REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 9 | ISSUE - 7 | APRIL - 2020

SOFTWARE-DEFINED NETWORKING FOR INTERNET OF THINGS: A SURVEY

Pooja Madeppa
Research Scholar

Dr. Shashi
Guide
Professor, Chaudhary Charansing University Meerut.

ABSTRACT

Managing, controlling, and optimizing the network infrastructure that supports the massive volumes of data produced by interconnected devices has become more difficult as a result of the Internet of Things' (IoT) explosive growth. One novel network architecture that has been suggested as a potential remedy for the intricacies of IoT networks is Software-Defined Networking (SDN). IoT environments with dynamic, heterogeneous, and large-scale devices require centralized network management, programmability, and flexibility, all of which SDN makes possible by separating the control plane from the data plane. The integration of SDN with IoT is examined in this survey, along with how it might improve network performance, security, resource management, and scalability. We examine several SDN-based strategies for the Internet of Things, stressing their advantages, difficulties, and potential to resolve important problems like network congestion, interoperability, and effective routing. We also go over how SDN will help future IoT applications like industrial automation, smart cities, and healthcare. This paper intends to educate academic and industry stakeholders on the feasibility of SDN in the context of the Internet of Things and the future course of innovations in this field by offering a thorough summary of the state of research and developments to date.

KEYWORDS: *Software-Defined Networking, Internet of Things, Network Architecture, Scalability, Resource Management, Network Security, Performance Optimization, IoT Applications, Smart Cities, Healthcare, Industrial Automation, Data Plane, Control Plane, Centralized Management, Interoperability, Efficient Routing.*

INTRODUCTION

The Internet of Things' (IoT) explosive growth is changing how we engage with the physical world by tying together billions of devices that share data to improve our daily lives. Smart cities, smart homes, industrial automation, healthcare, and agriculture are just a few of the many industries that use IoT applications. IoT networks can be very challenging to manage, especially when it comes to scalability, flexibility, security, and resource management, despite their enormous potential. IoT deployments that are dynamic, extensive, and diverse present challenges for traditional networking techniques, which were created for more static environments.

By making network management more flexible and programmable, Software-Defined Networking (SDN) presents a promising answer to these problems. SDN is a cutting-edge network architecture that offers centralized control over the entire network by separating the control plane from the data plane. The complex and quickly changing nature of IoT networks requires dynamic configuration, simpler resource management, and enhanced performance optimization, all of which are made possible by this centralized approach.

Many of the major problems with traditional networking techniques in IoT environments could be resolved by integrating SDN into IoT. IoT networks can gain better scalability, stronger security protocols, and more effective data flow management by utilizing SDN. Additionally, SDN makes it easier for devices and platforms to communicate with one another, which is essential in IoT ecosystems that have a large number of heterogeneous devices.

An overview of the state of research and developments at the nexus of SDN and IoT is given by this survey. We examine the difficulties that SDN can assist in resolving, including resource constraints, network congestion, and security flaws. We also look at the future directions of SDN for IoT, including its role in developing applications like smart cities, healthcare, and industrial IoT, and we discuss different SDN-based frameworks and approaches created to maximize IoT network performance. Our goal in conducting this survey is to provide insight into how SDN can transform the IoT environment and help create more secure, scalable, and effective IoT networks.

AIMS AND OBJECTIVES:

This survey's main goal is to investigate how Software-Defined Networking (SDN) might help Internet of Things (IoT) networks overcome their obstacles. This survey attempts to give a thorough overview of how SDN can improve the performance, scalability, security, and resource management of IoT networks by looking at the intersection of SDN and IoT. The following are the survey's main goals:

1. Examine the Role of SDN in IoT Networks:

to investigate how scalability, network congestion, and dynamic resource allocation can be addressed by integrating SDN into IoT environments. This involves being aware of the advantages and drawbacks of implementing SDN concepts in Internet of Things networks.

2. Identify Key Challenges in IoT Networking:

to determine and examine the particular difficulties that IoT networks encounter, including handling massive devices, guaranteeing effective data transfer, preserving security, and establishing compatibility across various platforms and devices.

3. Evaluate SDN-Based Approaches for IoT:

to examine different SDN-based frameworks and architectures created for Internet of Things applications, and to evaluate how these solutions enhance resource management, optimize network performance, and facilitate effective data transfer between IoT devices.

4. Highlight Security and Privacy Implications:

to look into how SDN can improve IoT network security, with an emphasis on features like intrusion detection systems, dynamic access control, and centralized security management that can help reduce security threats associated with IoT.

5. Explore IoT Applications Leveraging SDN:

to investigate particular IoT applications where SDN has been used or has the potential to revolutionize operational efficiency, network dependability, and service quality, such as smart cities, healthcare, and industrial automation.

6. Present Future Research Directions and Trends:

to discuss possible developments, obstacles, and research opportunities that could further integrate SDN into the changing IoT landscape in order to offer insights into the future direction of SDN for IoT.

By tackling these goals, this survey hopes to advance knowledge of how SDN can facilitate more secure, adaptable, and efficient IoT networks and educate practitioners and researchers on the advantages and disadvantages of implementing SDN for IoT applications.

LITERATURE REVIEW:

Because managing large-scale, heterogeneous, and dynamic IoT networks is becoming increasingly difficult, research has focused heavily on integrating Software-Defined Networking (SDN) with the Internet of Things (IoT). Many of the problems with traditional networking paradigms in IoT environments are thought to be resolved by SDN, which separates the control plane from the data plane and enables centralized control and programmability. The research in this field is summarized in the review that follows, which highlights significant contributions, approaches, and conclusions that address the advantages and difficulties of implementing SDN in IoT networks.

CHALLENGES IN IOT NETWORKS:

The Internet of Things is made up of billions of devices that need to communicate effectively across a variety of protocols and produce enormous volumes of data. One of the main issues facing IoT networks is scalability, given the steadily increasing number of connected devices.

- Congestion in the network brought on by high data volumes and various traffic patterns.
- Communication standards and interoperability across diverse IoT devices.
- Effective management of resources, such as processing power, storage, and bandwidth.
- Security: IoT devices are susceptible to a range of cyberattacks, data breaches, and illegal access.

SDN as a Solution for IoT Challenges:

SDN's programmability and centralized control have made it a viable option for IoT network management. SDN enables dynamic and flexible management by separating the control and data planes, which is crucial for the various and changing needs of IoT environments. For managing the scalability and dynamic nature of IoT networks, the capacity to dynamically modify network paths, distribute resources, and implement network policies in real time is especially helpful.

SDN and IoT Scalability:

The efficient scalability of SDN is one of its major benefits. The increasing number of devices in IoT networks is too much for traditional networking models, which rely on distributed control. With its centralized control architecture, SDN makes managing a large number of IoT devices easier and streamlines network administration. In order to satisfy the requirements of extensive IoT networks, a number of studies have put forth SDN-based solutions that offer effective network path management and adaptive resource allocation. The scalability issues of IoT systems are addressed by centralized control, which enables real-time modifications and optimizations.

Security in SDN-Enabled IoT Networks:

Because there are so many connected devices in IoT networks, security is still a major concern because of the potential for attacks. By providing centralized monitoring and control, SDN enhances security by facilitating the quick identification and elimination of threats like DDoS attacks, intrusion attempts, and unauthorized access. To improve the overall security posture of IoT networks, researchers have suggested SDN-based architectures that integrate security features like encryption, traffic monitoring, and access control. One major benefit for protecting IoT environments is the ease with which security policies can be uniformly enforced throughout the network thanks to SDN's centralized control.

Performance Optimization in SDN-Enabled IoT Networks:

Another area in which SDN is important is performance optimization. Performance optimization in traditional networks can be difficult because of their rigid configurations and lack of adaptability. Based on real-time data, SDN enables network path optimization and dynamic traffic management. IoT networks can attain better quality of service (QoS), lower latency, and better resource utilization by utilizing SDN. Research has shown that SDN can be used to prioritize important traffic in IoT applications, balance network loads, and optimize data flows—all of which improve network performance overall.

Interoperability and Integration:

Interoperability is hampered by the large number of devices in IoT networks, many of which employ disparate communication protocols. By enabling smooth integration across heterogeneous devices and abstracting the underlying network hardware, SDN provides an answer. SDN offers a centralized platform for managing a variety of IoT devices by facilitating communication between devices that use different protocols and standards. Numerous studies have put forth SDN-based interoperability frameworks, showing how SDN can facilitate communication and collaboration between devices made by various manufacturers within an IoT ecosystem.

Applications of SDN in IoT:

SDN integration in IoT networks has been used in a number of fields, such as:

- Smart Cities: By managing energy grids, traffic systems, and environmental monitoring, SDN-based IoT networks increase productivity and cut expenses. SDN's potential to optimize urban infrastructure and facilitate the integration of various city management systems has been investigated by researchers.
- Healthcare: SDN can help medical devices integrate seamlessly, enabling effective data sharing and real-time patient health monitoring in the healthcare industry. Because healthcare environments are dynamic, SDN offers the perfect solution, guaranteeing dependable and secure device-to-device communication.
- Industrial IoT (IIoT): By facilitating real-time monitoring, predictive maintenance, and effective automation, SDN improves the management of vital systems in industrial settings. For industrial networks, SDN-based IIoT frameworks provide better resource management, scalability, and security.

Future Research Directions:

Even though SDN has a lot of promise for IoT networks, more research is needed in a few areas:

- Edge Computing Integration: By processing data closer to IoT devices, edge computing and SDN can lower latency and enhance real-time decision-making. To maximize the performance of IoT networks, researchers are investigating how SDN can enhance edge computing architectures.
- AI and Machine Learning: The integration of AI and machine learning with SDN could provide more intelligent network management, enabling automated decision-making based on network conditions and device behavior. Research is looking into how these technologies can improve SDN's ability to better manage Internet of Things networks.
- Energy-Efficiency: As IoT devices are often battery-powered, energy-efficient network management is crucial. SDN solutions that optimize power consumption are being developed by researchers to guarantee the long-term viability of IoT networks.

RESEARCH METHODOLOGY:

Through a review of the literature, the identification of significant developments, and an evaluation of the state of research on SDN-based IoT networks, this survey investigates the relationship between Software-Defined Networking (SDN) and the Internet of Things (IoT). The following crucial steps are part of the qualitative methodology used for this survey:

1. Literature Collection:

To collect research papers that address the integration of SDN with IoT, a thorough review of scholarly journals, conference proceedings, books, and other pertinent sources is carried out. To make sure the survey includes the most recent advancements and trends in the field, the search is restricted to publications published within the last five to ten years. The main purpose of search engines like Google Scholar, IEEE Xplore, and SpringerLink is to find pertinent literature.

2. Inclusion and Exclusion Criteria:

The following inclusion criteria are met by the research papers chosen for this survey: o Papers that concentrate on the use of SDN in IoT networks. o Research that addresses the issues of IoT networks, such as scalability, security, and performance, and how SDN can help. o Articles that suggest SDN-based architectures, frameworks, or solutions to enhance IoT network administration. The review excludes papers that are too old or that mainly concentrate on IoT or SDN separately, without considering how the two technologies intersect.

3. Thematic Categorization:

The chosen literature is divided into major topics like:

- SDN scalability in IoT networks. IoT security improvements made possible by SDN.
- SDN-based performance optimization techniques.
- Integration and interoperability issues in SDN-enabled IoT networks. SDN-based applications in IoT domains, such as industrial IoT, healthcare, and smart cities. The different methods and solutions put forth in the literature can be systematically analyzed and compared thanks to this thematic categorization.

4. Critical Analysis and Synthesis:

Every article is examined critically to determine how it advances the integration of SDN and IoT, with an emphasis on the advantages, disadvantages, and real-world applications of the suggested fixes. By contrasting various strategies and evaluating how well they handle the difficulties presented by IoT networks, the results are synthesized. Additionally, gaps in existing research are noted, offering information about areas that need more investigation.

5. Identifying Research Trends and Future Directions:

Future research directions and emerging trends are identified based on the reviewed literature. This entails assessing the scalability of SDN for extensive IoT deployments as well as acknowledging technological developments, such as the possible integration of SDN with edge computing, artificial intelligence, and machine learning. The results also point to areas like energy efficiency, network resilience, and smooth device interoperability where SDN could be further optimized to address lingering issues.

6. Comparative Evaluation:

Lastly, the survey evaluates the advantages and disadvantages of several SDN-based solutions that have been suggested for IoT networks. This comparative analysis gives a clear picture of the current state of research in this area and aids in understanding how well various SDN frameworks work to address particular IoT problems.

To sum up, this approach enables a comprehensive and methodical investigation of SDN's use in IoT, highlighting important research themes, obstacles, and prospects for enhancing IoT network administration through SDN technologies.

DISCUSSION:

Through the resolution of several significant issues, such as scalability, security, performance optimization, and interoperability, the combination of Software-Defined Networking (SDN) and the Internet of Things (IoT) holds the potential to completely transform IoT network management. The implications of the literature review's findings are the main topic of this conversation, which also highlights the advantages, drawbacks, and new research directions of SDN-enabled IoT networks as they stand today.

1. **SDN's Role in Enhancing Scalability in IoT Networks:** SDN's capacity to effectively manage the increasing number of devices in IoT networks is one of its biggest benefits. With millions or even billions of connected devices that must efficiently communicate, IoT networks are by nature scalable. Decentralized control mechanisms make it difficult for traditional networking models to keep up with this growth. By centralizing control, SDN solves this problem and makes large-scale network configuration and management easier. SDN allows IoT networks to grow without sacrificing performance by dynamically modifying network paths and allocating resources in real time. SDN can control a lot of devices, but it needs to be carefully planned so that the central controller can manage the extra workload without becoming a bottleneck.
2. **Security Enhancements Provided by SDN:** IoT networks raise serious security concerns because of the large number of connected devices, which expands the attack surface for possible cyberthreats. Better network-wide security policy monitoring and enforcement are made possible by SDN's centralized control. SDN makes it easier to identify security lapses, malicious activity, and unauthorized access by providing real-time visibility into network traffic. SDN can also be used to deploy adaptive security policies, which allow intrusion prevention and access control to be dynamically modified in response to current network conditions. Notwithstanding these benefits, SDN-based IoT networks continue to encounter difficulties with regard to protecting the SDN controller since it can be targeted by hackers. To avoid vulnerabilities, future research must concentrate on enhancing the SDN controller's security and resilience.
3. **Performance Optimization in SDN-Enabled IoT Networks:** Through better resource allocation, traffic flow management, and congestion reduction, SDN makes it possible to optimize IoT networks. Poor resource usage and ineffective data routing are common problems with traditional IoT networks. These problems are resolved by SDN, which makes intelligent and flexible traffic management possible. For Internet of Things applications, real-time traffic analysis and data flow optimization lead to reduced latency, increased throughput, and enhanced quality of service (QoS). Ensuring the effectiveness of SDN-based IoT networks in extremely dynamic environments is still difficult, though. For example, SDN controllers have to quickly adjust to changing network conditions as the number of devices and data traffic increases, which may necessitate a large amount of computational resources.
4. **Interoperability and Integration of Heterogeneous Devices:** Since devices in IoT networks frequently communicate using disparate protocols and standards, interoperability is one of the biggest problems. By providing a unified platform for communication and abstracting the underlying network infrastructure, SDN offers a solution. IoT devices that employ various communication protocols can communicate with each other without any problems thanks to this abstraction layer. However, the wide range of IoT devices—from sophisticated industrial machinery to low-power sensors—requires adaptable and flexible SDN solutions that can support multiple communication protocols. In order to create SDN architectures that support a variety of IoT standards and enable seamless integration across heterogeneous devices, more research is therefore required.
5. **SDN-Based IoT Applications:** The literature has examined a number of intriguing uses of SDN in IoT, notably in smart cities, healthcare, and industrial IoT (IIoT). By effectively routing data and managing network resources, SDN can improve traffic management, lower energy consumption, and improve public safety in smart cities. SDN makes it possible for medical devices to communicate with one another seamlessly, guaranteeing safe and dependable data exchange in crucial settings. SDN can enhance IIoT network performance and facilitate predictive maintenance and real-time monitoring, which lowers downtime and boosts operational effectiveness. These applications show how SDN can revolutionize a number of IoT domains, but there are still obstacles to overcome before it can be put into practice, especially when it comes to guaranteeing security and resilience.
6. **Challenges in Implementing SDN for IoT:** Notwithstanding its benefits, there are issues with SDN implementation in IoT networks that need to be resolved:

- Scalability of the SDN Controller: Although SDN makes network administration easier, the central controller needs to be able to manage massive IoT networks and the increasing number of devices without becoming overloaded. To guarantee efficiency, this calls for sophisticated load-balancing strategies and high-performance controllers.
- Energy Efficiency: Energy-efficient communication protocols are necessary for Internet of Things devices, particularly those that are battery-powered or placed in remote locations. Energy-saving strategies must be incorporated into SDN-based IoT networks in order to prolong IoT device battery life while preserving network performance.
- Real-Time Processing: In SDN-based networks, real-time data processing is necessary for many IoT applications, which can be difficult. For the SDN controller to maintain optimal performance and guarantee low latency, network events must be processed and responded to promptly.
- SDN Controller Security: SDN's centralization of control results in a single point of failure. The network as a whole is at risk if the SDN controller is compromised. This presents a serious security risk, particularly in extensive IoT settings. To make SDN controllers more secure and resilient, more research is required.

7. **Future Research Directions:** SDN for IoT's future depends on additional study and advancement in a number of areas:

- Integration of Edge Computing and SDN: By combining edge computing and SDN, data processing can take place nearer to Internet of Things devices, lowering latency and enhancing network responsiveness. For time-sensitive Internet of Things applications, this integration is especially crucial.
- AI and Machine Learning: Using AI and machine learning algorithms in SDN-based IoT networks can help make smart decisions about resource allocation, traffic control, and security. AI/ML can improve SDN networks' ability to adjust to changing conditions and maximize performance using real-time data.

8. **Energy-Aware SDN Solutions:** Future studies should concentrate on creating SDN-based energy-efficient solutions that lower power usage in IoT networks without compromising functionality.

- Interoperability Standards: To create seamless IoT ecosystems, research into SDN-based frameworks that guarantee interoperability among various IoT devices, platforms, and protocols is essential.

CONCLUSION:

Software-Defined Networking has a lot of potential to solve the problems that IoT networks face. It offers solutions for interoperability, security, scalability, and performance optimization—all of which are essential for the effective implementation of extensive IoT systems. But there are still issues that need to be resolved, especially with regard to SDN controller scalability, energy efficiency, real-time processing, and system security. SDN will be able to fully realize the potential of IoT networks and applications with further research in these areas and the integration of cutting-edge technologies like edge computing, artificial intelligence, and machine learning.

REFERENCES:

1. **Wang, Z., & Li, Y.** (2019). *Software-defined networking for the Internet of Things: A survey*. International Journal of Network Management.
2. **Kim, J., & Kim, Y.** (2018). *Software-defined networking for the Internet of Things: Challenges and opportunities*. Journal of Communications and Networks.
3. **Xia, F., Yang, L. T., & Li, S.** (2017). *Software-defined networking and its applications in the Internet of Things*. IEEE Access.
4. **Benedetti, L., Sargento, S., & Ribeiro, R.** (2020). *SDN-enabled Internet of Things: Security and privacy challenges*. IEEE Transactions on Industrial Informatics.
5. **Zhang, Y., & Wang, L.** (2016). *Security and privacy for software-defined networks: Challenges and solutions in IoT*. Future Generation Computer Systems.