	75%
PS 10 (T.G. et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 11 (Kabdjou et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 12 (Ramalakshmi et al.)	Y	Y	Y	Y	P	N	4.5	75%
PS 13 (Kırmızıoğlu et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 14 (Anoushee et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 15 (Li et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 16 (Quadri et al.)	Y	P	Y	P	P	N	3.5	58.33%

Primary Study	QA1	QA2	QA3	QA4	QA5	QA6	Total Mark	Percentage (%)
PS 17 (Sarabia-Jácome et al.)	Y	Y	Y	Y	P	N	4.5	75%
PS 18 (Songa et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 19 (Sousa et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 20 (Pei et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 21 (Christila et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 22 (Razvan et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 23 (Banitalebi Dehkordi)	Y	Y	Y	Y	Y	P	5.5	91.67%
PS 24 (He et al.)	Y	Y	Y	Y	Y	P	5.5	91.67%

5.1 Theme 1: Security and Attack Mitigation in SDN and IoT Systems

The ongoing evolution of security strategies within software-defined networking (SDN) and Internet of Things (IoT) environments has driven researchers to develop innovative frameworks focused on attack mitigation and early threat detection. Abou El Houda et al.(19) explored the use of adaptive ensemble learning integrated with zero-touch multi-resource provisioning to secure Industrial Internet of Things (IIoT) applications in 6G environments, highlighting a significant reduction in vulnerability exposure. Similarly, Oyucu et al. (22) proposed an ensemble learning framework specifically targeting DDoS detection within SDN-based SCADA systems, demonstrating enhanced threat identification rates. Christila et al.(38) further emphasized the value of ensemble methods through the introduction of a deep ensemble framework capable of recognizing and mitigating DDoS attacks in cloud-based SDN environments, achieving improved accuracy and faster response times. Collectively, these studies validate the effectiveness of ensemble learning approaches in reinforcing network security and show convergence in their findings towards improved detection rates and system resiliency.

The challenge of securing fog and edge computing environments has also been a major focus. Snehi et al.(24) presented a real-time mitigation framework designed for IoT-DDoS attacks within fog-assisted software-defined cyber-physical systems, showcasing substantial latency reduction during mitigation processes. Kabdjou et al.(28) developed a cyber deception-based architecture that not only improved the quality of service (QoS) but also strengthened HTTPS DDoS detection capabilities in multi-access edge computing (MEC) environments. Ramalakshmi et al.(29) suggested the distribution of SDN multi-controllers across fog-based IoT systems as an effective countermeasure against DDoS attacks, leading to minimized single-point failures and increased system robustness. These findings collectively underline that distributing control functionalities and embedding deception tactics can significantly enhance defense mechanisms across fog and edge networks.

Parallel to DDoS-focused strategies, the domain of intrusion detection and cybersecurity within specialized sectors such as smart agriculture has been investigated. Quadri et al.(33) introduced an Intrusion Detection System (IDS) utilizing ABCIS techniques aimed at strengthening cybersecurity in smart agriculture environments, reporting noticeable improvements in threat recognition and system sustainability. Songa A.V.; Karri G.R. (35) proposed an integrated SDN framework emphasizing early detection of DDoS attacks in cloud computing systems, where real-time monitoring and centralized control led to rapid threat neutralization. Additionally, Razvan et al (39) discussed the integration of game theory principles within SDN frameworks to enhance decision-making processes during security incidents, offering an intelligent negotiation-based method to counter adversaries dynamically. These collective insights illustrate a rising interest in applying cross-disciplinary methods such as bio-inspired algorithms and game theory to reinforce detection accuracy and system resilience in various application areas.

Further contributions have been observed in optimizing resource efficiency while maintaining strong security guarantees. Banitalebi Dehkordi A. (40) introduced the EDBLSD-IIoT architecture, combining enhanced data security protocols with strategies for reducing latency and optimizing energy consumption across industrial IoT networks. The work by Songa A.V.; Karri G.R. (35) also partially aligns with this direction by emphasizing not only security but also efficient system performance through integrated SDN frameworks. Similarly, Abou El Houda et al.(19) discussed the necessity of multi-resource provisioning to maintain secure, adaptive IIoT systems within future 6G infrastructures. These studies collectively advocate for architectures that balance robust security measures with resource optimization, recognizing the interdependence between cybersecurity and operational efficiency in large-scale networked systems.

5.2 Theme 2: Intelligent Resource Management and Optimization in SDN, Fog, and Edge Systems

Recent studies have focused on enhancing intelligent resource management and optimization strategies across SDN, fog, and edge computing systems. Gilani et al.(23) introduced an SDN-based multi-level framework designed specifically for smart home environments, emphasizing efficient service orchestration and dynamic resource allocation to improve system responsiveness. Similarly, Nahar et al.(25) proposed a software-defined fog computing framework tailored for vehicular ad-hoc networks, which demonstrated significant improvements in resource utilization and service reliability through intelligent distribution mechanisms. Anoushee et al.(31) advanced this area further by utilizing reinforcement learning within SDN-based fog computing, allowing dynamic adjustments to resource management policies, leading to more efficient handling of variable network demands. These studies collectively emphasize that multi-level control structures and adaptive learning methods are critical to managing complex resource environments effectively.

The incorporation of virtualized components and decentralized systems has also been widely explored to optimize distributed services. Kırmızıoğlu et al (30) proposed the use of distributed virtual selective-forwarding units combined with SDN-assisted edge computing to optimize multi-party WebRTC videoconferencing, resulting in improved data flow control and enhanced system scalability. Pei et al.(37) introduced a deep reinforcement learning-based approach for multi-resource interleaving in cloud-edge systems, enabling more intelligent task scheduling and efficient resource usage, especially under high-load scenarios. T.G. et al.(27) developed EFraS, an emulated framework aimed at analyzing dynamic virtual network embedding strategies over SDN infrastructure, showing that flexible network configuration and management could significantly reduce resource wastage. These findings suggest that distributed frameworks and intelligent virtualized resource handling are essential for achieving high efficiency and service quality in evolving network environments.

In addition, several researchers have highlighted the critical role of cooperative and migration planning strategies for resource optimization. Li et al.(32) introduced a blockchain-based task offloading framework supporting edge-cloud cooperative workflows in the Internet of Medical Things (IoMT), ensuring reliable and secure task allocation while optimizing computational resources. He, He et al.(41) addressed large-scale resource management by proposing efficient migration planning and scheduling mechanisms for SDN-enabled edge computing environments, which demonstrated considerable benefits in minimizing downtime and enhancing service continuity. Nahar et al.(25) also contributed to this area by reinforcing the necessity of cooperative control between cloud and fog layers for intelligent vehicular network management. Overall, these works converge on the conclusion that collaboration across multiple layers, secured by emerging technologies like blockchain, plays a fundamental role in achieving sustainable and intelligent resource management across heterogeneous computing environments.

5.3 Theme 3: Network Management, Scalability, and Architectural Innovations

Recent advancements in network management have focused on improving flexibility, visibility, and dynamic control to address the increasing complexity of modern systems. Risdianto A.C.et al (18) proposed an intent-based flexible control mechanism empowered by efficient flow-centric visibility, significantly enhancing network management operations through adaptive control strategies. Similarly, Chen et al. (21) developed a human-aware dynamic hierarchical network control model tailored for distributed metaverse services, which effectively addressed latency and service continuity challenges by incorporating user-context awareness into the control architecture. Basu et al.(26) contributed to this area by evaluating supervised machine learning algorithms for traffic prediction in SD-WAN, demonstrating that intelligent traffic forecasting is critical for maintaining network performance and avoiding congestion. Together, these studies reveal that integrating intelligent control and predictive analytics is crucial for modernizing network management practices and sustaining high-quality service delivery in increasingly complex environments.

In the domain of scalability and architectural innovation, Sarabia-Jácome et al.(34) introduced the progressive adoption of the Recursive InterNetwork Architecture (RINA) model into IoT networks, highlighting its ability to enhance scalability and streamline network management through SDN integration. Their findings confirmed that layered and recursive approaches offer superior manageability and resource efficiency compared to traditional architectures. Sousa et al.(36) explored a different aspect by proposing FedAAA-SDN, a federated model for Authentication, Authorization, and Accounting in SDN controllers, which enabled distributed trust management while maintaining security and performance across diverse network segments. Additionally, Risdianto A.C.et al (18) emphasized that flexible and scalable architectures, when combined with intent-driven models, could substantially lower operational complexity. These contributions collectively underscore those architectural innovations, particularly those involving recursive layering, distributed trust, and intent-based designs, are pivotal in addressing the scaling and management demands of future network systems.

6.0 CONCLUSION

The primary objective of this study was to systematically review and synthesize the current research landscape surrounding cloud-assisted web filtering frameworks utilizing Software-Defined Networking (SDN). By applying the PRISMA methodology and analysing data sourced from Web of Science and Scopus databases, 24 primary studies were selected and thoroughly reviewed. The analysis was structured into three major themes: Security and Attack Mitigation in SDN and IoT Systems, Intelligent Resource Management and Optimization in SDN, Fog, and Edge Systems, and Network Management, Scalability, and Architectural Innovations. Across these themes, several key

findings emerged. Firstly, ensemble learning models and distributed SDN controllers were prominently utilized to enhance security and early attack detection capabilities. Secondly, the studies focusing on resource optimization highlighted the effectiveness of reinforcement learning, blockchain-based offloading strategies, and dynamic scheduling for handling the complexities of distributed systems. Thirdly, architectural innovations were found to be crucial in addressing scalability issues, where recursive frameworks, federated trust models, and intelligent traffic management strategies demonstrated notable success. These findings collectively indicate that the integration of SDN and cloud technologies significantly improves web filtering frameworks, providing enhanced adaptability, resilience, and efficiency, although certain challenges such as latency, interoperability, and cross-domain trust management persist.

This review contributes to the body of knowledge by offering a structured synthesis of the advancements and gaps in the development of cloud-assisted web filtering systems using SDN. The findings emphasize the need for a holistic approach that combines security, intelligent resource management, and scalable architectural design. Practical implications of this study suggest that industries aiming to deploy next-generation web filtering mechanisms should integrate AI-driven threat detection, dynamic edge-cloud resource coordination, and distributed control frameworks to ensure efficiency and robustness. Nevertheless, several limitations were identified, such as the confinement to two major databases and the limited consideration of very recent or grey literature, which may influence the completeness of the findings. Future research should explore large-scale experimental validations, real-world deployment scenarios, privacy-preserving mechanisms, and more extensive cross-domain orchestration strategies. Furthermore, deeper investigations into hybrid SDN-Blockchain-AI models and lightweight orchestration techniques for edge computing environments would be valuable to advance the field further. Overall, this systematic review underlines the critical role of cloud-assisted SDN frameworks in shaping the future of web filtering technologies, supporting the transition towards more secure, intelligent, and scalable digital infrastructures.

Author Contribution

Lukmanulhakim Ngah: Conceptualization, methodology, investigation, visualisation, writing and editing. Mohd Nordin bin Abdul Rahman: Investigation, supervision

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

- [1] Yu L, Qiu P, Gao J, Lu F. A knowledge-based filtering method for open relations among geo-entities. *ISPRS Int J Geo-Information*. 2019;
- [2] Yao L, Sheng QZ, Ngu AHH, Yu J, Segev A. Unified collaborative and content-based web service recommendation. *IEEE Trans Serv Comput*. 2015;
- [3] Wang Q, Gao D, Zhu W. Cloud-enabled software-defined vehicular networks: Architecture, applications and challenges. *J Internet Technol*. 2019;
- [4] Nkenyereye L, Nkenyereye L, Tama BA, Reddy AG, Song J. Software-defined vehicular cloud networks: Architecture, applications and virtual machine migration. *Sensors (Switzerland)*. 2020;
- [5] Thatha VN, Donepudi S, Safali MA, Praveen SP, Tung NT, Cuong NHH. Security and risk analysis in the cloud with software defined networking architecture. *Int J Electr Comput Eng*. 2023;
- [6] Goudarzi S, Anisi MH, Ahmadi H, Musavian L. Dynamic Resource Allocation Model for Distribution

- Operations Using SDN. *IEEE Internet Things J.* 2021;
- [7] Aujla GS, Chaudhary R, Kaur K, Garg S, Kumar N, Ranjan R. SAFE: SDN-Assisted Framework for Edge-Cloud Interplay in Secure Healthcare Ecosystem. *IEEE Trans Ind Informatics.* 2019;
 - [8] Shafi Q, Basit A, Qaisar S, Koay A, Welch I. Fog-Assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network. *IEEE Access.* 2018;
 - [9] Krishnan P, Jain K, Aldweesh A, Prabu P, Buyya R. OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. *J Cloud Comput.* 2023;
 - [10] Abdalqadder IH, Zhou S, Zou D, Aziz IT, Akber SMA. Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. *Comput Networks.* 2020;
 - [11] Issa T, Tiemoman K. Intrusion detection system based on the SDN network, Bloom filter and machine learning. *Int J Adv Comput Sci Appl.* 2019;
 - [12] Xiaofeng Q, Wenmao L, Teng G, Xinxin H, Xutao W, Pengcheng C. WoT/SDN : Web of things architecture using SDN. *China Commun.* 2015;12(11):177–87.
 - [13] Bartoli C, Bonanni M, Chiti F, Pierucci L. The Alliance of SDN and MQTT for the Web of Industrial Things. *IEEE Trans Ind Informatics.* 2025;
 - [14] Alotaibi FM, Vassilakis VG. Toward an SDN-Based Web Application Firewall: Defending against SQL Injection Attacks. *Futur Internet.* 2023;15(5).
 - [15] Kitchenham B. Guidelines for performing systematic literature reviews in software engineering. Tech report, Ver 23 EBSE Tech Report EBSE. 2007;
 - [16] Lockwood C, Munn Z, Porritt K. Qualitative research synthesis: Methodological guidance for systematic reviewers utilizing meta-aggregation. *Int J Evid Based Healthc.* 2015;13(3):179–87.
 - [17] Page MJ, McKenzie JE, Bossuyt P, Boutron I, Hoffmann TC, Mulrow CD, et al. The prisma 2020 statement: An updated guideline for reporting systematic reviews. *Med Flum.* 2021;57(4):444–65.
 - [18] Risdianto AC, Usman M, Rathore MA. Transforming Network Management: Intent-Based Flexible Control Empowered by Efficient Flow-Centric Visibility. *Futur Internet [Internet].* 2024;16(7). Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85199610627&doi=10.3390%2Ffi16070223&partnerID=40&md5=d9a1e0901c907111c2803e579e540dde>
 - [19] Abou El Houda Z, Brik B, Ksentini A. Securing IIoT applications in 6G and beyond using adaptive ensemble learning and zero-touch multi-resource provisioning. *Comput Commun [Internet].* 2024;216:260–73. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85183194528&doi=10.1016%2Fj.comcom.2024.01.018&partnerID=40&md5=c5828adfce19654a06dd7d95c5ace6d7>
 - [20] Krishnaveni S, Chen TM, Sathiyarayanan M, Amutha B. CyberDefender: an integrated intelligent defense framework for digital-twin-based industrial cyber-physical systems. *Cluster Comput [Internet].* 2024;27(6):7273–306. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85188165444&doi=10.1007%2Ffs10586-024-04320-x&partnerID=40&md5=163d08dbdf1525ab444a9a596a3b885e>
 - [21] Chen Q, Li R, Xu X, Wu J, Jiang H, Qiu M. Human-Aware Dynamic Hierarchical Network Control for Distributed Metaverse Services. *IEEE J Sel Areas Commun [Internet].* 2024;42(3):629–42. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85184814384&doi=10.1109%2FJSAC.2023.3345399&partnerID=40&md5=6d49e7b61efdc2360130e88a04a3b104>
 - [22] Oyucu S, Polat O, Türkoğlu M, Polat H, Aksöz A, Ağdaş MT. Ensemble Learning Framework for DDoS Detection in SDN-Based SCADA Systems. *Sensors [Internet].* 2024;24(1). Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85181954672&doi=10.3390%2Ffs24010155&partnerID=40&md5=23dd214633e6c285c581fb6e2152c73d>
 - [23] Gilani SMM, Usman M, Daud S, Kabir A, Nawaz Q, Judit O. SDN-based multi-level framework for smart home services. *Multimed Tools Appl [Internet].* 2024;83(1):327–47. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85159468552&doi=10.1007%2Ffs11042-023-15678-2&partnerID=40&md5=71b54c901bcf01a89d47f52e069dde2b>
 - [24] Snehi M, Bhandari A, Verma J. Foggier skies, clearer clouds: A real-time IoT-DDoS attack mitigation framework in fog-assisted software-defined cyber-physical systems. *Comput Secur [Internet].* 2024;139. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0->

- 85182660204&doi=10.1016%2Fj.cose.2024.103702&partnerID=40&md5=b98dae4d6663ff020fa5b8b015af58cd
- [25] Nahar A, Mondal KK, Das D, Buyya R. Clouds on the Road: A Software-Defined Fog Computing Framework for Intelligent Resource Management in Vehicular Ad-Hoc Networks. *IEEE Trans Mob Comput* [Internet]. 2024;23(12):12778–92. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85197602980&doi=10.1109%2FTMC.2024.3419016&partnerID=40&md5=84968760c161cbc800949ede8fa6ba92>
- [26] Basu K, Younas M, Peng S. A study of supervised machine learning algorithms for traffic prediction in SD-WAN. *Int J Web Grid Serv* [Internet]. 2024;20(2):206–29. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85193510442&doi=10.1504%2FIJWGS.2024.138600&partnerID=40&md5=394c0f9ab98f782feca225c8abcdccf1>
- [27] T.G. KK, Tomar S, Addya SK, Satpathy A, Koolagudi SG. EFraS: Emulated framework to develop and analyze dynamic Virtual Network Embedding strategies over SDN infrastructure. *Simul Model Pract Theory* [Internet]. 2024;134. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85192049758&doi=10.1016%2Fj.simpat.2024.102952&partnerID=40&md5=db39b4883adf5c6f45551b9d817f4d75>
- [28] Kabdjou J, Shinomiya N. Improving Quality of Service and HTTPS DDoS Detection in MEC Environment with a Cyber Deception-Based Architecture. *IEEE Access* [Internet]. 2024;12:23490–503. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85184342613&doi=10.1109%2FACCESS.2024.3361476&partnerID=40&md5=93fd0d92dfe69bd513a5bfb25c2b40c6>
- [29] Ramalakshmi R, Kavitha D. DDoS Attack Mitigation using Distributed SDN Multi Controllers for Fog Based IoT Systems. *Int J Intell Syst Appl Eng* [Internet]. 2024;12(4s):57–69. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85179689363&partnerID=40&md5=f2341a7bbc64466de3ee14c021093004>
- [30] Kirmızıoğlu RA, Tekalp AM, Görkemli B. Distributed virtual selective-forwarding units and SDN-assisted edge computing for optimization of multi-party WebRTC videoconferencing. *Signal Process Image Commun* [Internet]. 2025;130. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85204539259&doi=10.1016%2Fj.image.2024.117173&partnerID=40&md5=0d6a3ef3720eeb3bbb25f1da4323fbe5>
- [31] Anoushee M, Fartash M, Akbari Torkestani J. An intelligent resource management method in SDN based fog computing using reinforcement learning. *Computing* [Internet]. 2024;106(4):1051–80. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85145501043&doi=10.1007%2Fs00607-022-01141-x&partnerID=40&md5=243c355c849de1682f47d82610b17bd1>
- [32] Li J, Zhu M, Liu J, Liu W, Huang B, Liu R. Blockchain-based reliable task offloading framework for edge-cloud cooperative workflows in IoMT. *Inf Sci (Ny)* [Internet]. 2024;668. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85189360099&doi=10.1016%2Fj.ins.2024.120530&partnerID=40&md5=1cf64b57ead61397a3eb458b4b19cb31>
- [33] Quadri NS, K Durga Charan Y, Babu KS, Tanveer S, Reddy KSS, Kumar MK. INTRUSION DETECTION SYSTEM FOR CYBER SECURITY IN SMART AGRICULTURE WITH ABCIS TECHNIQUES. *J Theor Appl Inf Technol* [Internet]. 2024;102(10):5301–15. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85204162646&partnerID=40&md5=564539644eb38c70f79b0d2271d3fb86>
- [34] Sarabia-Jácome D, Giménez-Antón S, Liatifis A, Grasa E, Catalán M, Pliatsios D. Progressive Adoption of RINA in IoT Networks: Enhancing Scalability and Network Management via SDN Integration. *Appl Sci* [Internet]. 2024;14(6). Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85192563809&doi=10.3390%2Fapp14062300&partnerID=40&md5=cc4ea979451e6f1b7099ba593271682e>
- [35] Song A V, Karri GR. An integrated SDN framework for early detection of DDoS attacks in cloud computing. *J Cloud Comput* [Internet]. 2024;13(1). Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85188133077&doi=10.1186%2Fs13677-024-00625-9&partnerID=40&md5=02bdb3cac6a81b09ce382baaa6f9c64e>
- [36] Sousa B, Gonçalves C. FedAAA-SDN: Federated Authentication, Authorization and Accounting in SDN controllers. *Comput Networks* [Internet]. 2024;239. Available from:

- <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85180418078&doi=10.1016%2Fj.comnet.2023.110130&partnerID=40&md5=53cddc5e46ab9dda2d1c70860bf92d64>
- [37] Pei X, Sun P, Hu Y, Li D, Tian L, Li Z. Multi-resource interleaving for task scheduling in cloud-edge system by deep reinforcement learning. *Futur Gener Comput Syst* [Internet]. 2024;160:522–36. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85196662357&doi=10.1016%2Fj.future.2024.06.033&partnerID=40&md5=a503bbdf34aa3bb6765fb9e4d91ab27f>
- [38] Christila SA, Sivakumar R. A Deep Ensemble Framework for DDoS Attack Recognition and Mitigation in Cloud SDN Environment. *J Comput Sci* [Internet]. 2024;20(10):1281–90. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85202921073&doi=10.3844%2Fjcssp.2024.1281.1290&partnerID=40&md5=9cc3283b09825aef337a8de1b7d1352b>
- [39] Razvan F, Mitica C. Enhancing network security through integration of game theory in software-defined networking framework. *Int J Inf Secur* [Internet]. 2025;24(3). Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-105000699498&doi=10.1007%2Fs10207-025-01012-4&partnerID=40&md5=1b99e0330a2d7b6cc8a617051e111ec5>
- [40] Banitalebi Dehkordi A. EDBLSD-IIoT: a comprehensive hybrid architecture for enhanced data security, reduced latency, and optimized energy in industrial IoT networks. *J Supercomput* [Internet]. 2025;81(2). Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85213955733&doi=10.1007%2Fs11227-024-06872-6&partnerID=40&md5=4a2d71c9fad29161451459d9d8a453dd>
- [41] He T, Toosi AN, Buyya R. Efficient Large-Scale Multiple Migration Planning and Scheduling in SDN-Enabled Edge Computing. *IEEE Trans Mob Comput* [Internet]. 2024;23(6):6667–80. Available from: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85176351219&doi=10.1109%2FTMC.2023.3326610&partnerID=40&md5=15ab2b7dc6e566e203a1ba5f7df884c6>
- [42] Abouzahra A, Sabraoui A, Afdel K. Model composition in Model Driven Engineering: A systematic literature review. *Inf Softw Technol*. 2020;125(May):106316.