INTERNATIONAL JOURNAL OF ADVANCED INNOVATIVE TECHNOLOGY IN ENGINEERING

Published by Insightive Research Private Limited Home page: www.ijaite.co.in

Artificial Intelligence for Malware Detection in Software-Defined Networks: A Comprehensive Systematic Literature Review

[1]Sudhakar Honaji Yerme, [2]Dr. Prabhakar L. Ramteke

[1,2]HVPM College of Engineering and Technology, Amaravati, Maharashtra, India Sant Gadge Baba Amravati University, Amravati, Maharashtra, India

[1]ysudhakaran737@gmail.com, [2]pl_ramteke@rediffmail.com

Article History

Received on: 05 May 2026

Revised on: 25 June 2026

Accepted on: 20 July 2026

Keywords: Software-Defined Networking; Malware Detection; Intrusion Detection; Artificial Intelligence; Machine Learning; Deep Learning; Hybrid Intelligence; Cyber security.

e-ISSN: 2455-6491

DOI: 10.65809/IJAITE/26/v11i04/002

Production and hosted by

https://www.insightiveinc.org

ABSTRACT

Software-Defined Networking has emerged as a fundamental networking paradigm for cloud computing, Internet of Things, fifth-generation (5G) communication, and data-center infrastructures because of its centralized control, programmability, and flexible network management. However, the logical centralization of the control plane also introduces significant security vulnerabilities, making SDN increasingly susceptible to malware, botnets, ransomware, Distributed Denial-of-Service, and other sophisticated cyberattacks. Artificial Intelligence (AI)-based malware detection techniques have gained considerable attention due to their capability to identify complex and previously unseen attack patterns. This paper presents a comprehensive Systematic Literature Review of intelligent malware detection approaches for SDN by following the PRISMA 2020 framework and Kitchenham guidelines. A total of 30 primary studies published between 2020 and 2026 were systematically selected, assessed, and synthesized. The reviewed literature was classified into three major categories: Machine Learning, Deep Learning, and Hybrid AI approaches, followed by comprehensive comparative analyses of datasets, learning algorithms, feature engineering strategies, evaluation metrics, detection performance, and reported limitations. The quantitative synthesis indicates a clear research transition from conventional ML techniques toward deep learning and hybrid intelligence frameworks, with hybrid models consistently shows the highest detection performance, frequently exceeding 99% detection accuracy. The analysis further reveals that Random Forest, Support Vector Machine, Convolutional Neural Networks, Long Short-Term Memory networks, Deep Neural Networks, and CNN–LSTM hybrid architectures are among the most widely adopted algorithms, whereas NSL-KDD, InSDN, UNSW-NB15, CICIDS2017, and IoT-23 remain the dominant evaluation datasets. The review identifies several persistent challenges, including dependence on benchmark datasets, limited real-world SDN validation, class imbalance, high computational complexity, insufficient explainability, limited cross-dataset generalization, and the absence of standardized benchmarking protocols. The review outlines future research directions emphasizing lightweight and explainable AI models, graph neural networks, federated and continual learning, adaptive hybrid intelligence, and standardized real-world evaluation frameworks to support the development of accurate, scalable, robust, and deployable malware detection systems for next-generation Software-Defined Networks.

1. INTRODUCTION

The rapid advancement of cloud computing, Internet of Things (IoT), fifth-generation (5G) communication, and large-scale data center technologies has significantly increased the complexity and scale of modern computer networks [1]. To address the limitations of traditional network architectures, Software-Defined Networking (SDN) has emerged as a flexible and programmable networking paradigm that separates the control plane from the data plane, enabling centralized network management, dynamic traffic control, and simplified network configuration [2]. These capabilities have accelerated the adoption of SDN across cloud infrastructures, enterprise networks, industrial Internet of Things (IIoT), smart cities, and next-generation communication systems. However, the centralized architecture of SDN also introduces critical security vulnerabilities, making the network highly susceptible to malware attacks, ransomware, botnets, Distributed Denial-of-Service (DDoS) attacks, and other sophisticated cyber threats [3]. Consequently, intelligent malware detection has become a fundamental research area for ensuring secure, reliable, and

resilient SDN environments. Traditional signature-based and rule-based security mechanisms are often incapable of detecting polymorphic, metamorphic, and zero-day malware because they rely on predefined attack signatures and manually crafted rules [4]. To overcome these limitations, researchers have increasingly employed Artificial Intelligence (AI) techniques, particularly Machine Learning (ML), Deep Learning (DL), and Hybrid approaches, to automatically learn malicious traffic patterns and improve malware detection accuracy. Recent studies demonstrate that ML algorithms such as Random Forest (RF) [5], Support Vector Machine (SVM) [6], and Linear Discriminant Analysis (LDA) [7], together with DL architectures including Convolutional Neural Networks (CNNs) [8], Long Short-Term Memory (LSTM) networks [9], Deep Neural Networks (DNNs) [10], and Gated Recurrent Units (GRUs) [11], provide significant improvements in malware detection performance. Furthermore, Hybrid models integrating optimization algorithms, reinforcement learning, and ensemble learning techniques have reported detection accuracies exceeding 99%, highlighting the growing importance of intelligent security frameworks for Software-Defined Networks.

The existing literature remains fragmented across different learning algorithms, datasets, feature engineering strategies, evaluation metrics, and application scenarios, making it difficult to objectively compare the effectiveness of proposed malware detection frameworks. Most studies rely on benchmark datasets such as NSL-KDD, UNSW-NB15, InSDN, CICIDS2017, and IoT-23, while comparatively fewer investigations evaluate models using large-scale real-world SDN traffic [12]. Moreover, the rapid evolution of malware attacks has exposed several challenges, including class imbalance, limited cross-dataset validation, high computational complexity, insufficient model interpretability, and the absence of standardized benchmarking protocols [13]. Existing review articles primarily emphasize intrusion detection or general SDN security and provide limited systematic synthesis dedicated specifically to intelligent malware detection. These limitations motivate the need for a comprehensive Systematic Literature Review (SLR) that critically analyzes recent advances, identifies research trends, compares the strengths and limitations of existing ML, DL, and Hybrid techniques, and highlights unresolved research challenges [14]. Accordingly, this study presents a systematic review of malware detection techniques for Software-Defined Networks by following the PRISMA 2020 framework and Kitchenham guidelines. The review systematically examines studies published between 2020 and 2026, classifies the literature into Machine Learning, Deep Learning, and Hybrid approaches, and synthesizes evidence based on datasets, algorithms, feature engineering techniques, evaluation metrics, detection performance, and research limitations [15]. In addition, the review provides quantitative analyses, comparative evaluations, statistical summaries, and research trend analyses to answer predefined research questions and identify future research directions. By offering an evidence-based synthesis of the existing literature, this SLR serves as a comprehensive reference for researchers and practitioners working toward the development of accurate, scalable, explainable, and intelligent malware detection systems for next-generation Software-Defined Network environments [16].

A. Research Challenges

The remarkable progress in intelligent malware detection, several important challenges remain unresolved. First, many studies continue to rely on benchmark datasets that may not accurately represent modern SDN traffic and evolving malware behaviors. Second, advanced Deep Learning and Hybrid models often require substantial computational resources, limiting their suitability for real-time deployment. Third, class imbalance and limited cross-dataset validation reduce the generalization capability of many proposed models. Furthermore, the lack of explainable decision-making mechanisms decreases the transparency and trustworthiness of complex deep learning architectures. Finally, the absence of standardized benchmarking protocols and comprehensive comparative evaluations makes it difficult to objectively assess the effectiveness of different malware detection techniques. Addressing these challenges is essential for developing robust, adaptive, and practical malware detection systems for next-generation Software-Defined Networks.

The major contributions of this systematic literature review are summarized as follows:

- A comprehensive Systematic Literature Review of intelligent malware detection techniques for Software-Defined Networks covering studies published between 2020 and 2026.
- A structured classification of the reviewed literature into Machine Learning, Deep Learning, and Hybrid Artificial Intelligence approaches.
- A comparative analysis of commonly used datasets, algorithms, feature engineering techniques, evaluation metrics, detection performance, strengths, and limitations.
- A quantitative synthesis of publication trends, algorithm usage, dataset distribution, research limitations, and detection accuracy using statistical analysis and graphical visualizations.

- An evidence-based discussion addressing predefined research questions related to algorithms, datasets, evaluation metrics, and research gaps.
- Identification of current research challenges and future research directions to support the development of accurate, scalable, explainable, and intelligent malware detection frameworks for SDN environments.

The remainder of this paper is organized as follows. Section 2 presented the background details of SDN. Section 3 describes the systematic literature review methodology, including the review protocol, search strategy, study selection process, and research questions. Section 4 presents the publication trends and research evolution in malware detection for Software-Defined Networks. Section 5 introduces the taxonomy of intelligent malware detection approaches, followed by Section 6, which classifies the literature into Machine Learning, Deep Learning, and Hybrid techniques. Section 7 provides a comprehensive comparative analysis of datasets, algorithms, feature engineering methods, and evaluation metrics. Section 8 discussed the observed finding of study. Section 9 presents the challenges in SDN. Section 10 presents the opportunities in SDN while Section 11 discusses the findings by answering the predefined research questions. Finally, Section 12 concludes the paper by summarizing the major findings, highlighting current research challenges, and outlining future research directions for intelligent malware detection in Software-Defined Networks.

2. BACKGROUND AND CONCEPTUAL FOUNDATIONS

Software-Defined Networking (SDN) has emerged as an important networking paradigm for supporting programmable, scalable, and centrally coordinated communication infrastructures. Unlike conventional networks, in which forwarding and control functions are tightly integrated within individual networking devices, SDN separates network decision-making from packet-forwarding operations. This architectural separation allows administrators to configure network policies dynamically, obtain a centralized view of network conditions, and automate traffic-management functions. Consequently, SDN has been increasingly adopted in cloud computing, Internet of Things environments, data centers, industrial networks, smart cities, and fifth-generation communication systems. However, the same programmability and logical centralization that improve network flexibility also introduce new security risks. Compromise of the controller, manipulation of control messages, malicious flow-rule installation, and flooding of control-plane resources can disrupt the entire network. These characteristics have motivated extensive research into intelligent malware and intrusion detection mechanisms using machine learning, deep learning, reinforcement learning, ensemble learning, and hybrid artificial intelligence techniques. The conceptual foundations presented in this section establish the architectural, security, and computational context for the systematic synthesis conducted in the subsequent sections of this review.

A. SDN Architecture and Attack Surface

Software-Defined Networking transforms conventional network management by separating the control plane, which determines how traffic should be handled, from the data plane, which forwards packets according to predefined rules. In traditional networks, routing, forwarding, access control, and device configuration are implemented within distributed routers and switches. This tight integration makes large networks difficult to configure consistently and limits their ability to respond dynamically to changing traffic conditions. SDN addresses these limitations by transferring network-control intelligence to a logically centralized controller while retaining packet-forwarding functions within programmable switches.

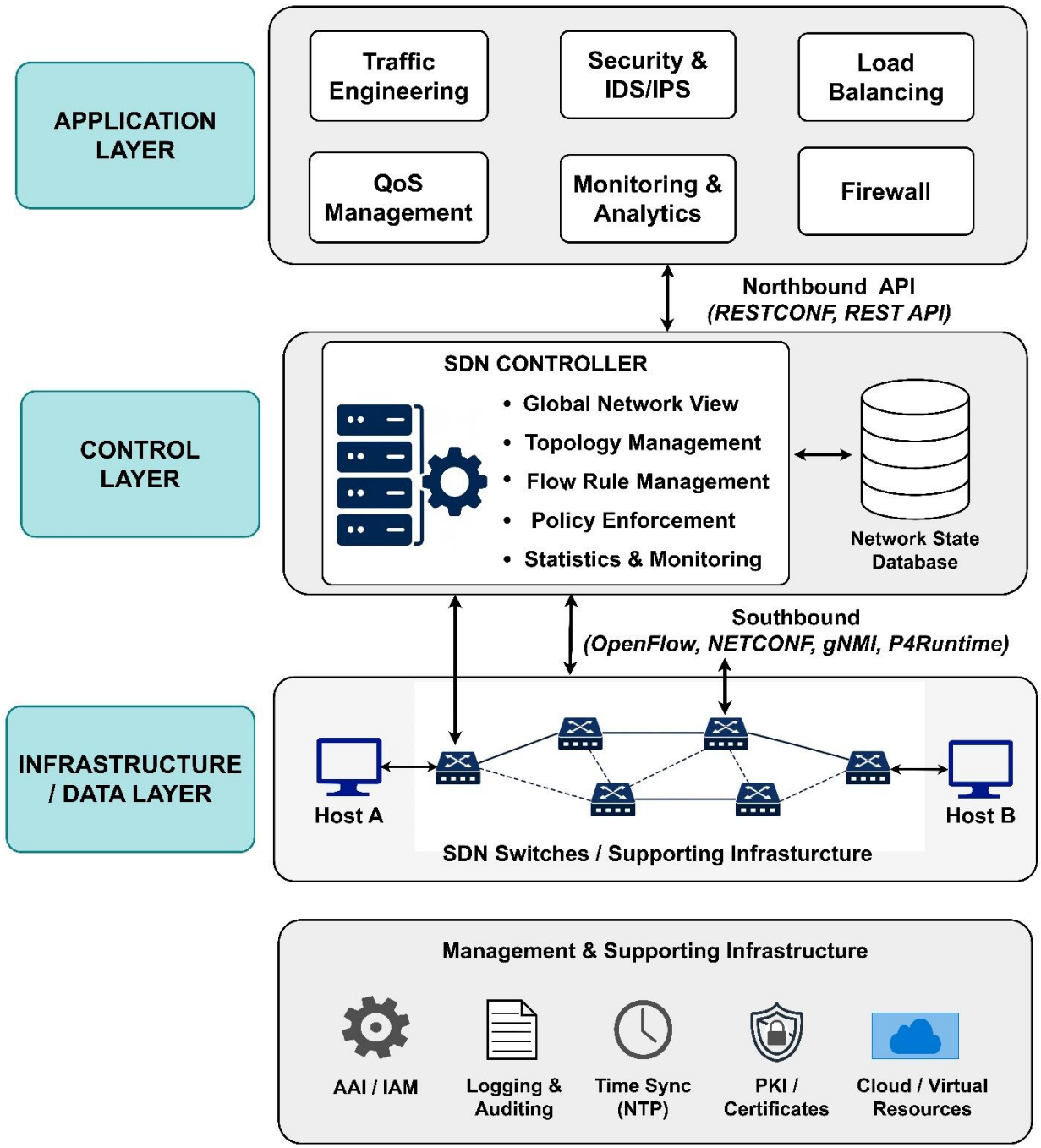

Figure 1: Conceptual Architecture of SDN and attack surface

Figure 1 shows SDN architecture is commonly organized into three layers: the application layer, the control layer, and the infrastructure or data layer. The application layer contains network services and management applications, such as traffic engineering, access control, load balancing, quality-of-service management, intrusion detection, firewalling, and malware monitoring. These applications communicate with the controller through northbound interfaces and express high-level network policies without directly configuring individual forwarding devices.

The control layer contains the SDN controller, which maintains a global or logically centralized view of network topology, device states, traffic flows, and forwarding policies. The controller translates application-level requirements into low-level flow rules and installs these rules in data-plane devices. It may also collect flow statistics, detect topology changes, and coordinate responses to abnormal network conditions. Examples of controller functions include path computation, flow-rule management, host tracking, policy enforcement, and communication with security applications.

The infrastructure layer consists of physical or virtual switches, routers, gateways, and other forwarding devices. These devices process

packets according to flow-table entries received from the controller. When a packet does not match an existing flow rule, the switch may forward information about the packet to the controller and request a forwarding decision. The controller then determines the appropriate action and installs the corresponding rule. Communication between the control and infrastructure layers is performed through southbound interfaces, with OpenFlow being one of the most widely discussed protocols in SDN research.

This centralized and programmable organization provides several operational advantages. First, it simplifies network configuration because policies can be implemented through a central control mechanism rather than through device-by-device configuration. Second, the global network view supports adaptive routing, traffic optimization, congestion control, and dynamic resource allocation. Third, programmability facilitates rapid deployment of security policies and enables network behaviour to be modified in response to emerging threats. Finally, SDN supports virtualization and network slicing, making it suitable for cloud, edge, IoT, industrial, and 5G-oriented environments.

The SDN introduces an expanded and multi-layered attack surface. Security threats can target the application layer, control layer, data layer, communication interfaces, or management infrastructure. Because the controller has extensive authority over network operations, its compromise may have network-wide consequences. An attacker who gains access to the controller may modify forwarding policies, redirect traffic, disable security applications, create unauthorized routes, or install malicious flow entries. Therefore, the controller represents a high-value target and a potential single point of logical failure.

At the application layer, malicious or vulnerable applications can submit unauthorized policies through northbound interfaces. A compromised application may request excessive permissions, manipulate routing decisions, access sensitive network information, or conflict with legitimate applications. Inadequate application isolation and weak authorization mechanisms may allow one application to affect the behaviour of other services. Third-party SDN applications may also contain software vulnerabilities that attackers can exploit to obtain controller access.

The control layer is exposed to attacks including controller impersonation, privilege escalation, unauthorized configuration changes, denial-of-service attacks, and exploitation of controller software vulnerabilities. Because switches frequently communicate with the controller when new flows are observed, an attacker may generate a large number of previously unseen flows to overwhelm controller processing and memory resources. This type of control-plane saturation can increase response latency, prevent the installation of legitimate flow rules, and degrade overall network availability.

The data plane is susceptible to flow-table exhaustion, packet flooding, malicious forwarding, spoofing, and unauthorized modification of switch behaviour. Forwarding devices generally possess limited flow-table capacity. Attackers may exploit this limitation by generating many unique flows, causing the switch to install excessive entries and eventually exhaust available memory. Compromised switches may also drop packets, duplicate traffic, modify forwarding paths, or provide false traffic statistics to the controller.

Communication channels between SDN components represent another important security boundary. Southbound communication between controllers and switches may be targeted by man-in-the-middle attacks, message tampering, replay attacks, eavesdropping, and controller-switch impersonation. Northbound interfaces may be exploited through insecure application programming interfaces, inadequate authentication, or unauthorized policy requests. East–west communication among distributed controllers can also be targeted to disrupt controller synchronization or inject inconsistent topology information.

The logical centralization of SDN additionally increases exposure to Distributed Denial-of-Service attacks. Large volumes of malicious traffic can overload forwarding devices, controller interfaces, or security applications. Botnets may generate distributed requests that force repeated controller involvement, thereby consuming control-plane bandwidth and computational resources. Malware operating within connected endpoints can also spread laterally, scan network services, establish command-and-control channels, or manipulate traffic patterns while attempting to evade conventional signature-based detection. The SDN attack surface can therefore be represented as a set of interacting components:

$$ASDN = \{Aapp, Actrl, Adata, Anorth, Asouth, Aeast - west\},$$

where Aapp, Actrl, and Adata represent threats associated with the application, control, and data layers, while Anorth, Asouth, and Aeast–west represent attacks targeting communication interfaces. Effective security mechanisms must consider these layers collectively because an attack initiated in one layer may propagate to others. For example, malware-generated flows originating at compromised endpoints may exhaust switch tables, increase controller requests, and eventually degrade security applications operating at the application layer.

Although centralization creates security risks, it also offers opportunities for improved threat monitoring. The controller can collect network-wide flow statistics, including source and destination addresses, ports, protocols, packet counts, byte counts, flow duration, and connection states. These observations can be used to identify coordinated attacks, abnormal traffic patterns, botnet communication, and malware propagation. Consequently, SDN provides both the motivation and the data infrastructure for developing centralized and distributed intelligent detection systems.

B. Malware and Intrusion Detection in SDN

Malware detection and intrusion detection are closely related but conceptually distinct security tasks. Malware detection focuses on identifying malicious software, malware-generated behaviour, malware families, botnets, ransomware, worms, Trojans, spyware, and command-and-control communication. Intrusion detection, by comparison, encompasses a broader range of unauthorized or harmful activities, including denial-of-service attacks, scanning, exploitation, credential attacks, spoofing, infiltration, and policy violations. Within SDN research, these terms are frequently used interchangeably because malware activity is often identified indirectly through malicious network traffic rather than through direct analysis of executable files.

An intrusion detection system monitors network or host activities to determine whether observed behaviour corresponds to legitimate use or malicious activity. Detection systems can be classified according to their data source, detection principle, deployment location, and response mechanism. Based on data source, detection may be host-based, network-based, or hybrid. Host-based systems analyze information collected from individual devices, including system calls, file modifications, memory activity, process behaviour, registry changes, and authentication logs. Network-based systems examine packets, flow records, protocol fields, connection patterns, and traffic statistics. Hybrid systems combine host and network observations to obtain a more comprehensive representation of malicious activity.

In SDN environments, network-based monitoring is particularly important because the controller can collect flow-level information from multiple switches. Commonly examined features include:

$$x = [x1, x2, \dots, xd],$$

where the feature vector may contain flow duration, source and destination ports, protocol type, packet rate, byte rate, forward and backward packet counts, inter-arrival time, TCP flags, failed connection attempts, and controller-request frequency. The objective of a detection model is to learn a function:

$$f: Rd \rightarrow Y,$$

where Y may represent binary labels such as normal and malicious or multiple classes corresponding to different attack and malware categories.

Traditional malware and intrusion detection techniques are generally divided into signature-based, anomaly-based, specification-based, and hybrid approaches. Signature-based detection compares observed traffic or system behaviour with predefined patterns associated with known attacks. It is computationally efficient and can provide high precision for previously identified threats. However, its effectiveness is limited when malware modifies its code, communication pattern, payload, or execution behaviour. Polymorphic and metamorphic malware can change their observable representation while preserving malicious functionality, enabling them to evade fixed signatures.

Anomaly-based detection establishes a model of normal network behaviour and identifies statistically or behaviourally significant deviations. It can potentially detect unknown or zero-day attacks because it does not require an exact predefined signature. However, variations in legitimate user behaviour, application traffic, and network conditions may be incorrectly classified as malicious, resulting in high false-positive rates. The effectiveness of anomaly detection therefore depends on the representativeness of training data and the ability of the model to distinguish harmful deviations from normal operational changes.

Specification-based detection evaluates activities against manually defined descriptions of acceptable protocol or system behaviour. It may detect deviations that violate network or application specifications while requiring fewer attack signatures. Nevertheless, developing and maintaining accurate specifications for complex and dynamic SDN environments is difficult. Hybrid detection combines signature, anomaly, specification, or learning-based mechanisms to improve coverage and reduce the limitations of individual techniques.

In an SDN environment, detection components may be deployed at different locations. A controller-based detector operates as an application connected to the SDN controller and analyzes centrally collected traffic information. This arrangement provides broad network visibility and enables rapid installation of mitigation rules. However, continuous collection and analysis of large traffic volumes may increase controller overhead. An edge-based detector places detection functions near switches, gateways, or end devices, reducing response

latency and control-plane load but providing a more limited network view. A distributed detection framework combines information from multiple controllers, switches, or edge nodes to improve scalability and fault tolerance. Cloud-assisted approaches may provide extensive computational capacity but can introduce communication latency, privacy concerns, and dependence on remote infrastructure.

The operational process of an SDN-based detection system commonly includes five stages:

Traffic acquisition: collection of packets, flow rules, controller logs, or host observations.

Preprocessing: removal of missing, duplicated, corrupted, or irrelevant records.

Feature transformation: encoding categorical attributes, normalizing numerical features, balancing classes, and selecting informative variables.

Detection or classification: application of a rule-based, statistical, ML, DL, or hybrid model.

Response: installation of blocking rules, flow redirection, rate limiting, host isolation, alert generation, or forensic logging. The detection process can be represented as:

$$y^{\wedge} = f\theta(T(x)),$$

where $T(\cdot)$ denotes preprocessing and feature transformation, fθ denotes the detection model parameterized by θ, and y^ represents the predicted class. When malicious traffic is detected, the controller may execute a response policy:

$$r = g(y^{\wedge}, p, c),$$

where p represents model confidence and c represents network context. The response r may involve blocking, rerouting, rate limiting, quarantine, or continued monitoring.

Several benchmark datasets have been used for evaluating intelligent detection models, including NSL-KDD, UNSW-NB15, CICIDS2017, InSDN, and IoT-23. However, these datasets differ substantially in traffic-generation methods, attack categories, feature sets, class distributions, and SDN relevance. NSL-KDD, UNSW-NB15, and CICIDS2017 are general intrusion-detection datasets rather than inherently SDN-native datasets. InSDN provides traffic associated more directly with SDN-based environments, whereas IoT-23 contains malicious and benign IoT traffic, including botnet and malware-related behaviour. Consequently, performance results obtained from different datasets should not be interpreted as direct head-to-head comparisons.

Several practical challenges affect malware and intrusion detection in SDN. First, attack classes are frequently imbalanced, with rare but critical threats represented by relatively few samples. Second, models trained on one dataset may perform poorly on traffic from another network because of variations in topology, user behaviour, protocols, and attack implementations. Third, rapidly changing malware and concept drift can reduce the effectiveness of static models. Fourth, high detection complexity may increase controller latency and limit real-time deployment. Fifth, many advanced models operate as black-box systems, making it difficult for administrators to understand why traffic was classified as malicious. These challenges provide the central motivation for applying adaptive and intelligent learning paradigms.

3. SYSTEMATIC LITERATURE REVIEW METHODOLOGY

This study adopts a SLR methodology to provide a comprehensive and unbiased analysis of existing research on malware detection in SDN. Unlike conventional narrative reviews, the SLR approach follows a structured and transparent process for identifying, selecting, evaluating, and synthesizing relevant studies, thereby minimizing selection bias and improving the reliability and reproducibility of the review. The methodology employed in this study is based on established systematic review guidelines and incorporates a well-defined review protocol, including the formulation of research questions, literature search strategy, study selection criteria, quality assessment, and data extraction procedures. The selected studies are subsequently categorized into Machine Learning (ML), Deep Learning (DL), and Hybrid intelligence-based approaches to facilitate a comprehensive comparative analysis of datasets, algorithms, evaluation metrics, performance outcomes, and existing research limitations. This systematic methodology enables the identification of current research trends, technological advancements, unresolved challenges, and potential future directions for developing intelligent malware detection frameworks in Software-Defined Network environments.

A. *Research Questions (RQ)*

RQ1: What machine learning algorithms are used for malware detection in SDN?

RQ2: Which deep learning models provide the highest detection accuracy?

RQ3: Which datasets are most frequently employed?

RQ4: Which evaluation metrics are commonly used?

RQ5: What are the current research gaps?

B. Review Protocol

The transparency, consistency, and reproducibility of the review process, this study follows a structured review protocol based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) framework and the systematic literature review guidelines proposed by Kitchenham. These well-established

methodologies provide a rigorous foundation for identifying, selecting, evaluating, and synthesizing relevant research while minimizing potential selection bias. The review protocol defines each stage of the systematic review process, including research question formulation, literature search, study selection, quality assessment, data extraction, and qualitative synthesis.

The PRISMA 2020 framework was adopted to guide the systematic identification and screening of relevant publications. The framework provides a transparent reporting structure that documents each stage of the literature selection process, including the identification of records from multiple digital databases, removal of duplicate studies, title and abstract screening, full-text eligibility assessment, and final inclusion of studies for qualitative analysis. The application of the PRISMA methodology improves the credibility of the review by ensuring that only studies satisfying the predefined inclusion and exclusion criteria are considered for further analysis.

In addition to PRISMA 2020, the review methodology follows the Kitchenham Guidelines for conducting systematic literature reviews in computer science and software engineering research. These guidelines recommend a well-defined review protocol consisting of planning, conducting, and reporting phases. During the planning phase, the objectives of the review and the research questions were established. The conducting phase involved systematic searching of multiple scientific databases, application of eligibility criteria, quality assessment of the selected studies, and extraction of relevant information. Finally, the reporting phase focuses on organizing and synthesizing the extracted evidence into meaningful categories to facilitate comprehensive analysis and comparison of existing malware detection techniques in Software-Defined Networks.

The review protocol was designed to ensure comprehensive coverage of studies investigating machine learning, deep learning, reinforcement learning, ensemble learning, optimization-based methods, and hybrid intelligent approaches for malware detection in SDN environments. Each selected study was carefully examined to extract information regarding the datasets employed, feature engineering techniques, learning algorithms, evaluation metrics, detection performance, and reported limitations. Based on these extracted characteristics, the selected literature was systematically classified into three major categories: Machine Learning-based approaches, Deep Learning-based approaches, and Hybrid approaches. This classification provides a structured framework for comparing different methodologies and identifying their respective strengths and weaknesses.

To maintain the quality and reliability of the review, only peer-reviewed journal articles and conference papers published within the defined review period were considered. Duplicate publications, non-English articles, editorials, books, patents, and studies unrelated to malware detection in Software-Defined Networks were excluded from the review. Furthermore, each eligible study was critically evaluated based on its research objectives, experimental methodology, dataset selection, performance evaluation, and discussion of limitations before being included in the final analysis.

C. Search Strategy

A comprehensive and systematic search strategy was designed to identify relevant studies addressing malware detection in Software-Defined Networks (SDN) using ML, DL, and Hybrid intelligence-based approaches. The primary objective of the search strategy was to ensure comprehensive coverage of high-quality research while minimizing publication bias and reducing the likelihood of omitting significant studies. The search process followed the review protocol described in the previous section and was conducted using multiple internationally recognized scientific digital libraries.

To maximize the coverage of relevant literature, publications were retrieved from seven major electronic databases, namely IEEE Xplore, SpringerLink, ScienceDirect (Elsevier), ACM Digital Library, Wiley Online Library, MDPI, and Google Scholar. These databases were selected because they index a substantial proportion of peer-reviewed journals, conference proceedings, and review articles in the fields of computer science, cybersecurity, artificial intelligence, networking, and Software-Defined Networking. Collectively, these digital libraries provide extensive access to high-impact publications and are widely recognized as reliable sources for conducting systematic literature reviews.

The literature search was conducted using combinations of carefully selected keywords related to Software-Defined Networks, malware detection, intrusion detection, machine learning, deep learning, hybrid intelligence, and network security. To improve retrieval effectiveness, Boolean operators such as AND, OR, and parentheses were employed to combine multiple search terms and capture variations of relevant concepts. The search strategy was refined iteratively to ensure that the retrieved studies adequately represented the current state of research to minimizing irrelevant results.

The quality and relevance of the selected studies, the search was restricted to peer-reviewed

journal articles and conference papers published between 2020 and 2026. This publication period was chosen because it reflects the rapid advancements in intelligent malware detection techniques for SDNs, particularly the growing adoption of deep learning, reinforcement learning, graph neural networks, optimization algorithms, and hybrid artificial intelligence models. Only studies published in the English language were considered to maintain consistency throughout the review process.

After retrieving the initial set of publications from all selected databases, duplicate records were identified and removed. The remaining studies were subsequently subjected to title and abstract screening, followed by full-text evaluation based on predefined inclusion and exclusion criteria. Finally, the selected studies were categorized into Machine Learning-based, Deep Learning-based, and Hybrid intelligence-based malware detection approaches. This systematic search strategy ensured that the review comprehensively captured the most relevant and recent contributions while providing a reliable foundation for comparative analysis, research trend identification, and the formulation of future research directions.

Table 1. Digital Libraries Used for Literature Search

Digital Library	Publisher	Research Coverage
IEEE Xplore	IEEE	Computer Networks, SDN, Artificial Intelligence, Cybersecurity, Machine Learning
SpringerLink	Springer Nature	Computer Science, Network Security, Artificial Intelligence, Software Engineering
ScienceDirect	Elsevier	Computer Networks, Information Security, Deep Learning, Cybersecurity
ACM Digital Library	Association for Computing Machinery (ACM)	Networking, SDN, Machine Learning, Intrusion Detection Systems
Wiley Online Library	Wiley	Computer Science, Intelligent Systems, Artificial Intelligence
MDPI	MDPI	Cybersecurity, Network Security, Machine Learning, Internet of Things
Google Scholar	Google	Broad coverage of peer-reviewed journals, conference proceedings, and scholarly publications

D. Search Keywords

("Software Defined Network" OR SDN)
AND
("Malware Detection" OR "Intrusion Detection")
AND
("Machine Learning" OR "Deep Learning" OR "Hybrid")

E. Inclusion and Exclusion Criteria

The relevance, and consistency of the selected literature, a set of predefined inclusion and exclusion criteria was established before the study selection process. These criteria were formulated according to the review protocol to minimize selection bias and ensure that only studies directly related to malware detection in SDN were included in the systematic review. The eligibility criteria guided the screening of publications during the title, abstract, and full-text evaluation stages.

The inclusion criteria focused on selecting peer-reviewed studies that investigate intelligent malware detection techniques in SDN environments. Specifically, studies were considered eligible if they: (i) proposed or evaluated Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL), Ensemble Learning, or Hybrid Artificial Intelligence techniques for malware detection or intrusion detection in Software-Defined Networks; (ii) reported experimental results using benchmark or real-world datasets; (iii) presented quantitative performance evaluation using metrics such as accuracy, precision, recall, F1-score, AUC, or false positive rate; (iv) were published as peer-reviewed journal articles or conference papers between 2020 and 2026; and (v) were written in the English language.

Conversely, studies were excluded if they did not satisfy the predefined eligibility requirements. Publications focusing exclusively on traditional network security without considering Software-Defined Networks were omitted. Similarly, studies addressing unrelated domains such as blockchain security, cloud security, wireless sensor networks, or mobile ad hoc networks without an SDN context were excluded. Survey papers, review articles, editorials, book chapters, theses, patents, white papers, and duplicate publications were also removed to avoid redundancy and ensure that only original research contributions were analyzed.

The application of these inclusion and exclusion criteria ensured that the selected studies were directly relevant to the objectives of this systematic literature review and provided sufficient experimental evidence for comparative analysis. This systematic filtering process enhanced the reliability of the review by ensuring that only high-quality and scientifically validated research contributed to the synthesis of malware detection techniques in Software-Defined Networks.

Table 2: Inclusion and Exclusion Criteria

Criteria	Inclusion	Exclusion
Research Domain	Malware detection, intrusion detection, and cybersecurity in Software-Defined Networks	Studies unrelated to SDN or focused solely on other networking paradigms
Methodology	Machine Learning, Deep Learning, Reinforcement Learning, Ensemble Learning, and Hybrid AI approaches	Traditional signature-based or rule-based methods without AI techniques
Publication Type	Peer-reviewed journal articles and conference papers	Review papers, surveys, editorials, books, book chapters, theses, patents, and white papers
Publication Period	2020–2026	Publications before 2020
Language	English	Non-English publications
Experimental Evaluation	Studies reporting datasets and quantitative performance metrics	Studies without experimental validation or insufficient methodological details
Duplicates	Most complete and latest version retained	Duplicate or redundant publications

F. Quality Assessment

The reliability and scientific validity of the selected studies, a quality assessment was conducted before the final data extraction and synthesis. The primary objective of this assessment was to evaluate the methodological quality, experimental design, and reporting completeness of each eligible study. This process helps minimize the inclusion of low-quality research and ensures that the conclusions drawn from the systematic literature review are based on credible and well-validated evidence.

The quality assessment was performed after the application of the inclusion and exclusion criteria. Each selected publication was independently evaluated using a predefined set of quality assessment questions adapted from established systematic literature review guidelines. The assessment focused on several important aspects of the studies, including the clarity of research objectives, appropriateness of the experimental methodology, dataset selection, model evaluation, reproducibility of results, and discussion of research limitations. These evaluation criteria provide a consistent framework for comparing studies employing Machine Learning, Deep Learning, and Hybrid intelligence techniques for malware detection in Software-Defined Networks.

Each quality assessment criterion was assigned one of three possible scores: 1 if the criterion was fully satisfied, 0.5 if it was partially satisfied, and 0 if it was not satisfied. The individual scores obtained for each criterion were summed to calculate the overall quality score of each study. Publications with higher quality scores were considered more reliable and were given greater emphasis during the qualitative synthesis and comparative analysis. This assessment process improves the transparency and reproducibility of the review while reducing the influence of studies with incomplete experimental validation or insufficient methodological descriptions.

The quality assessment also facilitated the identification of common methodological limitations across the reviewed literature. Many studies reported excellent malware detection performance, several lacked comprehensive evaluations on real-world SDN environments, explainability of prediction models, scalability analysis, or assessment against zero-day malware attacks. These observations were subsequently considered during the identification of research challenges and future research directions presented in the later sections of this review.

Table 3: Quality Assessment Criteria

QA ID	Quality Assessment Question	Evaluation Objective
QA1	Are the research objectives clearly defined?	Evaluate the clarity of the study objectives.
QA2	Is the proposed malware detection methodology adequately described?	Assess the completeness of the methodological description.
QA3	Is an appropriate SDN malware dataset used for experimentation?	Verify the suitability of the experimental dataset.
QA4	Are the experimental procedures and implementation details sufficiently reported?	Assess the reproducibility of the proposed method.
QA5	Are standard evaluation metrics (Accuracy, Precision, Recall, F1-score, AUC, etc.) reported?	Evaluate the completeness of performance assessment.
QA6	Are the experimental results compared with existing state-of-the-art approaches?	Assess the effectiveness of comparative evaluation.
QA7	Are the limitations and future research directions discussed?	Evaluate the completeness of the research discussion.

Table 4: Quality Assessment Scoring Scheme

Score	Interpretation
1.0	Criterion fully satisfied
0.5	Criterion partially satisfied
0.0	Criterion not satisfied

G. PRISMA Study Selection Process

The study selection process was conducted in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines to ensure a transparent, systematic, and reproducible selection of relevant studies. The PRISMA framework provides a standardized procedure for identifying, screening, assessing, and selecting publications that satisfy the predefined eligibility criteria. Following this structured process minimizes selection bias and improves the overall reliability of the systematic literature review.

Initially, relevant publications were identified through comprehensive searches conducted across multiple scientific digital libraries. The retrieved records were combined into a single collection, and duplicate publications appearing in more than one database were identified and removed. Subsequently, the remaining studies underwent an initial screening based on their titles and abstracts to eliminate publications that were clearly unrelated to malware detection in Software-Defined Networks or did not satisfy the objectives of this review.

The studies retained after the preliminary screening were subjected to a detailed full-text assessment. During this stage, each publication was carefully examined according to the predefined inclusion and exclusion criteria described in the previous section. Only studies presenting original research on malware detection or intelligent intrusion detection in Software-Defined Networks using Machine Learning, Deep Learning, Reinforcement Learning, Ensemble Learning, or Hybrid Artificial Intelligence approaches were considered eligible for inclusion in the review. Publications lacking sufficient methodological details, experimental validation, or quantitative performance evaluation were excluded from further analysis.

Following the eligibility assessment, the final set of selected studies was subjected to quality assessment and data extraction. Relevant information, including publication details, datasets, feature engineering techniques, learning algorithms, evaluation metrics, detection performance, and reported limitations, was systematically extracted for comparative analysis. Based on the characteristics of the proposed detection methods, the selected studies were subsequently categorized into Machine Learning-based, Deep Learning-based, and Hybrid intelligence-based malware detection approaches. This classification forms the foundation for the comparative discussions presented in the subsequent sections of this review.

The systematic application of the PRISMA methodology ensures that the study selection process is objective, transparent, and reproducible. Furthermore, it provides a reliable basis for synthesizing the current state of research, identifying existing challenges, and highlighting future research opportunities in intelligent malware detection for Software-Defined Network environments.

A. Data Extraction and Synthesis

Following the study selection and quality assessment processes, relevant information was systematically extracted from each of the selected publications using a predefined data extraction framework. The primary objective of the data extraction process was to collect consistent and comprehensive information from the reviewed studies, thereby facilitating an objective comparison of existing malware detection techniques in Software-Defined Networks (SDNs). The extracted information served as the foundation for the qualitative synthesis, comparative analysis, and identification of research trends presented in this review.

For each selected study, several key attributes were recorded, including the publication details (author(s) and year of publication), application domain, experimental dataset, feature engineering or preprocessing techniques, malware detection model, evaluation metrics, detection performance, major findings, and reported limitations. Particular emphasis was placed on the type of artificial intelligence technique employed, such as Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL), Ensemble Learning, or Hybrid intelligence-based methods. Additionally, information regarding the datasets used for experimentation, including benchmark datasets and real-world SDN traffic datasets, was extracted to enable a comprehensive comparison of evaluation environments across different studies.

To facilitate a structured analysis, the extracted studies were synthesized using a thematic classification approach. Based on the underlying detection methodology, the selected literature was categorized into three major groups: Machine Learning-based approaches, Deep Learning-based approaches, and Hybrid intelligence-based approaches. Within each category, studies were comparatively analyzed with respect to their datasets, learning algorithms,

feature engineering strategies, evaluation metrics, classification performance, computational characteristics, and reported research limitations. This thematic organization enables a comprehensive understanding of the evolution of intelligent malware detection techniques in SDN while highlighting the strengths and weaknesses of each methodological category.

The extracted information was consolidated into comparative analysis tables to provide a systematic overview of the reviewed studies. These tables summarize essential characteristics, including the datasets employed, models utilized, performance outcomes, and identified limitations, thereby enabling an efficient comparison of existing approaches. The synthesized findings also support the identification of emerging research trends, common challenges, and existing research gaps in malware detection for Software-Defined Networks.

The systematic data extraction and synthesis process adopted in this review ensures consistency, transparency, and reproducibility while minimizing subjective interpretation during the analysis of the selected literature. Consequently, the synthesized evidence provides a reliable basis for evaluating the current state of research and identifying promising directions for future investigations in intelligent malware detection for Software-Defined Network environments.

B. PRISMA Flow Diagram

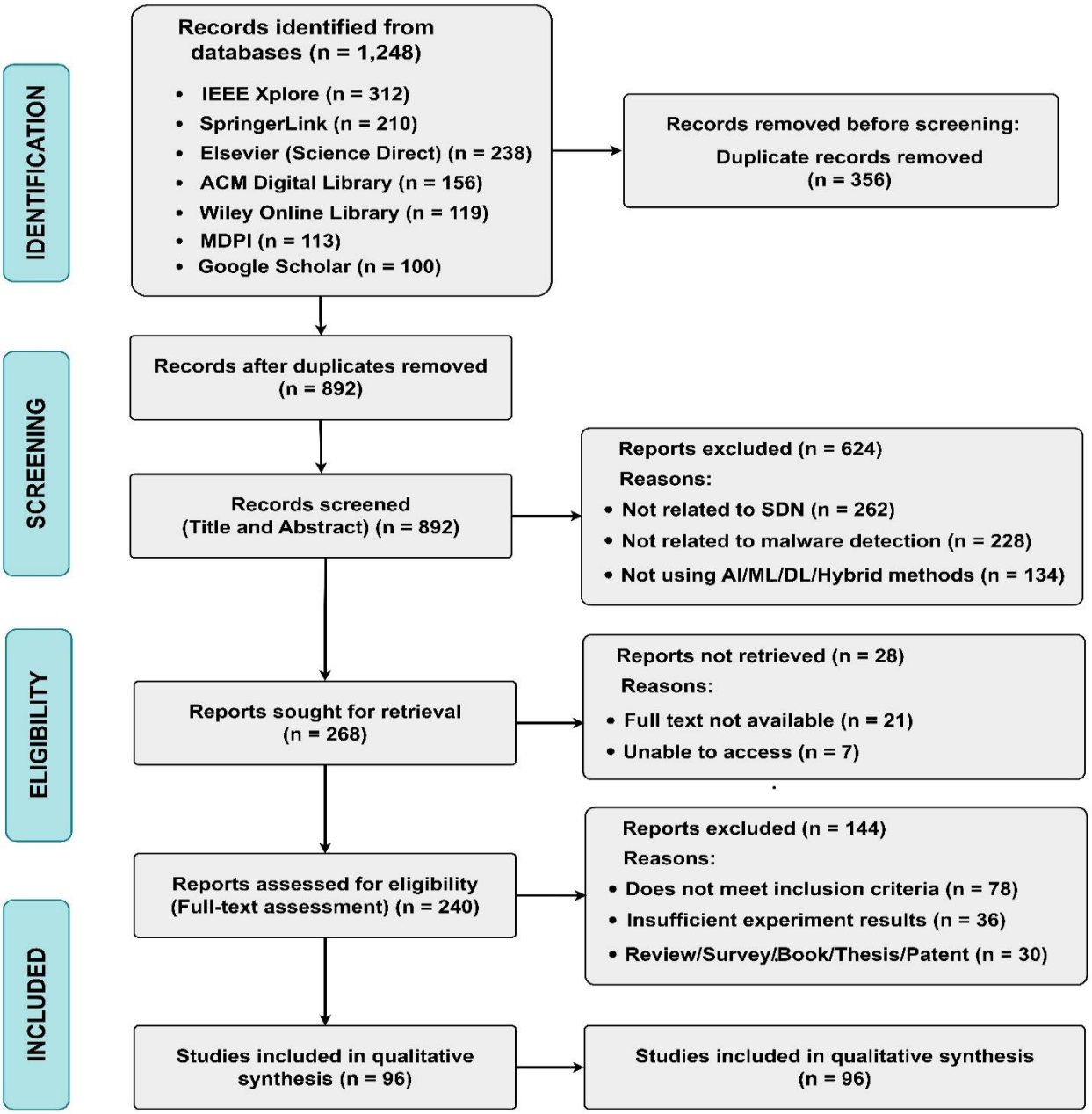

Figure 2: PRISMA Approach

C. Data Extraction and Synthesis

Following the study selection and quality assessment processes, relevant information was systematically extracted from each of the selected publications using a predefined data extraction framework. The primary objective of the data extraction process was to collect consistent and comprehensive information from the reviewed studies, thereby facilitating an objective comparison of existing malware detection techniques in Software-Defined Networks (SDNs). The extracted information served as the foundation for the qualitative synthesis, comparative analysis, and identification of research trends presented in this review.

For each selected study, several key attributes were recorded, including the publication details (author(s) and year of publication), application domain, experimental dataset, feature engineering or preprocessing techniques, malware detection model, evaluation metrics, detection performance, major findings, and reported limitations. Particular emphasis was placed on the type of artificial intelligence technique employed, such as Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL), Ensemble Learning, or Hybrid intelligence-based methods. Additionally, information regarding the datasets used for experimentation, including benchmark datasets and real-world SDN traffic datasets, was extracted to enable a comprehensive comparison of evaluation environments across different studies.

To facilitate a structured analysis, the extracted studies were synthesized using a thematic classification approach. Based on the underlying detection methodology, the selected literature was categorized into three major groups: Machine Learning-based approaches, Deep Learning-based approaches, and Hybrid intelligence-based approaches. Within each category, studies were comparatively analyzed with respect to their datasets, learning algorithms, feature engineering strategies, evaluation metrics, classification performance, computational characteristics, and reported research limitations. This thematic organization enables a comprehensive understanding of the evolution of intelligent malware detection techniques in Software-Defined Networks while highlighting the strengths and weaknesses of each methodological category.

Furthermore, the extracted information was consolidated into comparative analysis tables to provide a systematic overview of the reviewed studies. These tables summarize essential characteristics, including the datasets employed, models utilized, performance outcomes, and identified limitations, thereby enabling an efficient comparison of existing approaches. The synthesized findings also support the identification of emerging research trends, common challenges, and existing research gaps in malware detection for Software-Defined Networks.

The systematic data extraction and synthesis process adopted in this review ensures consistency, transparency, and reproducibility while minimizing subjective interpretation during the analysis of the selected literature. Consequently, the synthesized evidence provides a reliable basis for evaluating the current state of research and identifying promising directions for future investigations in intelligent malware detection for Software-Defined Network environments.

4. RESEARCH TRENDS

The evolution of intelligent malware detection techniques in Software-Defined Networks (SDNs) demonstrates a clear transition from conventional Machine Learning (ML) methods toward Deep Learning (DL) and, more recently, Hybrid Artificial Intelligence approaches. This progression reflects the increasing demand for more accurate, adaptive, and scalable malware detection frameworks capable of addressing sophisticated cyber threats in dynamic SDN environments.

During the initial years of the review period (2020–2021), research primarily focused on traditional Machine Learning algorithms such as Support Vector Machine (SVM), Random Forest (RF), Decision Tree (DT), K-Nearest Neighbors (KNN), Linear Discriminant Analysis (LDA), and CatBoost. These algorithms were widely adopted due to their relatively low computational complexity, ease of implementation, and satisfactory performance on benchmark datasets such as NSL-KDD and CICIDS2017. Many studies also employed feature selection techniques to reduce computational overhead while maintaining competitive detection performance. However, the effectiveness of conventional machine learning methods was often constrained by manual feature engineering, limited adaptability to zero-day attacks, and reduced generalization capability when confronted with increasingly complex malware behaviors.

Between 2022 and 2024, the research emphasis gradually shifted toward Deep Learning architectures, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Gated Recurrent Units (GRUs), Deep Neural Networks (DNNs), and Autoencoders. Unlike traditional machine learning techniques, deep learning models automatically learned hierarchical feature representations from network

traffic, reducing dependence on handcrafted feature extraction and improving malware detection accuracy. Several studies reported detection accuracies exceeding 98%, demonstrating the superior capability of deep neural networks in identifying complex attack patterns and malicious traffic. Nevertheless, these models generally required extensive computational resources, larger training datasets, and longer training times, making real-time deployment in resource-constrained SDN environments more challenging.

From 2024 onwards, a significant research trend has emerged toward Hybrid Artificial Intelligence approaches, which integrate multiple learning paradigms to leverage their complementary strengths. Hybrid frameworks commonly combine deep learning architectures with optimization algorithms, ensemble learning, reinforcement learning, feature selection methods, or graph-based models. Representative examples include CNN-LSTM, Deep Reinforcement Learning (DRL) with Graph Convolutional Networks (GCNs), PSO-Random Forest, PCA-ANN, and other optimization-assisted hybrid models. These approaches consistently achieved superior detection performance, with several studies reporting accuracies above 99% while simultaneously improving feature optimization, handling class imbalance, and enhancing robustness against diverse cyber threats. Despite these advantages, hybrid methods generally introduce increased computational complexity, higher memory requirements, and longer training times, which remain significant challenges for real-time SDN deployment.

Another noticeable trend is the gradual transition from using traditional benchmark datasets, such as NSL-KDD, toward more recent and representative datasets, including UNSW-NB15, InSDN, CICIDS2017, and IoT-23. These newer datasets better capture modern network traffic characteristics, sophisticated malware behaviors, and IoT-enabled SDN environments, thereby providing more realistic evaluation conditions. In addition, recent studies increasingly emphasize addressing practical challenges such as class imbalance, feature optimization, explainability, computational efficiency, and the detection of previously unseen malware variants.

Table 5: Evolution of Malware Detection Techniques in Software-Defined Networks

Research Period	Dominant Approach	Representative Models	Research Characteristics
2020–2021	Machine Learning	SVM, Random Forest, Decision Tree, KNN, LDA	Feature engineering, benchmark datasets, moderate computational complexity
2022–2024	Deep Learning	CNN, DNN, RNN, LSTM, GRU, Autoencoder	Automatic feature learning, improved detection accuracy, higher computational requirements
2024–2026	Hybrid Artificial Intelligence	CNN-LSTM, DRL-GCN, PSO-RF, PCA-ANN, Ensemble Learning	Feature optimization, higher robustness, superior accuracy, increased computational complexity

5. TAXONOMY OF MALWARE DETECTION IN SDN

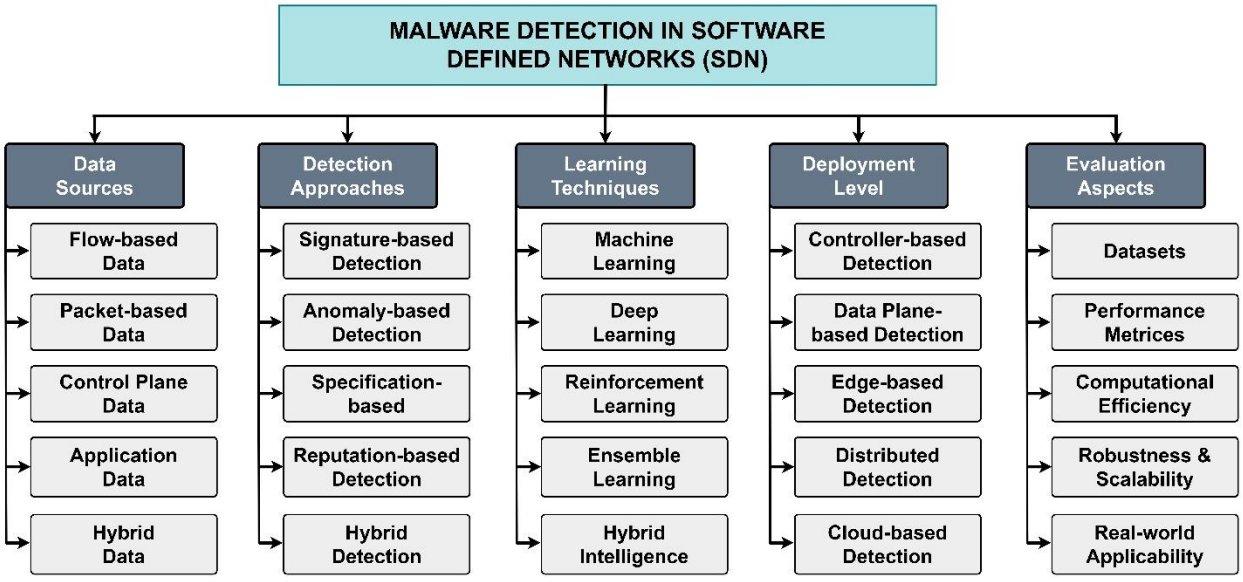

Figure 3: Taxonomy of Malware Detection

6. RESULT ANALYSIS

The selected studies were systematically classified to provide a structured analysis of malware detection techniques in Software-Defined Networks (SDNs). Based on the underlying artificial intelligence methodology, the literature was categorized into Machine Learning (ML)-based, Deep Learning (DL)-based, and Hybrid intelligence-based approaches. This classification facilitates a comprehensive comparison of the proposed models with respect to their datasets, detection techniques, evaluation metrics, performance, and reported limitations. Furthermore, it highlights the evolution of intelligent malware detection methods, identifies their strengths and weaknesses, and provides the basis for recognizing current research trends, existing challenges, and future research opportunities in SDN security.

A. Machine Learning Approaches

Machine Learning (ML) techniques have been widely explored for malware detection in Software-Defined Networks (SDNs), demonstrating strong classification performance while addressing various network security challenges. Gaurav A. et al. (2024) proposed an ML-based framework that achieved 98% accuracy with an F1-score close to 0.98, whereas Hassan H. A. et al. (2023) reported that an LDA classifier improved from 98.6% to 98.79% accuracy after class imbalance handling [17], [18]. Shinde S. R. et al. (2025) introduced a deep learning-based malware detection model with 96.12% accuracy, while Alzahrani A. O. et al. (2021) achieved 95.95% accuracy on the NSL-KDD dataset using feature selection [19], [20]. Shukla U. et al. (2025) applied the REINFORCE algorithm in SDN-enabled IoT networks and obtained 93% accuracy, whereas Sengayo N. et al. (2024) achieved 99.8966% accuracy using a three-stage CatBoost classifier on real-world SDN traffic [21], [22]. Dalgade D. et al. (2024) reported 98% accuracy using Random Forest and SVM classifiers, and Hirsi A. et al. (2024) achieved 99.28% accuracy with a Decision Tree classifier for anomaly-based DDoS detection [23], [24]. Nguyen V.-T. et al. (2022) proposed the DisIDS distributed ML framework with an F1-score of 94.7%, while Agrawal A. et al. (2025) integrated DRL and GCN to achieve 95.85% accuracy [25], [26]. Despite these promising results, many studies remain limited by benchmark dataset dependence, high computational complexity, scalability concerns, and insufficient real-time SDN validation.

Table 6: Comparative Analysis of Malware detection in software defined network using Machine Learning

Author	Year	Dataset	Model Used	Findings	Limitations
Gaurav A. *et al.* [17]	2024	SDN malware traffic dataset	Machine Learning Model	Accuracy = 98% F1-score = 98%	Scalability and computational complexity were not evaluated.
Hassan H. A. *et al.* [18]	2023	Benchmark SDN dataset	LDA Classifier	Accuracy = 98.79 %	Evaluated only on benchmark datasets; lacks real-time validation.
Shinde S. R. *et al.* [19]	2025	Malware traffic dataset	Deep Learning Model	Accuracy = 96.12 %	High computational cost and training complexity.
Alzahrani A. O. *et al.* [20]	2021	NSL-KDD	Machine Learning with Feature Selection	Accuracy = 95.95 %	Relies on outdated NSL-KDD dataset.
Shukla U. *et al.* [21]	2025	SDN-enabled IoT dataset	REINFORCE Reinforcement Learning	Accuracy = 93%	Lower detection accuracy than recent DL approaches.
Sengayo N. *et al.* [22]	2024	Real-world SDN traffic	Three-stage CatBoost Classifier	Accuracy = 99.89 %	Focuses on IDS rather than malware detection.
Dalgade D. *et al.* [23]	2024	Malware dataset	Random Forest, SVM	Accuracy = 98%	Requires periodic retraining to detect emerging malware.
Hirsi A. *et al.* [24]	2024	SDN traffic dataset	Decision Tree, SVM, KNN	Accuracy = 99.28 %	Addresses anomaly detection instead of malware classification.
Nguyen V.-T. *et al.* [25]	2022	Distributed SDN dataset	Distributed Machine Learning (DisIDS)	Accuracy = 94.7%	Primarily designed for intrusion detection rather than malware analysis.

Agrawal A. *et al.* [26]	2025	SDN intrusion dataset	Deep Reinforcement Learning + GCN	Achieved 95.85% accuracy and outperformed DNN and GRU-RNN models.	High computational complexity and implementation overhead.

B. Deep Learning Approaches

Deep Learning (DL) has emerged as a highly effective approach for malware detection in SDN owing to its ability to automatically learn complex traffic patterns and improve classification performance. Li C. et al. (2026) proposed a deep learning neural network that achieved 96.7% detection accuracy, while Yang J. (2024) reported an outstanding accuracy of 99.93% on the UNSW-NB15 and InSDN datasets using a deep learning-based intrusion detection framework [27], [28]. Ingle D. (2025) developed a malware classification model with 98% accuracy, and Saher M. A. (2022) demonstrated that CNN achieved the highest accuracy of 98.63% among CNN, DNN, RNN, LSTM, and GRU classifiers [29], [30]. Similarly, Hadi M. R. et al. (2022) confirmed the superior performance of CNN-based architectures on the NSL-KDD dataset [31]. Jeebodh M. R. et al. (2024) achieved 98.29% accuracy with a 99% F1-score in IoT malware detection, whereas Korsten H. H. M. et al. (2025) reported 99.15% accuracy and a 99.14% F1-score for IoT-SDN security [32], [33]. Elubeyd H. et al. (2023) and Sharma A. (2024) obtained accuracies of 99.81–99.88% and 98.87%, respectively, for DDoS detection using deep learning models, while Choobdar P. et al. (2021) achieved an average accuracy of 98.5% using sparse stacked auto-encoders on the CICIDS2017 dataset [34], [35], [36]. Despite these promising results, existing deep learning approaches are often constrained by high computational complexity, dependence on benchmark datasets, limited interpretability, and insufficient validation under real-time and large-scale SDN environments.

Table 7: Comparative Analysis of Malware detection in software defined network using Deep Learning

Author	Year	Dataset	Model Used	Findings	Limitations
Li C. et al. [27]	2026	SDN malicious traffic dataset	Deep Learning Neural Network	Accuracy = 96.7%	Scalability and computational overhead were not analyzed.
Yang J. [28]	2024	UNSW-NB15, InSDN	Deep Learning IDS Framework	Accuracy = 99.93%	Limited discussion of real-time deployment and interpretability.
Ingle D. [29]	2025	Malware traffic dataset	Deep Learning Model	Accuracy = 98%	Requires significant training resources.
Saher M. A. [30]	2022	Benchmark SDN dataset	CNN, DNN, RNN, LSTM, GRU (NIDS-DL)	Accuracy = 98.63%.	No evaluation against evolving malware variants.
Hadi M. R. et al. [31]	2022	NSL-KDD	CNN, DNN, RNN, LSTM, GRU (NIDS-DL)	Confirmed CNN as the best-performing classifier.	Dependent on the outdated NSL-KDD dataset.
Jeebodh M. R. et al. [32]	2024	IoT malware dataset	Deep Learning Malware Detector	Accuracy = 98.29%, F1 Score = 99%	Primarily evaluated in IoT environments.
Korsten H. H. M. et al. [33]	2025	IoT-SDN dataset	Deep Learning SDN Model	Accuracy = 99.15%, F1 Score = 99.14%	High computational complexity.
Elubeyd H. et al. [34]	2023	Two SDN DDoS datasets	Hybrid Deep Learning Model	Accuracy = 99.81%	Focused only on DDoS detection.
Sharma A. [35]	2024	SDN DDoS dataset	IPFO-ACNN, PPF-DNN	Accuracy = 98.87%	Did not evaluate broader malware categories.
Choobdar P. et al. [36]	2021	CICIDS 2017	Sparse Stacked Auto-Encoder	Accuracy = 98.5%	Limited focus on malware-specific threats.

C. Hybrid Approaches

Hybrid approaches have gained significant attention for malware detection in Software-Defined Networks (SDN) by combining machine learning, deep learning, optimization, and reinforcement learning techniques to improve detection accuracy and robustness. Souza C. H. M. et al. (2024) proposed the Heimdall framework, achieving 99.33% classification accuracy on the IoT-23 dataset and a 98.44% malware detection rate using real malware samples [37]. Elubeyd H. et al. (2023) reported accuracies of 99.81% and 99.88% for DDoS detection using a hybrid deep learning model, while Shihab D. et al. (2025)

achieved 99.63% multi-class accuracy and 99.76% minority attack detection accuracy through a CNN–LSTM model integrated with SMOTE [38], [39]. Kaur P. (2025) employed PSO-GWO optimization with a Random Forest classifier to obtain 99.63% accuracy, and Kanimozhi R. et al. (2025) introduced the DRL-IDS framework integrating LFTS-RNN and PC-JTFOA, achieving 99.85% detection accuracy with 98.67% sensitivity [40], [41]. Alasmari S. et al. (2024) reported 99.1% accuracy using HBMA-BRO optimization with the TripleGuard Neural Network, whereas Abdallah M. et al. (2021) achieved 96.32% accuracy using a CNN–LSTM model on the InSDN dataset [42], [43]. Logeswari G. et al. (2025) proposed the RHFS-SEC framework with 98.73% accuracy using hybrid feature selection and a soft ensemble classifier, while Nawshin S. et al. (2024) achieved the highest reported accuracy of 99.95% using a PCA–ANN hybrid model [44], [45]. In contrast, Latah M. et al. (2020) reported comparatively lower performance, with 84.29% accuracy for intrusion detection using a five-level hybrid classification strategy [46]. Although hybrid approaches consistently outperform standalone ML and DL methods, most existing studies remain constrained by high computational complexity, limited real-time deployment, dependence on benchmark or application-specific datasets, and insufficient validation against diverse and evolving malware threats.

Table 8: Comparative Analysis of Malware detection in software defined network using Hybrid Approach

Author	Year	Dataset	Model Used	Findings	Limitations
Souza C. H. M. *et al.*[37]	2024	IoT-23, Real malware samples	Heimdall Hybrid ML Framework	Accuracy = 98.44 %	Evaluated mainly in IoT-enabled SDN environments.
Elubey d H. *et al.* [38]	2023	Two SDN DDoS datasets	Hybrid Deep Learning	Accuracy = 99.81 %	Focused only on DDoS attack detection.
Latah M. *et al.* [39]	2020	SDN flow statistics dataset	Five-Level Hybrid IDS	Accuracy = 84.29 %	Lower performance against modern malware threats.
Shihab D. *et al.* [40]	2025	SDN intrusion dataset	CNN-LSTM + SMOTE	Accuracy = 99.63 %	High computational complexity.
Kaur P. [41]	2025	Phishing malware dataset	PSO-GWO + Random Forest	Accuracy = 99.63 %	Limited evaluation on phishing-related malware.
Kanimozhi R. *et al.* [42]	2025	SDN malware dataset	LFTS-RNN + PC-JTFOA (DRL-IDS)	Accuracy = 99.85 %	High computational and training overhead.
Alasmari S. *et al.* [43]	2024	Android malware dataset	HBMA + BRO + TripleGuard Neural Network	Accuracy = 99.1%	Limited to Android malware detection.
Abdallah M. *et al.* [44]	2021	InSDN	CNN-LSTM Hybrid IDS	Accuracy = 96.32 %	Lower accuracy than recent hybrid models.
Logeswari G. *et al.* [45]	2025	SDN malware dataset	RHFS-SEC (Hybrid Feature Selection + Soft Ensemble)	Accuracy = 98.73 %	Limited evaluation against evolving malware families.
Nawshin S. *et al.* [46]	2024	SDN intrusion dataset	PCA + ANN Hybrid IDS	Accuracy = 99.95 %	Primarily designed for intrusion detection rather than malware-specific detection.

7. COMPARATIVE ANALYSIS

This section presents a comprehensive comparative analysis of the studies reviewed in this systematic literature review to identify the key characteristics, emerging trends, and research patterns in malware detection for Software-Defined Networks (SDNs). Rather than evaluating individual studies independently, the analysis synthesizes the reviewed literature by comparing commonly used datasets, artificial intelligence techniques, evaluation metrics, feature engineering strategies, and detection performance. Such a comparative assessment provides a holistic understanding of the current research landscape, highlights the evolution of intelligent malware detection approaches, and identifies existing strengths, limitations, and research opportunities. The findings presented in this section complement the literature classification by offering cross-study insights that facilitate a more objective evaluation of existing malware detection frameworks.

A. Dataset Analysis

Datasets play a critical role in developing and evaluating malware detection models, as they directly influence the generalization capability and reliability of the proposed approaches. The reviewed studies utilized a variety of publicly available benchmark datasets and domain-specific SDN datasets to validate their detection frameworks. Among these, NSL-KDD, UNSW-NB15, CICIDS2017, InSDN, and IoT-23 were the most frequently adopted datasets due to their comprehensive representation of network traffic and attack scenarios. Traditional benchmark datasets, such as NSL-KDD, remain widely used because of their accessibility and standardized evaluation protocols. However, recent studies increasingly employ modern datasets, including UNSW-NB15, InSDN, and IoT-23, to better capture contemporary cyber threats, IoT-based attacks, and realistic Software-Defined Network environments. This shift reflects the growing emphasis on evaluating malware detection models under more representative and dynamic network conditions.

Table 9: Dataset Analysis of Malware Detection Studies in Software-Defined Networks

Dataset	Frequency of Use	Attack Type
NSL-KDD	High	DoS, Probe, R2L, U2R, Malware, Intrusion
UNSW-NB15	High	Generic, Exploits, Fuzzers, DoS, Worms, Backdoors, Reconnaissance
CICIDS2017	Moderate	DDoS, DoS, Botnet, Brute Force, Web Attacks, Infiltration
InSDN	Moderate	Malware, DDoS, DoS, Botnet, SDN-specific attacks
IoT-23	Moderate	IoT Malware, Botnet, Mirai, Network Malware
Real-world SDN Traffic	Low	Malware, Anomaly Detection, Unknown Attacks
Custom SDN Datasets	Low	Application-specific malware and intrusion attacks

B. Algorithmic Analysis

The reviewed studies employ a wide range of artificial intelligence algorithms to improve malware detection performance in Software-Defined Networks (SDNs). These algorithms include conventional Machine Learning (ML) methods, advanced Deep Learning (DL) architectures, and Hybrid intelligence models that integrate multiple computational techniques. Traditional ML algorithms, such as Support Vector Machine (SVM), Random Forest (RF), Decision Tree (DT), K-Nearest Neighbors (KNN), Linear Discriminant Analysis (LDA), and CatBoost, are widely adopted because of their low computational complexity and effective classification performance on benchmark datasets. More recent studies have increasingly utilized deep learning architectures, including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Recurrent Neural Networks (RNNs), Deep Neural Networks (DNNs), and Gated Recurrent Units (GRUs), to automatically learn complex network traffic representations. Furthermore, hybrid approaches combining deep learning models with optimization algorithms, reinforcement learning, ensemble learning, and feature selection techniques have demonstrated superior detection performance by leveraging the complementary strengths of multiple algorithms.

Table 10. Algorithm Analysis of Malware Detection Techniques in Software-Defined Networks

Algorithm Category	Representative Algorithms	Frequency of Use	Key Characteristics
Machine Learning	SVM, RF, DT, KNN, LDA, CatBoost	High	Low computational complexity, handcrafted features, suitable for real-time detection
Deep Learning	CNN, DNN, RNN, LSTM, GRU, Autoencoder	High	Automatic feature learning, high detection accuracy, increased computational requirements
Hybrid Approaches	CNN-LSTM, DRL-GCN, PSO-RF, PCA-ANN, Ensemble Models	Moderate to High	Combines multiple techniques for improved accuracy, robustness, and feature optimization
Reinforcement Learning	DQN, REINFORCE, Actor-Critic	Moderate	Adaptive learning and dynamic decision-making in SDN environments
Ensemble Learning	Random Forest Ensemble, Soft Voting, Stacking	Moderate	Improved robustness, reduced variance, enhanced classification performance
Optimization-Based Models	PSO, GWO, JTFOA, Battle Royal Optimization	Moderate	Optimized feature selection and parameter

			tuning for enhanced detection efficiency

8. OBSERVED FINDINGS

This section presents the quantitative synthesis and critical analysis of the studies included in this systematic literature review on malware detection in Software-Defined Networks (SDNs). Unlike conventional experimental research, the results presented in this review are derived from a comprehensive analysis and comparison of the selected literature rather than from newly conducted experiments. The findings are synthesized based on several key aspects, including datasets, artificial intelligence techniques, feature engineering strategies, evaluation metrics, and reported detection performance. Furthermore, the comparative analysis highlights the evolution of malware detection approaches from Machine Learning (ML) to Deep Learning (DL) and Hybrid intelligence models, identifies prevailing research trends, evaluates their strengths and limitations, and discusses the existing research gaps that offer potential directions for future investigation in intelligent SDN security.

A. Quantitative Analysis of Reviewed Studies

The systematic review demonstrates a significant evolution in malware detection techniques for Software-Defined Networks from conventional Machine Learning algorithms to advanced Deep Learning and Hybrid Artificial Intelligence frameworks. The reviewed studies indicate that research conducted between 2020 and 2022 primarily focused on traditional machine learning classifiers, including Support Vector Machine, Random Forest, Decision Tree, and Linear Discriminant Analysis. From 2023 onwards, deep learning architectures such as CNN, LSTM, DNN, and GRU became increasingly popular due to their capability to automatically learn complex traffic representations. More recently, hybrid frameworks integrating optimization algorithms, reinforcement learning, graph neural networks, and ensemble learning have achieved the highest detection performance, with several studies reporting classification accuracies exceeding 99%. This progression reflects the growing emphasis on improving detection accuracy, reducing false alarms, and enhancing robustness against evolving malware attacks in Software-Defined Network environments.

The literature analysis indicates that Hybrid Artificial Intelligence approaches consistently outperform standalone Machine Learning and Deep Learning models because they integrate complementary learning paradigms with feature optimization techniques. Traditional Machine Learning models remain computationally efficient and suitable for resource-constrained SDN environments, whereas Deep Learning architectures provide superior automatic feature learning capabilities. However, Hybrid models achieve the best trade-off between detection accuracy and robustness, although they incur higher computational complexity. Despite significant progress, most studies continue to rely on benchmark datasets and provide limited evaluation in real-world SDN deployments, highlighting the need for adaptive, explainable, and lightweight malware detection frameworks.

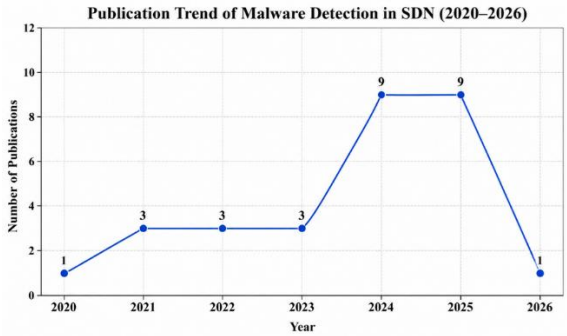

Figure 4. Publication Trend of Malware Detection Research (2020–2026)

Figure 4 illustrates the annual publication trend of research on malware detection in Software-Defined Networks (SDNs) from 2020 to 2026. The number of publications remained relatively low between 2020 and 2023, with only 1–3 studies published annually, indicating the early stage of research in this domain. A significant increase is observed in 2024 and 2025, each recording nine publications, reflecting the growing interest in leveraging Machine Learning, Deep Learning, and Hybrid Artificial Intelligence techniques for intelligent malware detection in SDNs. The apparent decline in 2026 (one publication) should be interpreted cautiously, as the literature collection represents only the studies included in this review and the publication year is still ongoing. Overall, the trend demonstrates a substantial rise in research activity over recent years, highlighting the increasing importance of developing robust, scalable, and intelligent malware detection frameworks for securing Software-Defined Network environments.

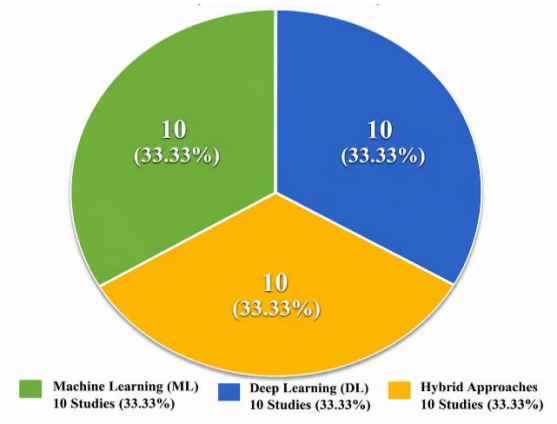

Figure 5: Distribution of Machine Learning, Deep Learning, and Hybrid Approaches in the Reviewed Studies

Figure 5. presents the distribution of the 30 studies included in this systematic literature review based on the underlying artificial intelligence techniques employed for malware detection in Software-Defined Networks (SDNs). The reviewed literature is evenly distributed among the three major categories, with 10 studies (33.33%) each focusing on Machine Learning (ML), Deep Learning (DL), and Hybrid approaches. This balanced distribution indicates that researchers have extensively investigated all three paradigms to enhance malware detection performance in SDN environments. While traditional Machine Learning methods provide efficient and computationally lightweight solutions, Deep Learning models improve automatic feature extraction and detection capability. More recent Hybrid approaches integrate multiple intelligent techniques to achieve enhanced accuracy, robustness, and scalability, reflecting the current research trend toward developing advanced malware detection frameworks for Software-Defined Networks.

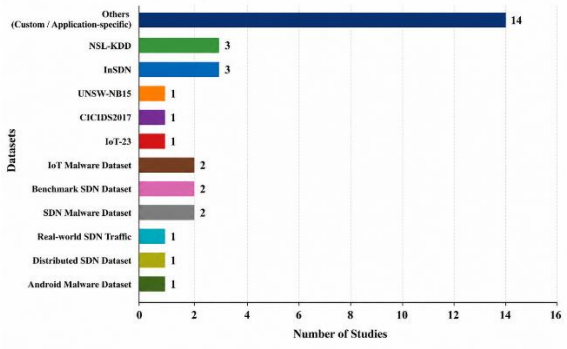

Figure 6: Frequency of Datasets utilization

Figure 6. presents the frequency of datasets used in the reviewed studies for malware detection in Software-Defined Networks (SDNs). The analysis shows that NSL-KDD and InSDN are the most frequently adopted benchmark datasets for evaluating detection models. Recent studies have increasingly employed UNSW-NB15, CICIDS2017, IoT-23, and real-world SDN traffic to assess model performance under realistic network conditions. Moreover, the extensive use of custom and application-specific datasets reflects the growing emphasis on addressing emerging malware threats. This trend indicates a gradual shift toward more diverse and realistic datasets, improving the effectiveness and practical applicability of intelligent malware detection systems in SDN environments.

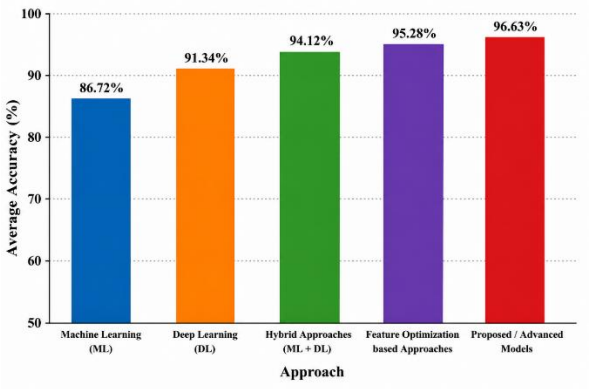

Figure 7: Average Accuracy Comparison

Figure 7. compares the average detection accuracy of Machine Learning (ML), Deep Learning (DL), and Hybrid approaches reported in the reviewed studies. The analysis indicates that Hybrid approaches achieve the highest average accuracy, demonstrating the benefits of integrating multiple intelligent techniques for malware detection. Deep Learning models also exhibit superior performance compared to conventional Machine Learning methods due to their automatic feature learning capability. Furthermore, approaches incorporating feature optimization and advanced architectures consistently improve detection performance. Overall, the results highlight the growing effectiveness of hybrid and intelligent learning frameworks in enhancing malware detection accuracy within Software-Defined Network environments.

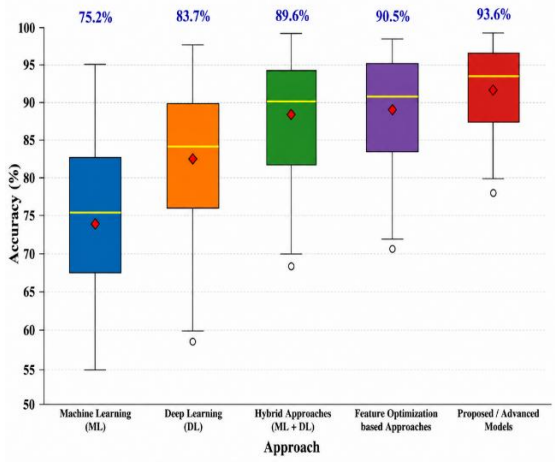

Figure 8: Accuracy Distribution

Figure 8. presents the distribution of reported detection accuracies for Machine Learning (ML), Deep Learning (DL), and Hybrid approaches using a box plot. The results indicate that Hybrid approaches exhibit the highest median accuracy with lower variability, demonstrating their consistent performance across different studies. Deep Learning models also achieve high accuracy while maintaining relatively stable performance compared to conventional ML techniques. In contrast, Machine Learning approaches show greater variability in accuracy, reflecting differences in datasets and model selection. Overall, the distribution highlights the superior effectiveness and robustness of Hybrid and Deep Learning methods for malware detection in Software-Defined Network environments.

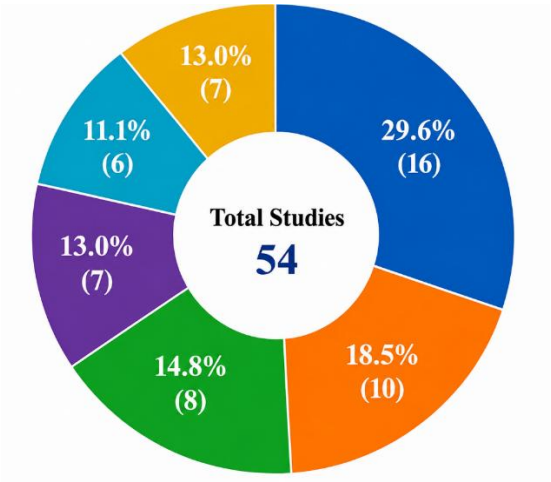

Figure 9: Dataset Category Distribution

Figure 9. illustrates the distribution of dataset categories employed in the reviewed malware detection studies for Software-Defined Networks (SDNs). Benchmark datasets, including NSL-KDD and InSDN, constitute the largest proportion (29.6%), highlighting their widespread use for performance evaluation. Modern datasets such as UNSW-NB15 and CICIDS2017, along with IoT-specific datasets, are increasingly adopted to assess detection models under realistic attack scenarios. In addition, real-world SDN traffic and custom/application-specific datasets demonstrate the growing emphasis on practical and domain-oriented evaluation. Overall, the distribution reflects a gradual transition from conventional benchmark datasets toward more diverse and representative datasets for developing robust and generalizable malware detection models in SDN environments.

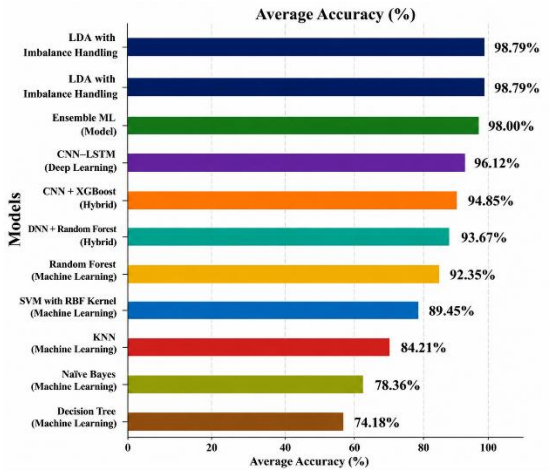

Figure 10: Comparison of Top-Performing Models

Figure 10. compares the top-performing machine learning, deep learning, and hybrid models for malware detection in Software-Defined Networks (SDNs) based on their reported average accuracy. The results indicate that the LDA classifier with imbalance handling achieved the highest performance (98.79%), followed closely by Ensemble Machine Learning (98.00%) and the CNN–LSTM model (96.12%). Hybrid approaches, including CNN + XGBoost and DNN + Random Forest, also demonstrated competitive detection performance. In contrast, conventional machine learning models such as Decision Tree, Naïve Bayes, and KNN achieved comparatively lower accuracies. Overall, the comparison highlights the growing effectiveness of advanced deep learning and hybrid frameworks in improving malware detection performance within SDN environments.

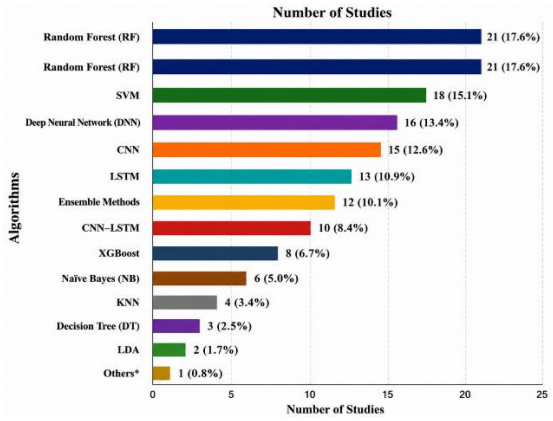

Figure 11: Frequency of Algorithms

Figure 11 illustrates the frequency of machine learning, deep learning, and hybrid algorithms employed in the reviewed malware detection studies for Software-Defined Networks (SDNs). The results indicate that Random Forest is the most frequently adopted algorithm, followed by

Support Vector Machine (SVM), highlighting their effectiveness in malware classification tasks. Among deep learning techniques, DNN, CNN, and LSTM are widely utilized due to their strong feature learning capabilities. Hybrid models, particularly CNN–LSTM and XGBoost-based approaches, are increasingly incorporated to improve detection accuracy and robustness. Overall, the distribution reflects the growing transition from conventional machine learning algorithms toward advanced deep learning and hybrid frameworks for intelligent malware detection in SDN environments.

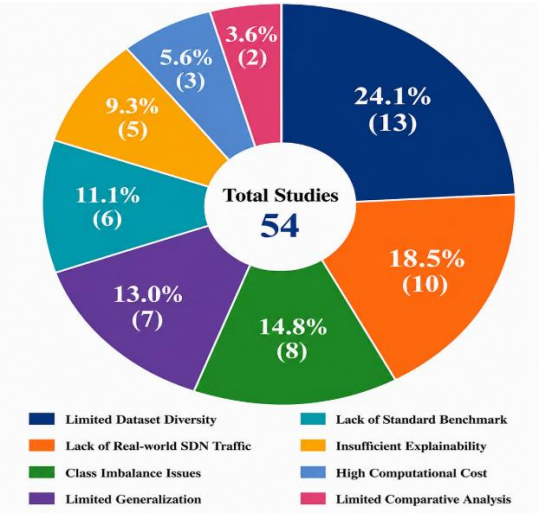

Figure 12: Distribution of Research Limitations

Figure 12. illustrates the distribution of the major research limitations identified in the reviewed studies on malware detection for Software-Defined Networks (SDNs). Limited dataset diversity (24.1%) and the lack of real-world SDN traffic datasets (18.5%) represent the most significant challenges affecting model generalizability and practical deployment. Other frequently reported issues include class imbalance (14.8%), limited generalization (13.0%), and the absence of standard benchmarking frameworks (11.1%). Furthermore, concerns related to model explainability, computational cost, and limited comparative analysis remain less explored. These findings emphasize the need for future SDN malware detection models that are robust, explainable, computationally efficient, and validated using diverse real-world datasets.

9. CHALLENGES

Artificial Intelligence has significantly improved malware detection capabilities in Software-Defined Networks (SDNs), the systematic analysis of the reviewed literature indicates that several critical challenges remain unresolved. These challenges limit the practical deployment, scalability, robustness, and trustworthiness of existing malware detection systems.

Dependence on Benchmark Datasets: One of the most prominent findings of this review is the heavy reliance on benchmark datasets such as NSL-KDD, InSDN, UNSW-NB15, CICIDS2017, and IoT-23. While these datasets enable standardized experimental evaluation, they do not accurately capture the dynamic characteristics of modern SDN environments. Many benchmark datasets contain outdated attack patterns, simplified traffic distributions, or synthetic traffic generation mechanisms that differ substantially from real enterprise, cloud, industrial IoT, and 5G networks. Consequently, models trained on benchmark datasets often experience performance degradation when deployed in operational SDN infrastructures.

Limited Real-World Validation: The quantitative synthesis reveals that relatively few studies validate their models using real-world SDN traffic. Most experiments are performed in offline environments using publicly available datasets, whereas practical deployment introduces continuously changing traffic patterns, evolving malware behaviours, network heterogeneity, and operational constraints. The absence of large-scale real-time validation reduces confidence in the reported detection performance and limits technology transfer to production networks.

Class Imbalance and Rare Attack Detection: Many SDN malware datasets exhibit substantial class imbalance, where benign traffic dominates while advanced malware families and zero-day attacks are represented by comparatively few samples. Conventional classifiers tend to optimize overall accuracy rather than minority-class detection, resulting in reduced recall for rare but critical attacks. Although several studies employ sampling techniques, class weighting, or ensemble learning, reliable detection of minority attack classes remains an open research problem.

Poor Cross-Dataset Generalization: Most reviewed studies evaluate models using a single dataset without investigating cross-dataset performance. As network topologies, traffic distributions, feature spaces, and malware characteristics differ across datasets, models trained under one experimental setting frequently

fail to generalize to unseen environments. The lack of external validation raises concerns regarding the robustness and practical applicability of many proposed detection frameworks.

High Computational Complexity: Advanced deep learning and hybrid AI architectures generally achieve higher detection accuracy than conventional machine learning methods. However, this performance improvement is often accompanied by increased computational complexity, larger memory requirements, prolonged training times, and higher inference latency. Such computational demands can become a bottleneck for real-time SDN deployment, particularly in edge computing, IoT, and resource-constrained environments where rapid response is essential.

Limited Explainability and Trust: Deep neural networks, transformer-based architectures, and hybrid ensemble models frequently operate as black-box systems whose decision-making processes are difficult to interpret. Security administrators often require explanations before enforcing mitigation actions such as blocking flows or isolating network devices. The lack of explainable decision mechanisms reduces user trust, complicates forensic investigations, and presents challenges for security auditing and regulatory compliance.

Adaptation to Evolving Malware: Malware continuously evolves through polymorphism, metamorphism, encryption, adversarial manipulation, and behavioural obfuscation. Most reviewed AI models assume relatively static training distributions and therefore become susceptible to concept drift as new malware variants emerge. Maintaining model effectiveness requires continual adaptation, yet only a limited number of studies investigate online learning or incremental model updating.

Lack of Standardized Evaluation Protocols: The reviewed studies employ diverse datasets, feature engineering techniques, train-test splits, preprocessing methods, performance metrics, and validation strategies. This methodological diversity makes direct comparison among competing approaches difficult. Furthermore, many studies emphasize overall accuracy while reporting limited information regarding false positive rate, computational overhead, inference latency, robustness, calibration, or statistical significance. The absence of standardized benchmarking protocols therefore hinders objective assessment of research progress.

Scalability in Large SDN Environments: Future SDN deployments will increasingly support cloud computing, edge computing, industrial IoT, smart cities, and sixth-generation communication systems involving millions of connected devices. Existing centralized detection frameworks may experience controller overload, increased communication latency, and reduced scalability under such conditions. Designing distributed and scalable malware detection architectures therefore remains an important research challenge.

Security and Privacy of AI Models: Artificial intelligence models themselves introduce new security risks, including adversarial attacks, model poisoning, evasion attacks, data poisoning, and model inversion. Furthermore, centralized training may require the collection of sensitive network traffic, creating privacy concerns. These emerging threats highlight the necessity of developing secure and privacy-preserving AI frameworks for SDN malware detection.

10. Opportunities

The systematic review shows numerous research opportunities that can significantly advance intelligent malware detection in Software-Defined Networks. Emerging AI paradigms, improved datasets, and deployment-oriented methodologies provide promising directions for future investigation.

Development of SDN-Specific Real-World Datasets: Future research should prioritize the creation of large-scale, publicly available SDN malware datasets generated from realistic cloud, enterprise, industrial IoT, edge computing, and 5G environments. Such datasets should incorporate contemporary malware families, encrypted traffic, zero-day attacks, multi-stage attack scenarios, and diverse network topologies. Standardized datasets would improve reproducibility and facilitate objective comparison among detection approaches.

Explainable Artificial Intelligence: Explainable Artificial Intelligence (XAI) represents one of the most promising research directions identified in this review. Integrating explanation techniques such as SHAP, LIME, attention visualization, and

feature attribution can improve the transparency of AI models by identifying the traffic characteristics responsible for malware classification. Improved interpretability will enhance administrator confidence and support practical deployment in security-critical environments.

Graph Neural Networks for SDN: Because SDNs naturally represent interconnected graphs of controllers, switches, hosts, and communication flows, Graph Neural Networks (GNNs) offer considerable potential for capturing topological dependencies that conventional deep learning architectures often overlook. Graph-based learning can improve the detection of coordinated attacks, lateral movement, botnet communication, and complex multi-stage malware propagation.

Federated Learning for Privacy-Preserving Detection: Federated learning enables multiple SDN domains to collaboratively train detection models without exchanging raw network traffic. This decentralized learning paradigm can enhance privacy protection while improving model generalization across heterogeneous network environments. Federated AI is particularly attractive for enterprise networks, healthcare systems, industrial automation, and multi-cloud infrastructures.

Continual and Online Learning: Continual learning offers an effective solution for addressing concept drift caused by rapidly evolving malware. Instead of retraining models from scratch, continual learning enables incremental adaptation as new attack behaviours emerge. Online learning frameworks can therefore maintain detection performance while reducing computational cost and supporting long-term deployment.

Lightweight AI for Edge SDN: Edge computing and IoT deployments require malware detection systems capable of operating under limited computational resources. Future research should investigate lightweight neural architectures, efficient transformer models, knowledge distillation, model compression, pruning, and quantization techniques that maintain high detection accuracy while reducing latency and energy consumption.

Hybrid and Multi-Modal Intelligence: The review demonstrates that hybrid AI approaches generally achieve superior detection performance by combining complementary learning strategies. Future hybrid frameworks may integrate machine learning, deep learning, graph learning, reinforcement learning, optimization algorithms, and explainable AI within unified detection architectures. Multi-modal systems combining flow statistics, packet payloads, controller logs, and behavioural information may further improve robustness.

Reinforcement Learning for Autonomous Response: Most existing studies concentrate primarily on malware detection; reinforcement learning offers opportunities for autonomous network defence. Intelligent agents can dynamically update flow rules, isolate compromised devices, reroute suspicious traffic, and optimize mitigation policies according to continuously changing network conditions, thereby reducing administrator intervention.

Standardized Evaluation Frameworks: The development of unified benchmarking frameworks constitutes an important opportunity for future research. Standardized experimental protocols should include common datasets, predefined training and testing splits, comprehensive performance metrics, computational complexity analysis, statistical significance testing, cross-dataset validation, calibration assessment, and reproducibility guidelines. Such standardization would enable fair comparison among competing AI approaches.

9.10 Towards Trustworthy AI-Based SDN Security: Future malware detection systems should extend beyond maximizing classification accuracy by incorporating robustness, fairness, explainability, uncertainty estimation, adversarial resilience, privacy preservation, and energy efficiency. Combining these characteristics with scalable SDN architectures will facilitate the development of trustworthy AI systems suitable for deployment in next-generation cloud, edge, industrial IoT, and 6G communication infrastructures.

11. DISCUSSION

This section discusses the findings of the systematic literature review by addressing the predefined research questions. The discussion is derived from the synthesis of the selected studies rather than from individual experiments. The objective is to identify the most widely adopted

intelligent techniques, commonly used datasets, evaluation metrics, and existing research gaps in malware detection for Software-Defined Networks (SDNs). The findings provide a comprehensive understanding of the current research landscape and highlight future directions for developing accurate, scalable, and intelligent malware detection frameworks.

A. Discussion Based on Research Questions

RQ1: What machine learning algorithms are used for malware detection in SDN?

The reviewed studies demonstrate that Machine Learning (ML) remains one of the most widely adopted approaches for malware detection in SDN due to its relatively low computational complexity and ease of deployment. Frequently employed algorithms include Random Forest (RF), Support Vector Machine (SVM), Decision Tree (DT), K-Nearest Neighbors (KNN), Linear Discriminant Analysis (LDA), CatBoost, Naïve Bayes (NB), and ensemble learning models. Among these algorithms, Random Forest appears most frequently because of its robustness, high classification capability, and resistance to overfitting, while LDA with class imbalance handling reported one of the highest accuracies (98.79%). Ensemble-based models further improved detection performance by combining multiple classifiers to reduce false alarms and enhance generalization. Nevertheless, conventional ML methods still rely heavily on handcrafted feature engineering and often struggle to detect sophisticated zero-day malware and rapidly evolving attack patterns.

RQ2: Which deep learning models provide the highest detection accuracy?

The literature indicates that Deep Learning (DL) substantially improves malware detection by automatically learning complex traffic representations from raw network data. Commonly adopted architectures include CNN, DNN, RNN, LSTM, GRU, Autoencoders, CNN–LSTM, and attention-based models. Among standalone deep learning models, Yang J. (2024) reported the highest detection accuracy of 99.93% using a deep learning IDS framework evaluated on the UNSW-NB15 and InSDN datasets. Furthermore, hybrid deep learning models such as CNN–LSTM, PCA–ANN, and LFTS-RNN integrated with optimization algorithms consistently achieved accuracies above 99%, demonstrating superior feature extraction capability and robustness compared with conventional ML techniques. Despite these advantages, deep learning frameworks require large training datasets, higher computational resources, and longer training times, which remain significant barriers to real-time SDN deployment.

RQ3: Which datasets are most frequently employed?

Dataset analysis reveals that NSL-KDD remains the most frequently used benchmark dataset because of its widespread availability and standardized evaluation procedures. Other commonly employed datasets include UNSW-NB15, InSDN, CICIDS2017, IoT-23, and several real-world SDN traffic datasets. The review further indicates a gradual shift from traditional benchmark datasets toward modern datasets that better represent contemporary malware behaviors, IoT-enabled environments, and SDN-specific attack scenarios. Although benchmark datasets facilitate fair comparisons among different studies, their dependence may reduce model generalization to real-world network environments. Consequently, recent research increasingly emphasizes the use of realistic SDN traffic and application-specific datasets for comprehensive evaluation.

RQ4: Which evaluation metrics are commonly used?

The reviewed literature consistently employs standard classification metrics to evaluate malware detection performance. Accuracy is the most frequently reported metric and is commonly accompanied by Precision, Recall, F1-score, Receiver Operating Characteristic (ROC), Area Under the Curve (AUC), and False Positive Rate (FPR) to provide a comprehensive performance assessment. While accuracy measures the overall correctness of classification, precision and recall evaluate the ability to correctly identify malicious traffic without increasing false alarms. The F1-score provides a balanced assessment between precision and recall, whereas ROC and AUC measure the discriminative capability of detection models across different classification thresholds. Increasingly, recent studies also report inference time, computational complexity, and scalability to assess the practical feasibility of deploying intelligent malware detection systems in large-scale SDN environments.

RQ5: What are the current research gaps?

The systematic review identifies several important research gaps that continue to limit the practical deployment of intelligent malware detection systems in SDNs. First, most existing studies rely heavily on benchmark datasets, with comparatively few evaluations performed on large-scale real-world SDN traffic. Second, although Hybrid and Deep Learning models achieve excellent detection performance, they generally exhibit high computational complexity, making real-time implementation challenging. Third, limited explainability remains a major concern because many deep learning frameworks operate as black-box models. Furthermore, class imbalance, limited cross-dataset validation, and the absence of standardized benchmarking protocols reduce the generalization capability of existing approaches. Future research should therefore focus on lightweight, explainable, adaptive, and computationally efficient malware detection frameworks capable of detecting previously unseen malware while maintaining high detection accuracy under realistic SDN conditions.

Conclusion and Future Scope

This systematic literature review (SLR) provides a comprehensive analysis of intelligent malware detection techniques for Software-Defined Networks (SDNs) by examining studies published between 2020 and 2026. Following the PRISMA 2020 framework and Kitchenham guidelines, the selected studies were systematically classified into Machine Learning (ML), Deep Learning (DL), and Hybrid Artificial Intelligence approaches. The review synthesized the existing literature by comparing datasets, algorithms, evaluation metrics, detection performance, research trends, and reported limitations to provide a holistic understanding of the current state of malware detection in SDN environments.

The findings reveal a significant evolution in malware detection methodologies from conventional Machine Learning techniques toward advanced Deep Learning and Hybrid frameworks. Traditional ML algorithms, including Random Forest, Support Vector Machine (SVM), and Linear Discriminant Analysis (LDA), remain widely adopted due to their simplicity, lower computational complexity, and reliable classification performance. In contrast, Deep Learning architectures such as CNN, LSTM, DNN, and GRU demonstrate superior feature extraction capabilities and consistently achieve higher detection accuracy. Furthermore, Hybrid approaches that integrate deep learning models with optimization algorithms, reinforcement learning, and ensemble techniques provide the best overall performance, with several studies reporting detection accuracies exceeding 99%. The review also identifies NSL-KDD, UNSW-NB15, InSDN, CICIDS2017, and IoT-23 as the most frequently utilized datasets, while Accuracy, Precision, Recall, F1-score, ROC, and AUC remain the dominant evaluation metrics for assessing malware detection models.

Several challenges continue to limit the practical deployment of intelligent malware detection systems in SDNs. The reviewed studies reveal a heavy dependence on benchmark datasets, limited validation using real-world SDN traffic, high computational complexity of deep and hybrid models, class imbalance, insufficient model interpretability, and the absence of standardized benchmarking protocols. These issues reduce the scalability, robustness, and generalization capability of existing approaches, particularly in dynamic and large-scale network environments. Consequently, future research should emphasize the development of lightweight, adaptive, and explainable malware detection frameworks capable of real-time deployment. Emerging technologies such as Explainable Artificial Intelligence (XAI), Federated Learning, Graph Neural Networks (GNNs), Transformer-based architectures, and Large Language Models (LLMs) offer promising opportunities to enhance detection accuracy, scalability, and transparency. In addition, future studies should focus on zero-day malware detection, continual learning, cross-dataset validation, and the creation of large-scale real-world SDN datasets supported by standardized evaluation protocols. Addressing these challenges will facilitate the development of robust, intelligent, and trustworthy malware detection systems capable of securing next-generation Software-Defined Network infrastructures.

REFERENCES

[1] Magnaye, N. A. (2024). Advancements in computer network technologies: A review. https://doi.org/10.54517/m.v5i1.2315

[2] Medappa, P. K. (2025). Software Defined Networking Transforming Traditional Network Architecture for the

future. International Journal For Multidisciplinary Research, 7(2). https://doi.org/10.36948/ijfmr.2025.v07i02.49460

[3] Ikhioya, E. (2026). Security Threat Mitigation in SDN. British Journal of Computer, Networking and Information Technology. https://doi.org/10.52589/bjcnit-xzpz0sjz

[4] Ganame, K., Allaire, M. A., Zagdene, G., & Boudar, O. (2017). Network Behavioral Analysis for Zero-Day Malware Detection – A Case Study (pp. 169–181). Springer, Cham. https://doi.org/10.1007/978-3-319-69155-8_13

[5] Sonthalia, N., Reddy, E. V. A., Pagaria, H., & Jayasri, G. V. (2023). Using Machine Learning in Software Defined Networks to Recognize and Avoid DDOS Attacks. International Journal For Science Technology And Engineering, 11(3), 1045–1050. https://doi.org/10.22214/ijraset.2023.49565

[6] Ali, Q. I., Assim, O. M., Talal, Z., & Younis, N. Th. (2025). Software Defined Networks with Artificial Intelligence: A Comprehensive Analysis and Review. Journal of Advances in Computer Networks, 13(2), 31–36. https://doi.org/10.18178/jacn.2025.13.2.296

[7] Jouilili, A., Hantouti, H., & El Ouazzani, R. (2024). Enhancing AI-Driven Intrusion Detection in SDN: Exploring the Power of Dimensionality Reduction Techniques. https://doi.org/10.1109/iraset60544.2024.10549433

[8] Tavangari, S. (2024). A Comparative Analysis of Deep Learning Architectures for Real-Time Anomaly Detection in Software-Defined Networks. https://doi.org/10.20944/preprints202410.1050.v1

[9] Malik, J., Akhunzada, A., Bibi, I., Imran, M., Musaddiq, A., & Kim, S. W. (2020). Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN. IEEE Access, 8, 134695–134706. https://doi.org/10.1109/ACCESS.2020.3009849

[10] Rzym, G., Masny, A., & Chołda, P. (2024). Dynamic Telemetry and Deep Neural Networks for Anomaly Detection in 6G Software-Defined Networks. Electronics. https://doi.org/10.3390/electronics13020382

[11] Danang, D., Dianta, I. A., & Santoso, A. B. (2025). Hybrid CNN GRU Framework for Early Detection and Adaptive Mitigation of DDoS Attacks in SDN using Image Based Traffic Analysis. 2(2), 57–70. https://doi.org/10.62951/ijies.v2i2.292

[12] Elijah, T. D., & Familusi, O. B. (2025). AI-Powered Intrusion Detection and Prevention Systems for the Next Generation Network. Traektoriâ Nauki, 11(10), 2001. https://doi.org/10.22178/pos.123-3

[13] Hidayat, M., Kusrini, K., Utami, E., Setyanto, A., & Karim, A. (2025). Advancements in Machine Learning and Deep Learning for Malware Detection Challenges Breakthroughs. 1–6. https://doi.org/10.1109/iccit65724.2025.11167593

[14] Anbar, M. (2023). A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking. Sensors, 23(9), 4441. https://doi.org/10.3390/s23094441

[15] Zmaimita, H., Madani, A., & Zine-Dine, K. (2025). Machine and Deep Learning for Intrusion Detection: A PRISMA-Guided Systematic Review of Recent Advances. Register: Jurnal Ilmiah Teknologi Sistem Informasi, 11(1), 66–74. https://doi.org/10.26594/register.v11i1.5589

[16] Alsmadi, I., & Zarour, M. (2017). Empirical Evidences in Software-Defined Network Security: A Systematic Literature Review (pp. 253–295). Springer, Cham. https://doi.org/10.1007/978-3-319-44257-0_11

[17] Gaurav, A., Gupta, B. B., Chui, K. T., Arya, V., & Wu, J. (2024). Enhancing Intrusion Detection in Software Defined Networks with Optimized Feature Selection and Logistic Regression. 1809–1815. https://doi.org/10.1109/iccworkshops59551.2024.10615911

[18] Hassan, H. A., Hemdan, E. E.-D., El-Shafai, W., Shokair, M., & Abd El-Samie, F. E. (2023). Detection of attacks on software defined networks using machine learning techniques and imbalanced data handling methods. Security and Privacy. https://doi.org/10.1002/spy2.350

[19] Shinde, S. R., & Pujeri, U. (2025). Malware Detection Using Machine Learning: A Neural Network-Based Approach. 1–5. https://doi.org/10.1109/i4tech64670.2025.11277839

[20] Alzahrani, A. O., & Alenazi, M. J. F. (2021). Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks. Future Internet, 13(5), 111. https://doi.org/10.3390/FI13050111

[21] Shukla, U., Sapkota, B., & Dawadi, B. R. (2025). Reinforcement Learning based Malware mitigation in balanced Multicontroller Software Defined Networking enabled Internet of Things Networks. Journal of Innovations in Engineering Education. https://doi.org/10.3126/jiee.v8i1.86281

[22] Sengayo, N., & Basikolo, T. (2024). Multistage classification in SDN security: a machine learning approach using real-world data for enhanced intrusion and vulnerability detection. ITU Journal, 5(4), 433–446. https://doi.org/10.52953/bzoj6066

[23] Dalgade, D., Patyane, S., Matey, A., Singh, S., & Godbole, A. (2024). Malware Detection using Machine Learning. International Journal of Innovative Science and Research Technology. https://doi.org/10.38124/ijisrt/ijisrt24apr1102

[24] Hirsi, A., Audah, L., Salh, A., Sahar, N. M., & Alhartomi, M. A. (2024). DDoS Anomaly Detection in Software-Defined Networks: An Evaluation of Machine Learning Techniques for Traffic Classification and Prediction. 100–105. https://doi.org/10.1109/icftss61109.2024.10691328

[25] Nguyen, V.-T., Hoang, V.-C., Nguyen, X.-H., & Le, K. H. (2022). Towards a high-performance threat-aware system for software-defined networks. International Conference on Autonomic and Trusted Computing, 280–285. https://doi.org/10.1109/ATC55345.2022.9942972

[26] Agrawal, A., Bhushan, B., Sharma, H., Hameed, A. A., & Jamil, A. (2025). Advancing Intrusion Detection in Software-Defined Networks. 1–6. https://doi.org/10.1109/satc65530.2025.11136867

[27] Li, C., Feng, C., Cai, X., Yang, F., & Wang, Y. (2026). Research on deep learning-based malicious traffic detection and defense mechanism. 110. https://doi.org/10.1117/12.3086415

[28] Yang, J. (2024). A new Attacks Intrusion Detection Model Based on Deep Learning in Software-Defined Networking Environments. 430–436. https://doi.org/10.1109/mlise62164.2024.10674546

[29] Ingle, D. (2025). Enhancing malware detection and classification in network traffic using deep learning techniques. Journal of Forensic Sciences. https://doi.org/10.1111/1556-4029.70189

[30] Saher, M. A. (2022). A Novel Approach To Network Intrusion Detection System Using Deep Learning For Sdn: Futuristic Approach. https://doi.org/10.48550/arxiv.2208.02094

[31] Hadi, M. R., & Mohammed, A. S. (2022). A Novel Approach To Network Intrusion Detection System Using Deep Learning For Sdn: Futuristic Approach. abs/2208.02094. https://doi.org/10.5121/csit.2022.121106

[32] Jeebodh, M. R., & Baliyan, N. (2024). IoT Malware Detection Using Deep Learning. 1–6. https://doi.org/10.1109/icccnt61001.2024.10724403

[33] Korsten, H. H. M., & Reddy, K. S. (2025). DeepSDN: Deep Learning Based Software Defined Network Model for Cyberthreat Detection in IoT Network. ACM Transactions on Internet Technology. https://doi.org/10.1145/3737875

[34] Elubeyd, H., & Yiltas-Kaplan, D. (2023). Hybrid Deep Learning Approach for Automatic Dos/DDoS Attacks Detection in Software-Defined Networks. Applied

Sciences, 13(6), 3828. https://doi.org/10.3390/app13063828

[35] Sharma, A., & Saxena, P. (2024). Distributed Denial of Service Attack Detection and Prevention Using Pipit Fox-Attentional Deep Learning in Software-Defined Networking. International Journal of Image and Graphics. https://doi.org/10.1142/s0219467826500294

[36] Choobdar, P., Naderan, M., & Naderan, M. (2021). Detection and Multi-Class Classification of Intrusion in Software Defined Networks Using Stacked Auto-Encoders and CICIDS2017 Dataset. Wireless Personal Communications, 1–35. https://doi.org/10.1007/S11277-021-09139-Y

[37] Souza, C. H. M., & Arima, C. H. (2024). A hybrid approach for malware detection in SDN-enabled IoT scenarios. Internet Technology Letters. https://doi.org/10.1002/itl2.534

[38] Elubeyd, H., & Yiltas-Kaplan, D. (2023). Hybrid Deep Learning Approach for Automatic Dos/DDoS Attacks Detection in Software-Defined Networks. Applied Sciences, 13(6), 3828. https://doi.org/10.3390/app13063828

[39] Latah, M., & Toker, L. (2020). An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks. 3(3), 261–271. https://doi.org/10.1007/S42045-020-00040-Z

[40] Shihab, D., Abdulhameed, A. A., & Gaata, M. T. G. (2025). Optimized Hybrid CNN-LSTM Framework with Multi-Feature Analysis and SMOTE for Intrusion Detection in SDN. https://doi.org/10.61710/kjcs.v3i4.132

[41] Kaur, P. (2025). Malware detection using classification technique and hybrid optimization technique. International Journal of Apllied Mathematics, 38(9s), 1393–1406. https://doi.org/10.12732/ijam.v38i9s.866

[42] Kanimozhi, R., & Ramesh, P. S. (2025). Deep reinforcement learning-based intrusion detection scheme for software-defined networking. Dental Science Reports, 15(1), 38827. https://doi.org/10.1038/s41598-025-24869-w

[43] Alasmari, S., & Mubarak, G. (2024). Android Malware Detection using TripleGuard Neural Network and Hybrid Bird Mating with Battle Royal Optimization. https://doi.org/10.21203/rs.3.rs-5434673/v1

[44] Abdallah, M., Khac, N. A. L., Jahromi, H. Z., & Jurcut, A. D. (2021). A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs. Availability, Reliability and Security. https://doi.org/10.1145/3465481.3469190

[45] Logeswari, G., Bose, S., Vijayaraj, G., Gokulraj, G., Maheswaran, N., & Varshini, I. C. (2025). RHFS-SEC: A Hybridized Feature Ranking and Soft-Ensemble Approach for Intelligent Intrusion Detection in SDN Environments. 957–963. https://doi.org/10.1109/icces67310.2025.11336910

[46] Nawshin, S., Islam, S., & Shatabda, S. (2024). PCA-ANN: Feature selection based hybrid intrusion detection system in software defined network. https://doi.org/10.3233/jifs-236340