International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group| Volume 7 Issue 1 PP 30-37, 2026
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V7I1P105

Original Article

Review: Software-Defined Networking (SDN) for IT Operations: Use Cases, Benefits, and Challenges

Niravkumar Prajapati
Independent Researcher.

Received On: 24/11/2025 ***Revised On: 28/12/2025*** ***Accepted On: 03/01/2026*** ***Published On: 11/01/2026***

Abstract - *The data plane and control plane are kept apart in a novel approach to network management called Software-Defined Networking (SDN). This lets one person control the networks from one place and makes them easier to program. This paper is a review of SDN evolution, architecture and its integration to the Network Function Virtualization (NFV) and its application in IT operations including data centre management, network security, and new technologies including 5G. The study is able to synthesize the main characteristics such as centralized management, automation, scalability, and improved security, as well as present the practical advantages such as agility, cost effectiveness and simplified network administration. Secondly, the paper looks at technical issues such as scalability of controllers, and compatibility with older systems as well as the vulnerability of centralized systems that impede its broad adoption. A review of the recent literature provides a variety of solutions such as traffic analysis frameworks and energy-conscious models up to blockchain-fathered security and distributed control, but most of them are oriented on a single point. This review, through its consolidation of these findings, reveals that there are gaps in the research and that holistic, adaptive, and interoperable SDN frameworks are necessary to support resilient and intelligent IT infrastructures.*

Keywords - *Software-Defined Networking (SDN), network programmability, network security, 5G, IT operation.*

1. Introduction

The networks used today are very complicated because every day, more and more devices connect to them and access more and more information. Detection of Intrusion. It's hard for one network supervisor to handle systems, switches, firewalls, and load balancers all by themselves. What they need is software-defined networking to fix this issue. The way they used to run the networks has changed because of it. The two types of Software-Defined Networking (SDN) work well together but are not mutually dependent. Network Function Virtualisation (NFV) is used to plan, manage, and separate network activities. Network services like Intrusion Detection System (IDS), Domain Name Services (DNS), and Network Address Translation (NAT) cannot work without NFV [1]. They need their own devices to run. Software-defined networking (SDN) simplifies the network, which makes it easier to program [2]. Because SDN technology can be programmed, it's easy for network managers and engineers to make new network apps and add them to the network. This gives the network more freedom [3]. Fig. 1 shows that SDN offers a number of security supports, but it also improves the automated networking control operations for policy definitions and routing.

Additionally, SDN's design lets the SDN manager see the whole network. The crucial part of the network is the processor, which acts as its brain. The part of the network that makes choices and collects smart data is called the SDN Controller. Viewing the whole network from one place makes it easy to come up with and apply important solutions like link failure, traffic engineering, and load-balancing. The goal of IT Operation Management is to make sure that all tasks and processes that rely on IT Services and IT Infrastructure [5], [6]. IT services are necessary for every business task [7]. IT Service Management is in charge of "anything that needs to be managed in order to deliver an IT service." It also manages systems and services.

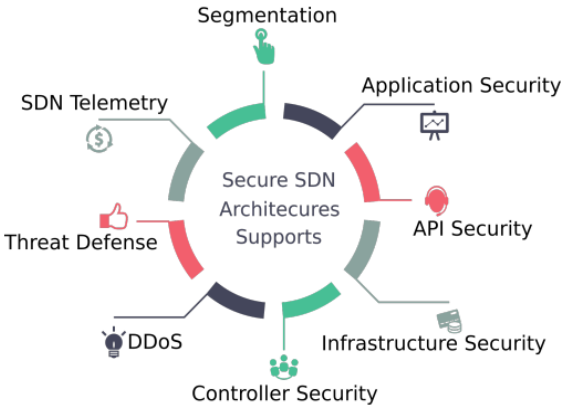

Fig 1: Security Support Provided by Secure SDN Technology [4]

1.1. Structure of the paper

The following is the paper's format: Section II presents an overview of SDN and its architecture. Section III highlights key SDN features relevant to IT operations. Section IV discusses major use cases. Section V outlines the benefits of SDN in IT operations, while Section VI examines the technical challenges associated with its adoption. Section VII provides a literature review and identifies existing gaps. Finally, Section VIII closes the report with noteworthy findings and recommendations for further research.

2. Overview of Software-Defined Networking (SDN)

An innovative approach to network design, software-defined networking (SDN) isolates control plane logic from routing plane logic [8]. SDN is a novel approach to network construction that differs from proprietary specified interfaces and locked boxes. When it knows how to design a network, it can leverage software's open interfaces to instantly manage, alter, and control network behavior [9]. The SDN structure lets it manage the whole data path from a single location, regardless of the network technology used to link the devices, which could be made by different companies. The main control has all the smarts and keeps an eye on the whole network, the data path, and the links that connect the different parts. Because this view is centralised and always up to date, the manager can manage the network and make simple changes to how it works through the centralised control plane. SDN design was first proposed by the ONF [10]. Since then, different groups have come up with their own versions to fit their needs. Furthermore, this design is the most well-known design in numerous areas, as seen in Fig. 2. From north to south, SDN is made up of the application plane, the control plane, and the data plane.

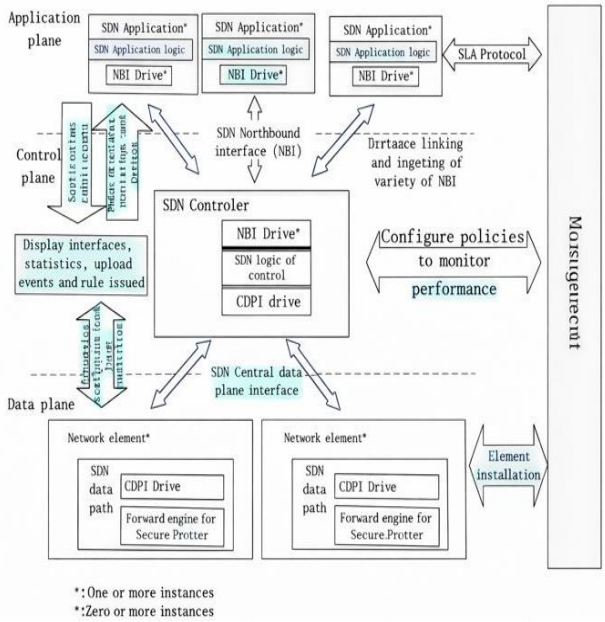

Fig 2: Software-Defined Networking Architecture

- People who work with networks, like switches, make up the data plane. Its major jobs are to process data, send it to other places, and collect status updates. Methods for devices to link to data on networks are available for completion of data forwarding.
- The southbound link lets the control plane talk to the data plane. The manager giving information about the data plane's devices lets the control plane set up the data plane's resources. In the meantime, the controller in this layer tries to abstract the distributed network of the data plane network device in order to support the SDN controller on the whole network of information unified setup control [11].
- Once the manager calls a certain network path through CDPI, it gives different users editable NBIs to make the application fit their needs and accomplish the logical management of the network.

2.1. Application of SDN in it operation

SDN Applications are computer programs that tell the SDN Controller through NBIs what their network needs and how they want it to behave. Additionally, they may use a simplified version of the network to help them make decisions internally. Although it is technically centralised, the SDN Controller is in charge of:

- Translating what the SDN Application layer needs into what the SDN Data paths need.
- A general picture of the network is given to the SDN applications. As a logical network device, the SDN Data path lets us see and have full control over its data processing and forwarding features. It's possible for the logical representation to include all or some of the actual substrate resources. An SDN data path is made up of a and functions, which may include simple passing between the functions of the data nation. There may be more than one SDN Data path in a single physical network element. This is a group of communications tools that are managed as a single unit. Parts of the network.

3. Key Features of SDN for It Operations

There are a lot of new ideas about SDN all the time. This part looks at some of the architectures, frameworks, and solutions that academics have come up with to deal with new problems in IT operation. It includes the parts, how they work together, and how they talk to each other [12]. Sets of rules, protocols, and tools called frameworks and solutions make making a system more organized. The material on SDN-IT operation systems is compared in Table based on architectures, models, frameworks, and solutions which were used.

3.1. Centralized Management

Using SDN) for Efficient Network Management means getting together the study results and explaining what they mean. SDN isolates the control plane and the data plane, which modify the management of networks considerably [13]. This is due to the ease of management and programming involved. The study examined various aspects of SDN, primarily the way it can enhance the performance, extensibility, and liberation of networks.

3.2. Network Automation

The future industrial network will connect a number of various types of industrial tools in one or more locations that can vary over time. An IP-based network structure should be used instead of the current mixed hierarchical localised network structure to make FOR easier [14]. This will make it easy to map data and make real-time communications more flexible. As the jobs that need to be done change, so do the production methods and machines that are used to do them.

So, in the future, networks in factories should use SDNs to allow for flexible design. The present study addresses a knowledge vacuum by using SDN and IP-based networking to the context of industrial automation. There will be more programming freedom, but the features and functions needed for real-time interactions will still be there.

3.3. Dynamic Scalability

Dynamic network slicing and the resource allocation problem as a game of forming overlapped coalitions with random outcomes. The model shows that the total amount of computing power goes up if fog nodes think about a belief function about the other fog nodes' unknown states and secret information. Xiao and Krum find the best way to slice a dynamic network using a belief-state partially visible Markov decision process. Number-based tests using information from 400 base stations in a real cellular network show that when each fog node works with its nearest partner, the amount of work it can do almost doubles.

3.4. Improved Security

Network tracking is one of the most important parts of keeping a network safe. Getting real-time data from the network and using different anomaly detection methods to look for security holes in it is one way to find data that shows strange traffic patterns. When someone wants to hack a network, they might first use scanning tools to get a feel for how it works [15], [16], [17]. It becomes more important to keep an eye on the network now. This is a normal open flow process in SDN. Watching a network based on open flow means collecting data based on flow at the controller level. Two times, one through the push action and one when a switch tells the processor that the flow has stopped.

5. Use Cases of SDN in IT Operations

Open Flow started to be used in places other than campuses for SDN use cases, like datacentre networks, where it was clear that traffic needed to be managed on a large scale. They said that SDN/Open flow "was born on campus and grew up in the data centre" because of this. Some ideas from earlier work on separating the control and data planes are used in Open Flow. However, the rise of Open Flow brought about a number of new ideas.

5.1. Data Centre Management

- Managing networks and changing how well they work is hard because of this, and things can go wrong. An additional issue that network managers and researchers are working to fix is the Traditional Data Centre Network (DCN). Increasing traffic and client numbers make it harder to set up. The biggest issues with standard DCN are that they can only handle a certain amount of traffic and the infrastructure is only used for one thing. Therefor, setting up and watching over new gadgets is very hard. Furthermore, some network resources are being used less and less because of static routes.
- This happens because the number of apps, websites, and storage space is growing so quickly [18]. Because of these problems, Software-Defined Networking (SDN) built on the OpenFlow Data Centre network architecture was created to improve performance metrics and support traffic engineering, such as load balancing. For less network congestion, the load balancing function spreads the traffic among the servers that are linked.

5.2. Network Security

- The development and deployment of SDN infrastructure and services could lead to improvements in network security based on six features [19]. It is easier to build more secure and reliable SDN applications or infrastructure when these traits are identified [20]. After looking at different study papers.

6. Benefits of SDN in IT Operations

The limitations of traditional networking are countered by the numerous benefits of Software-Defined Networking (SDN) [21]. SDN facilitates the more efficient, less costly and secure management of networks through increased programmability, flexibility and centralized control. This section lists the key benefits of SDN.

6.1. Agility and Flexibility

SDN enhances the responsiveness and flexibility of the network to new situations and changing business requirements by enabling dynamically configured and responsive networks:

- Dynamic Network Configuration: SDN eliminates the fact of human intervention by allowing configuration of network on the fly. This capacity is necessary in environments such as data centres and cloud services that require high amounts of changes [22].
- Scalability: SDN helps in making the network resources more demand-responsive. This is particularly useful in the case of clouds where resources have to be distributed on-demand to accommodate various types of workloads.
- Service Innovation: The programmability of SDN allows one to design and deploy new network services and applications very quickly, giving companies the ability to respond quickly to opportunities and market changes.

6.2. Cost Efficiency

Both capital expenses (CapEx) and operating expenditures (OpEx) may be reduced because to SDN:

- Reduced Hardware Costs: SDN allows the use of commodity devices to implement network devices by separating the control plane and the data plane. This reduces the purchase of expensive and exclusive hardware.
- Lower Operational Costs: Centralized management and automation systems of SDN remove the necessity of human configuration and maintenance, which leads to lower operating costs. Automated processes can take over routine tasks and IT staff can focus on more critical projects.

- Energy Efficiency: Saving energy via optimized resource utilization and dynamic network resource allocation makes SDN more cost-effective and ecologically beneficial.

6.3. Enhanced Security

SDN enhances network security by means of dynamic policy enforcement, improved visibility, and centralized control:

- **Centralized Security Policies:** SDN enables centralized security rules to be deployed which can consistently be applied in the entire network. This will ensure the uniform protection and eases the regulatory compliance.
- **Real-Time Threat Detection and Mitigation:** The SDN controllers can immediately detect and resolve security problems due to their global network view [23]. They can take proactive actions, including isolating affected areas or diversion of traffic to avoid susceptible areas [24].
- **Micro-Segmentation:** SDN minimizes the attack surface and prevents near-term lateral mobility within the network, through allowing fine-grained network segmentation. This micro-segmentation capabilities enhance network security in general.

6.4. Simplified Network Management

SDN streamlines network administration by automating and centralizing control:

- Centralized Network View: SDN provides network managers with a centralized perspective of the entire network, and thereby, makes it easier to monitor, manage, and to troubleshoot. This is an inclusive perspective, which simplifies the process of identifying and correcting network issues [25].
- Automation of Routine Tasks: SDN automation of routine management operations such as policy enforcement, updates as well as configuration changes. This reduces the risk of a human error and decreases the administrative burden.
- Policy-Based Management: SDN allows policy-based network management, in which managers can specify high-level rules that can be immediately translated into specific configurations and actions. This approach ensures uniformity and speed of network operations.

Software-Defined Networking benefits are diverse, including the ability to achieve better agility, lower costs, increased security, greater network performance, easier management, and an innovation platform. These strengths make SDN an interesting option in the contemporary network settings and overcome the difficulties of conventional networking and establish the path towards more dynamic, efficient, and secure networks. With SDN still being embraced by organizations, companies can look forward to tremendous gains in their network processes and business outcomes [26].

7. Technical Challenges of SDN

Although Software-Defined Networking (SDN) has many advantages, it has a number of challenges that should be overcome to make the most out of its potential. Also, SDN is evolving constantly, and new trends define its future [27]. Table I explains the most important challenges related to SDN deployment and adoption, and the most recent trends that will have an impact on its development.

Table 1: Key Challenges in Software-Defined Networking (SDN) Adoption and Deployment [28]

Challenge Category	Sub-Challenge	Description
Scalability	Controller scalability	A key issue that arises on the expansion of networks is ensuring that the SDN controller is capable of handling increased loads without affecting the performance. Real-time processing and management of enormous volumes of data necessitates scalable and reliable systems from controllers.
	Network size and complexity	Scalability issues arise in large-scale networks, particularly in data centres and service provider settings. It may be challenging to provide consistent performance and dependability across a large number of devices and connections.
Interoperability	Legacy system integration	The integration of SDN and legacy infrastructure is complicated and time-intensive and needs a mechanism to maintain smooth coexistence between SDN-enabled and traditional devices.
	Vendor diversity	Variations in vendor implementations of SDN protocols and APIs can lead to compatibility issues, emphasizing the need for standardized and interoperable solutions.
Security Concerns	Controller vulnerabilities	The SDN centralized control poses a possible single point of failure; failure to secure the controller may jeopardize the whole network, so the controller must be highly secured.
	Data plane attacks	SDN opens up new attack points, especially in controller–data plane communication channels, which should be secured by avoiding interception and manipulation.
	Policy management	Managing consistent and scalable security policies across large SDN deployments becomes increasingly complex and requires advanced policy enforcement mechanisms.

Transition Complexity	Skill gaps	Adoption of SDN demands new technical skills, requiring network administrators and engineers to undergo training for effective design and management.
	Operational disruptions	A switch to SDN may lead to service interruptions because it requires moving off the old networks, which means that it should be done in stages and with proper planning.
Reliability and Resilience	Failover mechanisms	High availability and rapid recovery from failures require robust controller redundancy and failover strategies.
	Network performance	Maintaining stable performance under dynamic traffic and load conditions necessitates continuous monitoring and adaptive optimization tools.

8. Literature Review

Numerous studies have been conducted that provide ways to enhance network security via the use of the SDN technique. Yang et al. (2025) adopt software-defined networking (SDN) technology to implement an EVPN-VXLAN architecture. Prior works either targeted data center networks (instead of geo-distributed sites) or used low-throughput virtualized switches. By contrast, the proposed approach targets geo-dispersed sites and uses P4 switches to accelerate data-plane performance. The approach integrates SDN host detection and EVPN host learning mechanisms for efficient host tracking and ARP suppression. It also supports Multi-Tenancy and Distributed Anycast Gateway (DAG). Experimental results demonstrate enhanced User Plane efficiency and reduced host communication latency [29].

Shah et al. (2024) propose FAST (Framework for analysing SDN traffic), SDN-clustering based mechanism. In their proposed approach i.e, FAST, Ensemble Learning (EL) implemented mainframe SDN controller works as the central entity for analyzing incoming traffic and diverting it to its respective SDN cluster. In this configuration, each cluster, equipped with limited yet efficient single-domain working SDNs can process a particular type of data and enhance the overall system performance dynamically. The performance evaluation of FAST includes precision, recall, f1-score and accuracy comparison between Machine Learning (ML) and EL algorithms as well as ROCcurve, Precision-Recall(PR) curve and Confusion Matrix [30].

Kondo et al. (2023) considers the energy-efficiency aspect of the network infrastructure to solve the CPP. To do so, it designed a model that includes delay constraints, whose effectiveness was assessed and confirmed to save about 20-30% more energy than a model that only considers the number of controllers. Moreover, it is confirmed that execution time can be decreased by 100 times while keeping the energy consumption low by reducing the number of pre-calculated paths between the SDN switches and the controllers [31].

Cheng (2023) examines blockchain technology in depth, with an emphasis on its potential applications in SDN, network security, and networking protocols, as well as its advantages and future prospects in these areas. By allowing safe, verifiable, and auditable contact and transactions, block chain could make computer networks more trustworthy and open. Furthermore, by enabling automated and decentralized network control, resource sharing, and orchestration, blockchain technology may simplify SDN management. Furthermore, it learns that blockchain technology may assist with network problems such as lowering DDoS assaults, enhancing intrusion detection and security, and maintaining the security of the routing protocol [32].

Giarré, Cominardi and Casari (2022) look at a distributed and decentralised approach to the SDN paradigm. They use the Zenoah framework to aim for zero-configuration scalability and transparency. As an east-west bound protocol for SDNs, Zen oh is looked at, and its performance is compared to that of a highly coupled HTTP-based option. Based on their tests, Zenoah's ability to handle distributed queries makes it possible for their SDN design to grow to hundreds of SDN controllers with no extra configuration work needed. It also supports fast east-west query throughput [33].

Gaur et al. (2021) discuss standard networks, Software Defined Networking (SDN), its layout, common controllers, topologies, and security issues that come up with SDN. SDN makes networks more programmable. SDN is built on three levels. The most popular protocol used to connect the control layer to the physical layer is OpenFlow Protocol. This protocol provides what are known as southbound APIs [34].

Table 2: Summary of Recent Studies on Software-Defined Networking Techniques and Applications

Author	Tools / Techniques	Focus	Key Contribution	Challenges	Future Work
Yang et al. (2025)	SDN, EVPN-VXLAN, P4 programmable switches	Geo-distributed network virtualization	Designed an SDN-based EVPN-VXLAN architecture using P4 switches to improve data-plane efficiency, reduce latency, and support multi-tenancy and DAG.	Deployment complexity and interoperability with legacy SDN devices.	Large-scale deployment validation and cross-vendor interoperability analysis.
Shah et al. (2024)	SDN clustering, Ensemble Learning, FAST	SDN traffic analysis	Proposed a clustered SDN traffic analysis framework leveraging ensemble	Increased system complexity and controller	Scalability evaluation under ultra-high traffic and

	framework		learning to enhance detection accuracy and performance.	coordination overhead.	real-time deployment.
Kondo et al. (2023)	Energy-aware SDN modeling, Controller Placement Problem (CPP)	Energy-efficient SDN control plane	Introduced a delay-constrained CPP model achieving 20–30% energy savings and significant execution time reduction.	Limited consideration of network failures and dynamic traffic conditions.	Extension to fault-tolerant and adaptive controller placement models.
Cheng (2023)	Blockchain, SDN, Network security frameworks	Secure and decentralized SDN	Analyzed blockchain integration in SDN to enhance security, transparency, and resistance to DDoS and routing attacks.	High computational overhead and latency introduced by blockchain operations.	Lightweight blockchain designs and performance-aware SDN integration.
Giarré et al. (2022)	Distributed SDN, Zenoah framework, East-West protocols	Scalable SDN control plane	Demonstrated a decentralized SDN architecture enabling zero-configuration scalability across hundreds of controllers.	Increased coordination complexity among distributed controllers.	Integration with data-plane optimization and fault-management mechanisms.
Gaur et al. (2021)	SDN architecture, OpenFlow, Southbound APIs	SDN fundamentals and security	Provided a comprehensive overview of SDN architecture, protocols, and associated security challenges.	Lacks quantitative evaluation and implementation-level insights.	Experimental validation of security mechanisms and emerging SDN protocols.

8.1. Research gap

Despite the recent developments in the area of SDN architecture and optimization strategies, as summarized in Table II, a number of research gaps are still obvious. The majority of the literature concentrates on improving individual features like data-plane acceleration, traffic analysis, energy efficiency, security or control-plane scalability, as opposed to offering a comprehensive and holistic SDN implementation. Very little validation is done in large, heterogeneous and geo-distributed settings, and little or no emphasis is placed on real world implementation in simulations or small testbeds. Also, upcoming solutions featuring programmability on P4, ensemble learning, and blockchain create an even greater complexity, overhead, and interoperability issues that are not thoroughly assessed. There is under exploration of issues associated with dynamic adaptability, fault tolerance, multi-tenancy, and cross-domain coordination. These gaps represent that there is a high demand of unified, scaled and experimentally verified SDN architectures that collectively meet the performance, energy efficiency and security needs.

9. Conclusion and Future Work

SDN is a paradigm change in IT operations that enables programmability, centralized control, and dynamic scalability due to the control and data planes' separation. This review has revealed that SDN has a variety of applications including data centre control, security in the network, and integration into other emerging technologies like 5G and provided the advantages in agility, cost-effectiveness and easier network management. Nevertheless, the problems still exist, such as the scale of controllers, compatibility with the existing systems, and weaknesses in centralized architectures, which draw the focus to the development of powerful solutions. As shown in the literature review, the recent works assume the separation between aspects traffic analysis, energy efficiency, blockchain-based security, or distributed control and do not consider them as a part of a single scheme, which creates a research gap. The potential of SDN can be fully achieved only by further studies with the attention to holistic methods of combining performance optimization, resilience, and security and using emerging technologies, including blockchain, fog/edge computing, and AI-based automation. These gaps can be filled in to transform SDN into an industry-ready solution that can support intelligent, secure, and resilient IT infrastructures.

References

[1] V. Prajapati, “Advances in Software Development Life Cycle Models: Trends and Innovations for Modern Applications,” *J. Glob. Res. Electron. Commun.*, vol. 1, no. 4, pp. 1–6, 2025.

[2] M. Menghnani, “Modern Full Stack Development Practices for Scalable and Maintainable Cloud-Native Applications,” *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 2, 2025, doi: 10.5281/zenodo.14959407.

[3] T. Semong *et al.*, “A review on Software Defined Networking as a solution to link failures,” *Sci. African*, vol. 21, p. e01865, 2023, doi: https://doi.org/10.1016/j.sciaf.2023.e01865.

[4] M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash, and M. Shaheed, “SDN Security Review: Threat Taxonomy, Implications, and Open Challenges,” 2022. doi: 10.1109/ACCESS.2022.3168972.

[5] S. Singh, “Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion

Detection and Mitigation," in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

[6] S. P. Kalava, "Enhancing Software Development with AI-Driven Code Reviews," *North Am. J. Eng. Res.*, vol. 5, no. 2, pp. 1–7, 2024.

[7] S. Phalke, Y. D. Athave, and B. N. Ilag, "A Multi-Layered Approach to IT Infrastructure Governance and Compliance: Security, Hardening, and Audit Readiness," *Int. J. Comput. Appl.*, vol. 187, no. 12, p. 9, 2025, doi: 10.5120/ijca2025925133.

[8] A. Hakiri, A. Gokhale, P. Berthou, D. Schmidt, and T. Gayraud, "Software-Defined Networking: Challenges and research opportunities for Future Internet," *Comput. Networks*, vol. 75, 2014, doi: 10.1016/j.comnet.2014.10.015.

[9] S. Singh, "Enhancing Observability and Reliability in Wireless Networks with Service Mesh Technologies," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 1, 2025, doi: 10.48175/568.

[10] S. S. S. Thangavel and K. C. Sunkara, "Software-Defined Networking (SDN) in Cloud Data Centers: Optimizing Traffic Management for Hyper-Scale Infrastructure," *Int. J. Emerg. Trends Comput. Sci. Inf. Technol.*, 2022.

[11] P. Chandrashekar, "Enhancing Software Application Efficiency Through Design-Centric Methodologies: An Empirical Evaluation," *ESP J. Eng. Technol. Adv.*, 2022, doi: 10.56472/25832646/JETA-V2I1P122.

[12] V. Pillai, "Anomaly Detection in Financial and Insurance Data-Systems," *J. AI-Assisted Sci. Discov.*, vol. 4, no. 2, 2024.

[13] B. Shalom, "Software-Defined Networking (SDN) for Efficient Network Management," *Int. J. Comput. Eng.*, vol. 6, no. 1, pp. 1–13, 2024, doi: 10.47941/ijce.2056.

[14] K. Ahmed, J. O. Blech, M. A. Gregory, and H. W. Schmidt, "Software Defined Networks in Industrial Automation," *J. Sens. Actuator Networks*, vol. 7, no. 3, 2018, doi: 10.3390/jsan7030033.

[15] S. Chatterjee, "Integrating Identity and Access Management for Critical Infrastructure : Ensuring Compliance and Security in Utility Systems," *Int. J. Innov. Res. Creat. Technol.*, vol. 8, no. 2, pp. 1–8, 2022.

[16] K. Rajchandar, M. Ramesh, A. Tyagi, S. Prabhu, D. S. Babu, and A. Roniboss, "Edge Computing in Network-based Systems: Enhancing Latency-Sensitive Applications," in *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, 2024, pp. 462–467. doi: 10.1109/IC3I61595.2024.10828607.

[17] J. Thomas, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.

[18] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *J. Glob. Res. Electron. Commun.*, vol. 2, no. 2, pp. 1–7, 2025, doi: 10.5281/zenodo.14955016.

[19] S. S. S. Neeli, "Optimizing Database Management with DevOps: Strategies and Real-World Examples," *J. Adv. Dev. Res.*, vol. 11, no. 1, 2020.

[20] A. Ajiya Ahmad, S. Boukari, A. Musa Bello, M. Alhaji Madu, and adatu Gimba, "A Review on Software Defined Network (SDN) Based Network Security Enhancements," *Quest Journals J. Softw. Eng. Simul.*, vol. 7, no. 9, pp. 2321–3809, 2021.

[21] V. Kumar, R. Kumar, and S. K. Pandey, "A secure and robust group key distribution and authentication protocol with efficient rekey mechanism for dynamic access control in secure group communications," *Int. J. Commun. Syst.*, vol. 33, no. 14, Sep. 2020, doi: 10.1002/dac.4465.

[22] S. Narang and V. G. Kolla, "Next-Generation Cloud Security: A Review of the Constraints and Strategies in Serverless Computing," *Int. J. Res. Anal. Rev.*, vol. 12, no. 3, pp. 1–7, 2025, doi: 10.56975/ijrar.v12i3.319048.

[23] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 584–591, Dec. 2023, doi: 10.14741/ijcet/v.13.6.11.

[24] G. Sarraf, "Behavioral Analytics for Continuous Insider Threat Detection in Zero-Trust Architectures," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 596–602, 2021.

[25] Dhruv Patel and Ritesh Tandon, "Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control and Authentication," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 749–758, Dec. 2022, doi: 10.48175/IJARSCT-7744D.

[26] S. Barman, P. Gupta, and S. Kashiramka, "Project Management Survey: A Review of Software Project Management Methodologies," in *2024 IEEE 11th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/UPCON62832.2024.10983518.

[27] S. Garg, "Next-Gen Smart City Operations with AIOps & IoT : A Comprehensive look at Optimizing Urban Infrastructure," *J. Adv. Dev. Res.*, vol. 12, no. 1, 2021.

[28] N. Shaik and D. C. K. Priya, "Navigating the Future: Unraveling the Potential of Software-Defined Networking," *Int. J. Res. Publ. Rev.*, pp. 2580–2590, Jun. 2024, doi: 10.55248/gengpi.5.0624.1504.

[29] Y. C. Yang, Z. Y. Jin, L. H. Yen, and C. C. Tseng, "SDN-Enabled EVPN-VXLAN With P4 Accelerated User Plane," in *APNOMS 2025 - 25th Asia-Pacific Network Operations and Management Symposium: Towards Smarter and Pervasive Management in the Era of 6G Networks*, 2025. doi: 10.23919/APNOMS67058.2025.11181298.

[30] D. Shah *et al.*, "FAST: AI-based Network Traffic Analysis and Load Balancing Framework Underlying SDN Clusters," in *Proceeding of 8th International Conference on Smart Cities, Internet of Things and Applications, SCIoT 2024*, 2024. doi: 10.1109/SCIoT62588.2024.10570111.

[31] T. Kondo, L. Guillen, S. Izumi, T. Abe, T. Mizuki, and T. Suganuma, "An Energy Efficient SDN Controller Placement with Delay Constraints," in *APNOMS 2023 - 24th Asia-Pacific Network Operations and Management Symposium: Intelligent Management for Enabling the*

Digital Transformation, 2023.

[32] M. J. Hossain Faruk and J. Q. Cheng, "Integration of Blockchain in Computer Networking: Overview, Applications, and Future Perspectives for Software-defined Networking (SDN), Network Security, and Protocols," in *2023 Tenth International Conference on Software Defined Systems (SDS)*, 2023, pp. 20–27. doi: 10.1109/SDS59856.2023.10329025.

[33] F. Giarré, L. Cominardi, and P. Casari, "Realizing Flat Multi-Zone Multi-Controller Software-Defined Networks using Zenoh," in *2022 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2022, pp. 45–51. doi: 10.1109/NFV-SDN56302.2022.9974876.

[34] K. Gaur, P. Choudhary, P. Yadav, A. Jain, and P. Kumar, "Software Defined Networking: A review on Architecture, Security and Applications," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1099, no. 1, p. 012073, Mar. 2021, doi: 10.1088/1757-899X/1099/1/012073.