International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 3, Issue 1, 162-172, 2022
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V3I1P117

Original Article

Review on Network Virtualization and SDN in Industrial IoT (IIoT)

Venkata Kishore Chilakapati[1], Srikanth Reddy Keshireddy[2], Venkata Teja Nagumotu[3], Harsha Vardhan Reddy Kavuluri[4], Akhil Kumar Pathani[5], Ajay Dasari[6]
[1]Technical Advisor, Microsoft.
[2]Senior Software Engineer, Keen Info Tek Inc.
[3]Sr Network Engineer, Techno-bytes Inc.
[4]Lead database administrator, Wissen infotech.
[5]Network Engineer, Ebay.
[6]Senior Support Engineer, Microsoft.

Abstract - *Network virtualization and Software-defined networking (SDN) is regarded as a breakthrough technology that has significantly altered factory communication systems. In the IIoT scenario, such technologies are the ones that provide the power of a highly versatile, scalable, and smart network architecture that can cater to the various industrial requirements. Through virtualization, physical resources are transformed into virtual machines, containers, and virtual network functions, thus cutting down the cost of resource utilization, increasing the number of users and providing quick access to the services in distributed industrial environments. SDN does the same thing by isolating control from the network nodes and data planes. The combination of both these technologies is what makes the virtual network embedding, secure multi-tenancy, dynamic slicing, and edge-fog-cloud orchestration essential for industrial automation happen together. The integration of these technologies improves the overall performance by making it more reliable, reducing the operational complexity, providing stronger security, and enabling the usage and storage of digital twins for predictive maintenance and real-time monitoring. In summary, SDN provides the foundation for highly resilient, adaptive, future-oriented IIoT systems and network virtualization.*

Keywords - *Network Virtualization, Software-Defined Networking (SDN), Industrial Internet of Things (IIoT), Virtual Network Embedding (VNE), Network Function Virtualization (NFV), Industrial Automation.*

1. Introduction

The “Internet of Things” (IoT) refers to scenarios where sensors and objects that are not computer-defined are provided network connectivity and computational power to generate, transmit, and consume data with the bare minimum intervention of human assistance [1]. The IoT encompasses a wide range of things, including consumer products, durable goods, industry and utility components, sensors, autos, and transportation [2]. IoT has several new opportunities regarding critical infrastructure and industrial implementation, which, however, also come with some challenges [3]. The rate at which IoT devices are proliferating inside the IoT ecosystem has accelerated due to the growing reliance on network-connected technology in daily life [4]. Nonetheless, numerous IoT elements are likely to provide a range of benefits in efficiency and automation, and they also introduce new issues, including scalability to support the massive scale of devices and data volume.

Virtualization, also known as notarization, is software-based logical abstraction of a network's underlying hardware components [5]. The abstraction makes it easier to manage, upgrade, and adjust jobs by separating control from hardware. Virtualisation and virtual infrastructure technologies are not disruptive because they don't significantly change user experiences. The advantage of virtual infrastructure, however, is that it is able to effectively control the pooled resources across the company so that the IT managers and administrators can respond to the changing circumstances faster. Administrative requirements and to make effective use of infrastructural investments [6].

NFV is an example of how virtualization methods may be used to decouple network services defined as software from the underlying hardware [7]. NFV benefits both network consumers and operators regarding the pricing of network services and services deployment because on-demand network features and services may be quickly created and provided at a reasonable price using commodity hardware [8], as SDN-fog integration has developed to process low-latency, secure communication schemes, and next-generation industrial wireless networks, and virtualized architecture has been developed to support digital twins, intelligent sensing, and cross-domain interoperability.

In this survey, the network virtualization and SDN methods in the IIoT setting are extensively reviewed with a focus on the facilitating technologies, architectural tendencies, areas of application, and unresolved research problems. This is aimed at

providing a systematic insight into the existing developments and outlining the future prospects of developing efficient, secure and programmable industrial networking infrastructures.

1.1. Structure of the Paper

The paper is organized as follows: Section II discusses Network Virtualization, including concepts, Section III focuses on SDN concepts and Architecture, Section IV Integration of Network Virtualization and SDN for IIoT, Section V provides a literature review of recent studies, Section VI concludes the report and offers next research directions

2. Network Virtualization: Concepts and Enabling Technologies.

Virtualization can be defined as a layer of indirection between the abstract view and the implementation of resources. First by thinking about the conventional network scenario. In this scenario, these many gadgets are dispersed over the whole network. Because each device has fixed network capabilities, the location of devices inside the network must be carefully evaluated [9]. These network devices must be reorganized, reconnected, and reconfigured separately if the network structure has to be updated over time to satisfy new demands. However, Figure. 1 illustrates the concept of future network topologies that primarily implement software virtualization. It is evident that the majority of the infrastructure consists of a hardware pool consisting of a bank of COTS servers and switches. Software-created virtual network functions use a common interface to access underlying hardware.

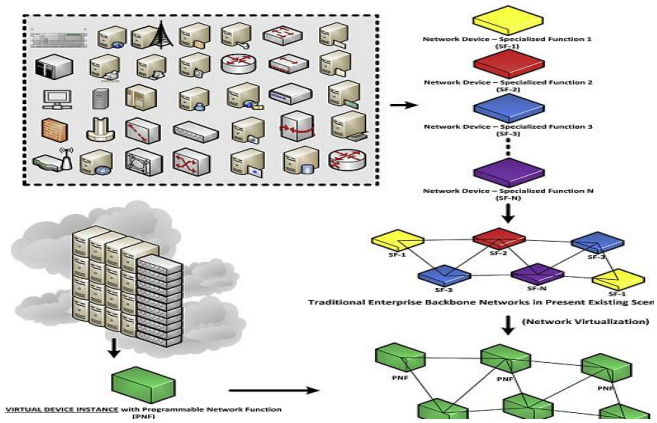

Fig 1: Architecture of Network Virtualization

Service providers may test new concepts without suffering major service interruptions thanks to the ability of virtual network devices established on a COTS-based server pool to be programmed. Network capacity is boosted by adding more COTS servers to the current server pool. These software-implemented network operations are the foundation of virtual networks, which are very adaptable and readily accommodate reconfigurations and new network architectures.

2.1. Types of Network Virtualization.

Network Virtualization includes technologies like VLANs, VXLANs, SDN overlays and NFV that abstract resources. These types enable a flexible, isolated, and scalable virtual network.

2.1.1. Network Function Virtualization (NFV)

An NFV architecture is used to accomplish function virtualization. Figure. 2 depicts a typical NFV architecture which creates communication services and provides connectivity by virtualizing everything with IT virtualization technology, network node functions are split into a set of building pieces [10]. Network Function Virtualization Infrastructure (NFVI), Network Function Virtualization Management and Orchestration architecture framework (NFVMANO), and Virtual Network Function (VNF) are its three fundamental components. NFV applies software, which is executed on NFVI, to perform network activities [11]. VNFs, which manage certain network functions operating on top of the hardware architecture, are typically used to implement these network services. NFVI is made up of processors, virtualization software, and both real and virtual storage. The NFV-MANO architectural architecture is made up of reference points and interfaces to specific VNFs and NFVI components.

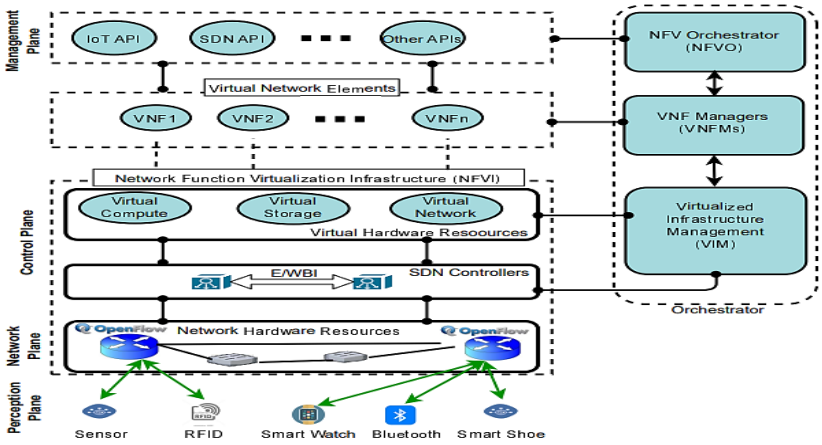

Fig 2: A Generic NFV Modular Structure

2.1.2.Network Device Virtual

The Switch virtualization is the process of data-plane virtualization of a switch employing logical abstractions among its components, or simply the functionality to be carried out across several operating systems. Virtualization tries to hide the actual features of a computer platform from users and offer an abstract platform that creates VNFs specific rules that switches must follow. A control program, often known as a hypervisor, is the software that manages virtualization [12]. In a similar line, sensor virtualization makes it easy for apps to use IoT resources through open APIs and enables software abstraction of external IoT devices. Any sensor device may be transparently located as a virtual switch by a virtual sensor using Zeroconf or comparable APIs.

2.1.3. Virtual Network Embedding (VNE)

The assignment of virtual nodes and virtual connections, together with their resource needs, to a shared physical substrate consisting of servers, switches, and communication links is referred to as VNE. In the case of IIoT environments, VNE plays a crucial role since diverse industrial applications with strict latency, QoS, and bandwidth demands must share limited resources at the edge-fog-cloud level [13]. Current VNE solutions comprise optimal ILP/MILP formulations for small-scale scenarios, heuristic and greedy algorithms for scalable approaches, metaheuristics for complex mappings, and dynamic schemes that respond to time-varying workloads.

Typically, the evaluations are carried out based on the parameters of acceptance ratio, revenue-to-cost ratio, resource utilization, latency, and reconfiguration overhead, utilizing either synthetic VN traces or edge/fog-aware testbeds [14]. The major challenges are real-time online embedding, joint computation-network optimization, energy and reliability-aware mapping, security in multi-tenant environments, and scalable orchestration for quick reconfiguration. A novel routes algebra technique was used to coordinate node and link mapping VNE. coordinated VNE node and link mapping with a novel route's algebra technique.

2.2. Virtualized Industrial Networks and Digital Twins

A flexible, software-defined communication infrastructure where all industrial devices, services, and control functions are isolated from the hardware is now feasible thanks to the virtualization of industrial networks. The latter also serves as the foundation for the deployment of Digital Twins, which are virtual replicas of actual machinery, procedures, or even entire industrial systems that consistently reflect their current operational conditions. The virtualized industrial networks are able to achieve dynamic network slice provisioning, low-latency communication, and scalable data processing, all of which are critical for precise and responsive Digital Twin operations by integrating SDN, NFV, and edge-fog-cloud resources.

Virtualized networks eventually be necessary for Digital Twins to obtain real-time telemetry, do predictive analytics, mimic system behaviour, and communicate prompt control instructions. By combining these technologies and techniques, industrial automation is transformed, remote monitoring and diagnostics are made easier, resource utilization is optimized, and quick reconfiguration is supported without interfering with physical operations. Ultimately, this results in IIoT environments that are more resilient, intelligent, and effective.

2.3. Benefits of challenges of Virtualization in IIoT

There are several benefits and challenges in virtualization in IIoT are as follows:

- Transforming hardware into VMs, containers, or VNFs virtualization fully utilizes heterogenous IIoT computing, storage, and network resources, which are thus very efficient to share. Moreover, this scaling of workloads according to real-time demand leads to a cut in infrastructure costs and the support of elastic large-scale industrial automation.

- Virtualized environments offer the chance to quickly make settings for and change the applications, edge functions, and network services. These changes are very important for flexible manufacturing systems (FMS), wherein the production lines require very fast adjustments brought about by the changes in the products.
- Through virtualization, physical separation is offered between different IIoT processes that are critical to the mission. One of the virtual components going down does not bring down the others, thus making it possible to have a strong fault tolerance. Snapshotting and live migration, in turn, facilitate redundancy, high availability, and proactive disaster recovery in industrial systems.
- It is a common occurrence for industrial plants to have several apps running monitoring, control, analytics using the same hardware. With virtualization, secure multi-tenancy with overheads almost reduced to nothing is allowed, thus making it possible to merge workloads onto a lower number of physical devices while at the same time cutting down on operational expenditures.
- Virtualization, by unlinking hardware from software, makes the processes of updating, patching, and carrying out maintenance easier. It is possible to move or copy the virtualized IIoT applications across nodes reducing the downtime and guaranteeing the continuation of production in the areas of continuous production.
- isolation, but at the same time, hypervisors and containers have created new attack surfaces. The tenants of a multi-tenant model may inadvertently share the vulnerabilities of the IIoT through side-channel attacks, VM escape attacks, and unauthorized movements within the virtual network.
- IIoT installations are dispersed across different places and consist of the edge, fog, and cloud layers [15]. It is going to be a very tricky job to manage the virtual machines, virtual networks, and orchestration tools with the increasing number of devices.
- There are many IIoT edge nodes which have very low CPU, memory, and energy capability. The virtualization workload especially the full VMs would be too much for the resources and life of the battery reduced. The lightweight virtualization is still under development to provide full support for industrial-grade reliability.

3. Software-Defined Networking (Sdn): Concepts and Architecture.

SDNs divide the network control logic (the control plane) from the underlying switches and routers that route traffic (the data plane). By separating the control and data planes and putting the control logic into a logically centralized controller, network switches may be reduced to basic forwarding devices that enable policy enforcement, network (re)configuration, and evolution. Therefore, SDNs' capacity to directly create networks is their most fascinating and potentially profitable feature [16]. Around 2010, SDNs gained popularity in cloud and enterprise networks. As far as are aware, SDN technologies are novel in the field of industrial automation. SDNs provide repeatable designs and configurations that enhance system efficiency.

SDNs offer assured temporal behavior for real-time communication, complementing and expanding upon technologies including wireless, network, and industrial Ethernet, SDNs are characterized by:

- Disconnecting the network devices' data and control planes.
- The provision of programmability in network services.
- Making judgements about forwarding centered more on flow than destination.
- A controller or Network Operating System (NOS) are examples of an external networked components that host control logic.
- Communicating with the underlying data plane devices with NOS-based software.

3.1. SDN Architecture and OpenFlow Protocol

Compared to controllers in traditional networks, network operators may be able to regulate flows more accurately with SDN architecture and the OpenFlow protocol. The longest destination IP prefixes, destination MAC addresses, and combinations of IP addresses and TCP/UDP port numbers are the attribute combinations in the packet header that are most likely to be used to regulate flows (or packets) in a normal network [17]. SDN simplifies the control of flows through a Controller-Data Plane Interface (C-DPI) through other packet header attributes, including the OpenFlow protocol. Separating the SDN architecture in a vertical manner, Figure 3 illustrates how the Open Networking Foundation (ONF)1 splits it into three main planes.

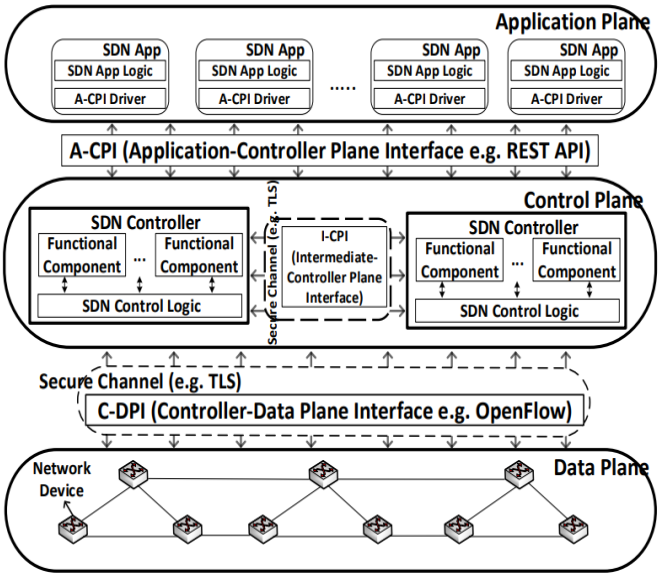

Fig 3: Architecture of SDN

3.1.1. Data Plane

The bottom plane, sometimes called data plane, consists of network hardware that consists of routers, physical switches, and virtual switches as well as access points. These devices may be accessed and controlled by SDN controllers using C-DPIs. Secure connections, including TLS, may be utilized for communication between the network components and the controller or controllers. The most used standard C-DPI for data plane device and controller communication is the OpenFlow protocol.

3.1.2. Control Plane

A collection of SDN software-based SDN controllers that enable control functionality to track network forwarding behavior using C-DPI is known as an SDN control plane. Its interfaces enable communication between controllers and network equipment (C-DPI), between controllers and applications (Application-Controller Plane Interface, or A CPI), and between controllers in a control plane (Intermediate-Controller Plane Interface, or ICPI, optionally secured through TLS). Network applications and services can communicate with one or more controllers for network security, administration, etc., thanks to an A-CPI2 [18]. The two main components of a controller are control logic and functional components. To control the behaviors of the controllers, there are many functional units of controllers, including Coordinator, Virtualize, etc. In addition, Application networking needs are converted into network element resources by SDN control logic in a controller.

3.1.3. Application Plane

One or more end-user apps (security, visualization, etc.) make up an SDN application plane that communicate with a controller or controllers to make internal decisions using an abstract network view. These programs use an open A-CPI (such as a REST API) to interact with the controller or controllers. An SDN application consists of an A-CPI Driver and an SDN App Logic.

The three essential components of a switch in an SDN network that uses switches with OpenFlow capabilities are the Flow table, the Secure Channel, and the OpenFlow Protocol. An OpenFlow switch contains a list of flow entries in several flow tables. The interface that allows a remote controller to connect to data-plane components is called Secure Channel. The controller uses the secure channel to operate and configure switches.To put up a new flow rule in SDN, Reactive, proactive, and hybrid are the three ways in which a controller can function.

3.1.4. Reactive Mode

A network device (such as a switch) is in reactive mode; it retrieves a flow rule from its flow tables upon receiving a new packet. If the flow cannot be matched, the controller selects how to treat the packet after obtaining it from the switch via CDPI. After processing the packet in compliance with network requirements, a flow entry is prepared by the controller and forwarded to the network device.

3.1.5. Proactive Mode

The switches' flow tables are updated in the proactive mode prior to the arrival of fresh flows. When a switch receives a packet, it already knows how it should be handled. In this instance, there is no flow rule setup procedure involving the controller.

3.1.6. Hybrid Mode

If a controller is in the hybrid mode, it benefits from both proactive and reactive modes. data plane devices may have specific flow entries installed proactively by network administrators, while the controller or controllers may react to incoming traffic by adding, removing, or updating flow entries.

4. Integration Of Network Virtualization And Sdn For Iiot.

The IoT is a network of sensors, actuators, and smart devices that are connected to one another over the Internet and employ embedded technology to interact and communicate with their environment. Connection and administration are two of the largest challenges to the implementation of the IoT. IoT solutions are often developed with a specific technology and aim. IoT relates to any gadget or large-scale machinery, building, and industries, appliances, body sensors, and cloud computing. The forecasts indicate the untapped market worth of IoT technologies and devices are estimated at $14 trillion by 2021 because it has fundamentally permeated all aspects of life. Other hardware vendors such as Apple, Cisco, Samsung and others have also invested heavily in some of the IoTs areas.

The IoT idea NFV is where network virtualisation first emerged in relation to SDN and cloud computing. Functionality in real-devices can be just developed as a software bundle and easily sent to the cloud by NFV. IoT is integrated into commonplace things for remote monitoring and control, and it makes it possible for tiny sensing and communication devices to be linked to the Internet [19]. The development of SDN theory, which allows for horizontal expansion with distributed SDN controllers and separates the control and data planes.

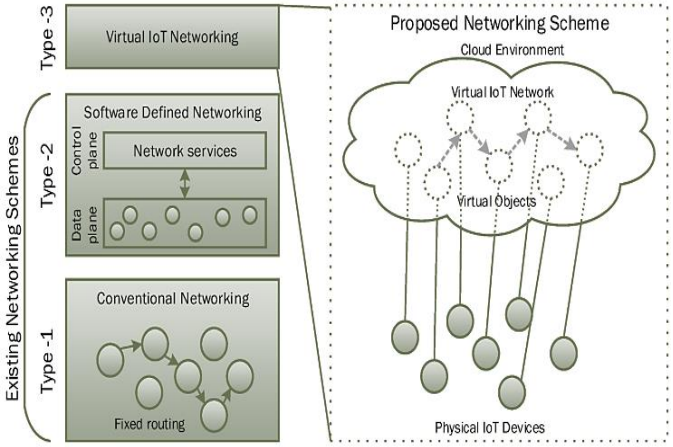

Fig 4: Conceptual View of a Virtualized Iot Network.

As with virtual machines and virtualized network activities, a cloud-based virtual representation of IoT devices, also known as virtual objects, might. The conceptual formation of virtual IoT networks is shown in Figure 4, and the progression of different types of networks is summarized. Traditional physical networks are denoted as Type-1, where routing is done individually at each router, making it hard to scale. In Type-2, the standard network model is split into control and data planes, enabling SDN implementation. A centralized controller could efficiently manage the network configurations. Type-3 illustrates virtualized IoT networks, which involve creating virtual objects in the cloud that connect devices, thereby providing greater flexibility and scalability.

4.1. Software-Defined Network-Based (SDN) IoT

The concept of SDN based IoT proposes applying SDN principles to the IoT environment to increase data delivery and routing efficiency, network administration, and resource distribution to satisfy the growing needs of the IoT systems used in contemporary applications [20]. SDN solutions attempt to overcome a number of constraints of the conventional IoT networking, such as heterogeneity of devices, interoperability issues, scalability issues, inefficient service deployment, slowness of adapting to new services, as well as limited guarantees to user experience, such as minimum bandwidth guarantees.

To address these issues, numerous SDN-based IoT architecture solutions, including the AR2500 Series agile IoT gateways, have been made available both commercially and in the literature. These solutions are further broadened by academic research, and they may be classified in general as architectural, security and management oriented [21]. The control plane monitors network traffic and policy enforcement, whereas the data plane manages packet forwarding in conformity with controller-defined regulations [22]. The SDN-IoT solutions that are management-focused characterize the interaction of the applications in the administration layer with the control plane, enabling coordinated and policy-based control mechanisms that are managed by both administrative users and the SDN controller.

4.2. Applications and Use Cases in Industrial IoT.

IoT Applications is becoming increasingly important in many use case applications. Benefits are obtained on a modest to large scale. A quick overview of some of these application cases and their advantages for various sectors is provided below.

- *Hospitals & Healthcare:* In addition to remote monitoring, IoT applications in hospital settings and e-health systems provide an automated healthcare environment. This process makes use of several IoT devices, including smart watches, wearable sensors and data collectors, linked inhalers, monitoring cameras, ingestible sensors, smart insulin delivery systems, and connected ambulances.
- *Intelligent Transportation Systems:* In this field, IoT applications have a variety of purposes. For effective parking management solutions, sensors are employed to get data on available parking spaces [23]. Alongside roadways, a smart signboard with an Internet connection may distribute emergency information. Businesses can identify and keep an eye on fleets of vehicles and other mobile assets with ease thanks to asset monitoring. Fleet management assists transportation firms in lowering the risks associated with vehicle investments.
- *Industrial Automation & Supply Chain:* Industrial automation automates the supply chain process by utilizing IoT technologies and artificial intelligence. Logistics are optimized, inventory levels are maintained, quality problems are avoided, and theft is detected when supply chain and asset tracking are combined. Smart machines and other intelligent manufacturing systems have a big impact on Industry 4.0 production lines.
- *Smart Homes:* In these kinds of applications, IoT offers a whole intelligent ecosystem for linked devices, from security and safety to lighting management. Human engagement often takes place via a smart central hub or gateway, which in turn regulates device automation.

5. Literature Review

This literature summary outlines key advancements in SDN-enabled IIoT, including SDN–fog integration for low-latency networking, strengthened security using Software Defined Perimeter and Physical Layer Security, and adaptive communication techniques for improved QoS. It also highlights challenges in secure wireless connectivity and controller reliability, pointing to the need for continued optimization of SDN-driven IIoT systems.

Bedhief et al. (2019) flexible as well as dynamic system design management is made possible with the advancement of SDN theory, which allows for horizontal expansion with distributed SDN controllers and separates the control and data planes. Furthermore, fog computing has lately emerged as the optimum solution for IIoT devices that offer rapid processing with acceptable latency. They suggest integrating SDN as well as fog computing in this new, dynamic, developing environment to offer a scalable, adaptable system that provides the low latency needed for IIoT scenarios. More specifically, they describe the topology of their suggested Fog node improved by SDN after presenting a revolutionary IIoT architecture based on SDN-Fog [24].

O'Raw, Laverty and Morrow (2019) Software Defined Networks (SDN) offer defence against remote assaults that take advantage of local area networks. Applying similar ideas to the WAN might enhance performance as well as availability while offering detailed information on connection attributes. In order to prevent unauthorised remote access, IIoT devices can stratify their connections by system using concepts like the Software Defined Perimeter. Lastly, assaults on the device's integrity or the privacy and security of its communications may be prevented by the division of labour at the IIoT device. There is further work to be carried out on DDoS mitigation [25].

Petroulakis et al. (2019) the architectural layout of the Semiotics framework which handles those problems is described in this study. Particularly, an outline of the proper realisation processes is provided together with the functional elements of the suggested design. In order to illustrate how the suggested design may be used to various IoT-enabled systems, in the end, They map one horizontal in the domain of intelligent sensing use, which includes smart objects, devices, and networks, and two verticals in the domains of energy and health care [26].

Lipps et al. (2019) they want to provide a method for wireless networks' SKG. They primarily emphasise on the application of the PhySec paradigm to NGMN, including the impending 5G or LTE+. This article presents an LTE testbed to assess the suitability of the cellular channel PUF approach for protecting the next generation of industrial wireless networks. In addition, initial findings are shown and contrasted with WLAN-PhySec results [27].

Li et al. (2018) if the coarse-grained approach is not feasible in the extreme deadline scenario, an adaptive power mechanism is employed in a fine-grained method to provide an effective transmission link with minimal delay. Lastly, simulation is employed to test the recommended strategy's success. The results show that the recommended methodology outperforms similar approaches in terms of download time, PDD, goodput, throughput, and average time delay. Therefore, the suggested approach offers a superior IIoT data transfer option [28].

Baddeley et al. (2017) suggests isolating the SDN control cost by creating customized forwarding channels over TSCH systems using 6TiSCH tracks, a Layer-2 slicing mechanism. By employing the characteristics of 6TiSCH tracks, a predictable,

low-latency connection to the SDN controller is made possible, in addition to preventing control traffic from impairing the efficiency of additional data flows. They first show how SDN control traffic affects app information flows throughout a 6TiSCH network using their own lightweight SDN implementation for Contiki OS [29].

A comparison of recent research on SDN and network virtualization in IIoT is shown in Table I, outlining each work's focus, application domain, addressed challenges, and evaluation methods across industrial networking and security contexts.

Table 1: Existing Literature On Software-Defined Networking (SDN) In Industrial Iot (Iiot)

Author	Focus / Contribution	Application Domain	Problem Addressed	Simulation / Evaluation Method
Bedhief et al., (2019)	Integration of SDN and Fog computing for IIoT	Industrial IoT (IIoT), Fog Computing, SDN	Need for flexible, low-latency, and scalable network architecture for IIoT	Conceptual architecture and SDN-enhanced Fog node design (no specific simulation mentioned)
O'Raw, Laverty & Morrow (2019)	Security improvements using SDN concepts	IIoT Security, WAN/LAN networks	Remote attack mitigation, data integrity, DDoS prevention (partial)	No simulation – theoretical and conceptual discussion
Petroulakis et al., (2019)	Design of SEMIoTICS architecture	Healthcare, energy, intelligent sensing	Need for adaptable IIoT architecture across diverse platforms	Use-case mapping & prototype architecture validation
Lipps et al., (2019)	Secret Key Generation (SKG) using PUF-based wireless security	Wireless industrial networks, LTE+, 5G	Secure communication in next-generation IIoT networks	LTE testbed experiments; comparison with WLAN-PhySec
Li et al., (2018)	Low-latency transmission using adaptive power method	IIoT data transmission	Need for reduced delay and improved throughput under high deadlines	Simulation-based performance evaluation
Baddeley et al., (2017)	Isolation of SDN control traffic using 6TiSCH tracks	TSCH Networks, Contiki OS, IIoT	SDN control traffic causing latency in network data flows	Lightweight SDN implemented in Contiki OS with experimental evaluation

6. Conclusion and Future Work

Network virtualization and SDN, which provide an environment for networks that is flexible and programmable, and capable of scaling up or down in response to the industry's changing demands, provide an innovative foundation for the next generation of Industrial Internet of Things (IIoT) systems. The abstraction of the physical resources in the form of virtualized components and the provision of centralized control through SDN facilitate the realization of better resource management, easier operations, and faster reaction times among industries. Both technologies are instrumental in bringing to life IIoT capabilities such as network slicing, virtual network embedding, secure multi-tenancy, and seamless edge–fog–cloud coordination, all of which are critical for automation, remote monitoring, and predictive decision-making. The combination of virtualization and SDN also brings about greater reliability, lower latency communication, and the use of Digital Twins for effectively creating models of the systems. However, security, interoperability, large-scale orchestration, and the management of resource-constrained edge devices remain issues that need to be addressed.

Security frameworks development and optimization of real-time orchestration across edge–fog–cloud layers are the next and most important steps in research with light-weight virtualization techniques that will be implemented in constrained IIoT devices being the last one. AI-driven network automation, autonomous slice management, and standardized interoperability will be the facilitators of the integration of SDN and virtualization in industrial environments on a larger scale.

References

[1] P. Pathak, A. Shrivastava, and S. Gupta, "A survey on various security issues in delay tolerant networks," J Adv Shell Progr., vol. 2, no. 2, pp. 12–18, 2015.
[2] I. Ud Din et al., "The Internet of Things: A Review of Enabled Technologies and Future Challenges," IEEE Access, vol. 7, pp. 7606–7640, 2019, doi: 10.1109/ACCESS.2018.2886601.
[3] Y. Kim, J. Nam, T. Park, S. Scott-Hayward, and S. Shin, "SODA: A software-defined security framework for IoT environments," Comput. Networks, vol. 163, p. 106889, Nov. 2019, doi: 10.1016/j.comnet.2019.106889.
[4] F. A. Ruambo and J. A. Mwakatobe, "Virtualizing the Iot Ecosystem: a Brief Review, Addressing Nfv Strategies," Int. J. Eng. Appl. Sci. Technol., vol. 4, no. 3, pp. 322–331, 2019, doi: 10.33564/ijeast.2019.v04i03.053.
[5] R. Horvath, D. Nedbal, and M. Stieninger, "A Literature Review on Challenges and Effects of Software Defined Networking," Procedia Comput. Sci., vol. 64, pp. 552–561, 2015, doi: 10.1016/j.procs.2015.08.563.
[6] Y. Li and M. Chen, "Software-Defined Network Function Virtualization: A Survey," IEEE Access, vol. 3, pp. 2542–2553,

2015, doi: 10.1109/ACCESS.2015.2499271.
[7] W. Ben Jaballah, M. Conti, and C. Lal, "A Survey on Software-Defined VANETs: Benefits, Challenges, and Future Directions," May 2019, doi: 10.48550/arXiv.1904.04577.
[8] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," J. Ind. Inf. Integr., vol. 6, pp. 1–10, Jun. 2017, doi: 10.1016/j.jii.2017.04.005.
[9] B. Rodrigues, F. Cerveira, R. Barbosa, and J. Bernardino, "Virtualization: Past and Present Challenges," in Proceedings of the 13th International Conference on Software Technologies, 2018, pp. 755–761. doi: 10.5220/0006910707550761.
[10] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges," IEEE Commun. Surv. Tutorials, vol. 18, no. 1, pp. 236–262, 2016, doi: 10.1109/COMST.2015.2477041.
[11] I. Alam et al., "IoT Virtualization: A Survey of Software Definition & Function Virtualization Techniques for Internet of Things," pp. 1–30, 2019.
[12] S. K. Tayyaba, M. A. Shah, O. A. Khan, and A. W. Ahmed, "Software Defined Network (SDN) Based Internet of Things (IoT)," in Proceedings of the International Conference on Future Networks and Distributed Systems, 2017, pp. 1–8. doi: 10.1145/3102304.3102319.
[13] C. Tipantuna and P. Yanchapaxi, "Network functions virtualization: An overview and open-source projects," in 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), IEEE, Oct. 2017, pp. 1–6. doi: 10.1109/ETCM.2017.8247541.
[14] X. Hesselbach, J. R. Amazonas, S. Villanueva, and J. F. Botero, "Coordinated node and link mapping VNE using a new paths algebra strategy," J. Netw. Comput. Appl., vol. 69, pp. 14–26, Jul. 2016, doi: 10.1016/j.jnca.2016.02.025.
[15] A. Kushwaha, P. Pathak, and S. Gupta, "Review of optimize load balancing algorithms in cloud," Int. J. Distrib. Cloud Comput., vol. 4, no. 2, pp. 1–9, 2016.
[16] K. E. U. Ahmed, J. Blech, M. A. Gregory, and H. (Heinz) W. Schmidt, "Software Defined Networks in Industrial Automation," J. Sens. Actuator Networks, vol. 7, no. 3, p. 33, Aug. 2018, doi: 10.3390/jsan7030033.
[17] M. Karakus and A. Durresi, "A survey: Control plane scalability issues and approaches in Software-Defined Networking (SDN)," Comput. Networks, vol. 112, pp. 279–293, Jan. 2017, doi: 10.1016/j.comnet.2016.11.017.
[18] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," IEEE Commun. Surv. Tutorials, vol. 16, no. 3, pp. 1617–1634, 2014, doi: 10.1109/SURV.2014.012214.00180.
[19] A. R, Samiksha, A. S, and J. S. K, "Efficient operating system level virtualization techniques for cloud resources," IOP Conf. Ser. Mater. Sci. Eng., vol. 263, p. 042002, Nov. 2017, doi: 10.1088/1757-899X/263/4/042002.
[20] A. Wang, Z. Zha, Y. Guo, and S. Chen, "Software-Defined Networking Enhanced Edge Computing: A Network-Centric Survey," Proc. IEEE, vol. 107, no. 8, pp. 1500–1519, Aug. 2019, doi: 10.1109/JPROC.2019.2924377.
[21] N. M. M. K. Chowdhury and R. Boutaba, "Network virtualization: state of the art and research challenges," IEEE Commun. Mag., vol. 47, no. 7, pp. 20–26, Jul. 2009, doi: 10.1109/MCOM.2009.5183468.
[22] I. Ullah, S. Ahmad, F. Mehmood, and D. Kim, "Cloud Based IoT Network Virtualization for Supporting Dynamic Connectivity among Connected Devices," Electronics, vol. 8, no. 7, p. 742, Jun. 2019, doi: 10.3390/electronics8070742.
[23] H. Yang, S. Kumara, S. T. S. Bukkapatnam, and F. Tsung, "The internet of things for smart manufacturing: A review," IISE Trans., vol. 51, no. 11, pp. 1190–1216, Nov. 2019, doi: 10.1080/24725854.2018.1555383.
[24] I. Bedhief, L. Foschini, P. Bellavista, M. Kassar, and T. Aguili, "Toward Self-Adaptive Software Defined Fog Networking Architecture for IIoT and Industry 4.0," in 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1–5. doi: 10.1109/CAMAD.2019.8858499.
[25] S. Gupta and C. Ravishankar, "Lower bounds for Arrangement-based Range-Free Localization in Sensor Networks," 2012.
[26] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, "Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT," IEEE Access, vol. 3, pp. 622–637, 2015, doi: 10.1109/ACCESS.2015.2435000.
[27] K. Gopalakrishnan and B. Chander, "Security vulnerabilities and issues of traditional wireless sensors networks in IoT," in Principles of internet of things (IoT) ecosystem: Insight paradigm, Springer, 2019, pp. 519–549.
[28] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 7, no. 2, 2019, doi: 10.5281/zenodo.15362327.
[29] M. Fahim and A. Sillitti, "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review," IEEE Access, vol. 7, pp. 81664–81681, 2019, doi: 10.1109/ACCESS.2019.2921912.
[30] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," Sensors, vol. 18, no. 9, 2018, doi: 10.3390/s18092796.
[31] J. Sen, "A survey on wireless sensor network security," arXiv Prepr. arXiv1011.1529, 2010.
[32] M. El Barachi, A. Kadiwal, R. Glitho, F. Khendek, and R. Dssouli, "A Presence-based architecture for the integration of the sensing capabilities of Wireless Sensor Networks in the IP Multimedia subsystem," IEEE Wirel. Commun. Netw. Conf. WCNC, pp. 3116–3121, 2008, doi: 10.1109/wcnc.2008.544.
[33] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas,

Security Threats, and Solution Architectures," IEEE Access, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
[34] H. I. Ahmed, A. Nasr, S. Abdel-Mageid, and H. K. Aslan, "A survey of IoT security threats and defenses," Int. J. Adv. Comput. Res., vol. 9, no. 45, pp. 325–350, Oct. 2019, doi: 10.19101/IJACR.2019.940088.
[35] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to the Internet of Things," IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1636–1675, 2019, doi: 10.1109/COMST.2018.2874978.
[36] Z. Ma, M. Xiao, Y. Xiao, Z. Pang, H. V. Poor, and B. Vucetic, "High-Reliability and Low-Latency Wireless Communication for Internet of Things: Challenges, Fundamentals, and Enabling Technologies," IEEE Internet Things J., vol. 6, no. 5, pp. 7946–7970, Oct. 2019, doi: 10.1109/JIOT.2019.2907245.
[37] M. Ahmad, "Reliability Models for the Internet of Things: A Paradigm Shift," in 2014 IEEE International Symposium on Software Reliability Engineering Workshops, IEEE, Nov. 2014, pp. 52–59. doi: 10.1109/ISSREW.2014.107.
[38] M. Rassam, A. Zainal, and M. Maarof, "Advancements of Data Anomaly Detection Research in Wireless Sensor Networks: A Survey and Open Issues," Sensors, vol. 13, no. 8, pp. 10087–10122, Aug. 2013, doi: 10.3390/s130810087.
[39] A. Ukil, S. Bandyoapdhyay, C. Puri, and A. Pal, "IoT Healthcare Analytics: The Importance of Anomaly Detection," in 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016, pp. 994–997. doi: 10.1109/AINA.2016.158.
[40] A. Chirayil, R. Maharjan, and C.-S. Wu, "Survey on Anomaly Detection in Wireless Sensor Networks (WSNs)," in 2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), IEEE, Jul. 2019, pp. 150–157. doi: 10.1109/SNPD.2019.8935827.
[41] D. ElMenshawy and W. Helmy, "Detection techniques of data anomalies in IoT: A literature survey," Int. J. Civ. Eng. Technol., vol. 9, pp. 794–807, 2018.
[42] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges," IEEE Access, vol. 8, pp. 3343–3363, 2019, doi: 10.1109/ACCESS.2019.2962829.
[43] E. Siow, T. Tiropanis, and W. Hall, "Analytics for the internet of things: A survey," ACM Comput. Surv., vol. 51, no. 4, pp. 1–36, 2018, doi: 10.48550/arXiv.1807.00971.
[44] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for Internet of Things," Int. J. Mach. Learn. Cybern., vol. 9, no. 8, pp. 1399–1417, 2018.
[45] X. Ma et al., "A Survey on Deep Learning Empowered IoT Applications," IEEE Access, vol. 7, pp. 181721–181732, 2019, doi: 10.1109/ACCESS.2019.2958962.
[46] G. M. Dias, B. Bellalta, and S. Oechsner, "A survey about prediction-based data reduction in wireless sensor networks," ACM Comput. Surv., vol. 49, no. 3, pp. 1–35, 2016.
[47] D. Kateris, D. Moshou, X.-E. Pantazi, I. Gravalos, N. Sawalhi, and S. Loutridis, "A machine learning approach for the condition monitoring of rotating machinery," J. Mech. Sci. Technol., vol. 28, no. 1, pp. 61–71, 2014.
[48] M. El-Shamouty, K. Kleeberger, A. Lämmle, and M. Huber, "Simulation-driven machine learning for robotics and automation," tm - Tech. Mess., vol. 86, no. 11, pp. 673–684, Nov. 2019, doi: 10.1515/teme-2019-0072.
[49] Polu, A. R., Buddula, D. V. K. R., Narra, B., Gupta, A., Vattikonda, N., & Patchipulusu, H. (2021). Evolution of AI in Software Development and Cybersecurity: Unifying Automation, Innovation, and Protection in the Digital Age. Available at SSRN 5266517.
[50] Padur, S. K. R. (2020). From centralized control to democratized insights: Migrating enterprise reporting from IBM Cognos to Microsoft Power BI. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, 6(1), 218-225.
[51] Bitkuri, V., Kendyala, R., Kurma, J., Mamidala, V., Enokkaren, S. J., & Attipalli, A. (2021). Systematic Review of Artificial Intelligence Techniques for Enhancing Financial Reporting and Regulatory Compliance. International Journal of Emerging Trends in Computer Science and Information Technology, 2(4), 73-80.
[52] Padur, S. K. R. (2019). Machine learning for predictive capacity planning: Evolution from analytical modeling to autonomous infrastructure. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(5), 285-293.
[53] Attipalli, A., Enokkaren, S., BITKURI, V., Kendyala, R., KURMA, J., & Mamidala, J. V. (2021). Enhancing Cloud Infrastructure Security Through AI-Powered Big Data Anomaly Detection. Available at SSRN 5741305.
[54] Singh, A. A. S., Tamilmani, V., Maniar, V., Kothamaram, R. R., Rajendran, D., & Namburi, V. D. (2021). Predictive Modeling for Classification of SMS Spam Using NLP and ML Techniques. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 2(4), 60-69.
[55] Padur, S. K. R. (2020). AI augmented disaster recovery simulations: From chaos engineering to autonomous resilience orchestration. International Journal of Scientific Research in Science, Engineering and Technology, 7(6), 367-378.
[56] Reddy Padur, S. K. (2021). From Scripts to Platforms-as-Code: The Role of Terraform and Ansible in Declarative Infrastructure Rollouts. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 621-628.
[57] Kothamaram, R. R., Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., & Maniar, V. (2021). A Survey of Adoption Challenges and Barriers in Implementing Digital Payroll Management Systems in Across Organizations. International Journal of Emerging Research in Engineering and Technology, 2(2), 64-72.

[58] Padur, S. K. R. (2018). Autonomous cloud economics: AI driven right sizing and cost optimization in hybrid infrastructures. International Journal of Scientific Research in Science and Technology, 4(5), 2090-2097.
[59] Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., Maniar, V., & Kothamaram, R. R. (2021). Anomaly Identification in IoT-Networks Using Artificial Intelligence-Based Data-Driven Techniques in Cloud Environmen. International Journal of Emerging Trends in Computer Science and Information Technology, 2(2), 83-91.
[60] Padur, S. K. R. (2021). Bridging Human, System, and Cloud Integration through RESTful Automation and Governance. the International Journal of Science, Engineering and Technology, 9(6).
[61] Attipalli, A., BITKURI, V., KURMA, J., Enokkaren, S., Kendyala, R., & Mamidala, J. V. (2021). A Survey of Artificial Intelligence Methods in Liquidity Risk Management: Challenges and Future Directions. Available at SSRN 5741342.
[62] Padur, S. K. R. (2021). From Control to Code: Governance Models for Multi-Cloud ERP Modernization. International Journal of Scientific Research & Engineering Trends, 7(3).
[63] Routhu, K. K. (2021). Harnessing AI Dashboards in Oracle Cloud HCM: Advancing Predictive Workforce Intelligence and Managerial Agility. International Journal of Scientific Research & Engineering Trends, 7(6).
[64] Padur, S. K. R. (2021). Deep learning and process mining for ERP anomaly detection: Toward predictive and self-monitoring enterprise platforms. Available at SSRN 5605531.