IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Impact Factor: 7.301
Volume 3, Issue 2, February 2023

The Future of Networking: Embracing Software-Defined Solutions

T. Aditya[1], A. David Donald[1], G. Thippanna[2],M. Mohsina Kousar[3], K. Swetha[3]
Ashoka Women's Engineering College, Dupadu, Andhra Pradesh, India[1,2,3]

Abstract: *Software-Defined Networking (SDN) is a unique approach to network administration with the potential to radically alter how companies approach network design, implementation, and management. By decoupling the control plane from the data plane, SDN makes it possible for businesses to centralise and automate network design, management, and optimization. Hence, the organisation gains in speed, adaptability, and scalability. This research looks into where networking is headed and how businesses may use software-defined networking to speed up digital transformation, cut costs, and boost efficiencies. The concepts and components of software-defined networking (SDN), such as the controller, southbound and northbound application programming interfaces (APIs), and network virtualization, are introduced in this article. The advantages of SDN in terms of network programmability, security, and application performance are also explored. It also draws attention to some of the challenges of putting SDN into practise, such as integrating it with existing systems, being tied to a single vendor, and a lack of adequate industry standards. Finally, this research presents case studies of businesses that have successfully used SDN and seen significant benefits as a result of this implementation. It concludes that software-defined networking (SDN) is the networking technology of the future and that companies that adopt this technology will have an advantage in the modern digital economy.*

Keywords: Software-Defined Networks(SDN)

I. INTRODUCTION

Software-defined networking(SDN), is an emerging technology with the potential to revolutionise the way organisations approach network design, deployment, and management. Using SDN, businesses can automate and centralise network configuration, management, and optimization, allowing for greater speed, adaptability, and scalability. Traditionally, networks have used a dispersed architecture in which several network nodes (such as routers, switches, and firewalls) are responsible for directing data packets throughout the network. This approach is often cumbersome since it necessitates individual manual configuration and control of each network device, is inflexible in its application, and is difficult to deploy. SDN, on the other hand, allows for centralised network control and configuration by separating the control plane from the data plane. Network nodes run hardware code for the data plane, while a central controller runs software code for the control plane. The brain of the operation is programmed using software. With this partition in place, network automation and programmability can reach new heights.

Due to the fact that SDN is constructed on open standards and open APIs, it allows devices from different suppliers to work together and reduces the likelihood of being locked into a single provider. Quality of Service (QoS), security, and application performance are only some of the business requirements and policies that can be taken into account by the centrally located controller when making decisions about network traffic. The controller has the authority to make such calls so long as they are consistent with legal and company guidelines.

SDN's popularity has been on the rise in recent years, thanks in large part to the spread of cloud computing, big data, and the Internet of Things (IoT). Because of its importance in facilitating digital transformation, it is now widely adopted by companies seeking to boost their responsiveness, decrease costs, and streamline internal operations. SDN is a potent tool for both network administrators and developers since it allows for the creation of dynamic and flexible network topologies. With SDN, businesses may drastically simplify their networks, which in turn leads to significant savings in time and money. SDN can also facilitate the fast provisioning of network resources, allowing businesses to promptly respond to fluctuating consumer demands.

A higher standard of network security is one of SDN's major benefits. Because of their complex structures, traditional networks are often vulnerable to attacks. This is because it can be difficult to monitor and safeguard traffic. Due to these flaws, traditional networks may be vulnerable to attack. Yet, thanks to SDN's unified network view, traffic can be monitored and any threats may be easily identified with significantly less effort. Furthermore, SDN permits the creation of compartmentalised networks that are less vulnerable to assault, which further enhances the network's general security.SDN also improves application performance, which is a major plus. Using SDN, you can give certain types of traffic—like audio or video—a higher priority, which can improve the overall speed of your apps. To further improve performance, software-defined networking enables the development of unique network topologies that meet the needs of certain applications.

Businesses that are considering deploying SDN should be cognizant of not just the many benefits of SDN but also the many challenges that may arise from employing it. In order to enable SDN, businesses may need to invest in new hardware and software, and the process of integrating SDN with legacy systems can be challenging. Another significant barrier to SDN adoption is the need for both network administrators and developers to acquire new skill sets.SDN is a promising new technology that could drastically alter the processes involved in building and maintaining a company's network. Because of its potential to automate network management, enhance network security, and centralise network control, SDN is quickly becoming a preferred option for businesses seeking to boost the agility, efficiency, and overall performance of their networks.

II. SDN REQUIREMENTS

Software-defined networking (SDN) is an approach to networking that enables network administrators to manage network services and traffic flows through the use of software-based controllers, which can be programmed to dynamically manage network traffic based on real-time network conditions. In order to implement SDN effectively, there are several key requirements that must be met:

1. **Programmable Infrastructure:** The network infrastructure must be programmable, which means that it can be configured, monitored, and managed through software. This requires hardware devices that can be controlled and managed through software, such as switches and routers that support open standards like OpenFlow.
2. **Centralized Control:** SDN requires a centralized controller that can manage the network, including configuring network devices, monitoring network performance, and managing network traffic flows. The controller must be able to communicate with all network devices and have a global view of the network.
3. **Open APIs:** The SDN controller must provide open APIs (Application Programming Interfaces) that enable network administrators to program network behavior and services. This enables network administrators to develop custom applications and services that can be used to manage the network.
4. **Security:** SDN networks must be secure, with mechanisms to authenticate and authorize network administrators and devices. This includes secure communication channels between network devices and the controller, as well as secure APIs that enable network administrators to manage the network.
5. **Scalability:** SDN networks must be scalable, able to support large numbers of network devices and network flows. This requires the use of efficient protocols and algorithms for managing network traffic and distributing network resources.
6. **Resiliency:** SDN networks must be resilient, able to recover from failures and adapt to changes in network conditions. This requires the use of fault-tolerant and self-healing mechanisms, as well as the ability to dynamically adapt to changes in network topology and traffic flows.

III. SDN ARCHITECTURE

Software-defined networking (SDN) architecture is designed to enable network administrators to manage network traffic and services through a centralized software-based controller, which communicates with network devices using open standards like OpenFlow. The following are the main components of an SDN architecture:

1. **Application Layer**: This layer includes the applications and services that run on top of the SDN controller, such as network management tools, security applications, and traffic engineering applications. These applications interact with the SDN controller using open APIs provided by the controller.
2. **Control Layer**: The control layer includes the SDN controller, which is responsible for managing the network and configuring network devices. The controller communicates with network devices using open standards like OpenFlow, which allows the controller to program the behavior of network devices.
3. **Infrastructure Layer**: The infrastructure layer includes the physical network devices, such as switches and routers, that make up the network. These devices are programmable and can be controlled by the SDN controller using open standards like OpenFlow.
4. **Southbound APIs**: The southbound APIs are the interfaces used by the SDN controller to communicate with network devices. These APIs are used to program the behavior of network devices, such as configuring network ports and managing network traffic flows.
5. **Northbound APIs:** The northbound APIs are the interfaces used by the SDN controller to communicate with applications and services running on top of the controller. These APIs provide a way for applications to access and control the network through the SDN controller.

The SDN architecture enables network administrators to manage network traffic and services more efficiently and dynamically, by separating the control and data planes of the network and centralizing network management in a software-based controller.

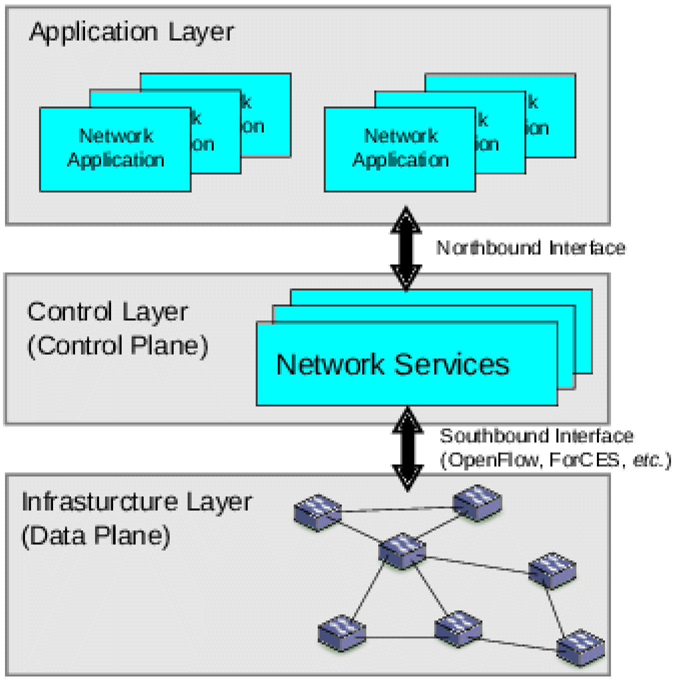

Fig.1 SDN Architecture

IV. CHARACTERISTICS OF SDN

The main characteristics of Software-Defined Networking (SDN) are:

1. **Centralized Control:** SDN architecture has a centralized controller that manages and controls the network. The controller manages the forwarding of network traffic, implements network policies, and enforces security measures.
2. **Separation of Control and Data Planes:** SDN separates the control and data planes, which allows the network to be more flexible and dynamic. The control plane manages the network policies and traffic flows, while the data plane forwards the actual network traffic.

3. **Programmable Network Infrastructure:** SDN network infrastructure is programmable, which means that it can be configured and managed using software. This allows network administrators to automate network management tasks, customize network services, and rapidly deploy new network applications.
4. **Open Standards:** SDN is based on open standards like OpenFlow, which allows network devices to be programmed and managed through a standardized interface. This enables interoperability between different vendors' network devices and facilitates the development of custom network applications.
5. **Simplified Network Management:** SDN provides a simplified approach to network management, by enabling network administrators to manage the network centrally and programmatically. This reduces the complexity of network management, improves network efficiency, and enables rapid network deployment and configuration.
6. **Improved Network Security:** SDN provides improved network security by enabling network administrators to centrally manage and enforce network security policies. This allows for more granular control over network access, enables rapid threat response, and improves network visibility and monitoring.
7. **Dynamic Network Provisioning:** SDN enables dynamic network provisioning, which allows network administrators to quickly and easily provision network resources based on changing network demands. This reduces the time and effort required to configure network devices and services, and enables faster response times to network issues and service requests.
8. **Better Traffic Management**: SDN provides better traffic management capabilities, by enabling network administrators to direct network traffic along optimized paths, based on network conditions, policies, and requirements. This improves network performance, reduces congestion, and enables more efficient use of network resources.
9. **Vendor-Neutral Network Management:** SDN provides vendor-neutral network management capabilities, which enables network administrators to use a mix of network devices from different vendors, without being locked into a single vendor's network management platform. This reduces costs, promotes competition, and enables greater innovation in network device development.
10. **Cloud-Native Network Architecture:** SDN is well-suited for cloud-native network architectures, which require networks to be more agile, scalable, and resilient. SDN provides a programmable, centralized, and open approach to network management, which enables networks to be more responsive to changing workload demands, more easily integrated with cloud platforms, and more resilient to network failures.
11. **Network Virtualization:** SDN enables network virtualization, which allows network administrators to create virtual networks that are isolated from each other, and can be managed independently. This enables the network to be more flexible, by allowing different network services to be allocated to different virtual networks, and enables better resource utilization by allowing multiple tenants to share the same physical network infrastructure.
12. **Analytics and Reporting**: SDN provides advanced analytics and reporting capabilities, which enable network administrators to gain insights into network performance, traffic patterns, and usage. This allows network administrators to identify network issues, optimize network resources, and plan for future network growth and development.
13. **Scalability:** SDN is highly scalable, which enables networks to grow and adapt to changing requirements. The centralized control and programmability of SDN allows network administrators to easily add new network devices, configure network policies, and provision network resources, without having to manually configure each device separately.
14. **Service Orchestration:** SDN enables service orchestration, which allows network administrators to manage network services and applications holistically, rather than on a device-by-device basis. This simplifies network management, reduces the time and effort required to configure and deploy network services, and enables more efficient use of network resources.
15. **Open Source Community:** SDN has a large and active open-source community, which contributes to the development of new SDN technologies, tools, and applications. This promotes innovation, collaboration, and

IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 3, Issue 2, February 2023

Impact Factor: 7.301

knowledge-sharing among network administrators and developers, and enables the development of customized, vendor-neutral network solutions.

The characteristics of SDN enable network administrators to build more flexible, efficient, and secure networks, by separating the control and data planes, centralizing network management, and programmatically managing the network infrastructure.

V. SDN AND NFV RELATED STANDARDS

Software-Defined Networking (SDN) and Network Function Virtualization (NFV) are two complementary technologies that are transforming the way networks are designed, deployed, and managed. Both SDN and NFV rely on a range of standards and specifications to ensure interoperability, performance, and security. Here are some of the key standards and specifications related to SDN and NFV:

1. **OpenFlow:** OpenFlow is a protocol that enables SDN controllers to communicate with network switches and routers. OpenFlow is managed by the Open Networking Foundation (ONF), which is a non-profit organization dedicated to promoting open standards and software-defined networking.
2. **Open Platform for NFV (OPNFV):** OPNFV is an open-source project that provides a reference implementation for NFV infrastructure. OPNFV is managed by the Linux Foundation, and it aims to accelerate the adoption of NFV by providing a flexible and interoperable NFV platform.
3. **Network Service Interface (NSI):** NSI is a specification developed by the Metro Ethernet Forum (MEF) that provides a standard interface for the orchestration and management of network services. NSI is designed to support both SDN and NFV, and it enables service providers to offer more flexible and customizable network services.
4. **European Telecommunications Standards Institute (ETSI) NFV:** ETSI NFV is a set of specifications developed by the European Telecommunications Standards Institute (ETSI) to define the requirements, architecture, and interfaces for NFV. ETSI NFV provides a framework for the implementation of virtualized network functions (VNFs) and the orchestration of NFV infrastructure.
5. **OpenStack:** OpenStack is an open-source cloud computing platform that provides infrastructure as a service (IaaS) capabilities. OpenStack includes components that are relevant for both SDN and NFV, such as Neutron (the OpenStack networking module), Nova (the OpenStack compute module), and Heat (the OpenStack orchestration module).
6. **Virtual Network Function Descriptor (VNFD):** VNFD is a specification developed by ETSI that defines the structure and characteristics of a VNF. VNFD provides a standard way to describe the requirements and capabilities of a VNF, and it enables the automated orchestration and management of VNFs in an NFV environment.
7. **Open Network Automation Platform (ONAP):** ONAP is an open-source platform for the automation and orchestration of network services, including SDN and NFV. ONAP is managed by the Linux Foundation, and it provides a comprehensive framework for the management and optimization of network services.
8. **YANG:** YANG is a data modelling language that is used to define the configuration and operational parameters of network devices. YANG is managed by the Internet Engineering Task Force (IETF), and it is widely used in both SDN and NFV environments to describe the structure and behavior of network devices and services.
9. **NETCONF:** NETCONF is a protocol that is used to manage network devices and services over the network. NETCONF is managed by the IETF, and it provides a standardized way to configure, monitor, and manage network devices using YANG data models.
10. **Open vSwitch Database Management Protocol (OVSDB):** OVSDB is a protocol that is used to manage the configuration of Open vSwitch (OVS) instances in an SDN environment. OVS is an open-source virtual switch that is widely used in SDN deployments, and OVSDB provides a standardized way to manage and configure multiple instances of OVS.

These standards and specifications are constantly evolving and being updated to reflect the changing needs of the networking industry. By following these standards and specifications, network operators and service providers can

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Impact Factor: 7.301
Volume 3, Issue 2, February 2023

ensure that their SDN and NFV solutions are interoperable, scalable, and secure, and that they can take full advantage of the benefits of these transformative technologies.

VI. STANDARDS DEVELOPING ORGANIZATIONS

Standards Developing Organizations (SDOs) are entities that develop and promote industry standards, specifications, and best practices in various fields. Here are some of the major SDOs that are relevant to the networking industry:

1. **International Telecommunication Union (ITU):** The ITU is a United Nations agency that develops global standards and recommendations for telecommunications and information and communication technologies (ICTs). The ITU is responsible for a wide range of standards related to networking, including those related to SDN and NFV.
2. **Institute of Electrical and Electronics Engineers (IEEE):** The IEEE is a professional association that develops standards for a wide range of technologies, including networking. The IEEE has developed numerous standards related to networking, such as the IEEE 802 series of standards for local area networks (LANs) and wireless LANs (WLANs).
3. **Internet Engineering Task Force (IETF):** The IETF is a community of engineers, researchers, and network operators who collaborate to develop and promote standards and protocols for the Internet. The IETF is responsible for many of the core networking standards, such as the Transmission Control Protocol (TCP) and the Internet Protocol (IP).
4. **Open Networking Foundation (ONF):** The ONF is a nonprofit organization that promotes open standards and software-defined networking. The ONF is responsible for managing the OpenFlow protocol and promoting the adoption of SDN in the networking industry.
5. **European Telecommunications Standards Institute (ETSI):** ETSI is a nonprofit organization that develops standards for information and communications technologies (ICTs), including those related to networking. ETSI is responsible for developing many of the standards related to NFV and 5G.
6. **Metro Ethernet Forum (MEF):** The MEF is an industry association that develops standards and specifications for carrier Ethernet services. The MEF is responsible for developing the Network Service Interface (NSI) specification, which provides a standard interface for the orchestration and management of network services.
7. **Open Networking and Edge Summit (ONES):** ONES is a series of industry events organized by the Linux Foundation that brings together experts in the networking industry to discuss the latest developments in open networking, cloud native networking, and edge computing.
8. **Internet Engineering Steering Group (IESG):** The IESG is responsible for the technical management of IETF activities and the approval of standards and specifications developed by IETF working groups. The IESG consists of a group of volunteers who are responsible for overseeing the development of Internet standards and ensuring that they are technically sound and relevant to the needs of the industry.
9. **Broadband Forum:** The Broadband Forum is an industry organization that develops standards and best practices for broadband networks. The Broadband Forum is responsible for developing the TR-069 protocol, which is widely used for remote management of network devices.
10. **Small Cell Forum:** The Small Cell Forum is an industry organization that promotes the development and deployment of small cell technologies for mobile networks. The Small Cell Forum is responsible for developing standards and specifications for small cell networks, such as the Femto Forum, which is focused on the deployment of femtocell technologies.
11. **Wi-Fi Alliance:** The Wi-Fi Alliance is an industry organization that promotes the development and deployment of Wi-Fi technologies. The Wi-Fi Alliance is responsible for developing and certifying Wi-Fi standards, such as the 802.11 series of standards for wireless LANs.
12. **Open Platform for NFV (OPNFV):** OPNFV is an open-source project that develops and integrates NFV components and tests them for interoperability and performance. OPNFV is managed by the Linux Foundation, and it provides a reference platform for NFV deployment.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, February 2023
Impact Factor: 7.301

These SDOs and industry organizations play a critical role in developing and promoting standards and best practices for the networking industry. By following these standards and best practices, network operators and service providers can ensure that their solutions are interoperable, scalable, and secure, and that they can take full advantage of the latest developments in networking technologies.

VII. INDUSTRY CONSORTIA

Industry consortia are groups of companies, organizations, and individuals who collaborate to develop and promote common interests and goals in a particular industry or technology area. In the networking industry, there are several consortia that play an important role in promoting innovation, interoperability, and standardization. Here are some examples of industry consortia in the networking space:

1. **Open Networking Foundation (ONF):** The ONF is a non-profit organization that promotes open standards and software-defined networking (SDN). The ONF manages the OpenFlow protocol and promotes the adoption of SDN in the networking industry. The ONF is supported by a diverse group of members, including network operators, vendors, and researchers.
2. **Open Networking and Edge Summit (ONES):** ONES is a series of industry events organized by the Linux Foundation that brings together experts in the networking industry to discuss the latest developments in open networking, cloud native networking, and edge computing. ONES is supported by a wide range of members, including network operators, vendors, and developers.
3. **Telecom Infra Project (TIP):** TIP is a global community of companies and organizations that collaborate to accelerate the development and deployment of open, disaggregated, and standards-based network infrastructure. TIP is supported by a diverse group of members, including network operators, vendors, and system integrators.
4. **Open Compute Project (OCP):** The OCP is a community of companies and organizations that collaborate to develop open standards for data center hardware and software. The OCP is focused on developing efficient, scalable, and interoperable data center solutions that can reduce the cost and complexity of deploying and operating data centres.
5. **Industrial Internet Consortium (IIC):** The IIC is a global non-profit organization that promotes the development and adoption of industrial Internet of Things (IIoT) technologies. The IIC is focused on developing standards, best practices, and reference architectures that can enable the interoperability and security of IIoT systems.
6. **Edge Computing Consortium (ECC):** The ECC is a global organization that promotes the development and adoption of edge computing technologies. The ECC is focused on developing standards and reference architectures that can enable the deployment of edge computing systems that can provide low latency, high bandwidth, and secure connectivity.
7. **Cloud Native Computing Foundation (CNCF):** The CNCF is a non-profit organization that promotes the adoption and development of cloud native technologies. The CNCF is focused on developing open standards and reference architectures for cloud native applications, such as containerization, microservices, and Kubernetes.
8. **Industrial Data Space Association (IDSA):** The IDSA is a non-profit organization that promotes the development and adoption of secure data sharing in the industrial sector. The IDSA is focused on developing standards and best practices for data sovereignty, data security, and data interoperability in the industrial sector.
9. **Automotive Grade Linux (AGL):** AGL is a collaborative open-source project that develops a common platform for automotive infotainment systems, telematics, and instrument clusters. AGL is focused on developing a secure, scalable, and open platform for the automotive industry.
10. **Open Networking Automation Platform (ONAP):** ONAP is an open-source project that develops a common platform for automating network and service orchestration. ONAP is focused on developing open standards and reference architectures for network automation and orchestration, which can enable the deployment of new network services and applications.

These industry consortia are just a few examples of the many organizations that collaborate to promote innovation, standardization, and interoperability in the networking industry. By participating in these consortia, companies and organizations can stay informed about the latest developments in their industry, collaborate with others to develop best practices, and influence the direction of the industry.

VIII. OPEN DEVELOPMENT INITIATIVES

Open development initiatives are collaborative efforts that bring together diverse stakeholders to develop open standards, technologies, and best practices. These initiatives are typically driven by non-profit organizations, industry consortia, or open-source communities, and are focused on promoting innovation, standardization, and interoperability.

Here are some examples of open development initiatives in the technology industry:

1. **OpenStack:** OpenStack is an open-source cloud computing platform that enables users to deploy and manage virtual machines, containers, and storage resources. OpenStack is managed by the OpenStack Foundation, which is a nonprofit organization that promotes the adoption and development of the platform.
2. **Hyperledger:** Hyperledger is an open-source project that develops blockchain technologies for enterprise applications. Hyperledger is managed by the Linux Foundation, which is a non-profit organization that promotes the development of open-source software.
3. **Apache Software Foundation:** The Apache Software Foundation is a nonprofit organization that manages over 350 open-source projects, including the Apache web server, Hadoop, and Kafka. The Apache Software Foundation provides governance, legal, and financial support to these projects, and promotes the development of open standards and technologies.
4. **Kubernetes:** Kubernetes is an open-source container orchestration platform that automates the deployment, scaling, and management of containerized applications. Kubernetes is managed by the Cloud Native Computing Foundation (CNCF), which is a nonprofit organization that promotes the adoption and development of cloud native technologies.
5. **Open Compute Project (OCP):** The Open Compute Project is a community of companies and organizations that collaborate to develop open standards for data center hardware and software. The OCP is focused on developing efficient, scalable, and interoperable data center solutions that can reduce the cost and complexity of deploying and operating data centers.
6. **OpenAI:** OpenAI is an AI research laboratory that develops cutting-edge AI technologies and promotes the safe and beneficial use of AI. OpenAI is a nonprofit organization that is dedicated to advancing AI in an open and collaborative manner.
7. **OpenPOWER:** OpenPOWER is an open development initiative that aims to develop open standards and technologies for power-efficient, high-performance computing systems. OpenPOWER is managed by the OpenPOWER Foundation, which is a nonprofit organization that promotes the adoption and development of the OpenPOWER platform.
8. **OpenBSD:** OpenBSD is a free and open-source operating system that is focused on security and cryptography. OpenBSD is managed by the OpenBSD Project, which is a volunteer organization that develops and maintains the operating system.
9. **OpenEHR:** OpenEHR is an open development initiative that develops open standards and technologies for electronic health records (EHRs). OpenEHR is focused on developing interoperable, scalable, and future-proof EHR systems that can improve the quality of patient care and reduce the cost of healthcare delivery.
10. **OpenMP:** OpenMP is an open standard for parallel programming in shared-memory systems. OpenMP is managed by the OpenMP Architecture Review Board (ARB), which is a consortium of companies and organizations that collaborate to develop the OpenMP standard.

These open development initiatives demonstrate the power of collaboration and open innovation in driving progress and innovation in technology. By working together to develop open standards, technologies, and best practices, companies and organizations can create a more vibrant and interoperable technology ecosystem that benefits everyone.

IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 7.301

Volume 3, Issue 2, February 2023

IX. CONCLUSION

There is a rich ecosystem of groups in the IT industry that collaborate to promote development, standardisation, and interoperability in the industry. The expansion and enhancement of technology rely on the efforts of many different groups working together, including standards-creating organisations, industry consortiums, and open development initiatives. These institutions are also helpful in the aforementioned cooperative endeavours. To improve interoperability, reduce costs, and stimulate innovation, these groups are creating open standards, technologies, and best practises. Participating firms and organisations can tap into the community's pooled expertise and use it to move their respective areas forward more quickly through participation in these joint endeavours.Finally, these collaborative efforts are necessary to foster an open and collaborative technological ecosystem that benefits individuals, businesses, and society as a whole.

REFERENCES

[1]. https://opennetworking.org/sdn-definition/

[2]. https://www.vmware.com/topics/glossary/content/software-defined-networking.html

[3]. Gyu-Min Lee, Byeong-HeeRoh, Dong Kuk Ryu, and Gyudong Park. "Software-defined networking approaches for link failure recovery: A survey." Sustainability 12, no. 10 (2020): 4255.

[4]. Nguyen, Kien, Quang Tran Minh, and Shigeki Yamada. "A software-defined networking approach for disaster-resilient WANs." In 2013 22nd International Conference on Computer Communication and Networks (ICCCN), pp. 1-5. IEEE, 2013.

[5]. https://opennetworking.org/wp-content/uploads/2014/10/Framework_for_SDN_-Scope_and_Requirements.pdf

[6]. Wickboldt, Juliano Araujo, WandersonPaim De Jesus, Pedro HelenoIsolani, Cristiano Bonato Both, Juergen Rochol, and Lisandro Zambenedetti Granville. "Software-defined networking: management requirements and challenges." IEEE Communications Magazine 53, no. 1 (2015): 278-285.

[7]. Braun, Wolfgang, and Michael Menth. "Software-defined networking using OpenFlow: Protocols, applications and architectural design choices." Future Internet 6, no. 2 (2014): 302-336.

[8]. https://www.nutanix.com/info/software-defined-networking

[9]. https://www.geeksforgeeks.org/software-defined-networking/

[10]. https://www.informit.com/articles/article.aspx?p=2451956&seqNum=3

[11]. https://sdn.ieee.org/newsletter/may-2016/ieee-sdn-nfv-standardization

[12]. https://www.healthit.gov/playbook/sdo-education/chapter-2/#:~:text=SDOs%20are%20member%2Dsupported%20organizations,%2C%20care%20givers%2C%20and%20others.

[13]. https://www.standardsportal.org/usa_en/resources/sdo.aspx

[14]. Zhao, Kexin, Mu Xia, and Michael J. Shaw. "Vertical e□business standards and standards developing organizations: A conceptual framework." Electronic Markets 15, no. 4 (2005): 289-300.

[15]. https://www.ecommerce-digest.com/industrial-consortia.html