



E-ISSN: 2707-6628
P-ISSN: 2707-661X
www.computersciencejournals.com/ijcit
IJCIT 2025; 6(1): 133-144
Received: 09-04-2025
Accepted: 12-05-2025

Rawand Salih
Department of Computer
Science, University of Kirkuk,
Kirkuk, Iraq

Essa Essa
Department of Computer
Science, University of Kirkuk,
Kirkuk, Iraq

Systematic review methodology for performance analysis optimization in software-defined networking/internet of things

Rawand Salih and Essa Essa

DOI: <https://www.doi.org/10.33545/2707661X.2025.v6.i1b.127>

Abstract

When merging Software-Defined Networking and the Internet of Things, performance evaluation becomes challenging due to IoT ecosystems' dynamic and heterogeneous nature. This extensive study examines the inefficiencies in data management, network congestion, and security challenges in Software-Defined Network-enabled Internet of Things devices. This study utilized a thorough literature review methodology, examining recent research implementing machine learning techniques for performance assessment across several domains. A comprehensive literature review methodology was applied to explore recent studies employing machine learning techniques for performance analysis through various application categories. Hybrid machine learning models, which integrate supervised and unsupervised techniques, are advised for effectively adapting to the highly dynamic nature of Internet of Things networks. Also, future research should focus on creating uniform performance evaluation metrics to make studies and applications more comparable.

Keywords: Software defined network, internet of things, optimization, machine learning, performance

1. Introduction

In the last few years, large developments have been made in the field of the Internet of things (IoT), and Software Defined Networks (SDN), they facilitate the process of enabling billions of devices with network connectivity to exchange and collect real time information to provide advanced services. SDN has been praised to be one of most appropriate solution for the future of internet. Many network architectures and, network systems, and data centers adopted SDN and turned it into a mainstream approach in network design ^[1]. The SDN model consist of three layers, namely an infrastructure layer, a control layer, and application layer, arranged in a stack. The main objective of the SDN is to separate the control plane from the data plane involving the forwarding devices. Controllers in the control plane preside the network infrastructure and offers an effective and flexible platform to execute varied services and network applications. SDN makes it possible to have a centralized control plane that manages network resources and routes traffic ^[2]. Evaluation of SDN architecture focused mainly on performance evaluation of control plane of SDN. In the framework, the role of network devices is exchanged to the devices that only transfer data such as switches that can be side by side with the control plane in the structure of software or in different term called controller ^[3]. In recent years, SDN technology become a popular topic for researchers, the development involves integrating Internet of Things (IoT) devices within the SDN network architecture. Due to its efficiency and flexibility, researchers highly regard SDN for optimizing performance on IoT devices. The IoT landscape has three layers: IoT device layer, IoT network platform and IoT application. IoT is the network of correlated devices whether mechanical or digital with capability of transmitting data via network without human intervention. IoT devices have the ability of observing, analyzing and making intelligent decisions according to collected information from the environments and adjustment of the network infrastructure, and for managing those devices, the traditional management approaches are slowly getting obsolete due to the evolution of new technologies and trends ^[4]. Hence, many researchers made several studies on SDN-based IoT networks, they conclude that the SDN in IoT communication networks could emphasize bandwidth to reduce wasted bandwidth resources ^[5]. Therefore, the existence of IoT devices applies more complication to maintaining and managing networks.

Corresponding Author:
Rawand Salih
Department of Computer
Science, University of Kirkuk,
Kirkuk, Iraq

The IoT attack vector may causing successful cyber attacks, and dynamic network security defenses are essential to protect critical data and assets ^[6]. However, this growth of underlying infrastructure as result will increase the complexity, so this growing complication demands creative methods to build the prospective of computer networks, where the complexity can be handled. All of the devices connected to the Internet generate a large amount of information creating, resource allocation, traffic management, and security that is challenging to maintain in the IoT network Centralized control for real-time traffic management, and the common network view for higher reliability suggested by SDN are essential to address the matters related to IoT ^[7]. Thus, the authors highlighted some of the key challenges existing in wireless networks that can be managed by using the perception of SDN using the concept of SDN. Sood *et al* ^[8]. Discussed different opportunities and challenges of SDN in the context of IoT, and indicated that SDN-based technologies will have significant impact on IoT to make it successful in the connected world. Similarly, minimizing the response time is one of the crucial issues for SDNs to optimize the load

distribution on the controllers. In this context, switch emigration is an effective way to solve this problem. Choosing an misplaced target controller and a numerous switches migrations between controllers minimize throughput by increasing the standard network response time ^[9]. Researchers determined that SDN-based solutions offer significant advantages in addressing the challenges of developing IoT applications when compared to traditional networking approaches. In this piece of work, we discuss how SDN take an important aspect in network technologies recent last years, and how SDN effect IoT devices and make it easier to work on it. Thus, we consider that SDN-based solution methods have the potential to address various issues and meet different requirements of IoT effectively. As a result, we investigate different options of SDN methods in the context of IoT, whereas displaying diverse challenges. Figure 1 illustrate the diversity in functional planning between a traditional and an SDN networks. SDN puts the data plane logic in the network elements, whilst, the control layer manages traffic flow and manages a global vision of the network through a centralized controller included in it ^[10].

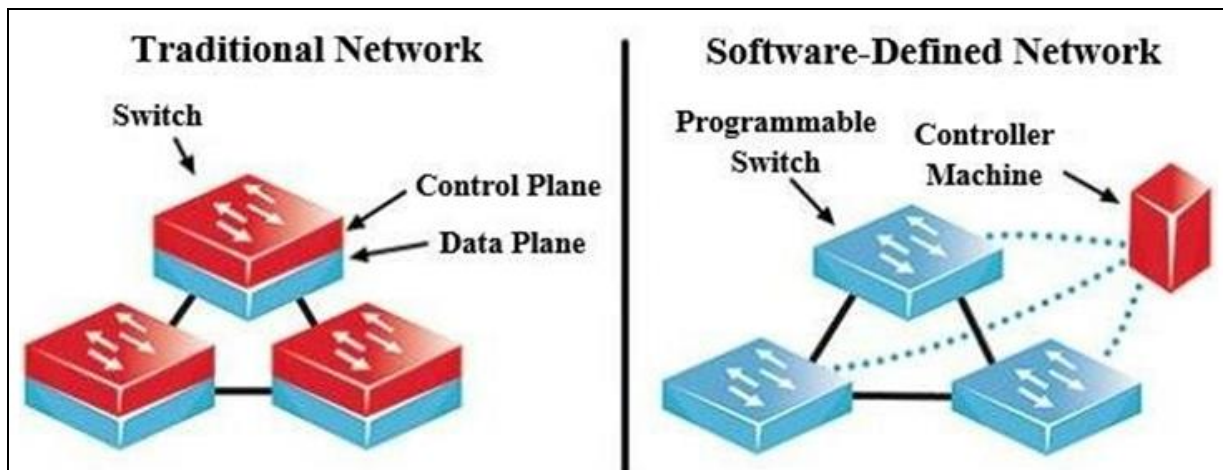


Fig 1: Comparison between traditional network and SDN ^[11]

2. Methods of systematic review

The systematic review method for performance analysis optimization in SDN/IoT encompass an exhaustive procedure of defining the area of research, precisely searching and evaluating the literature, synthesizing and extracting relevant information, and then identifying key insights and research gaps. This approach ensures a comprehensive understanding of the current state of research and provides a foundation for future advancements in SDN/IoT networks. A comprehensive literature research follows, employing databases like IEEE Xplore, Scopus, and ACM. Where the studies are chosen based on exclusion and inclusion criteria. Then the data will be extracted from these studies and synthesized to determine trends, common findings, and gaps. This analysis helps pinpoint areas requiring further exploration, like optimization algorithms and IoT-security enhancement ^[12].

2.1 Source of information

Sources for SDN and IoT performance analysis and optimization include academic journals such as IEEE Internet of Things Journal, ACMT transactions on

Networking, and Elsevier's Computer Networks, which publish peer-reviewed research. In addition, books such as SDN and Open Flow ^[13] and Internet of Things: Principles and Paradigm provide in-depth technical insights. Open-source communities on GitHub and forums like Stack Over flow provide real-world tips; IETF and ITU standards provide protocols and methodologies for performance tuning; and these resources are researcher and practitioner are comprehensive and valuable to researchers and practitioners ^[14].

2.2 Selection of the study

The selection of a study on performance analysis optimization for SDN/IoT involves choosing a specific area within the broader topic, guided by factors such as target application, performance metrics, SDN features, and optimization techniques. For instance, focusing on a specific use case like smart cities, healthcare, or industrial IoT can provide a relevant context, as suggested by various academic sources including IEEE journals and conference proceedings from IEEE INFOCOM and ACM SIGCOMM. Performance metrics such as latency, throughput, and

energy efficiency can be considered based on studies available in journals like IEEE Internet of Things Journal and Computer Networks (Elsevier). The study may also target specific SDN techniques like dynamic resource allocation or traffic engineering, as discussed in books like SDN: Anatomy of OpenFlow. Furthermore, understanding different IoT network characteristics, including edge computing and low-power networks, aligns with standards from IETF and insights from white papers by industry leaders like Cisco and VMware. For optimization approaches, methods such as machine learning, heuristic algorithms, or mathematical modeling are frequently explored in peer-reviewed sources and technical guides available through platforms like SpringerLink and ScienceDirect. The references mentioned here provide a comprehensive foundation to guide the choice of study in this specialized area ^[15]. The following key steps involved in the process of selection the study:

- **Defining the scope of study:** The very first step is to define the specific perspective of SDN/IoT performance analysis. This should involve some applications which present exceptional challenges and optimization requires.
- **Identifying performance metrics:** Performance metrics such as latency, packet loss, throughput, and energy efficiency that the study's focus on. These metrics are important for assessing the effectiveness of SDN in dealing with IoT networks.
- **Evaluating SDN features:** The studies may focus on particular SDN functionalities like dynamic resource allocation, traffic flow management, and load balancing, which are important for improving IoT performance.
- **IoT network characteristic considerations:** Specific selection study might involve analyzing specific IoT features like edge computing, low-power networks, or heterogeneous device integration, to determine how SDN can improve their operation ^[16].
- **Selecting optimization techniques:** Methods such as machine learning algorithms, heuristic optimizations are often investigated by researches, which provide innovation solutions for network performance enhancement ^[17].

2.3 Search Scenario

A "search scenario" in this context implies and exploring different strategies, algorithms, or configurations to achieve optimal performance in SDN-based IoT networks. For example, it could mean simulating different traffic patterns, evaluating various SDN controller placements, testing different routing algorithms, or exploring different methods for dynamic resource management. The goal of a search scenario in performance analysis and optimization for SDN/IoT is to identify the best approaches to meet specific performance requirements while reducing costs and resource usage ^[18]. In the field of performance analysis and optimization for SDN/IoT networks, a search scenario defines the context, conditions, and objectives for testing it with different algorithms or configurations. It aims to determine how different factors impact the system and find the best way to optimize its performance.

2.4 Process of data collecting

The data and information were collected in systematic approach through several steps, initially I start by defining clear research questions or objectives, then identifying relevant sources, including academic databases, and certitude journals, which can be used as an essential key for collecting evidence about the topic. Make a list of keywords and terms related to the research questions. Then use a systematic search through these databases, and effectively combine terms by using Boolean operators. Then applying inclusion and exclusion criteria to filter studies based on parameters like publication date, peer-review status, relevance to the topic, clarify the selection, and methodological rigor. Screening abstracts that involve reviewing abstracts for determining initial relevance, next a detailed examination made to the studies to evaluate their contributions. The produced data was organized by research gaps that identified by SDN/IoT literature, with using a structured body to categorize studies by methodologies, findings, and related to the review's objectives. Lastly, the entire process of data collection including search terms, databases, and gauge was documented in a meticulous manner to ensure transparency and maintain the review's replicability. A solid substructure was provided Int. this systematic approach for a comprehensive review. This structured approach ensures accurate actionable insights into SDN/IOT networks for future optimizations ^[19].

2.5 Research Literature Taxonomy

The taxonomy classifies reviews based on: (a) goal (b) focus (c) coverage (d) perspective (e) organization and (f) audience. The Literature reviews are playing an increasingly important role in applied sciences definition of knowledge. Data on the consistency of taxonomy coding's when proposed by readers is presented. In the Results of a survey of review authors gives baseline data on how regularly different types of reviews occur in the learning and technology literature. How the taxonomy can help in assessing the quality of literature reviews is discussed, including more general standards for estimating reviews ^[20].

2.5.1 Articles of IOT

IOT is considered a revolutionary technology which will transform the real-world objects into intelligent virtual objects, due to the extensive volume of data they generate and the fast number of connected devices ^[18]. All facets of human life are covered by the services provided by IoT applications, for instance, home and building automation, smart industry, smart cities, smart health, intelligent traffic management, smart health monitoring, emergency and surveillance services, retail, and supply chain ^[21]. However, there are many research take IoT as a study with other machine learning studies for explore IoT applications and challenges in the context of SDN and how emerging IOT with SDN could enable new services. The main focus will be how to achieve heights performance for this technology, more than one of the studies use Machine learning approaches as K-mean, K-NN. Future researches focus on optimizing security, enhancing the efficiency of energy, and developing architecture to handle IoT demands. The articles used in this review focuses on more work on autonomous IoT systems, sustainable energy solutions, and frameworks

that address the evolving needs of IoT ecosystems. An adequate survey on IoT is demonstrated by Laghari *et al.* In ^[22], mentioning each field of IoT, application, scenarios, and issues. A comprehensive study on cybersecurity challenges in IoT by Tariq *et al.* in ^[23], focusing on vulnerabilities and find solutions for ensuring confidentiality, integrity, and availability in IoT networks.

2.5.2 Articles of SDN

SDN give intelligent and adapted network capabilities by breaking traditional networks into a centralized control plane and a programmable data plane. The network performance improvement depends on the intelligent control plane, which set up switches flow paths. Within the control plane, the centralized architecture of SDN enables a programmatic control over the entire network devices and allows for real-time management of underlying devices. SDN Execution simplifies network management and removes the constraints related to rigid network structures. Alexander *et al.* ^[1] present a study on performance analysis in SDN. In this review we, we focused on comparing SDN with traditional networks, working on protecting SDN and how to improve its performance in IoT networks with SDN. Several distributed but logically centralized controllers of SDN were evaluated in a specific network scenario called Mininet. The study done by Sheikh *et al.* ^[24] comprehensively assessed 13 controllers based on their capabilities, attributes, and performance measures, in addition to bandwidth, delay, jitter, round trip time (RTT), throughput, and packet loss. Which revealed that Ryu controller exceed the Open Day Light controller in latency, packet loss, and RTT, while Open Day Light excelled in, bandwidth, throughput, and jitter performance. Hussain *et al.* ^[25] highlighted SDN's advantages along with illustrated management and programmability, as well as detailing flow rule mechanisms (reactive, proactive, hybrid). In ^[26]. Bhuiyan *et al.* focused on evolving security challenges in the control plane of SDN, analyzing the risks made by its programmability and centralization.

2.5.3 Other research related to IOT/SDN

In addition to specialized studies and research in the fields of the SDN/IoT, there are many sources that have worked to integrate both SDN and IoT. Quin *et al.* ^[21, 22]. Developed an innovation to combine SDN with IoT. SDNs and IOTs are a trending issues and grabbing the focus in many aspects. Research communities doing a comprehensive study to explore detailed perspectives, suggestions applications, and technical needs within both fields. Ray *et al.* ^[27] propose a study about the emerging technologies of SDN, IoT, and NFV (Network Function Virtualization), as well as how this service innovation in the Cloud and big data era although, a comprehensive review on the merging of IoT in SDN focus attention from the research association.

In this work, we show various studies which provide SDN based approaches for IoT technologies. We survey the literature spanning the period from (2020-2024), by shedding lights on different perspectives of the IoT integration with the SDN. Also focus on how to keep divers IoT environments that use the flexible and programmable features of SDN in high performance and reduce risks on those devices. Rafique *et al.* ^[19] proposed a comprehensive

study about leveraging SDN for large-scale IoT devices improving programmability and scalability. Indrason *et al.* ^[28] analyzed how SDN improves IoT network efficiency thorough adaptive resource management and security enhancements.

2.6 Motivations, Challenges and Recommendations

In the subsequent subsection, we present the motivating methods, issues associated with SDN/IoT, and the corresponding advice.

2.6.1 Motivation

In today's interconnected world, the integration of SDN and IoT offers an exceptional opportunity and a forbidden challenge. While billions of IoT devices flood data with networks, analysis of performance optimization is a critical issue for unlocking SDN's for managing and securing these complex dynamic domains. The backbone for this transformation is performance analysis optimization. It authorizes network controllers and developers to obtain real-time perceptions, pinpoint bottleneck, allocate resources in a proactive manner for best efficiency. Latency, bandwidth, and power consumption are critical factors. Without powerful performance analysis these connected devices may overwhelm the system, which leads to slowdowns and disruption. The process of performance optimization qualifies the networks to scale intelligently adjust to traffic demands.

Moreover, performance optimization goes on the farther side of enhancing speed it's more about build that are more adaptive, and intelligent. The programmability of SDN enables an automated adjustment, customizing network resources to meet the unique demands of IoT applications ^[29]. This flexible approach not only enhance the effectiveness of the infrastructure but also minimize operational costs by optimizing resource allocation and decreasing wastage. As well as improving speed, performance optimization simplifies the design of more intelligent and adaptive network infrastructure. By leveraging SDN's programmability, networks can dynamically reallocate resources to meet the specific demands of various IoT applications. This flexibility improves efficiency of network while minimizing resource utilization and reducing wastes. The convergence of SDN not only transform network management but also tackling critical issues like security and scalability, providing a flexible framework for future IoT-systems ^[30].

2.6.2 Benefits related to IOT

IoT has produced more openings for integrating the world into the systems created by the latest computing technologies ^[31]. IoT applications engaged in every aspect of life and impact on socio-economic factors such as security, healthcare services, disaster response, remote connectivity and more. IoT results in a large amount of big data ^[32]. The IoT gives users intelligent recommendations. For instance, in smart mobility systems as in-car, self-driving systems, and smart highways, route optimization assists drivers with taking into consideration constraints associated with traffic, cost, and time. Shortly, IoT can bring different benefits related to both real-time measurement and sensors data effectiveness in services analysis, enrich

performance of services, and improve adaptability of services in analyzing historical data trends over time. The IoT might yield many advantages and they are transformative. One of the most important issues is to supply security insurance for the data because the data are easily attacked at each layer of IoT^[33]. Possible benefits of the IoT are 1. Strategic and political-improved trends analysis and forecasting, simulating government transparency, enhanced citizen empowerment; 2. operational-enhanced coordinating with considers to maintenance and management, more effective enforcement of policies and compliance measure, enhanced safety standards, cost minimization, additional revenue resources; 3. Operational enhanced service efficiency, enhanced services flexibility.

2.6.3. Benefits related to SDN

SDN offers several advantages, including enhanced network flexibility, centralized control, and simplified the management process. Through decoupling the control plane from the data plane, SDN authorized network administrators to dynamically optimize network resources and configure them based on real-time demands. This centralized control also improve the ability to orchestrate and automate network functions that can reduce operational costs and improve effective. SDN enables Programmability through the entire network. SDN enables administrators to manage and modify network behavior programmatically. Instead of deploying traditional protocols or configurations SDN centralizes these operations at the control plane. This programmability simplifies traffic flow optimization, minimize network congestion, and allows seamless adjustments to network behavior. The controller can dynamically enhance traffic management and efficiently address bottlenecks within the network. Though, SDN improve network security by allowing the rapid deployment of security policies through the network, and making it easier to manage and respond to potential threats. Observed that only Huge Service Providers like Google has moved there from the globe deployed network to be SDN based. The main reason for this slow-moving extricate cost is related to the higher required to change typical network equipment's along with Open Flow enabled buttons^[34].

2.6.4. Benefits related to application activities

The traditional equipment and network protocols are not designed to support the high amount of traffic and mobility, high level of scalability^[35]. There are several benefits for application activities for performance analysis optimization for SDN/IoT provide a wide range of benefits, enabling networks to function more efficiency, scalability, and security. Through dynamically allocating bandwidth based on real time demand and managing devices efficiently, application activities make sure of optimal resource utilization, reducing idle time, and preventing stoppage. Also, these activities help reduce latency, and enhance response time by data routing optimization, and preemptively addressing potential issues. For IoT applications that work in real-time, such as autonomous vehicles or smart healthcare devices, low latency is critical, and intelligent data routing ensures that data is transmitted with least delays. Efficient energy is further improved

through optimized power usage, as applications can modify device operations to preserve energy, extending the lifespan of IoT devices. These capabilities help for lower operational costs through optimizing maintenance schedules and allocating resources more efficiently, which reduces expenses associated with repairs and hardware. SDN allow an IoT network to be more secure, scalable, reliable, and ensures optimal performance. SDN improves the flexibility of IoT networks and provides substantial advantages to mitigate possible attacks efficiently. This advancement enhances the quality of our life significantly. As a part of this growth, we embrace the enormous benefits of IoT such as seamless collecting of data from remote areas and the, monitoring, and controlling devices wirelessly.

2.7. Article Challenges

Here are some common challenges that articles on topics like IoT-SDN integration often address.

2.7.1 Challenges concerned to SDN-IOT

Despite the high efficiency of applying SDN technology on IoT devices for enhancing the performance, many issues prevent the usage of these technologies. Some of these challenges include the issue associated with SDN-IoT and another in the performance optimization. One of the crucial security issues in SDN-based IoT is the DDoS and DoS attacks. Resource limitations in SDN-based IoT systems often lead to vital challenges with DDoS attacks posing a particularly severe threat to the SDN controller layer^[36]. Considering the promises of improved configuration, performance, and motivate innovation, SDN still in its formative phase. There is a list of SDN challenges consist of: Scalability, performance, security, reliability, and interoperability. Some common security threats on SDN are unauthorized access, malware and viruses, data breaches, man-in-the-middle attacks, insider threats and Distributed Denial of Service (DDoS) attacks^[37]. The control plane in SDN also concerned with some challenges such as security, queuing mechanisms, and so on. If controller is compromised or influenced by attackers, this called massive attack caught on SDN and network execution degraded strictly^[38]. For IoT devices the authors presented a comprehensive overview of the key challenges faced by IoT middleware solutions, which include collaboration, distribution, deployment, infrastructure support, security, and privacy. Presently standard internet protocols are inadequate for meeting the various demands for SDN techniques within IoT devices. This challenge will lead development of various of interoperability solutions^[39]. To have the extremely large number of interconnected technologies, settings and administering of these devices which do not seem feasible if we do not have automated approaches^[40].

2.7.2 Recommendations

The subsequent parts present ideas for the development of SDN/IoT, which will be considered in research advancement.

A. Recommendations to developers

The advises for developers are to work on security through improve security for IoT systems. As all powered devices

can become vulnerable to attack, scalability as the SDN used in IoT networks grows over time, and data privacy ensure compliance with data privacy regulation to protect user information. However, it is recommended to use approximate algorithms.

Here are some additional recommendations for developers work on IoT integrated with SDN

- Utilize encryption protocols.
- Strengthen device authentication.
- Implement adaptive traffic management.
- Improve threat detection mechanism.
- Provide secure communication protocols.
- Apply privacy by design principles.

B. Recommendations to researchers

Researchers should focus on developing flexible resource appropriation algorithms and integrating edge devices and fog computing to reduce latency and improve responsiveness, especially for applications requiring rapid response. Security is also critical, therefore developing lightweight, scalable security frameworks for SDN-based IoT networks may protect against cyber threats while

managing performance. In addition, as IoT devices propagate, improving scalability in controller architectures, in distributed or hierarchical models, will ensure efficient handling of increased traffic. Investigating cross-layer optimization techniques can improve resource utilization by aligning optimizations through the data, network, and application layers [4]. Also, they encouraged to explore progress in machine learning algorithms to improve predictive anomaly detection in SDN-based IoT systems discussing both security and performance challenges. Developing energy efficient algorithms tailored for IoT devices with limited power resources is crucial for prolonging device life-time and ensuring network verifiability. Researchers should also investigate dynamic load balancing for dispensed SDN controllers to enhance resource utilization and prevent bottlenecks [41]. Searching blockchain technology for transparent and secure data sharing in IoT environment can decrease security risks and enhance data integrity [42]. Moreover, developing interoperability frameworks to connect the gap between different IoT protocols and SDN architectures will ensure seamless integration and minimize communication overhead [43].

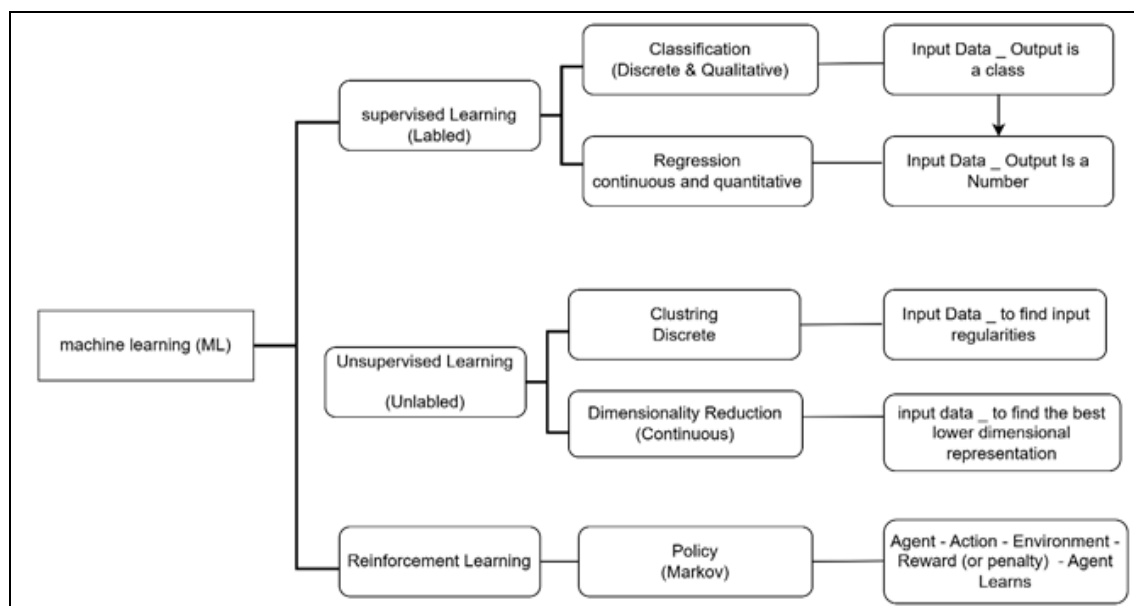


Fig 2: Overview diagram of machine learning algorithms [48].

3. Previous research methodology aspects based on machine learning

Machine learning is the scientific study of algorithms and statistical models that used by computer systems to perform a particular task without any direct programming instructions. Machine learning which is part of Artificial Intelligence (AI), is used in the designing of algorithms based on the recent trends of data [44]. Machine learning have become integral to make SDN security more efficient, more flexible, and update efficient approaches with SDN to emphasize security, development, and management, establishing a new essential element that improve flexibility in these areas. For protecting information security, the discovery of attacks is extremely critical which helps to take the required metrics promptly. In this review we proposed different methods in Machine learning that shows better

accuracy of prevention and detection, such as detecting Distributed Denial of Service (DDoS) attacks by distinguishing between different benign and malicious patterns, for example random forests (RF) and Decision Tree (DR), are broadly used because of their classification abilities giving high accuracy in determining anomalies. Another supervised learning algorithms like Linear Regression and Logistic Regression can be widely used, which are essential for predicting categorical and continuous outcomes. There is another valuable ML tool called the Support Vector Machine (SVM) and K-Nearest Neighbors (KNN), used especially for classification tasks like separating data into distinct categories based in their patterns. Unsupervised algorithms like K-Means clustering and principal component analysis (PCA) used to uncover hidden patterns and reduce dimensionality in large datasets.

The ML methods can be employed to analyze traffic to detect an attack pattern. The progressive network attributes like a comprehensive view of the network facilitate it for us to mitigate and detect DDoS attacks ^[45]. Deep learning models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) can be used for tasks involves sequential data. These algorithms contribute to SDN's ability to automate responses and safeguard against cyber threats ^[46]. It is crucial to recognize that legacy machine learning approaches have limitations when it comes to detecting and preventing cyber-attacks. As threat and penetration strategies and tools continue to develop, the execution of these techniques may be less effective ^[47].

4. Literature Review: Synthesis

Gelberger *et al.* ^[1] proposed an in-depth performance analysis of SDN architecture especially concentrating on OpenFlow and ProGFE, to determine how SDN effect raw network performance measures like throughput and latency. Tayyaba *et al.* ^[3] conducted to the integration of SDN with IoT, by focusing on the advantages of SDN centralized control in conducting heterogeneous IoT networks addressing matters such as security resource allocation. Bera *et al.* ^[4] proposed a comprehensive survey SDN-based technology for IoT applications, explaining how of SDN addressing IoT challenges through access, edge, and centralize networks by enabling effective data accumulation, resource controlling, and security across programmable management. They identified the role of SDN in improving IoT's flexibility and scalability while showing the limitations in existing approaches, such as the need for optimized algorithms to manage the vast amount of IoT data traffic. Setiawan *et al.* ^[5] conducted a performance analysis using a mininet-IoT and ONOS controllers on 6LoWPAN-based IoT networks, determining how SDN have impact on reducing latency and jitter while controlling throughput effectively through different network conditions, they discover that centralized SDN control can stabilize network performance even if the number of connected devices get larger. Sood *et al.* ^[8] proposed a review on the integration of software defined wireless networking (SDWN) with IoT, determining SDN's capability to simplify network control mechanisms and enhance IoT network scalability and agility across centralized management. As well as they noted the challenges in security and resource allocation within SDN-IoT networks and highlighted the potential of edge computing and intelligent algorithms to address these limitations. Caraguay *et al.* ^[7] discusses the inflexibility of traditional networks and show how SDN offers an adaptable, programmable architecture that benefits IoT applications by allowing efficiency policy implementations as IoT's growing needs. Stalling. ^[13] Proposed an overview of SDN using an OpenFlow protocol describing how disconnecting of data and control plane and centralized management can improve IoT networks by enhancing resource allocation and traffic flow control. Abderrahmane *et al.* ^[9] conducted on the Controller Placement Problem (CPP) within SDN-IoT networks, addressing optimum controller placement for improved latency, energy efficiency, and load balancing. Its critical for supporting IoT's scalability requirements. Cooper. ^[20] Proposed a comprehensive taxonomy for literature reviews. His

framework categorizes literature reviews by focusing on six key characteristics: focus, goal, perspective, coverage, organization, and intended audience. Each category offers a structured approach to understanding the purpose and design of a literature review. Shafiq *et al.* ^[21] established a study that employs a systematic approach to estimate selected publications focusing on related technologies to SDN-IoT such as DC, BC, and 5G/6G to gain access to their impacts and applications. The review also determines open research questions, enhancing challenges in security, scalability, and resource management, and provides a plan for future SDN-IoT developments. Qin *et al.* ^[49] proposed a multi-network SDN architecture created to handle different requirements of IoT environments, using layered approach with tools such as network calculus and genetic algorithms for dynamically allocating resources and enhance traffic flow across multiple IoT tasks. Ray *et al.* ^[27] explains the requirements for IoT middleware and its character in addressing security, interoperability, and scalability matters. It also improves the limitations of standard internet protocols for SDN-IoT integration and the development of cross compatibility solutions.

5. Methods and Materials

Several simulation tools, protocols, and optimization techniques are used to manage resources effectively and improve efficiency. The materials examined include included journal articles, conference papers, and technical reports from leading sources on SDN, IoT, and network optimization. Our method included systematically collecting literatures published between years [2019-2024] from academic data bases like IEEE Xplore, Springer Link, and Science Direct. Using Keywords such as "SDN performance optimization" "IOT network efficiency, and "SDN-based IoT security. We analyzed each source depending on particular metrics like latency, throughput, packet loss, and resource utilization. We studied key optimization techniques included load balancing, traffic engineering, network function virtualization (NFV), and machine learning algorithms. The results were synthesized to highlight challenges, trends, and emerging solutions for improving SDN/IoT performance.

6. Authentication methods in previous studies

In the previous studies concerned in SDN/IoT networks, different authentication methods have been examined to ensure security and protect the integrity of the data and devices within the network. These methods typically aim to approve the identity of IoT devices, prevent unauthorized actions, and control access to network resources. Those methods incorporate many sources such as IP addresses and external authentication protocols to verify user identity. IoT and SDN work together to decouple the control plane and the data plane in order to connect items via the internet. We predict that there will be billions of connected devices in IoT networks in the future, and managing and controlling them will be a dynamic activity that presents significant challenges for IoT networks. Verify user and device identity. ^[50]. One of the big limitations in this field is that despite the fact of security and privacies in an IoT system, they are still in a problem because these devices are more that despite the fact of security and privacies in an IoT

system, they are still in a problem because these devices are more vulnerable and prone to security attacks and threats, while the adversaries are always on the hunt for new ways to get into the usually unsecured and opened devices; in the public. We show our method brings flexibility, easier network management, easier network maintenance, and acceptable privacy-protecting level [22]. Lately the methods used for network configuration, can have a network strategy that manage the current state of the network at a certain time, yet the state of the network changes oftentimes [7]. Network forensic is divided into several distinct phases, which are explained individually with reference to analysis, preparations, and activities of investigations [51], with these phases being preservation, collection, examination, analysis and presentation [52].

7. Comparison of previous related works

This table highlights the objectives, methods, and Results of these studies, considering each approach's unique strengths and limitations when it is applied to SDN-IoT environments. In general, the goal of this comparative study is to contribute to the existing branch of knowledge in the field of network security by shedding light on different approaches to securing SDN architecture data transfer for IoT devices. Through comprehending the strengths and limitations of different security mechanisms [53].

Below is an expanded table comparison between the previous related studies in SDN-IoT environments. Each entry focus on the objectives, methods, results, strengths, and limitations, referencing the provided documents.

Table 1: References Summary

Ref.	Problem	Objectives	Methods	Results	Strength Points	Limitation
1	Limited scalability in SDN-based IoT frameworks	Evaluate the scalability of SDN frameworks in large IoT devices	Modeling and simulation using Mininet and custom SDN controller	Showed improved scalability in treating large number of devices with enhanced data flow	Allowed scalable handling with large IoT networks through enhanced SDN controllers	Restricted to simulated real-world results
2	High latency in IoT data transmissions	Decrease latency in SDN-IoT by optimizing the path of data	Experimental tests in different path optimization algorithms in SDN controllers	Significant latency reduction using dynamic path adjustment	Effective latency reduction, enhancing IoT response time	Limited scope in algorithm variety; needs broader testing
3	Security vulnerabilities in SDN-IoT environments	Improve security mechanisms for SDN managing IoT networks	Implementation and design of adaptive security policies in SDN controllers	Increased network resilience to attacks via flexible security measures	Improved security through integrating adaptive, real-time policies	High computational costs for constant adaptation
4	Inefficient resource allocation in SDN-IoT	Enhance resource allocation through IoT devices in SDN	Using SDN controller and ML for modeling resource allocation	Optimized resource use, balanced load, reduced congestion	Balanced resource usage improved performance	Complexity in integrating ML with real-time IoT
5	Managing dynamic IoT devices in SDN	Improve device management in mobile IoT networks with frequent changes	Modularized SDN framework for real-time management	Enhanced stable connectivity in mobile IoT devices	Effective management for dynamic environments	Limited to specific device types and scenarios
6	Managing tasks/resources in multi-network IoT	Improve resource allocation and flow in IoT	SDN architecture, network calculus, Genetic Algorithms	Efficient management of tasks, flow, and network	Layered SDN controller supports heterogeneous environments	Complexity in integrating diverse IoT protocols
7	Inadequate clustering to minimize energy consumption	Improve cluster head selection for energy efficiency and lifetime	Improved Sailfish Optimization (ISFO) in SDN	Minimized energy drain by 21.42% (150 nodes), 37.84% (300 nodes), prolonged lifetime	Centralized SDN supports energy-efficient clustering	Dependent on topology and number of nodes; needs more scalability testing
8	Poor SDN controller placement in IoT networks	Reduce latency, energy, and balance load	Graph-based modeling and heuristic techniques	Reduced delay, better load balancing and energy savings	Centralized control enhances management and efficiency	Limited to certain network settings and constraints
9	Managing various IoT devices and ensuring scalability	Enable centralized control and dynamic resource allocation	Integration of SDN controllers with IoT architecture	Improved resource use, latency reduction, traffic optimization	Scalable and flexible for various IoT apps	Needs testing in highly dynamic and heterogeneous environments
10	Evaluation of varied SDN controllers	Comparison of SDN controllers in different topologies	Ryu and POX tree-based SDN topologies simulation	Latency, RTT and packet loss variance of performance	Assists in the identification of best controller with respect to topology	Only controller types (Topologies) are supported
11	The need of flexible IoT architectures	Survey self-adaptive architectures in IoT	Systematic literature review	The recognized improvement of flexibility in IoT	A good coverage of self adaptive designs	Small scale practical verification in the real world
12	Conventional networks meant to be rigidly designed	Flexibility through promoting SDN using OpenFlow	Summary of OpenFlow decoupling and SDN Race	Improved traffic control and configurability	Easy architecture of network administration	Neither performance measures nor experiments data was present
13	Ideal location of SDN controller/Survey location	Controller optimization strategies of placement of surveys	Review of literature in an area of Controller Placement Problem (CPP)	Description-latency/load placement trade-offs	Significant to large SDN-IoT implementation	Theoretical in nature; ought to be tested on the ground
14	Scalability of SDN-IoT networks	Use SDN to scale IoT using ICN concepts	ICN approaches based on SDN: survey and classification	Integer programmability and scalability	End-to-end convergence plan of big IoT	It is concerned with concept integration, rather than deployment
15	Adverse literature review taxonomy	Suggest taxonomy on reviews classification	Taxonomy-based framework	Better categorisation of types of literature review	Useful for research design	Is not exclusive to the field of SDN and IoT

8. Machine Learning

Machine learning has significant place within the field of

information technology, possibility, statistics, artificial intelligence, neurobiology, psychology and many more

fields ^[54]. Machine learning is the process of generating algorithms that enable the computer to learn. Since their progression, humans have relied on wide range of tools to perform different tasks in a straightforward way. The inventiveness of the human brain led to the creation of various machines. Machine learning algorithms are limited by algorithm bias and data bias, which can produce systematically skewed predictions ^[55]. These machines have simplified human life by enabling people fulfill different life needs, such as travelling, industries, and computing, and machine learning is one of them. Machine learning is the scientific propriety concentrated in particular algorithms and statistical models that help computer systems to execute specific tasks without require for explicit programming. It is an AI that learns how to predict patterns in a provided dataset, these predictions can later be applied and tested on real-world cases ^[56]. A machine learning based Intrusion Detection System (IDS) proposed to improve security on the SDN networks using a machine learning algorithms ^[57]. In

this method, new income traffic is distinguished between anomalous traffic and normal traffic using entropy ^[58].

There are three types of machine learning methods, which they are:

1. Supervised Learning

Supervised machine learning is the process of learning functions which plans an input to an output based on example of input-output pairs it derives a function from labeled training data which is composed of a set of training instances. Where the set of annotated data is called the training sets, while an annotated data is called the testing set ^[59]. The training sets are discrete and unordered, they are called class labeled, when they are continuous numerical values, they are called output variables. The external assistant utilized supervised algorithms are as follows. The dataset is split into train and test dataset. The work flow of supervised machine learning is given in the figure below:

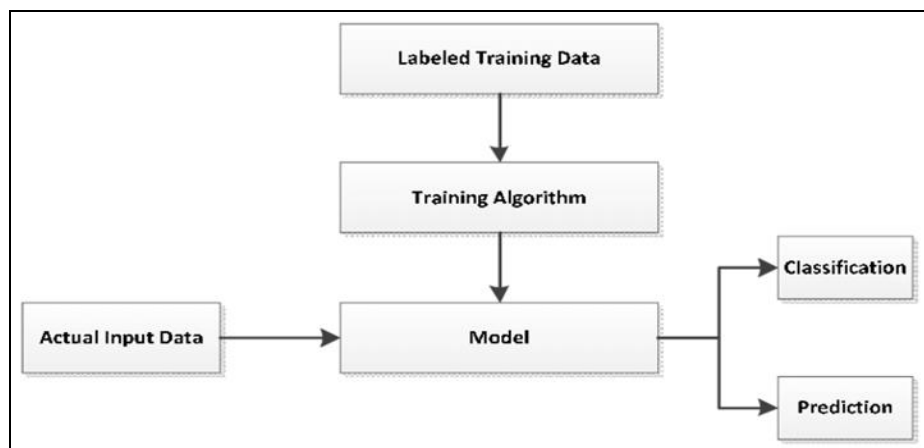


Fig 3: Block diagram for supervised learning principle ^[19].

2. Unsupervised learning

Unsupervised learning is a major category of learning algorithms that assist in discovering the attendant structure of the data without supervision (as provided in supervised learning). The purpose of a most unsupervised learning task is mainly to identify similarity in a set of examples, where it is refer as clustering, or to estimate the probability of data distribution, it is termed as density estimation, or to perform dimensionality reduction, where it regarded as subspace learning ^[60]. In unsupervised learning algorithms, the models are given unlabeled data and allowed to discover

patterns and insights without any explicit guidance or instruction. Unsupervised learning algorithms uses self-learning they learn without any prior-training or labels. The one thing that unsupervised learning methods need to work with are the observed input patterns, where they often assumed to be independent samples from an inherent unknown probability distribution. The motivation of unsupervised learning is that though the data that goes through the unsupervised learning algorithms has a rich essential structure, the ground truth and the measure used for training are typically sparse ^[61].

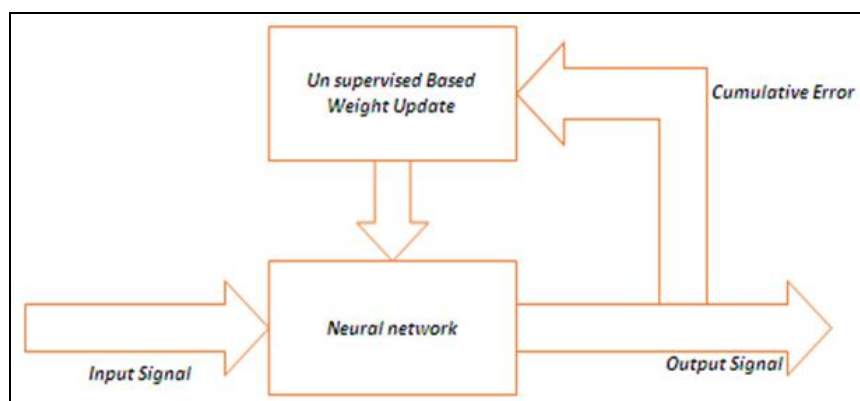


Fig 4: Is block diagram for unsupervised learning ^[62]

3. Reinforcement learning

Reinforcement Learning (RL) is a machine learning technique to learn successive determining complicated problems [63]. RL is motivated by trial and error in human/animal learning. Reinforcement learning is one of the machine learning subfields dealing with what a software agent should do in an environment to achieve some cumulative reward [16]. It simulates the trial-and-error learning process that humans use to reach their goals. It is one of the three fundamental paradigm of machine learning, along with supervised and unsupervised learning. When implementing reinforcement learning, specifically to real-world applications, it is acceptable to have algorithms that dependably achieve high levels of performance without needing expert knowledge or crucial human intervention [64].

9. Conclusion

In last few years the advancement of SDN and IoT reconstruct the networking landscape and how the advancement in the SDN and IoT have covered the way of connecting millions of devices and improving real-time data transmission to provide enhanced services. SDN, which split data and control planes, is considered as essential solution for the future of internet and networking, also it is widely demanded in data centers and network systems for its efficient, and for the centralized control over the network resources. We focused on researches that increasingly integrated IoT into SDN and using techniques for optimizing performance of the devices that engage SDN with IoT. A systematic review of existent literature reveals the function of SDN in optimizing IoT networks through flexible dynamic resource allocation, traffic management, and advanced security measures. This paper concludes by presenting recommendations for leveraging SDN to unlock IoT full potential, paving the way for better, more efficient networks.

10. References

1. Gelberger A, Yemini N, Giladi R. Performance analysis of software-defined networking (SDN) in 2013 IEEE 21st International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems. IEEE, 2013, p. 389-393. DOI: 10.1109/MASCOTS.2013.58.
2. Hafeez I. A systematic mapping study on self-adaptation SDN based Iot Networks [Internet], 2023.
3. Bhardwaj S, Panda SN, Datta P. Comparison and performance evaluation of software-defined networking controllers in 2020 international conference on emerging smart computing and informatics (ESCI). IEEE, 2020, p. 276-281. DOI: 10.1109/ESCI48226.2020.9167554.
4. Tayyaba SK, Shah MA, Khan NS, Asim Y, Naeem W, Kamran M. Software-defined networks (SDNs) and internet of things (IoTs): A qualitative prediction for 2020. Int J Adv Comput Sci Appl. 2016;7(11). DOI: 10.14569/IJACSA.2016.071151.
5. Setiawan DY, Hertiana SN, Negara RM. 6LoWPAN performance analysis of IoT software-defined-network-based using mininet-Io in 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS). IEEE, 2021, p. 60-65. DOI: 10.1109/IoTaIS50849.2021.9359714.
6. Chaganti R, Suliman W, Ravi V, Dua A. Deep learning approach for SDN-enabled intrusion detection system in IoT networks. Information. 2023;14(1):41. DOI: 10.3390/info14010041.
7. Zemrane H, Baddi Y, Hasbi A. SDN-based solutions to improve IoT: survey in 2018 IEEE 5th international congress on information science and technology (CiSt). IEEE; 2018:588-593. DOI: 10.1109/CiSt.2018.00099.
8. Sood K, Yu S, Xiang Y. Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review. IEEE Internet Things J. 2015;3(4):453-463. DOI: 10.1109/JIOT.2015.2480421.
9. Mohammadi R, Akleyek S, Ghaffari A. SDN-IoT: SDN-based efficient clustering scheme for IoT using improved Sailfish optimization algorithm. PeerJ Comput Sci. 2023;9:e1424. DOI: 10.7717/peerj-cs.1424.
10. Rashid SJ, Alkababji AM, Khidhir ASM. Performance evaluation of software-defined networking controllers in wired and wireless networks. TELKOMNIKA (Telecommunication Comput. Electron. Control). 2023;21(1):49-59. DOI: 10.12928/TELKOMNIKA.v21i1.23468.
11. Cabarkapa D, Rancic D. Performance Analysis of Ryu-POX Controller in Different Tree-Based SDN Topologies. Adv. Electr. Comput. Eng. 2021;21(3). DOI: 10.4316/AECE.2021.03004.
12. Alfonso I, Garcés K, Castro H, Cabot J. Self-adaptive architectures in IoT systems: A systematic literature review. J. Internet Serv. Appl. 2021;12:1-28. DOI: 10.1186/s13174-021-00145-8.
13. Stallings W. Software-defined networks and openflow. Internet Protoc. J. 2013;16(1):2-14.
14. Ali J, *et al.* Performance optimization of software-defined industrial internet-of-things (SD-IIoT). IEEE Access, 2024. DOI: 10.1109/ACCESS.2024.3466186.
15. Zhang Z, Wang R, Cai X, Jia Z. An SDN-based network architecture for internet of things in 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE, 2018, p. 980-985. DOI: 10.1109/HPCC/SmartCity/DSS.2018.00162.
16. Silva JC, Pereira PHM, Souza DLL, Marins CNM, Marcondes GAB, Rodrigues JJP. Performance evaluation of IoT network management platform in 2018 International conference on advances in computing, communications and informatics (ICACCI). IEEE, 2018, p. 259-265. DOI: 10.1109/ICACCI.2018.8554364.
17. Amin R, Rojas E, Aqduş A, Ramzan S, Perez CD, Arco JM. A survey on machine learning techniques for routing optimization in SDN. IEEE Access. 2021;9:104582-104611. DOI: 10.1109/ACCESS.2021.3099092.
18. Abderrahmane A, Drid H, Behaz A. A Survey of Controller Placement Problem in SDN-IoT Network. Int. J. Networked Distrib. Comput, 2024, p. 1-15. DOI: 10.1007/s44227-024-00035-y.
19. Rafique W, Hafid AS, Cherkaoui S. Complementing

- IoT services using software-defined information centric networks: A comprehensive survey. *IEEE Internet Things J.* 2022;9(23):23545-23569. DOI: 10.1109/JIOT.2022.3151234.
20. Cooper HM. Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowl Soc.* 1988;1(1):104. DOI: 10.1007/BF03177550.
 21. Shafiq S, Rahman MS, Shaon SA, Mahmud I, Hosen ASM. A Review on Software-Defined Networking for Internet of Things Inclusive of Distributed Computing, Blockchain, and Mobile Network Technology: Basics, Trends, Challenges, and Future Research Potentials. *Int J Distrib Sens Netw.* 2024;2024:9006405. DOI: 10.1155/2024/9006405.
 22. Laghari AA, Wu K, Laghari RA, Ali M, Khan AA. A review and state of art of Internet of Things (IoT). *Arch Comput Methods Eng.* 2021;1-19. DOI: 10.1007/s11831-021-09622-6.
 23. Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors.* 2023;23(8):4117. DOI: 10.3390/s23084117.
 24. Sheikh MNA, Hwang IS, Raza MS, Ab-Rahman MS. A qualitative and comparative performance assessment of logically centralized SDN Controllers via Mininet Emulator. *Computers.* 2024;13(4):85. DOI: 10.3390/computers13040085.
 25. Hussain M, Shah N, Amin R, Alshamrani SS, Alotaibi A, Raza SM. Software-defined networking: Categories, analysis and future directions. *Sensors.* 2022;22(15):5551. DOI: 10.3390/s22155551.
 26. Bhuiyan ZA, Islam S, Islam MM, Ullah ABM, Naz F, Rahman MS. On the (in) security of the control plane of SDN architecture: A survey. *IEEE Access.* 2023. DOI: 10.1109/ACCESS.2023.3307467.
 27. Ray PP, Kumar N. SDN/NFV architectures for edge-cloud oriented IoT: A systematic review. *Comput. Commun.* 2021;169:129-153. DOI: 10.1016/j.comcom.2021.01.018.
 28. Indrason N, Mawblei M, Jyndiang K, Thakur AK. A survey on the applications of SDN-based IoT Network in 2023 Second International Conference on Informatics (ICI). *IEEE;* 2023:1-6. DOI: 10.1109/ICI60088.2023.10420869.
 29. Sousa DAL, OKey OD, Rosa RL, Saadi M, Rodriguez DZ. A Novel Resource Allocation in Software-Defined Networks for IoT Application in 2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). *IEEE,* 2023, p. 1-5. DOI: 10.23919/SOFTCOM55756.2023.10000000.
 30. Restuccia F, D'oro S, Melodia T. Securing the internet of things in the age of machine learning and software-defined networking. *IEEE Internet Things J.* 2018;5(6):4829-4842. DOI: 10.1109/JIOT.2018.2849079.
 31. Ibrahim M, *et al.* SDN based DDos mitigating approach using traffic entropy for IoT network. *C. Comput. Mater. Contin.* 2022;70:5651-5665. DOI: 10.32604/cmc.2022.021907.
 32. Sasaki Y. A survey on IoT big data analytic systems: Current and future. *IEEE Internet Things J.* 2021;9(2):1024-1036. DOI: 10.1109/JIOT.2021.3051234.
 33. Dagnaw GA, Tsige SE. Impact of Internet of Thing in developing country: Systematic review. *Internet Things Cloud Comput.* 2019;7(3):65. DOI: 10.11648/j.iotcc.20190703.12.
 34. Thirupathi V, Sandeep CH, Kumar N, Kumar PP. A comprehensive review on SDN architecture, applications and major benefits of SDN. *Int J Adv Sci Technol.* 2019;28(20):607-614.
 35. Caraguay VÁL, Peral A, Lopez BLI, Villalba GLJ. SDN: Evolution and opportunities in the development IoT applications. *Int J Distrib Sens Netw.* 2014;10(5):735142. DOI: 10.1155/2014/735142.
 36. Ahmadvand H, Lal C, Hemmati H, Sookhak M, Conti M. Privacy-preserving and security in SDN-based IoT: A survey. *IEEE Access.* 2023;11:44772-44786. DOI: 10.1109/ACCESS.2023.3267764.
 37. Brous M, Janssen M, Herder P. The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *Int. J Inf Manag.* 2020;51:101952. DOI: 10.1016/j.ijinfomgt.2019.05.008.
 38. Aziz IT, Abdulqadder IH. An overview on SDN and NFV security orchestration in cloud network environment. *Cihan Univ Sci J.* 2021;5(1):20-27. DOI: 10.24086/cuesj.v5n1y2021.pp20-27.
 39. Udoh IS, Kotonya G. Developing IoT applications: Challenges and frameworks. *IET Cyber-Physical Syst. Theory Appl.* 2018;3(2):65-72. DOI: 10.1049/iet-cps.2017.0068.
 40. Khalaf R, Mohammed A, Essa E, Ali H. Controlling smart home activities Using IoT in 2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA). *IEEE;* 2019:1-6. DOI: 10.1109/ICCISTA.2019.8830664.
 41. Zakia U, Ben Yedder H. Dynamic load balancing in SDN-based data center networks in 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). *IEEE;* 2017:242-247. DOI: 10.1109/IEMCON.2017.8117206.
 42. Dedeoglu V, *et al.* Blockchain technologies for Iot in Advances in Applied Blockchain Technologies. *Springer,* 2020, p. 55-89. DOI: 10.1007/978-981-13-8775-3_3.
 43. Prasad JR, Bendale SP, Prasad RS. Semantic internet of things (IOT) interoperability using software defined network (SDN) and network function virtualization (NFV) in Semant. *IoT Theory Appl. Interoperability, Proven. Beyond.* 2021:399-415.
 44. Dhall D, Kaur R, Juneja M. Machine learning: A review of the algorithms and its applications. *Proc. ICRIC 2019 Recent Innov. Comput,* 2020, p. 47-63.
 45. Shankaraiah S, Shashank S. Software-Defined Networking Security System Using Machine Learning Algorithms and Entropy-Based Features in Sustainable Communication Networks and Application: *Proceedings of ICSCN 2021.* Springer, 2022, p. 507-520.
 46. Mahesh B. Machine learning algorithms-a review. *Int J Sci Res (IJSR).* 2020;9(1):381-386.
 47. Al-Hwaidi ORJ. A new software defined networks (SDN) in IoTs based deep learning techniques

- [Internet]. 2023. Altınbaş Üniversitesi/Lisansüstü Eğitim Enstitüsü.
48. Rashidi HH, Tran NK, Betts EV, Howell LP, Green R. Artificial intelligence and machine learning in pathology: The present landscape of supervised methods. *Acad Pathol.* 2019;6:2374289519873088. DOI: 10.1177/2374289519873088.
 49. Qin Z, Denker G, Giannelli C, Bellavista P, Venkatasubramanian N. A software defined networking architecture for the internet-of-things in 2014 IEEE network operations and management symposium (NOMS). *IEEE*, 2014, p. 1-9. DOI: 10.1109/NOMS.2014.6838365.
 50. Siddiqui S, *et al.* Toward software-defined networking-based IoT frameworks: A systematic literature review, taxonomy, open challenges and prospects. *IEEE Access.* 2022;10:70850-70901. DOI: 10.1109/ACCESS.2022.3188311.
 52. Koroniotis N, Moustafa N. Enhancing network forensics with particle swarm and deep learning: The particle deep framework. *ArXiv preprint arXiv:2005.00722* [Internet]. 2020. Available from: <https://doi.org/10.48550/arXiv.2005.00722>
 53. Askarinejadamiri Z, Nourani N, Zanjani N. Comparative Study of Data Transfer in SDN Network Architecture in IoT. *Int. J Web Res.* 2023;6(1):95-104. DOI: <https://doi.org/10.22133/ijwr.2024.421267.1186>
 54. Nasteski V. An overview of the supervised machine learning methods. *Horizons.* 2017;4:51-62. DOI: 10.20544/HORIZONS.B.04.1.17.P05
 55. Bzdok D, Krzywinski M, Altman N. Machine learning: a primer. *Nat Methods.* 2017;14(12):1119. DOI: <https://doi.org/10.1038/nmeth.4526>
 56. Andersson V. Machine Learning in Logistics: Machine Learning Algorithms: Data Pre-processing and Machine Learning Algorithms [Internet], 2017.
 57. Li J, Zhao Z, Li R. A machine learning based intrusion detection system for software defined 5G network. *ArXiv preprint arXiv:1708.04571* [Internet], 2017. Available from: <https://doi.org/10.48550/arXiv.1708.04571>
 58. Abdulqadder IH, Zou D, Aziz IT, Yuan B. Enhanced attack aware security provisioning scheme in SDN/NFV enabled over 5G network in 2018 27th International Conference on Computer Communication and Networks (ICCCN). *IEEE*; 2018:1-9. DOI: <https://doi.org/10.1109/ICCCN.2018.8487339>
 59. Fabris F, Magalhães DJP, Freitas AA. A review of supervised machine learning applied to ageing research. *Biogerontology.* 2017;18:171-188. DOI: 10.1007/s10522-017-9683-y
 60. Alwahedi F, Aldhaheeri A, Ferrag MA, Battah A, Tihanyi N. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet Things Cyber-Physical Syst.* 2024. DOI: 10.1016/j.iotcps.2023.12.003
 61. Tyagi K, Rane C, Sriram R, Manry M. Unsupervised learning in Artificial Intelligence and Machine Learning for Edge Computing. *Elsevier*, 2022, p. 33-52. DOI: <https://doi.org/10.1016/B978-0-12-824054-0.00012-5>
 62. Dike HU, Zhou Y, Deveerasetty KK, Wu Q. Unsupervised learning based on artificial neural network: A review in 2018 IEEE International Conference on Cyborg and Bionic Systems (CBS). *IEEE*; 2018:322-327. DOI: <https://doi.org/10.1109/CBS.2018.8612259>
 63. Shakya AK, Pillai G, Chakrabarty S. Reinforcement learning algorithms: A brief survey. *Expert Syst Appl.* 2023;231:120495. DOI: <https://doi.org/10.1016/j.eswa.2023.120495>
 64. Jordan Y, Chandak Y, Cohen D, Zhang M, Thomas P. Evaluating the performance of reinforcement learning algorithms in International Conference on Machine Learning. *PMLR*, 2020, p. 4962-4973. DOI: 10.5555/3454287.345442.