





Review

A Topical Review on Machine Learning, Software Defined Networking, Internet of Things Applications: Research Limitations and Challenges

Imran ¹, Zeba Ghaffar ², Abdullah Alshahrani ³, Muhammad Fayaz ⁴, Ahmed Mohammed Alghamdi ⁵ and Jeonghwan Gwak ^{6,7,8,9,*}

- ¹ Department of Computer Science, Bahria University, Islamabad 44000, Pakistan; research@imranjamal.com
- ² Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan; zebaghaffar05@gmail.com
- ³ Department of Computer Science and Artificial Intelligence, College of Computer Science and Engineering, University of Jeddah, Jeddah 21493, Saudi Arabia; asalshahrani2@uj.edu.sa
- ⁴ Department of Computer Science, University of Central Asia, 310 Lenin Street, Naryn 722918, Kyrgyzstan; muhammad.fayaz@ucentralasia.org
- ⁵ Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 21493, Saudi Arabia; amalghamdi@uj.edu.sa
- ⁶ Department of Software, Korea National University of Transportation, Chungju 27469, Korea
- ⁷ Department of Biomedical Engineering, Korea National University of Transportation, Chungju 27469, Korea
- ⁸ Department of AI Robotics Engineering, Korea National University of Transportation, Chungju 27469, Korea
- ⁹ Department of IT & Energy Convergence (BK21 FOUR), Korea National University of Transportation, Chungju 27469, Korea
- * Correspondence: jgwak@ut.ac.kr; Tel.: +82-43-841-5852



Citation: Imran; Ghaffar, Z.; Alshahrani, A.; Fayaz, M.; Alghamdi, A.M.; Gwak, J. A Topical Review on Machine Learning, Software Defined Networking, Internet of Things Applications: Research Limitations and Challenges. *Electronics* **2021**, *10*, 880. <https://doi.org/10.3390/electronics10080880>

Academic Editor: Habib Mostafaei

Received: 8 February 2021

Accepted: 25 March 2021

Published: 7 April 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: In recent years, rapid development has been made to the Internet of Things communication technologies, infrastructure, and physical resources management. These developments and research trends address challenges such as heterogeneous communication, quality of service requirements, unpredictable network conditions, and a massive influx of data. One major contribution to the research world is in the form of software-defined networking applications, which aim to deploy rule-based management to control and add intelligence to the network using high-level policies to have integral control of the network without knowing issues related to low-level configurations. Machine learning techniques coupled with software-defined networking can make the networking decision more intelligent and robust. The Internet of Things application has recently adopted virtualization of resources and network control with software-defined networking policies to make the traffic more controlled and maintainable. However, the requirements of software-defined networking and the Internet of Things must be aligned to make the adaptations possible. This paper aims to discuss the possible ways to make software-defined networking enabled Internet of Things application and discusses the challenges solved using the Internet of Things leveraging the software-defined network. We provide a topical survey of the application and impact of software-defined networking on the Internet of things networks. We also study the impact of machine learning techniques applied to software-defined networking and its application perspective. The study is carried out from the different perspectives of software-based Internet of Things networks, including wide-area networks, edge networks, and access networks. Machine learning techniques are presented from the perspective of network resources management, security, classification of traffic, quality of experience, and quality of service prediction. Finally, we discuss challenges and issues in adopting machine learning and software-defined networking for the Internet of Things applications.

Keywords: SDN; machine learning; IoT; SDN leveraging ML; IoT leveraging SDN; topical review

1. Introduction

Internet of Things (IoT) is the connectivity of the enormous amount of physical devices to the internet to collect, share, and analyze massive chunks of data. Kevin Ashton introduced the concept of IoT 17 years ago [1], and the concepts become fundamentals for the 2nd digital revolution [2]. A survey conducted by Cisco forecasts that 50 billion things will be interconnected through the internet [3]. Interconnection of such a huge number of devices leads to management and scalability issues. For IoT device management, the traditional management approaches are slowly getting obsolete due to the evolution of new technologies and trends. IoT orchestration is one recent advancement in the development to handle management and scalability issues. Orchestration is considered as the more flexible and scalable approach for the management of the enormous number of connected devices through IoT [4,5].

Due to IoT's tremendous economic potential, technology companies and research institutions invest in the development and research in the IoT field to propose sustainable IoT solutions. They have developed various IoT commercial and open source projects over the past decade. Due to the lack of interoperability between these IoT platforms, different data formats are used by these platforms, which rise to the vital challenge of heterogeneity. Thus the need for more efficient network management techniques to handle an enormous amount of data produced by this large number of connected devices increase day by day. The paradigm for centralizing processing and storage of data is currently not feasible; hence, edge computing (EC) plays a vital role in data analysis to improve these consequences in IoT. A new concept called IoT Big Data refers to semantics and type of massive generated data by large-scale IoT connected devices. The realization of IoT, security, and privacy are current research's challenging issues.

In the literature, several surveys have tackled different IoT challenges and aspects including IoT applications, challenges, and opportunities [6], IoT frameworks, IoT security [7–9], IoT standardization [10], application of in software-defined networking (SDN) in IoT [11], IoT and cloud integration [12]. However, previous survey studies of IoT did not review all the challenges in detail. For example, in the context of internet applications, quality of service (QoS) and security issues are discussed. However, in IoT applications, these challenges are even more crucial. The existing solutions do not provide solutions and address the IoT challenges partially. In this study, we discuss the SDN and machine learning hybrid approaches based on feasible solutions that can deal with some of IoT's main challenges and overcome IoT applications' issues. SDN can address the challenges of security, cost of hardware, centralization, and management of resources in the IoT environment. Machine learning helps analyze the big heterogeneous data produced by the IoT platforms. SDN paradigm fundamental concept in networking is to separate the control and data planes, enabling network controller to perform network management and engineer traffic dynamically [13]. SDN's controller role includes management of the network resources and programming the network dynamically. Furthermore, the controller monitors and collects the network configuration data, network state, information, and packet flow in real-time.

Machine learning models are trained on historical network data to perform optimization of the network, data analysis, and automated network services provisioning intelligently [14]. In the literature, recent contributions to machine learning provide promising directions to apply machine learning to networking. Machine learning improves the performance, efficiency, and security of SDN solutions. The machine learning-based SDN can improve the performance, security, and efficiency of the IoT network. This review study is divided as follows: Section 2 presents the methodology of this topical research study. Section 3 presents existing studies to understand the background of IoT, and Section 4 presents SDN background. Section 5 explains machine learning techniques currently applied to SDN. In Section 6, we discuss IoT and SDN adaptation efforts and research contributions. Section 7 presents limitations and challenges for the adaptations of IoT leveraging SDN and future research direction. Finally, Section 8 concludes the study.

2. Methodology

This section presents the methodology of the research study for topical review on IoT, SDN, machine learning approaches, and IoT leveraging SDN techniques. Research questions, objectives, and research studies identification criteria of the proposed study are discussed. This research study investigates existing research studies proposed in the literature to machine learning, SDN, and secure IoT systems. Firstly, we present background sections to understand SDN, machine learning, and IoT to understand the theme of the study. Secondly, we will investigate different machine learning techniques applied to SDN-based networking solutions. Lastly, we will investigate the researchers' interest and contributions in IoT leveraging SDN solutions. Table 1 presents the research questions identified to reach the goals of this study.

Table 1. Research questions for the topical review.

S.No	Research Question	Description
1	What are the major challenges addressed in the literature regarding IoT networks-based applications?	To investigate different IoT concepts, challenges, and solutions used to address these challenges.
2	What techniques were used in the literature to protect IoT systems?	To understand and investigate techniques and solutions proposed by researchers to protect and enhance IoT systems.
3	What is SDN, and different concepts related to SDN ?	Investigate research contribution to SDN and identifying known solutions based on SDN.
4	What machine learning techniques have been applied to SDN?	To identify the most used and recommended machine learning methods used with SDN based solutions.
5	What measures are taken for IoT leveraging SDN?	To investigate solutions proposed for IoT leveraging SDN by the researchers to address IoT systems challenges.
6	How often is machine learning-based SDN proposed as a solution for IoT challenges?	Analysis and comparison of machine learning-based SDN solutions for IoT challenges. Identifying if machine learning-based SDN significantly improves IoT solutions.

We searched for IoT, SDN IoT, and Machine learning in IoT, SDN, and IoT keywords for the answers to the above questions. For example, keyword machine learning in SDN to narrow down the articles and review papers search criteria. SDN and IoT were explicitly added in all our keywords because they were the main topics of this topical review. Search for all the sub-topics was done using the Jeju national university of south Korea, google scholar, research gate, science direct, and IEEE. The main searches were conducted using the science direct portal. However, some of the research articles were searched through google and other search engines. Table 2 presents the search keywords strings used to retrieve relevant research papers related to IoT leveraging SDN, machine learning in SDN, IoT challenges, and its solutions using SDN and machine learning.

Table 2. Search keywords and criteria.

Key	Criteria
Search keyword	(SDN OR "software defined networking") AND (IoT OR "Internet of Things") AND (machine learning OR applications of SDN OR "IoT challenges" OR IoT solutions using SDN)
Limiters	Article date between 2015 and 2020.
Expanders	Without the word "optimization".
Search keyword	Search keyword occur anywhere in the article.

This topical review aimed to focus on the most recent research studies and future trends in IoT, SDN, and machine learning hybrid applications. Without this limitation on

the scope of this research study, studies to be investigated during this topical review were large. Another advantage of limiting and filtering the studies distinguished our research study from previous survey and review papers. Therefore, to conduct effective topical research, the most relevant and scholarly literature from the last 2 years was collected as a first priority, and research studies older than 2 years were used for background knowledge of the topics mentioned in the paper. Some research papers and survey papers were excluded based on the publisher and publication venue parameters such as impact factor, journal citation reports. The research papers selected for this study mostly focused on IoT, machine learning techniques to analyze SDN network traffic, and techniques for IoT leveraging SDN. Figure 1 represents our approach towards investigating the applications of intelligent SDN in the field of IoT and its wide deployment.

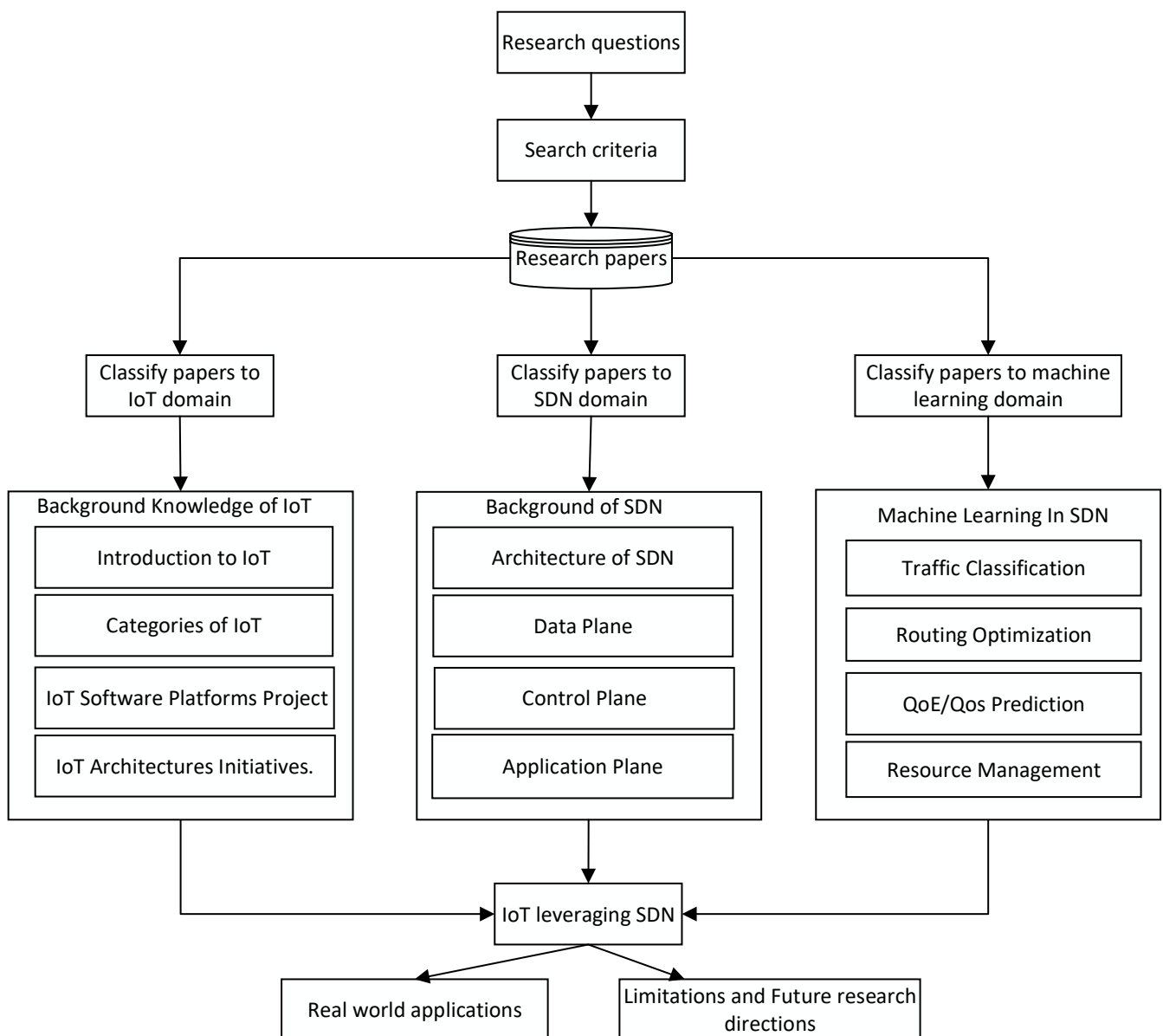


Figure 1. Proposed research flow for Internet of Things (IoT) leveraging software-defined networking (SDN).

3. Background of SDN

SDN has recently received much attention to address some of the enduring networking challenges. SDN’s concept is based on ideas of generalization network hardware and

decoupling the network controls software from the implementation devices [15]. SDN is a new intelligent architecture for network programmability. SDN's main idea is to separate the control plane from the network devices, enabling the data control from a central and external software entity called an SDN controller. The Open Networking Foundation (ONF) [16] is a non-profit consortium dedicated to the development, standardization, and commercialization of SDN for the transport and IP network layer. Figure 2 presents SDN layered architecture, consisting of [17] four planes: data plane, management plane, control plane and application plane. The Data plane presents a forwarding table that forwards the incoming packets to a network device. Management plane provides intelligent provisioning and orchestration systems for entire network management. The control plane is also termed as the brain of the networks that control different types of data planes using SBIs and protocols. The application plane defines the layer on different northbound applications that exist, which can help out SDN perform and solve future challenges of 5G, as this plane brings innovation, openness, and flexibility for the network vendors. SDN architecture provides dynamicity, network flexibility, and management capabilities. Research studies suggest SDN is the most reliable and promising for separating strategic network computation and data forwarding.

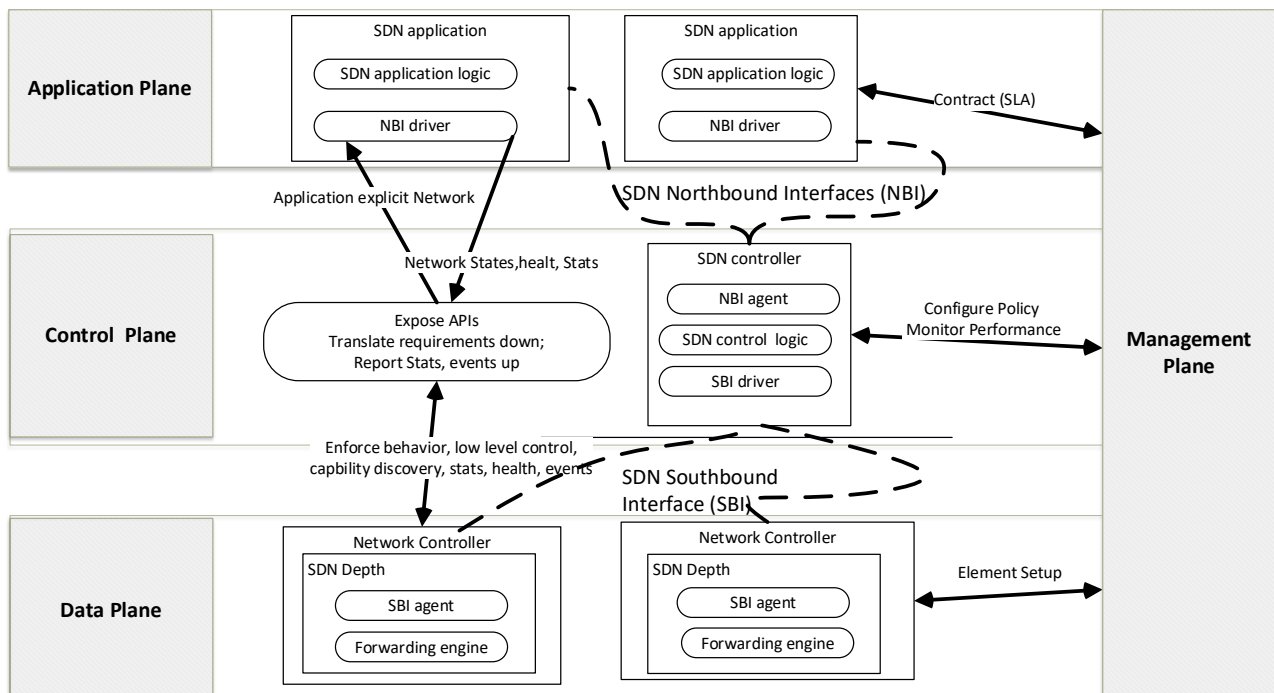


Figure 2. SDN Architecture.

Several northbound interfaces (NBIs) between the control plane and applications were introduced to provide high-level abstractions to the applications that reside on the control plane and in the form of various network-level services. OpenFlow [18] is a significant addition to the southbound interfaces (SBIs) that enable the network to be managed efficiently. Nevertheless, SDN can not be limited to OpenFlow as other less conventional protocols exist such as ForCES [19], NETCONF [20], OVSDB [21], Pollex [22], LISP [23], and OpenState [24]. OpenFlow deports all the intelligence to a centralized entity called SDN controller, which enables the separation of the control plane from the forwarding plane. There are three SDN functions in the panorama of OpenFlow, status reporting for each device connection, slicing, and flow-based forwarding. OpenFlow-based interconnection device matches the packets against a flow table inside the forwarding plane. FlowVisor controller is responsible for handling the flows, decisions, and publishing of the policies.

3.1. OpenFlow

OpenFlow provides an interface-based communication among the infrastructure and control layer based on open networking Foundation (ONF) [25,26]. Moreover, it provisions a way for controlling switches regardless of source code disclosure by the vendors. In summary, Openflow provides a way to directly access and manipulate the forward plan of switches and routers [27]. Furthermore, it grants access towards the flowable and provides instructions to the switches on managing and direct traffic of the network. It allows the network managers to alter the network flow in a short time span [28]. According to studies, there are two main categories of OpenFlow-based switches: OpenFlow-only and OpenFlow-hybrid. OpenFlow support is limited to OpenFlow operations, while the hybrid version supports operations and normal Ethernet switches [29].

The OpenFlow controllers are responsible for managing the OpenFlow switches based on a secure channel protocol called OpenFlow protocol. One or more flow tables are contained within a switch for performing a forwarding operation and packet tracing. A flow table includes a flow entry; each entry possesses header fields, specific counters, and actions. The purpose of a header field is to match up against packets with information related to VLAN, ID, source and destination ports and IP address, etc. There are counters for keeping information about the number of packets their sizes. Action provides information associated to processing and matching packets; Their forwarding action is also specified, such as being sent to the controller or a port or sometimes dropped [30–32]. OpenFlow channel provides an interface for connecting the switches and controllers. Using this interface, the switches are being managed and configured by the controller; additionally, the events are received, and packets are sent through the switches. Various messages are sent using this channel, including asynchronous messages that involve messages for updating the controller regarding the network event and state change. The second type is controller-to-switch messages; these messages are for managing and inspection of switch states. Lastly, symmetric messages are initiated by the switch or the controller and are sent unsolicited [33–35]. OpenFlow controller is responsible for managing, allocating, and updating instructions and policies to the networking devices. It can decide how to handle packets with invalid flow entries and control the switch flow table. OpenFlow switch can establish communication with one or more controllers. A multiple-controller architecture can increase network reliability if a switch fails. OpenFlow starts operations when the switch is connected to all its configured controllers simultaneously, whereas related messages are only sent to the next switch [36–39].

3.2. Data Plane

The Data plane resides at the bottom layer of SDN architecture, consisting of forwarding devices such as routers and switches, whether virtual or physical. Virtual switches are software-based switches that run on a common operating system (OS), examples of virtual switches are Open vSwitch [40], Pantou [41], and Indigo [42]. Physical switches are hardware-based switches, implemented either on open network hardware such as NetFPGA [43], or on a merchant switch from networking hardware vendors. ServerSwitch [44] and switchBlade [45] are two examples of NetFPGA-based physical switches. Hardware vendors design their's merchant switches with the support of SDN protocols, for example virtual switches are more flexible and have complete feature support for SDN protocols. Physical switches have a high rate of flow forwarding as compared to virtual switches. Both are used to forward, drop, and modify packets using the control plane logic.

3.3. Control Plane

In SDN, the control plane acts as the brain that performs a set of actions; for example, it applies flow rules to handle the received ethernet frames that decide the traffic destination ports. SDN controller program network resources, control communication between applications and forwarding devices. SDN controller translates application plane requirements into policies and distributes these custom policies into forwarding devices. Control plane

functionalities include network topology storage, configuration of devices, notification of state information, and shortest path routing. Some of the SDN controller architectures proposed in literature are NOX [46], Floodlight [47], POX [48], OpenDayLight [49], Ryu [50], and Beacon [51]. SDN controller has three interfaces for communication: southbound, eastbound westbound. Control data plane interfaces (CDPIs) are interfaces between the data and control plane. CDPIs are also called SBIs, used for forwarding devices to exchange control policies and network state information with the control plane of an SDN controller. SBIs allow programmatic-based control of all device capabilities such as event notifications, advertisements, statistic reports, and forwarding operations. NBIs are exploited by applications to get an abstract view of the network to facilitate automation, analyze specific network behaviors, and analyze network requirements. Eastbound interfaces (EBIs) and westbound interfaces (WBIs) are used in the multi-controller SDN solutions. In multi-controller SDN networks, the exchange of information is important between controllers to provide a global network view to the applications. Examples of distributed control architectures are HyperFlow [52] and Onix [53]. EBIs and WBIs are private and cannot communicate with each other. SDN communication-interfaces [54], distributed-control plane (CIBC) [55], and east-west bridge [56] are some proposals for communication between different SDN controllers.

3.4. Application Plane

The top layer in the SDN is called the application plane, consisting of business applications. Business applications provide management and optimization of business services. These applications implement the control logic based on the network state information received from controller NBIs to modify the network behavior. In the study, [57] the solutions of SDN for traffic engineering are discussed. In paper [58], a security-based survey study is conducted. Yan et al. [59] proposed analysis of distributed denial of service (DDoS) attacks in SDN networks in a cloud computing environment. A survey on fault management issues in SDN and its solutions is presented in [60]. SDN is deployed in real-time scenarios including transport network, wireless networks [61,62], optical networks [63], wide area networks (WAN) [64], IoT, EC [65], and cloud computing [66].

3.5. P4 (Programming Protocol-Independent Packet Processors)

P4 is a programming language to access the hardware without the knowledge of the architecture of hardware. P4 is used to modify the packet-forwarding mechanisms of the SDN switches [67]. Initially, P4 was used to write software programs and program hardware switches. Hardware resources including network interface cards, networking appliances, FPGA, and ASIC. P4 is used to set the custom headers and dynamic parsing of headers from the packet [68]. P4 provides the custom match and action tables and other constructs such as counters, registers, etc. This makes the P4 language entirely protocol-free. If a definite protocol is used in the network, it is easy to reconstruct the P4 program for new header field maintenance. Other P4 features include configurations, making new P4 applications reusable if needed rather than purchasing new networking devices. Furthermore, the P4 is free from any target device specifications and characteristics. Nonetheless, P4 is dependent upon the design of a device. The P4 application written for a distinct architecture is deployable beyond all destination devices with the same architectural design [69]. The P4 program is specially created for the data planes layer; however, the destination device may hold both the control and data planes. P4 is also used in literature for defining the interfaces between the control and data plane partially, but it cannot manage the control plane's functionality.

4. Background of IoT

IoT is the connectivity of things to the internet for collecting and sharing data between devices. IoT real-world applications are the basis of the second digital revolution. IoT platforms recognize connected things by unique addresses using protocols suites of

transmission control protocol (TCP) and Non-TCP. IoT is the connectivity of sensing and actuating devices such as sensors to the network. Devices virtualization is the process of virtualizing physical resources such as sensors and actuators into virtual objects [70–73]. IoT connects physical devices and virtual objects through communication protocols such as Bluetooth low energy (BLE), WiFi, ZigBee, Z-Wave, Long Range Wide Area Network (LoRaWAN), to name a few. These IoT devices have dynamic configuration and remotely accessible interfaces [74]. Recent development and contributions in the IoT field introduced new concepts and IoT terms such as machine-to-machine (M2M), industrial IoT (IIoT), Internet of everything (IoE), Internet of anything (IoA), social IoT (SIoT), and web of things (WoT).

BLE is an improved Bluetooth variant, extensively used wireless technology for effective communication with a range of about 10 m. The newest version of Bluetooth 5.2 adds an innovative IP support profile. Literature shows that BLE is completely developed and optimized for IoT devices [75]. WiFi is another broadly used protocol for communication between IoT devices, and most electronic devices manufacturer preferred due to the infrastructure it bears. The range for device communication using WiFi is around 50 m that is much higher than BLE communication [76]. ZigBee is another short-range wireless communication protocol with a 250 kbps data transmission rate. ZigBee is suitable for effective communication between IoT devices due to low power consumption, security, durability, and high scalability [77]. Like ZigBee, Z-Wave is a low-power communication protocol using radiofrequency designed for automation systems such as lamp controllers and sensors. Z-Wave communication protocol range is about 30–100 m, so the interruption of Z-Wave with other protocols such as Bluetooth, ZigBee, and WiFi is negligible. The data transmission rate ranges from 40 kbps to 100 kbps approximately [78]. LoRaWAN protocol is used for long-range battery-operated IoT devices. It communicates in long-range with the least power consumption and detects the noise level of signals based on a threshold range. LoRaWAN is mainly used in smart homes, smart hospitals, and smart cities applications where enormous devices are interconnected for secure communication using less power and memory [79–81].

Cisco introduced the concept of IoE [82], IoE is the connection of things, humans, devices, and global network data [83]. Apart from the capability of IoE, IoA considers the connectivity of imagined things [84]. M2M is the study of the communication between machines as well as machine and human [85]. M2M automates communication between machines without the intervention of human beings [86]. Due to IoT's tremendous economic potential, technology companies are investing in the development of real IoT solutions. These companies have developed various IoT commercial and open source projects over the past few years.

Table 3 presents some popular IoT commercial and open source projects. Due to the lack of interoperability between these IoT platforms and different data formats used by these platforms, heterogeneity issues have arisen. IoT applications have been deployed in different domains; the industrial domain is considered the most significant. Application of IoT in the industry needs careful deliberations and efforts [87]. IoT with the fourth industrial revolution is a step toward industry 4.0, which integrates industrial practices using smart technologies. Security and privacy are the two main challenges to IIoT applications [88]. To address and investigate these challenges, AT and T, Cisco, GE, and IBM founded a consortium for the IIoT [89]. A newly comparative analysis study was performed between IoT and WoT in a white paper presented in Auto-ID Labs. The comparison results present that IoT has unique identification of things. WoT cannot be used for resolving structural concerns [90]. WoT is a web-based framework that connects physical and virtual things through internet connection. WoT provides accessibility and data analysis, whereas IoT is used for connectivity of devices, automated configuration, and device management IoT.

Table 3. Summary of IoT software platforms projects.

IoT Software Platforms Projects	Company	Open Source
AWS IoT platform [91]	Amazon	No
Smart World Sensor [92]	Libelium	No
vCore [93]	Hewlett Packard Enterprise	No
Watson IoT, IBM IoT Foundation Device Cloud [94]	IBM	No
ThingWorx - MDM IoT Platform [95]	ThingWorx	No
M2M/IoT [96]	InterDigital	yes
Particle.IO	Particle	No
ThingsBoard [97]	ThingsBoard	Yes
Cisco IoT System [98]	Cisco	yes
Google Cloud IoT [99]	Google	No
Intel IoT Platform [100]	Intel	No
Microsoft .NET Gadgeteer [101], Azure IoT Suite [102]	Microsoft	Yes
Edge Gateway [103]	Dell	yes
OpenMTC [104]	Frankhauser FOKUS	yes

SIoT enables devices to form their social network [105]. The concepts of SIoT and WoT are considered very correlated. Now social media networks generate a huge amount of data, analysis of this immense data effectively requires the development of new data science applications [106,107]. This concept of socialization can be applied in the context of IoT [108] for the empowerment of all networks mentioned above to introduce a global network called future internet (FI). FI will be made possible using the principles of collaboration, connectivity, cognition, content, context, and cloud [109]. Things with constrained resources are connected to IoT to generate enormous data, and cloud-based applications will be used to process the data. This data shift from constrained things to a cloud-based collaborative environment will result in a cognitive world [110].

IoT gateway layer functionality includes protocols translation [111], security, service chaining, QoS management, data mining, handover management, mobility, forwarding packets, and routing [112]. In paper [113] IoT gateway based on oneM2M is proposed. oneM2M gateway performs three functions, device management, data analysis, and resource discovery. This study proposes fog and cloud-based computing architecture to the gateway layer for service management [114]. In EC, the edge node has the limitation of computing resources. Therefore migration of computing to the cloud is important for solving large computing tasks [115]. Cloud of Things (CoT) has the challenge of data trimming, to handle data trimming, functional architecture-based smart gateway was proposed [116,117]. Some of the tasks performed by this gateway are data collection, data preprocessing, data filtering, and reconstruction of data into a more valuable format. This smart gateway uploads necessary data to the cloud, track the activities of IoT objects and sensors, track the energy consumption of constrained IoT nodes, manages privacy and security of the data, monitor and manage IoT services [118].

In [119] authors proposed IoT gateway based on mobile phone for transmission of data over wide area network(WAN). IoT gateway with the capability of data requests and replies translations is proposed in [120]. The data is collected from IoT sensors and transmitted to applications installed on the mobile phone. A two-way approach is used for the accessibility of the data, pooling, and registration requests for notification to the gateway. With the revolution of SDN and NFV technologies, Software-defined service chaining is proposed in [121]. In [122] software-defined edges based service chaining mechanism is proposed. The deployment of these edges as software engines in a data center is made using virtual machines. Mininet based simulations are performed for the evaluation and performance analysis of IoT architectures. SDN controller(Pox) is used for the configuration of the routers and switches edge nodes. Paradrop, an edge-computing platform used for IoT gateway, is presented in [123]. Paradrop characteristics include management using OpenFlow, dynamicity, security functionalities, and APIs support. A comparison of the

device-centric approach to a data-centric approach is discussed in [124]. Data-centric approach relies on the collection and provision of data without the consideration of device identity. Examples of some data-centric cloud-based IoT architectures are IoT6, FI-WARE, and IoT-A. A service-centric approach relies upon the provisioning of services. In a User-centric approach, the identity of devices is based on relevancy to the owner identity.

Now we discuss IoT scalability from an architectural perspective. Due to Many IoT architectures are proposed in the literature, which connects a huge number of objects to the internet. To address the issues of Interoperability, a standard architecture is needed to propose sustainable IoT solutions. Heterogeneity, diversity, and interoperability among these architectures make it inefficient for IoT-wide deployment [125]. SDN provides a common control layer over the top of these architectures to handle the heterogeneity. SDN handles privacy, communication resilience, security, big data management [126]. Moreover, SDN performs efficiently in traffic engineering and QoS guarantee. Table 4 list IoT architectures providing complete IoT deployment and IoT e architectures leveraging SDN.

Table 4. IoT architectures initiatives.

Architecture	Description
FIWARE [127]	IoT applications development based on APIs
iCore [128]	An IoT project providing user level management and abstracting the heterogeneity
IEEE Project P2413 [129]	enable compatibility between different architectures
IoT-A [130].	IoT Architecture Reference Model (ARM).
TRESCIMO [131].	Smart City M2M Communications Testbeds
OneM2M [132].	A service layer abstraction to overcome the vertical heterogeneity
COMPOSE [133].	Collaborative Open Market to Place Objects at your Service
IoTDM [126]	data Broker for M2M
SAM [134]	proprietary DIY IoT platform with offline access and cloud support
Dweet.IO [135]	Open source middleware based IoT platform
Particle.IO [136]	Proprietary middleware based IoT platform
Glue.thing [137]	Proprietary DIY based IoT platform
Node-red [138]	Open source partial DIY supported IoT platform

5. Machine Learning Algorithms for SDN

SDN controller has a global view of the networks providing centralize network control and management. Machine learning algorithms can be used as a separate module or placed with the other northbound applications of the SDN controller to bring intelligence to SDN. SDN controllers using machine learning performs network data analysis, optimization, and automation of the network. In this section, we survey machine learning-based research studies applied to SDN. We categorize the studies as routing optimization, QoS prediction, quality of experience (QoE) prediction, network traffic classification, resource management, and security management. Table 5 presents machine learning algorithms categories applicable in the SDN domain.

Table 5. Machine learning algorithms applied to SDN Controller.

Supervised Learning	Unsupervised Learning	Reinforcement Learning
K nearest neighbour	K means	Reinforcement Learning (RL)
Decision Tree	Self organizing map	Deep RL (DRL)
Neural Network (DNN)		RL game Theory
BayeBaye's Theorem		
Hidden Markov Model		

5.1. Traffic Classification

Traffic classification plays an indispensable role in network management. Traffic classification enables network operators to control and allocate different services. Currently, the most used traffic classification approach includes dynamic port-based approaches and machine learning [139]. Port-based approaches such as deep packet inspection (DPI) have the advantage of high classification accuracy. DPI limitations include recognition of applications based on pattern availability and high computational cost to check traffic flow. DPI is unable to identify the encrypted flow of traffic. Therefore, compared to traditional DPI approaches, machine learning-based approaches are used to analyze encrypted traffic with a low computational cost. Traffic classification also includes collecting massive traffic flow data, extracting knowledge from the traffic data using machine learning approaches. Machine learning approaches are applied to the SDN controller for the analysis of collected traffic data. Machine learning-based traffic classification such as elephant flow-aware(EF), QoS-aware, and application-aware traffic classification.

EF traffic classification is used to classify traffic flow to elephant flow and mice flow. Elephant flows are bandwidth-hungry persistent flows, whereas mice flow is weak flow and delay intolerant. There are 80 mice flows in data centers, and the rest of the traffic flow is elephant flow [140]. In such environments, elephant flow identification is essential for controlling the traffic flow efficiently. Hybrid data center-based traffic flow scheduling issues are discussed in paper [141]. Machine learning approaches are used to implement EF traffic classification at the edge level; SDN controller-based optimization algorithms further use these analysis results for efficient traffic flow management. Xiao et al. propose a two-stage algorithm with efficient learning cost in SDN for identification of elephant flow [142]. Firstly suspicious elephant flow is differentiated from mic flow using a head packet measuring technique. Secondly, a decision tree classification model is used to classify the suspicious traffic as elephant flow or not.

In literature, application-aware traffic classification is proposed to identify applications based on the traffic flow. In study [139], an OpenFlow-based SDN system is proposed for the collection of data in enterprise networks. Several machine learning classifiers are trained to classify applications based on traffic flow. A hybrid approach of multi-classifier and DPI-based classifier is proposed in paper [143] to identify and classify applications. Rossi et al. proposed a behavioral engine for UDP protocol-based application-aware traffic classification [144]. SVM-based model is used to classify UDP traffic according to its Netflow records with more than 90 percent classification accuracy. TrafficVision, an SDN-enabled edge network, is proposed for mobile application-aware traffic classification [145]. The main component of Trafficvision is TrafficVision Engine(TV Engine). TV Engine performs tasks such as collecting data, storing data, extracting flow statistics, and data of ground truth training from access devices and end devices. A decision tree classifier model is used to classify different applications. In contrast, a KNN classifier-based model is used to classify flow types such as video content, an audio file, video chat, etc.

QoS-aware traffic classification is used to classify the traffic flow into QoS classes. QoS classes are assigned to different applications based on QoS requirements such as jitter, delay, and loss rate. Traffic flow classification, according to QoS classes, is the most efficient approach towards traffic flow classification. A semi-supervised learning algorithm and DPI-based approach are proposed for QoS aware traffic classification [146]. DPI approach is used to label the well-known applications. Laplacian SVM or other semi-supervised learning-based models are trained on the labeled data from DPI to classify applications into QoS classes known and unknown.

5.2. Routing Optimization

Mathematical optimization or optimization is selecting the best decisions or choice or selection regarding some measure, model or criterion, from some set of available choices. Optimization has been used in different fields including, optimal route recommendation [147], optimal policy-making [148], energy optimization [149], to name a few. Routing

is one of the primary functionality of a network; the SDN controller manages the routing functionality of traffic flow by modifying the network devices' flow tables such as routers and switches. SDN controller may guide a network device to route a traffic flow through specific paths, or it may also decide to discard a specific type of traffic. Inefficient decisions related to traffic flow can affect the SDN network's performance in terms of network overload and transmission delay. There are two types of algorithms used for routing optimization: shortest path first and heuristic algorithms. Shortest path first algorithms are simple best routing protocols, but it does not enhance the network resource utilization [150]. On the other hand, heuristic algorithms best utilize the network resources with a high computational cost [151]. SDN controller devises policies for each routing flow. Machine learning is used widely to overcome the issues of routing optimization using fast near-optimal routing solutions. These routing optimization issues are considered decision-making tasks; hence, machine learning approaches such as Reinforcement Learning (RL) perform well for routing optimization. In RL-based routing optimization approaches, the controller is considered as an agent and the network as the platform. The state-space consists of network and traffic states. Actions represent routing solutions, and the agent rewards are devised based on optimization metrics such as network delay and throughput. A distributed intelligent protocol for routing in SDN network using RL is proposed in paper [152].

In paper [153], a routing optimization algorithm in the domain of SDN-based inter-data center overlay network is proposed. A time-efficient QoS aware adaptive routing technique to forward the adaptive packet by using RL algorithms is proposed in paper [154]. The proposed approach selects a routing path with maximum QoS aware reward according to the user applications and traffic types. Literature also presents studies based on supervised learning techniques for routing optimization. Supervised learning-based routing optimization considers network and traffic states as the input of a training dataset. The routing solution of the heuristic algorithm is considered the output of the training dataset. Learning based on supervision can lead to optimal routing solutions like heuristic-like routing. In [151] dynamic routing based on supervised learning called NeuRoute is proposed. In NeuRoute, the long short-term memory (LSTM) part is used to estimate future traffic. The estimated network traffic and network state are used as input, and output is the results of the heuristic algorithms to a neural network model. The neural network is trained using these input and output data to predict heuristic-like results.

Traffic Prediction

Prediction process involves predictive modeling using regression models to predict the likelihood of an outcome. Predictive modeling is usually practiced in the domain of machine learning and artificial intelligence [155,156]. On the other hand, predictive analytics is used to predict the outcome of undiscovered future events using modeling and machine learning techniques from current data to predict future problems. Predictive modeling is used in literature for real-life potential applications [157–160]. Traffic prediction is an important research topic in the field of routing optimization. Traffic prediction used to predict the patterns of network traffic volume using analysis of historical traffic data [161]. Traffic prediction results are utilized by the SDN controller for efficient traffic routing decisions in advance and distribute the dynamic routing policies to devices in the data plane. These routing policies are used as a guideline for traffic flow routing soon. Traffic prediction enables the SDN controller to avoid traffic congestion, improve QoS, and proactively provide the network. For dynamic optical routing, a dynamic optimal routing meta-heuristic algorithm is proposed in the literature [162]. These meta-heuristic algorithms consist of three stages: offline scheduling, offline planning, and online routing. In the offline scheduling phase, a neural network is used to predict network traffic load for optimal resource allocation. Online routing decisions are made based on the routing path with minimum cost.

A load balance strategy is proposed for the optimization of path load [163]. SDN controllers use four features for predicting the path load through a neural network model, packet loss rate, transmission latency, transmission hop, and bandwidth utilization ratio. The path with the least load is selected for the new traffic flows. In paper, [164] LSTM based framework NeuTM is proposed to predict the network traffic matrix. GEANT backbone network [165] based real traffic data are used to train the LSTM model. Results from the simulation environment show that LSTM prediction performance is good for routing optimization. Researchers use QoS parameters such as throughput, delay, loss rate, and jitter for network performance assessment. User satisfaction level and perception are essential to service providers and network operators. QoE is used for the assessment of the performance of the network from user-oriented metrics. Service providers use prediction algorithms to predict QoS and QoE to provide network services to users with great customer satisfaction. Machine learning algorithms are applied to SDN controller collected statistics and information for the QoS and QoE prediction [166]. QoS management can be improved by predicting QoS parameters according to the key performance indicators (KPIs). Prediction of QoS parameters is considered a regression task because these QoS metric values are continuous.

Algorithms based on supervised machine learning such as random forest, support vector regression, ANN-based regressor are used for QoS parameters prediction. QoE identifies a subjective metric over the network such as mean opinion score (MOS) [167]. MOS classifies the QoE values into five classes: excellent, good, fair, poor, and bad. QoE values are usually obtained from a feedback form regarding the QoS. The customers rate the quality of the services in 5 stars or a scale of 1 to 10. The subjective method is time-consuming as QoE is dependent on QoS parameters. Machine learning algorithms can be used to find the relationship between QoS parameters and QoE values. In the paper, ref. [168] QoE prediction experiment is performed in the case study of a video streaming. MoS value is estimated using network parameters such as delay, bandwidth, jitter, and RTT. SDN controller can adjust video parameters to improve the user QoE. In paper [167], QoE values are predicted based on video quality parameters using four machine learning algorithms, decision tree, K-NN, ANN, and random forest. Pearson correlation coefficient and root mean square error (RMSE) is used for the performance analysis.

5.3. Resource Management

Network operators and service providers use resource management techniques to improve the performance of the network. SDN maximizes resource utilization using network-based resources management. Data plane level resource management includes the utilization of computing, networking, and caching resources. Networking resources include bandwidth, spectrum, and power, which are used to fulfill user QoE and QoS requirements. Caching techniques to store the most frequently requested data at the device end to remove data redundancy and reduce data transmission delay. Recent technology trends such as face recognition and augmented reality require high computation at the device end to enhance QoS and QoE. Due to scarce computation and battery capacity, the device resources fail to perform these computational tasks. One solution to offload such computational tasks is by deploying computing resources near the end-users using EC [169].

SDN networks are deployed in single and multi-tenant environments for the efficient resources management of data plane. In a single tenancy SDN network, a logically centralized controller manages all data plane resources. In a multi-tenancy SDN network, multiple tenants share data plane layer resources, SDN controller of each tenant manages their isolated resources. In the paper, [170] a framework for software-defined virtualized vehicular ad-hoc-network (VANET) is proposed that enhances the network performance using data plane resources allocation dynamically. A multi-objective optimization problem is formulated from the resource allocation problem. Deep Reinforcement Learning (DRL) algorithms are used to solve the problem and obtain policies regarding resource allocation.

Solution of multi-objective optimization resource allocation problem is proposed for the case study of smart cities [170,171]. Multi-tenancy SDN network-based resource allocation challenges in mobile network operators are addressed [172] in C-RAN. For this, a resource allocation problem is formulated as a non-cooperative game-theoretic problem. Each player selects an optimal set of mobile network operators using a learning algorithm based on regret matching to solve the problem. The computational offloading issue in mobile edge computing (MEC) is also addressed as a non-cooperative game-theoretic problem [173]. MEC servers are the players, and each player performs two actions, active and inactive. The optimization goal of each player is to minimize the consumption of energy. Each player learns optimal actions using RL based model.

Network virtualization's latest advancements enable multi-tenancy SDN networks for sharing data plane resources using network hypervisor installation between the control and data plane. Each tenant manages its isolated network resource using a network hypervisor such as FlowVisor [174] and OpenVirteX [175]. Hypervisors use machine learning algorithms for efficient resource management. In paper [176], hypervisor's CPU consumption monitoring tool is proposed, which is named hvbench. Hvbench is a benchmarking tool used to measure the control message rate. Three regression models are trained to learn the correlation between control message rate and consumption of CPU. These trained models are used to detect the overload of network hypervisors in real-time. Control-plane resource management in SDN is done using the SDN controller placement, which has a significant impact on the SDN network performance. SDN controller processes traffic flows from switches installed at different locations. If the distance between network devices and SDN controller is long, the delay in traffic flow processing will be considered by the resource management. In literature, heuristic algorithms are proposed to solve the problem of controller placement, but these algorithms have a high computational cost. Thus supervised learning algorithms are used to obtain an optimal controller placement [177,178]. The input of these supervised learning models is traffic distribution data, and the output is a controller placement solution from heuristic algorithms. This hybrid approach based on supervised learning and heuristic algorithms leads to an optimal controller placement solution with a low computational cost.

6. IoT Leveraging SDN

IoT plays an important role in the development of intelligent systems such as smart health-care [179], smart transportation systems [180], and smart energy systems [181] using large scale distributed systems. These distributed systems connect billions of RFID nodes and sensors, and hence there is a need for designing a secure, efficient, intelligent, and cost-effective, salable IoT architecture [182]. A sensing network is made up of sensing nodes capable of collecting and monitoring information from the environment, such as temperature, pressure, humidity, and motion. These sensing nodes usually have scarce resources such as limited computing power, battery, and bandwidth, which raise issues of heterogeneity and network configurations. SDN is an effective solution for network management and network configurations. SDN is integrated with the sensing network for sustainability and efficiency of the sensing network [183]. In paper [119], a model of a software-defined wireless sensor network (SDWSN) is proposed to solve heterogeneity and network configurations of scarce resources.

Large-scale distributed systems will generate massive data; machine learning techniques are applied for the predictive analytics of such massive data. Predictive machine learning models are trained using a centralized approach; however, transferring such a massive amount of data to a centralized SDN controller requires large network bandwidth [74]. For low bandwidth consumption, EC-based solutions are used to preprocess the data and improve the system response time. The prepared data are then transferred to the SDN controller to speed up the machine learning training process. To improve IoT services' response time, these trained models are deployed on edge servers [184]. Machine learning and SDN hybrid techniques are applied for route optimization, data analysis,

event detection, node clustering, localization [66], intrusion, and fault detection [185] in IoT applications. In Figure 3, a conceptual IoT architecture based on intelligent SDN architecture with machine learning modules is presented.

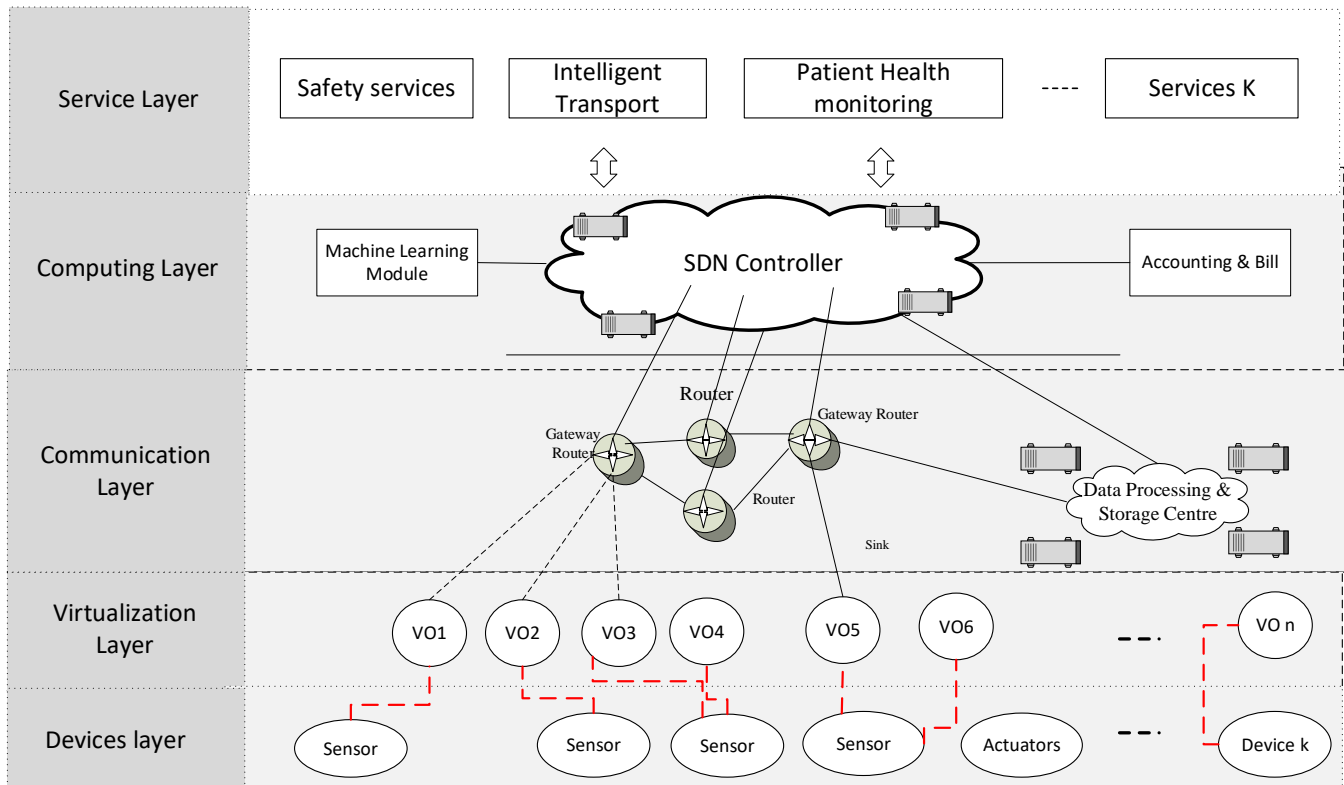


Figure 3. Conceptual IoT Architecture based on Intelligent SDN with Machine learning module.

The benefits of SDN in IoT architecture are discussed in detail by Omnes et al. [186]. SDN allows the dynamic configurations to define the policies and rules for different data planes. They also discussed IoT architecture requirements such as common service layer, big data management, QoS, and network access management. In paper [187], a restful application programming interfaces (APIs) based IoT architecture consisting of several modules such as northbound and southbound APIs is proposed. The control plane consists of a processor and database modules. SBIs module deals with protocols such as HTTP, COAP, and LoRaWAN. In literature, free scale SDN platforms such as vortiQa open network switch director and vortiQa open network are discussed [188]. SDN-based Majord' home management platform is proposed in [189]. Due to the extensive use of the internet, device management has become a difficult task. In Majord' home management, the connected object is represented by CO, and coCO represents a community of the connected objects. The virtual object is represented using Vo, and avatar is used for the management of VOs.

Boussard et al. [190] expand the proposed home automation platform further using a generalization of the concept to any smart environment. CO is generalized to a home device, VO is the abstract view of a device, whereas coVO is a community of the virtual objects. Proposed SDN architecture is composed of four layers, a management layer spanning vertically and three horizontal layers. The data layer performs data generation without routing and forwarding functions. The Control layer is composed of a network controller, CO controller, and coVO controller. The management layer consists of a network manager, application, and VO manager. In paper [191], SDN and distributed data service are applied to IoT architecture. SDN provides data agility, flexibility, and mobility handling, whereas distributed data service is used to manage big data. The proposed approach is needed in

IoT as its applications and services depend upon the collection and analysis of sensing data. The architecture addresses three domains: M2M, networks, and application domains of IoT. In [192], a software-defined infrastructure (SDI) manager-based approach is proposed. SDI Manager consists of cloud computing controllers such as OpenStack and network controllers such as FlowVisor. Cloud computing controller performs user-level management of computing resources. Network controller performs network-level management such as network resource management and collection of topology information of the network. The network controller also interacts with openswitches for the configuration of the data plane's forwarding tables.

Heterogeneity is addressed using the network operating system (NOS) to allow the deployment of different applications on a set of devices of different networks. In paper [193], an operating system has been developed based on ONOS SDN controller for IoT systems to support SDN-WISE. SDN-WISE is a protocol for extending the capabilities of SDN for wireless sensor networks. In paper [194], the issue of heterogeneity in the IoT environment is addressed and solved using a multi-SDN environment. The proposed approach consists of an IoT controller which communicates with the IoT devices. IoT controller handles communication requests and estimates forwarding rules. The proposed approach has some limitations, such as scalability, heterogeneity of identity schemes, routing protocols, and IoT agents' integration. In paper [195], management, security, and scalability relevant issues of IoT are addressed and solved using a layered architecture. The physical layer consists of IoT devices, and the middleware or control layer consists of software-defined blocks. Software-defined blocks include blocks for security, storage, IoT controller, and software-defined controller. Data collectors process the data received from an IoT gateway, where a software-defined security block authenticates and flags the data as positive and negative. IoT controller block computes forwarding rules, and forwarding rules are forwarded to software-defined controller block. Software-defined controller downloads the data into the network switches. SDN-based WoT architecture has limitations of security, data management, and things in web technologies [196]. SDN layer on top of WoT resources provides security and management of devices. SDN-based WoT architecture comprises three layers, the access layer, control layer, and the application layer. The access layer provides WOT gateways to the things, the control layer provides control functions and manages the resources database, and the application layer provides application-level management.

The need for Universal customer premises equipment (uCPE) based edge gateway is increasing to facilitate various SDN/NFV functions. These functions include sensing data aggregation, policy management, data storage, protocol translation, and cloud-specific functions. To make easier flow data between SBI and NBI, MQTT protocol is deployed. Bluetooth and ZigBee modules were adapted to setup the uCPE [197,198]. Softwareized WiFi networks require dedicated softwares for wireless functionalities realization, which is not fully flexible and causes management complexities. In, the authors proposed Po-Fi, highly flexible architecture for SDWSN based on Protocol-Oblivious Forwarding (POF) for WiFi-based innovations. Po-Fi abstract WiFi Access point as a programmable forwarding pipeline based on SDN consensus [199]. The data traffic collected at the Macro Base Station (MBS) increases due to the wide usage of mobile phones. The MBS cannot manage all user's requirements, and to get the expected services, some users are offloaded to the nearby small cells [200]. The tradeoff between the admittance load and economic incentive to achieve optimal offloading SDN assisted Stackelberg Game is proposed. Stackelberg Game model selects the users precisely to aggregate the service with Access Point at MBS to improve QoE. Every player of the game maximizes their payoff utilities in a real-time scenario. The authors obtained maximum throughput per user, which experiences the best data service without any lack of QoE. The Stackelberg Game model proves better as compared with other game theory models in achieving optimal data offloading [201].

Research studies claim that the core network will utilize SDN soon, as some of the data centers and networks of service providers are already benefiting from SDN. This will sim-

plify network function deployment and effective feedback to observe network conditions. In one paper, an SDN mechanism is applied to incorporate wireless IoT edge networks. Long Range (LoRa) was selected as the IoT communication protocol. The study proposes integration architecture for LoRa-SDN [202]. In large-scale IoT networks such as LoRaWAN based IoT, SDN with network slicing must manage network slices flexibly and provide optimized parameter configuration in IoT. Samir Dawaliby et al. proposed SDN-based network slicing architecture for LoRaWAN. The network slices are isolated and deployed virtually over LoRa’s physical gateways. The study also improves large-scale network configurations using TOPG. TOPG is network slicing-based optimization to improves the parameters configuration of LoRa based on each slice QoS thresholds. Simulation results using NS3 highlighted that the proposed optimization approach improves the network performance of LoRa slices. Network performance was evaluated in terms of reliability and QoS thresholds in dense deployments of IoT networks [203].

Real World Applications

IoT security is a hot research topic; in literature, machine learning is applied to SDN to improve IoT security. SDN provides an easy approach to handle simple and distributed DDoS attacks [204,205]. Flow-based dynamic security schemes can be implemented at the network edge [206]. A deep learning network-based approach is proposed in paper [207] for anomaly detection at the edge server. In paper [208], a support vector machine is applied to analyze sensing data and detect abnormal activities. In paper [209], deep learning is applied to edge networks for the detection of IoT attacks. SDN provides significant advantages in the domain of network security, especially in large-scale IoT networks. In summary, EC, SDN, and machine learning can enable intelligent and sustainable IoT solutions. IoT real-world applications of IoT and machine learning leveraging SDN are given in Table 6.

Table 6. Real world applications.

Literature	Approach	Complementary Technologies	Relative Merits
Heterogeneous IoT SDN [210]	Intent-based management and orchestration	NFV and VNF	Orchestration and high level management capabilities to improve scalability and latency.
Virtualized IoT network [186]	NFV and SDN based programmable information technology infrastructure	NFV	Interoperability, security, but too general and insufficient in the components working details. Lack of new scenarios discussions, and presentation of cooperation functionalities between SDN and NFV.
Network architecture for IoT [208]	Software-Defined Fog based IoT architecture	Fog Computing	Supports mobility, flexibility, real-time delivery, fast latency resolving services and increase efficiency.
IoT-fog based systems [211]	SDN and Fog based IoT systems	Fog Computing	Decrease latency, enabling IoT nodes leverage cloud capabilities and increase bandwidth.
Trustable Framework for IoT Devices [212]	QoE based Trustable SDN approach	Mobile edge computing	Orchestrate based on resource abstraction, security using authentication mechanism, coordinate management.
IoT edge cloud architecture [213]	SDN based IoT mobile edge cloud architecture	Mobile edge computing	Improve latency of control and data plane, reduce overhead and improve flexibility.
IoT monitoring framework [214]	Software defined 5G mobile networks based framework	NFV	Data filtering using MQTT, custom monitoring system, handle load balance through NFV, and improve network intelligence.

Table 6. Cont.

Literature	Approach	Complementary Technologies	Relative Merits
Smart homes [215]	Residential functionalities virtualization	NFV and VNF	Low cost, Security updates with no service disruption, flexible gateway but there are limitations of VNF distribution and Management of tunnels.
Centralized IoT devices management [216]	Software development for virtualization	No	Network management for monitoring smart home sensors.
Vehicular networks [217]	Software-defined architecture	No	Maintain functional state stability, reduce control overhead, high rates of delivered data but poor resources allocations and management using the controller.
Smart grid application [218]	IIoT SDN platform	NFV	Reliable and flexible to adapt to natural troubles or failure. Backup to the smart grid resiliency but fault detection and latency management is poor.
E-health medical applications [219]	Control IoT using SDN	No	Transmission optimization during high peak load.
Smart healthcare systems [220]	Traffic management using SDN	No	Heterogeneous traffic management, improve reliability and usability but management functionalities.

7. Limitations and Future Research Directions

This section lists the limitation of current IoT platforms, such as lack of interoperability, compatibility, realizability, and security. Proposing absolute SDN-based solutions is not realistic; however, machine learning applied to SDN controllers will lead to IoT's realization. Figure 4 presents limitations of current IoT. Although SDN with machine learning algorithms addresses some IoT network issues, significant research issues still need to be addressed through SDN. A high-quality training dataset is required to achieve high accuracy of machine learning models in SDN [221]. There are no standard open-source datasets of IoT network data. Comprehensive IoT network datasets will encourage researchers to analyze IoT network data using machine learning models. IoT network flow data is a challenge to develop heterogeneous IoT applications [222]. SDN-based IoT controller decreases the complexities and obtained flexible IoT management. However, attackers can overload the IoT controller through a massive flow of requests. Machine learning-based approaches such as generative adversarial network (GAN) [206] is a practical approach to solve this vulnerability by predicting the new attacks. There are two neural networks in GAN; one neural network generates new data while evaluating the new data authenticity according to a real dataset. GAN generates possible new attacks based on existing attack data; machine learning models can be trained using the new attack data to detect both known and unknown attacks.

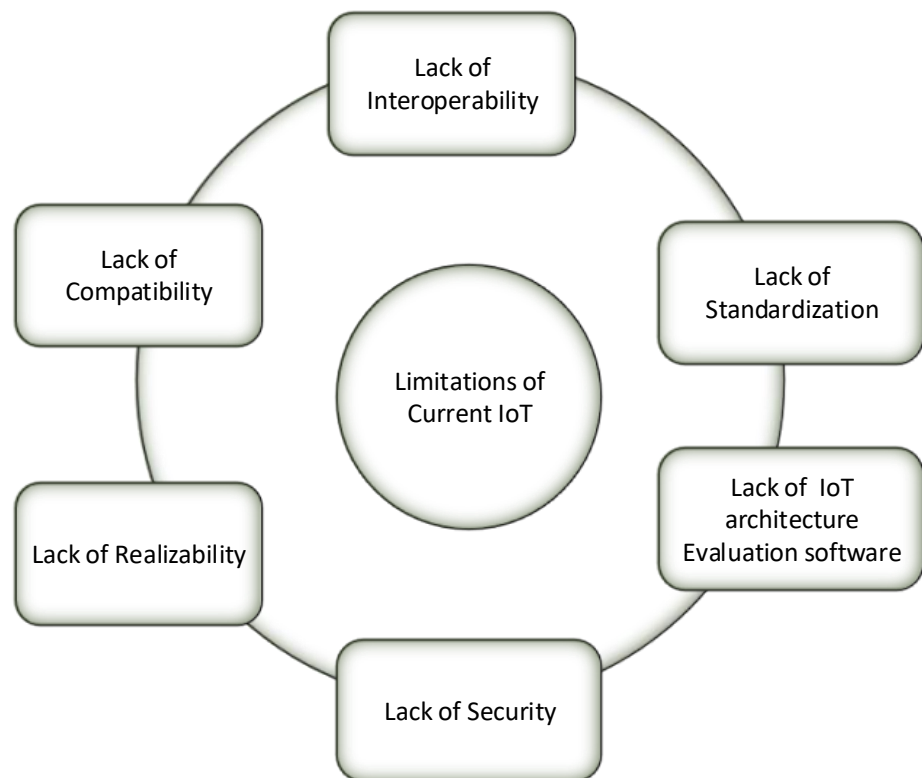


Figure 4. Limitations of current IoT.

IoT devices' scalability raises new issues regarding QoS and security, which can be addressed through machine learning-based SDN solutions. CISCO IoX is one such solution for flexible device management in a real-time IoT environment. To ensure QoS and security in the IoT domain, Microsoft proposed architecture to implement data analytics over the network's edge. Many intelligent applications were proposed to collect data, such as IBM Watson, to develop cognitive systems. However, the realization of IoT is still challenging from both a practical and theoretical perspective [223]. Lack of compatibility means that thousands of research were published in the IoT domain proposing IoT platforms and architectures, raising the need for new network schemes. IoT realization involves many parties, network services providers, data services providers, device manufacturers, and application developers. IoT devices manufacturing companies develop monitoring tools to maintain and manage their devices. Some of the manufacturers provide cloud-based solutions for IoT devices and services management. SDN coupled with cloud computing can hide the complexity of data services and devices management; for example, Amazon provides Amazon web services (AWS) [224] for the management of devices and IoT services.

Based on the presented limitations, we believe that there are imperative directions that have to be considered in the future for IoT research studies. One of the critical challenges which need to be addressed is the interoperability of the proposed IoT platforms with existing platforms. Well-known research institutes and journal publishers should define the main IoT challenges as special issues to reduce the number of partial solutions proposed in the literature. These research institutes and research groups should also work towards the standardization of IoT. IoT simulation software should be developed to test the different IoT architectures, algorithms, and protocols. The real implementation of IoT solutions and performance analysis tools should be developed to test the platforms proposed in the IoT domain. Machine learning applied to SDN coupled with NFV will overcome the management complexity of high-scaled IoT networks. SDN enables the programmability of

network functions to overcome IoT heterogeneity challenges. EC coupled with a machine learning-based SDN controller will enable real-time management of big data.

8. Conclusions

Innovations and development to the communication technologies such as SDN address heterogeneous communication, quality of service requirements, unpredictable network conditions, and a massive influx of data. SDN aims to deploy rule-based management to control and add intelligence to the network using high-level policies to have integral control of the network without knowing issues related to low-level configurations. This paper aims to discuss IoT leveraging SDN solutions to address security challenges, cost of hardware, centralization, and resources management in the IoT environment. Machine learning-based SDN solutions perform optimization of the IoT network, data analysis, and automated and intelligent services provisioning. Machine learning-based SDN solutions also improve the performance, efficiency, and security of IoT solutions. We also addressed potential real-world applications and their relative demerits. The limitations presented in this study provide promising directions towards IoT research studies. Interoperability of the IoT platforms, cooperation functions between SDN and NFV, VNF distribution, and management of tunnels problems are still needed to be addressed. In vehicular networks, software-defined architectures are used to maintain functional stability, reduce control overhead, but poor resource allocations should be addressed. Research institutes and research groups should work towards the standardization of IoT. IoT-SDN simulation software should be developed to test the different software-defined IoT architectures, algorithms, and protocols. IoT leveraging machine learning-based SDN solutions have limited healthcare, smart homes, smart cities for sustainable solutions. Lastly, the problem of fault detection and poor management should be addressed in smart grid environments.

Author Contributions: I. conceived the idea for this paper, designed the methodology, and wrote the paper. Z.G. assisted in the experimental design and paper write-up. J.G. and M.F. assisted in review and editing. A.M.A., A.A. and J.G supervised and proofread the study of a topical review on machine learning, software-defined networking, Internet of Things Applications: research limitations and challenges. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. NRF-2020R111A3074141), the Brain Research Program through the NRF funded by the Ministry of Science, ICT and Future Planning (Grant No. NRF-2019M3C7A1020406), and “Regional Innovation Strategy (RIS)” through the NRF funded by the Ministry of Education.

Acknowledgments: We acknowledge and Thank Shabir Ahmad and Asif Mehmood for their help and support during research data collection and their valuable recommendations and suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ande, R.; Adebisi, B.; Hammoudeh, M.; Saleem, J. Internet of Things: Evolution and technologies from a security perspective. *Sustain. Cities Soc.* **2020**, *54*, 101728. [CrossRef]
2. Sestino, A.; Prete, M.I.; Piper, L.; Guido, G. Internet of Things and Big Data as enablers for business digitalization strategies. *Technovation.* **2020**, *98*, 102173. [CrossRef]
3. Weber, R.H.; Weber, R. *Internet of Things*; Springer: Singapore, 2010; Volume 12.
4. Metcalfe. Available online: https://en.wikipedia.org/wiki/Metcalfe%27s_law (accessed on 13 March 2021).
5. Deore, R.K.; Sonawane, V.R.; Satpute, P.H. Activating the Internet of Thing. *Guest Ed. Introd.* **2015**, *48*, 16–20.
6. Sezer, O.B.; Dogdu, E.; Ozbayoglu, A.M. Context-aware computing, learning, and big data in internet of things: a survey. *IEEE Internet Things J.* **2018**, *5*, 1–27. [CrossRef]
7. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. *Future Gener. Syst.* **2018**, *78*, 544–546. [CrossRef]
8. Amirinasab, M.; Shamshirband, S.; Chronopoulos, A.T.; Mosavi, A.; Nabipour, N. Energy-efficient method for wireless sensor networks low-power radio operation in internet of things. *Electronics* **2020**, *9*, 320. [CrossRef]

9. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
10. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Fourthquarter* **2015**, *17*, 2347–2376. [CrossRef]
11. Bera, S.; Misra, S.; Vasilakos, A.V. Software-defined networking for internet of things: A survey. *IEEE Internet Things J.* **2017**, *4*, 1994–2008. [CrossRef]
12. Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; Markakis, E.K. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Commun. Surv. Tutorials.* **2020**, *22*, 1191–1221. [CrossRef]
13. Graur, F. Dynamic network configuration in the Internet of Things. In Proceedings of the 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Mures, Romania, 26–28 April 2017; pp. 1–4.
14. Xu, G.; Mu, Y.; Liu, J. Inclusion of artificial intelligence in communication networks and services. *ITU J. ICT Discov. Spec.* **2017**, *1*, 1–6.
15. Klimis, V. Abstractions and optimisations for model-checking software-defined networks. Ph.D. Thesis, University of Sussex, Falmer, Brighton, UK, 2021.
16. Open Networking Foundation. Available online: <https://www.opennetworking.org/> (accessed on 13 March 2021).
17. Haleplidis, E.; Pentikousis, K.; Denazis, S.; Salim, J.H.; Meyer, D.; Koufopavlou, O. Software-defined networking (SDN): Layers and architecture terminology. *Internet Res. Task Force (IRTF) RFC 7426* **2015**, 7426. [CrossRef]
18. Alsaeedi, M.; Mohamad, M.M.; Al-Roubaiey, A.A. Toward adaptive and scalable OpenFlow-SDN flow control: A survey. *IEEE Access.* **2019**, *7*, 107346–107379. [CrossRef]
19. Forwarding and Control Element Separation (ForCES) Protocol Specification. Available online: <https://rfc-editor.org/rfc/rfc5810.tx> (accessed on 13 March 2021).
20. Popic, S.; Vuleta, M.; Cvjetkovic, P.; Todorović, B.M. Secure Topology Detection in Software-Defined Networking with Network Configuration Protocol and Link Layer Discovery Protocol. In Proceedings of the 2020 International Symposium on Industrial Electronics and Applications (INDEL), Banja Luka, Bosnia and Herzegovina, 4–6 November 2020.
21. The Open vSwitch Database Management Protocol. Available online: <https://rfceditor.org/rfc/rfc7047.txt> (accessed on 13 March 2021).
22. Asadollahi, S.; Goswami, B.; Sameer, M. Controller’s scalability experiment on software defined networks. In Proceedings of the 2018 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), Bangalore, India, 1–2 February 2018.
23. The locator/ID Separation Protocol (LISP). Available online: <http://www.rfc-editor.org/rfc/rfc6830.txt> (accessed on 13 March 2021).
24. Dargahi, T.; Caponi, A.; Ambrosin, M.; Bianchi, G.; Conti, M. A survey on the security of stateful SDN data planes. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1701–1725. [CrossRef]
25. Bakhshi, T. State of the art and recent research advances in software defined networking. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 71916472017. [CrossRef]
26. Dong, L.; Chen, L.; He, B.; Wang, W. The research on designs of multiple flow tables in the openflow protocol. In Proceedings of the 27th International Conference on Computer Communication and Networks, Hangzhou, China, 30 July–2 August 2018.
27. OpenFlow Version Roadmap. *Tech. Rep.* Available online: http://speed.cis.nctu.edu.tw/ydlin/miscpub/indep_frank.pdf (accessed on 13 March 2021).
28. Mondal, A.; Misra, S.; Maity, I. AMOPE: Performance analysis of OpenFlow systems in software-defined networks. *IEEE Syst. J.* **2019**, *14*, 124–131. [CrossRef]
29. Salih, M.A.; Cosmas, J.; Zhang, Y. OpenFlow 1.3 extension for OMNeT++. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, 26–28 October 2015.
30. Kuźniar, M.; Perešini, P.; Kostić, D.; Canini, M. Methodology, measurement and analysis of flow table update characteristics in hardware openflow switches. *Comput. Networks* **2018**, *136*, 22–36. [CrossRef]
31. Zhao, B.; Zhao, J.; Wang, X.; Wolf, T. RuleTailor: Optimizing flow table updates in openflow switches with rule transformations. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 1581–1594. [CrossRef]
32. Samociuk, D. Secure communication between OpenFlow switches and controllers. *AFIN* **2015**, *39*, 2015.
33. González, S.; De la Oliva, A.; Bernardos, C.J.; Contreras, L.M. Towards a resilient OpenFlow channel through MPTCP. In Proceedings of the 2018 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Valencia, Spain, 6–8 June 2018.
34. Kotani, D.; Okabe, Y. Fast failure detection of OpenFlow channels. In Proceedings of the AINTEC 15: Asian Internet Engineering Conference, Bangkok, Thailand, 18–20 November 2015.
35. Li, W.; Meng, W.; Kwok, L.F. A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. *J. Netw. Comput. Appl.* **2016**, *68*, 126–139. [CrossRef]
36. Azzouni, A.; Braham, O.; Nguyen, T.M.T.; Pujolle, G.; Boutaba, R. Fingerprinting OpenFlow controllers: The first step to attack an SDN control plane. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016.

37. Games, E.; Tovar, D.; Cavadia, A. Design and implementation of a benchmarking tool for OpenFlow controllers. *Int. J. Inf. Technol. Comput. Sci.* **2018**, *10*, 1–13. [CrossRef]
38. Darianian, M.; Williamson, C.; Haque, I. Experimental evaluation of two openflow controllers. In Proceedings of the 25th International Conference on Network Protocols, Toronto, ON, Canada, 10–13 October 2017.
39. Priya, A.V.; Radhika, N. Performance comparison of SDN OpenFlow controllers. *Int. J. Comput. Aided Eng. Technol.* **2019**, *11*, 467–479. [CrossRef]
40. Open vSwitch, March. 2021. Available online: <https://www.openvswitch.org/> (accessed on 27 August 2020).
41. Pantou: OpenFlow 1.3 for OpenWRT," March 2021. Available online: <https://github.com/CPqD/ofsoftswitch13/wiki/OpenFlow-1.3-forOpenWRT> (accessed on 27 August 2020).
42. Yang, C.; Liu, J.; Chen, W.; Leu, F.; Chu, W.C. Implementation of a virtual switch monitoring system using OpenFlow on cloud. *Int. J. Hoc Ubiquitous Comput.* **2017**, *24*, 162–172. [CrossRef]
43. Chu, T.-W.; Shen, C.; Wu, C. The hardware and software co-design of a configurable QoS for video streaming based on OpenFlow protocol and NetFPGA platform. *Multimed. Tools Appl.* **2018**, *77*, 9071–9091. [CrossRef]
44. Zeng, T.; Wang, S.; Liu, S. Research on Intelligent Linkage Server Switch in Case of Power Loss in Computer Room. In Proceedings of the IEEE 11th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 16–18 October 2020; pp. 493–496.
45. Yan, J.; Jia, C.; Tang, L.; Li, T.; Lv, G.; Quan, W.; Yang, H. Network Programming Interface in General-Purpose Multi-core Processor: A Survey. In Proceedings of the 15th International Conference on Computer Science & Education (ICCSE), Delft, The Netherlands, 18–22 August 2020; pp. 675–680.
46. Badotra, S.; Panda, S.N. Evaluation and comparison of OpenDayLight and open networking operating system in software-defined networking. *Clust. Comput.* **2019**, *23*, 1–11. [CrossRef]
47. Badotra, S.; Singh, J. Open Daylight as a Controller for Software Defined Networking. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*.
48. Pox. Available online: <http://www.noxrepo.org/pox/> (accessed on 27 August 2020).
49. Chandramouli, M.; Clemm, A. Model-driven analytics in SDN networks. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 July 2017; pp. 668–673.
50. Islam, M.T.; Islam, N.; Al Refat, M. Node to node performance evaluation through RYU SDN controller. *Wirel. Pers. Commun.* **2020**, *112*, 1–16. [CrossRef]
51. Mamushiane, L.; Lysko, A.; Dlamini, S. A comparative evaluation of the performance of popular SDN controllers. In Proceedings of the Wireless Days, Dubai, United Arab Emirates, 3–5 April 2018; pp. 54–59.
52. Aly, W.H.F.; Al-anazi, A.M.A. Enhanced CONTROLLER Fault Tolerant (ECFT) model for software defined networking. In Proceedings of the Fifth International Conference on Software Defined Systems (SDS), Barcelona, Spain, 23–26 April 2018; pp. 217–222.
53. Paliwal, M.; Shrimankar, D.; Tembhrune, O. Controllers in SDN: A review report. *IEEE Access.* **2018**, *6*, 36256–36270. [CrossRef]
54. Latif, Z.; Sharif, K.; Li, F.; Karim, M.M.; Biswas, S.; Wang, Y. A comprehensive survey of interface protocols for software defined networks. *J. Netw. Comput. Appl.* **2020**, *156*, 102563. [CrossRef]
55. Benamrane, F.; Benaini, R. An East-West interface for distributed SDN control plane: Implementation and evaluation. *Comput. Electr. Eng.* **2017**, *57*, 162–175. [CrossRef]
56. Sarmiento, D.E.; Lebre, A.; Nussbaum, L.; Chari, A. Decentralized SDN Control Plane for a Distributed Cloud-Edge Infrastructure: A Survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 256–281. [CrossRef]
57. Mendiola, A.; Astorga, J.; Jacob, E.; Higuero, M. A survey on the contributions of software-defined networking to traffic engineering. *IEEE Commun. Surv. Tutor.* **2016**, *25*, 918–953. [CrossRef]
58. Ahmad, I.; Namal, S.; Ylianttila, M.; Gurtov, A. Security in software defined networks: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 2317–2346. [CrossRef]
59. Yan, Q.; Yu, F.R.; Gong, Q.; Li, J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 602–622. [CrossRef]
60. Fonseca, P.C.; Mota, E.S. A survey on fault management in software-defined networks. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2284–2321. [CrossRef]
61. Haque, I.T.; Abu-Ghazaleh, N. Wireless software defined networking: A survey and taxonomy. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2713–2737. [CrossRef]
62. Chen, T.; Matinmikko, M.; Chen, X.; Zhou, X.; Ahokangas, P. Software defined mobile networks: Concept, survey, and research directions. *IEEE Commun. Mag.* **2015**, *53*, 126–133. [CrossRef]
63. Thyagaturu, A.S.; Mercian, A.; McGarry, M.P.; Reisslein, M.; Kellerer, W. Software defined optical networks (SDONs): A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2738–2786. [CrossRef]
64. Michel, O.; Keller, E. SDN in wide-area networks: A survey. In Proceedings of the 2017 Fourth International Conference on Software Defined Systems (SDS), Valencia, Spain, 8–11 May 2017; pp. 37–42.
65. Baktir, A.C.; Ozgovde, A.; Ersoy, C. How can edge computing benefit from software-defined networking: A survey, use cases, and future directions. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2359–2391. [CrossRef]

66. Rafique, W.; Qi, L.; Yaqoob, I.; Imran, M.; Rasool, R.U.; Dou, W. Complementing IoT services through software defined networking and edge computing: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1761–1804. [[CrossRef](#)]
67. Zolfaghari, H.; Rossi, D.; Nurmi, J. A custom processor for protocol-independent packet parsing. *Microprocess. Microsys.* **2020**, *72*, 102910. [[CrossRef](#)]
68. Han, S.; Jang, S.; Choi, H.; Lee, H.; Pack, S. Virtualization in Programmable Data Plane: A Survey and Open Challenges. *IEEE Open J. Commun. Soc.* **2020**, *1*, 527–534. [[CrossRef](#)]
69. Dang, H.T.; Wang, H.; Jepsen, T.; Brebner, G.; Kim, C.; Rexford, J.; Soulé, R.; Weatherspoon, H. Whippersnapper: A p4 language benchmark suite. In Proceedings of the Symposium on SDN Research, Santa Clara, CA, USA, 3–4 April 2017; pp. 95–101.
70. Imran, S.A.; Kim, D.H. Design and implementation of thermal comfort system based on tasks allocation mechanism in smart homes. *Sustainability* **2019**, *11*, 5849. [[CrossRef](#)]
71. Imran, S.A.; Kim, D.H. A task orchestration approach for efficient mountain fire detection based on microservice and predictive analysis In IoT environment. *J. Intell. Fuzzy Syst.* **2021**, *40*, 5681–5696. [[CrossRef](#)]
72. Imran, I.N.; Ahmad, S.; Kim, D.H. Health Monitoring System for Elderly Patients Using Intelligent Task Mapping Mechanism in Closed Loop Healthcare Environment. *Symmetry* **2021**, *13*, 357. [[CrossRef](#)]
73. Imran, I.N.; Ahmad, S.; Kim, D.H. Towards Mountain Fire Safety Using Fire Spread Predictive Analytics and Mountain Fire Containment in IoT Environment. *Sustainability* **2021**, *13*, 2461. [[CrossRef](#)]
74. Minerva, R.; Biru, A.; Rotondi, D. Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiat.* **2015**, *1*, 1–86.
75. Park, B.; Kwon, K. 2.4-GHz Bluetooth Low Energy Receiver Employing New Quadrature Low-Noise Amplifier for Low-Power Low-Voltage IoT Applications. *IEEE Trans. Microw. Theory Tech.* **2020**, *69*, 1887–1895. [[CrossRef](#)]
76. Alladi, T.; Chamola, V.; Sikdar, B.; Choo, K.R. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consum. Electron. Mag.* **2020**, *9*, 17–25. [[CrossRef](#)]
77. Babun, L.; Aksu, H.; Ryan, L.; Akkaya, K.; Bentley, E.S.; Uluagac, A.S. Z-iot: Passive device-class fingerprinting of zigbee and z-wave iot devices. In Proceedings of the ICC 2020–2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020.
78. Krasniqi, Z.; Vershevc, B. Smart Home: Automatic Control Of Lighting Through Z-Wave Iot Technology. In Proceedings of the UBT International Conference, Lipjan, Kosovo, 31 October 2020 .
79. Fraga-Lamas, P.; Celaya-Echarri, M.; Azpilicueta, L.; Lopez-Iturri, P.; Falcone, F.; Fernández-Caramés, T.M. Design and empirical validation of a lorawan IoT smart irrigation system. *Multidiscip. Digit. Publ. Inst. Proc.* **2020**, *42*, 62. [[CrossRef](#)]
80. Basford, P.J.; Bulot, F.M.J.; Apetroaie-Cristea, M.; Cox, S.J.; Ossont, S.J. LoRaWAN for smart city IoT deployments: A long term evaluation. *Sensors* **2020**, *20*, 648. [[CrossRef](#)]
81. Codeluppi, G.; Cilfone, A.; Davoli, L.; Ferrari, G. LoRaFarM: A LoRaWAN-based smart farming modular IoT architecture. *Sensors* **2020**, *20*, 2028. [[CrossRef](#)]
82. Langley, D.J.; van Doorn, J.; Ng, I.C.L.; Stieglitz, S.; Lazovik, A.; Boonstra, A. The Internet of Everything: Smart things and their impact on business models. *J. Bus. Res.* **2021**, *122*, 853–863. [[CrossRef](#)]
83. de Amorim Silva, R.; Braga, R.T.V. Enhancing Future Classroom Environments Based on Systems of Systems and the Internet of Anything. *IEEE Internet Things J.* **2020**, *7*, 10475–10482. [[CrossRef](#)]
84. Rahman, M.A.; Asyhari, A.T. The emergence of Internet of Things (IoT): Connecting anything, anywhere. *Computers* **2019**, *8*, 40. [[CrossRef](#)]
85. Chen, S.; Ma, R.; Chen, H.H.; Zhang, H.; Meng, W.; Liu, J. Machine-to-machine communications in ultra-dense networks—A survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1478–1503. [[CrossRef](#)]
86. Tur, M.R.; Bayindir, R. The Requirements of the Technique of Communication from Machine to Machine Applied in Smart Grids. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*; Springer: Singapore, 2020; pp. 405–418.
87. Gonçalves, P.; Ferreira, J.; Pedreiras, P.; Corujo, D. Adapting SDN datacenters to support Cloud IIoT applications. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 8–11 September 2015.
88. Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 7–11 July 2015.
89. Dujovne, D.; Watteyne, T.; Vilajosana, X.; Thubert, P. 6TiSCH: deterministic IP-enabled industrial internet (of things). *IEEE Commun. Mag.* **2014**, *52*, 36–41. [[CrossRef](#)]
90. Espinoza, H.; Kling, G.; McGroarty, F.; O’Mahony, M.; Ziouvelou, X. Estimating the impact of the Internet of Things on productivity in Europe. *Heliyon* **2020**, *6*, e03935. [[CrossRef](#)] [[PubMed](#)]
91. Andore, D.B. AWS IOT Platform based Remote Monitoring by using Raspberry Pi. *Int. J. Latest Technol. Eng. Manag. Appl. Sci.* **2017**, *6*, 38–42.
92. Libelium: Connecting Sensors to the Cloud. Available online: <http://www.libelium.com> (accessed on 27 August 2020).
93. Hewlett Packard Enterprise (HPE). Available online: <https://www.hpe.com/us/en/home.html> (accessed on 27 August 2020).
94. IBM Watson Internet of Things (IoT). Available online: <http://www.ibm.com/internet-of-things/> (accessed on 27 August 2020).
95. Enterprise IoT Solutions and Platform Technology. Available online: <https://www.thingworx.com/> (accessed on 12 July 2020).
96. IoT InterDigital. Available online: <http://www.interdigital.com/iot/> (accessed on 27 August 2020).

97. De Paolis, L.T.; de Luca, V.; Paiano, R. Sensor data collection and analytics with thingsboard and spark streaming. In Proceedings of the 2018 IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems (EESMS), Salerno, Italy, 21–22 June 2018.
98. Internet of Things, Cisco. Available online: <http://www.cisco.com/c/en/us/solutions/internet-of-things/iot-products/solutions.html> (accessed on 27 August 2020).
99. Pflanzner, T.; Kertész, A. A survey of IoT cloud providers. In Proceedings of the 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 30 May–3 June 2016; pp. 730–735.
100. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [[CrossRef](#)]
101. Guan, G.; Dong, W.; Gao, Y.; Fu, K.; Cheng, Z. TinyLink: A Holistic System for Rapid Development of IoT Applications. *ACM Trans. Sens. Netw. (TOSN)*. **2020**, *17*, 1–29.
102. Lueth, K.L. Get started with the Internet of Things in your organization. *Introd. Microsoft Azur. Internet Things Suite. Microsoft Corp* **2015**.
103. Internet of Things, Dell United States. Available online: <http://www.dell.com/en-us/work/learn/internet-of-things-solutions> (accessed on 27 August 2020).
104. OpenMTC. Available online: <http://www.openmtc.org/index.html> (accessed on 27 August 2020).
105. Antonio, I.; Morabito, G.; Atzori, L. The Social Internet of Things, Cloud Engineering (IC2E). In Proceedings of the 2015 IEEE International Conference, Tempe, AZ, USA, 9–13 March 2015; p. 1.
106. Amato, F.; Moscato, V.; Picariello, A.; Sperlí, G. Recommendation in social media networks. In Proceedings of the IEEE Third International Conference on Multimedia Big Data (BigMM), Laguna Hills, CA, USA, 19–21 April 2017.
107. Amato, F.; Moscato, V.; Picariello, A.; Sperlí, G. Kira: A system for knowledge-based access to multimedia art collections. In Proceedings of the IEEE 11th international conference on semantic computing (ICSC), San Diego, CA, USA, 30 January–1 February 2017.
108. Chahal, R.K.; Kumar, N.; Batra, S. Trust management in social Internet of Things: A taxonomy, open issues, and challenges. *Comput. Commun.* **2020**, *150*, 13–46. [[CrossRef](#)]
109. Leminen, S.; Rajahonka, M.; Wendelin, R.; Westerlund, M. Industrial internet of things business models in the machine-to-machine context. *Ind. Mark. Manag.* **2020**, *84*, 298–311. [[CrossRef](#)]
110. Raju, P.S.; Rajendran, R.A.; Mahalingam, M. Perspectives of Machine Learning and Deep Learning in Internet of Things and Cloud: Artificial Intelligence-Based Internet of Things System. In *Challenges and Opportunities for the Convergence of IoT, Big Data, and Cloud Computing*; IGI Global: Enver, CO, USA, 2021; pp. 279–295.
111. Kim, G.; Kim, J.; Lee, S. An SDN based fully distributed NAT traversal scheme for IoT global connectivity. In Proceedings of the 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 28–30 October 2015.
112. Gazis, V.; Görtz, M.; Huber, M.; Leonardi, A.; Mathioudakis, K.; Wiesmaier, A.; Zeiger, F.; Vasilomanolakis, E. A Survey of Technologies for the Internet of Things. In Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 24–28 August 2015; pp. 1090–1095.
113. Datta, S.K.; Bonnet, C.; Haerri, J. Fog computing architecture to enable consumer centric internet of things services. In Proceedings of the 2015 International Symposium on Consumer Electronics (ISCE), Madrid, Spain, 24–26 June 2015.
114. Pourghebleh, B.; Hayyolalam, V.; Anvigh, A.A. Service discovery in the Internet of Things: review of current trends and research challenges. *Wireless Netw.* **2020**, *26*, 5371–5391. [[CrossRef](#)]
115. Salam, A. Internet of things for sustainable mining. In *Internet of Things for Sustainable Community Development*; Springer: Cham, Switzerland, 2020; pp. 243–271.
116. Alhaidari, F.; Rahman, A.; Zagrouba, R. Cloud of Things: architecture, applications and challenges. *J. Ambient. Intell. Humaniz. Comput.* **2020**, 1–19. [[CrossRef](#)]
117. Chowdhury, A.U.; Elahi, M.M. Design of a Smart Gateway for Edge Enabled IoT Applications. In Proceedings of the IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, 5–7 June 2020; pp. 417–420.
118. Balasubramanian, S.; Meyyappan, T. Game Theory Based Offload and Migration-Enabled Smart Gateway for Cloud of Things in Fog Computing. In *Computing in Engineering and Technology*; Springer: Singapore, 2020; pp. 253–266.
119. Seol, S.; Shin, Y.; Kim, W. Design and realization of personal IoT architecture based on mobile gateway. *Int. J. Smart Home* **2015**, *9*, 133–144. [[CrossRef](#)]
120. Al Asif, M.R.; Mahfuz, N.; Momin, M.A. An SDN-Enabled IoT Architecture with Fog Computing and Edge. In *Proceedings of International Joint Conference on Computational Intelligence*; Springer Nature: Singapore, 2020; p. 409.
121. Sun, L. Service Chaining Security Based on Blockchain. *J. Phys. Conf. Ser. Publ.* **2020**, *1634*, 012031. [[CrossRef](#)]
122. Callegati, F.; Cerroni, W.; Contoli, C.; Santandrea, G. Dynamic chaining of virtual network functions in cloud-based edge networks. In Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft), London, UK, 13–17 April 2015.
123. Czarnecka, P. The Multi-Tenant Cloud Computing Architecture Allows the Service Consumers to Share the Computing. *Tenn. Res. Int. Soc. Sci.* **2020**, *2*, 1–21.

124. Distefano, S.; Merlino, G.; Puliafito, A. A utility paradigm for IoT: The sensing Cloud. *Pervasive Mob. Comput.* **2015**, *20*, 127–144. [CrossRef]
125. Atzori, L.; Iera, A.; Morabito, G. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Netw.* **2017**, *56*, 122–140. [CrossRef]
126. Sandor, H.; Genge, B.; Sebestyeny-Pal, G. Resilience in the Internet of Things: The Software Defined Networking approach, In Intelligent Computer Communication and Processing (ICCP). In Proceedings of the 2015 IEEE International Conference on, Cluj-Napoca, Romania, 3–5 September 2015; pp. 545–552.
127. Home-FIWARE. Available online: <https://www.fiware.org/> (accessed on 11 November 2020).
128. iCore. Available online: <http://www.iot-icore.eu/> (accessed on 11 November 2020).
129. Miladinovic, I.; Schefer-Wenzl, S. A highly scalable iot architecture through network function virtualization. *Open J. Internet Things (OJIOT)* **2017**, *3*, 127–135.
130. Sobin, C.C. A survey on architecture, protocols and challenges in iot. *Wirel. Pers. Commun.* **2020**, *112*, 1383–1429. [CrossRef]
131. Why Elastic Scalability Matters in Network Functions Virtualization. Available online: <https://www.metaswitch.com/blog/why-elastic-scalability-matters-in-network-functions-virtualization> (accessed on 27 August 2020).
132. Moon, J.-H.; Shine, Y.-T. A study of distributed SDN controller based on apache kafka. In Proceedings of the 2020 IEEE International Conference on Big Data and Smart Computing (BigComp), Pusan, Korea, 19–22 February 2020; pp. 44–47.
133. Ahmad, M.; Alowibdi, J.S.; Ilyas, M.U. vIoT: A first step towards a shared, multi-tenant IoT Infrastructure architecture. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 20–24 May 2017.
134. SAM, The Ultimate Internet Connected Electronics Kit. Available online: <https://www.kickstarter.com/projects/1842650056/sam-the-ultimate-internet-connected-electronics-ki> (accessed on 12 July 2020).
135. Dweet, Share Your Thing- Like It Ain'T no Thang. Available online: <http://dweet.io/> (accessed on 12 July 2020).
136. Particle, Connect Your Internet of Things (IoT) Devices. Available online: <https://www.particle.io/> (accessed on 12 July 2020).
137. Mahapatra, T. Composing high-level stream processing pipelines. *J. Big Data* **2020**, *7*, 1–28. [CrossRef]
138. How IBM's Node-RED is Hacking Together the Internet of Things. Available online: <http://www.techrepublic.com/article/node-red/> (accessed on 12 July 2020).
139. Amaral, P.; Dinis, J.; Pinto, P.; Bernardo, L.; Tavares, J.; Mamede, H.S. Machine learning in software defined networks: Data collection and traffic classification. In Proceedings of the 2016 IEEE 24th International Conference on Network Protocols (ICNP), Singapore, 8–11 November 2016.
140. Alqahtani, J.; Alanazi, S.; Hamdaoui, B. Traffic Behavior in Cloud Data Centers: A Survey. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 27 July 2020; pp. 2106–2111.
141. Glick, M.; Rastegarfar, H. Scheduling and control in hybrid data centers. In Proceedings of the 2017 IEEE Photonics Society Summer Topical Meeting Series (SUM), San Juan, PR, USA, 21 August 2017.
142. Xiao, P.; Qu, W.; Qi, H.; Xu, Y.; Li, Z. NAN efficient elephant flow detection with cost-sensitive in SDN. In Proceedings of the IEEE INISCom'15, Tokyo, Japan, 16 July 2015; pp. 24–28.
143. Owusu, A.I.; Nayak, A. An Intelligent Traffic Classification in SDN-IoT: A Machine Learning Approach. In Proceedings of the 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Odessa, Ukraine, 26–29 May 2020; pp. 1–6.
144. Wang, P.; Hao, W.; Jin, Y. Fine-grained traffic flow prediction of various vehicle types via fusion of multisource data and deep learning approaches. *IEEE Trans. Intell. Transp. Syst.* **2020**. [CrossRef]
145. Uddin, M.; Nadeem, T. rafficVision: A case for pushing software defined networks to wireless edges. In Proceedings of the 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Brasilia, Brazil, 10–13 October 2016.
146. Wang, P.; Lin, S.-C.; Luo, M. A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs. In Proceedings of the IEEE SCC'16, San Francisco, CA, USA, 1 September 2016; pp. 760–765.
147. Ahmad, S.; Jamil, F.; Iqbal, N.; Jamil, F.; Kim, D. Optimal Route Recommendation for Waste Carrier Vehicles for Efficient Waste Collection: A Step Forward Towards Sustainable Cities. *IEEE Access.* **2020**, *8*, 77875–77887. [CrossRef]
148. Ahmad, S.; Imran, Iqbal, N.; Jamil, F.; Kim, D. Optimal Policy-Making for Municipal Waste Management Based on Predictive Model Optimization. *IEEE Access.* **2020**, *8*, 218458–218469. [CrossRef]
149. Wahid, F.; Fayaz, M.; Aljarbouh, A.; Mir, M.; Amir, M.; Imra. Energy consumption optimization and user comfort maximization in smart buildings using a hybrid of the firefly and genetic algorithms. *Energies.* **2020**, *13*, 4363. [CrossRef]
150. Awad, M.K.; Ahmed, M.H.H.; Almutairi, A.F.; Ahmad, I. Machine learning-based multipath routing for software defined networks. *J. Netw. Syst. Manag.* **2021**, *29*, 1–30. [CrossRef]
151. Azzouni, A.; Boutaba, R.; Pujolle, G. NeuRoute: Predictive dynamic routing for software-defined networks. In Proceedings of the 2017 13th International Conference on Network and Service Management (CNSM), Tokyo, Japan, 26–30 November 2017.
152. Sendra, S.; Rego, A.; Lloret, J.; Jimenez, J.M.; Romero, O. Including artificial intelligence in a routing protocol using software defined networks. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017.

153. Francois, F.; Gelenbe, E. Optimizing secure SDN-enabled inter-data centre overlay networks through cognitive routing. In Proceedings of the 2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), London, UK, 19–21 September 2016.
154. Lin, S.-C.; Akyildiz, I.F.; Wang, P.; Luo, M. QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach. In Proceedings of the 2016 IEEE International Conference on Services Computing (SCC), San Francisco, CA, USA, 27 June–2 July 2016.
155. Azzouni, A.; Boutaba, R.; Pujolle, G. NeuRoute: Predictive dynamic routing for software-defined networks. *IEEE Access*. **2020**, *8*, 46193–46205.
156. Iqbal, N.; Jamil, F.; Ahmad, S.; Kim, D. A Novel Blockchain-Based Integrity and Reliable Veterinary Clinic Information Management System Using Predictive Analytics for Provisioning of Quality Health Services. *IEEE Access*. **2021**, *9*, 8069–8098. [[CrossRef](#)]
157. Jamil, F.; Iqbal, N.; Imran; Ahmad, S.; Kim, D. Peer-to-Peer Energy Trading Mechanism based on Blockchain and Machine Learning for Sustainable Electrical Power Supply in Smart Grid. *IEEE Access*. **2021**, *9*, 39193–39217. [[CrossRef](#)]
158. Iqbal, N.; Ahmad, R.; Jamil, F.; Kim, D. Hybrid features prediction model of movie quality using Multi-machine learning techniques for effective business resource planning. *J. Intell. Fuzzy Syst.* **2021**, 1–22. [[CrossRef](#)]
159. Khan, A.N.; Iqbal, N.; Ahmad, R.; Kim, D. Ensemble Prediction Approach Based on Learning to Statistical Model for Efficient Building Energy Consumption Management. *Symmetry*. **2021**, *13*, 405. [[CrossRef](#)]
160. Iqbal, N.; Jamil, F.; Ahmad, S.; Kim, D. Toward effective planning and management using predictive analytics based on rental book data of academic libraries. *IEEE Access* **2020**, *8*, 81978–81996. [[CrossRef](#)]
161. López-Raventós, Á.; Wilhelmi, F.; Barrachina-Muñoz, S.; Bellalta, B. Combining Software Defined Networks and Machine Learning to enable Self Organizing WLANs. In Proceedings of the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 21–23 October 2019.
162. Alvizu, R.; Troia, S.; Maier, G.; Pattavina, A. Matheuristic with machine-learning-based prediction for software-defined mobile metro-core networks. *J. Opt. Commun. Netw.* **2017**, *9*, D19–D30. [[CrossRef](#)]
163. Cui, C.-X.; Xu, Y.-B. Research on load balance method in SDN. *Int. J. Grid Distrib. Comput.* **2016**, *9*, 25–36.
164. Azzouni, A.; Pujolle, G. NeuTM: A neural network-based framework for traffic matrix prediction in SDN. In Proceedings of the NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018.
165. Michael, S.; Anna, Z.J. An Identity Provider as a Service platform for the eduGAIN research and education community. In Proceedings of the 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Arlington, VA, USA, 8–12 April 2019.
166. Carner, J.; Mestres, A.; Alarcón, E.; Cabellos, A. Machine learning-based network modeling: An artificial neural network model vs a theoretical inspired model. In Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 4–7 July 2017.
167. Abar, T.; Letaifa, A.B.; El Asmi, S. Machine learning based QoE prediction in SDN networks. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017.
168. Letaifa, A.B. Adaptive QoE monitoring architecture in SDN networks: Video streaming services case. In Proceedings of the IEEE IWCMC 17, Valencia, Spain, 26–30 June 2017; pp. 1383–1388.
169. Huo, R.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Leung, V.C.M.; Liu, Y. Software defined networking, caching, and computing for green wireless networks. *IEEE Commun. Mag.* **2016**, *54*, 185–193. [[CrossRef](#)]
170. He, Y.; Yu, F.R.; Zhao, N.; Yin, H.; Boukerche, A. Deep reinforcement learning (DRL)-based resource management in software-defined and virtualized vehicular ad hoc networks. In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, Miami, FL, USA, 13–17 November 2017.
171. He, Y.; Yu, F.R.; Zhao, N.; Leung, V.C.M.; Yin, H. Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach. *IEEE Commun. Mag.* **2017**, *55*, 31–37. [[CrossRef](#)]
172. Narmanlioglu, O.; Zeydan, E. Learning in SDN-based multi-tenant cellular networks: A game-theoretic perspective. In Proceedings of the 2017 IFIP IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017.
173. Ranadheera, S.; Maghsudi, S.; Hossain, E. Mobile edge computation offloading using game theory and reinforcement learning. *arXiv* **2017**, arXiv:1711.09012.
174. Xiang, Z.; Pandi, S.; Cabrera, J.; Granelli, F.; Seeling, P.; Fitzek, F.H.P. An Open Source Testbed for Virtualized Communication Networks. *IEEE Commun. Mag.* **2021**, *59*, 77–83. [[CrossRef](#)]
175. Yang, G.; Yu, B.; Jin, H.; Yoo, C. Libera for programmable network virtualization. *IEEE Commun. Mag.* **2020**, *58*, 38–44. [[CrossRef](#)]
176. Sieber, C.; Basta, A.; Blenk, A.; Kellerer, W. Online resource mapping for SDN network hypervisors using machine learning. In Proceedings of the 2016 IEEE NetSoft Conference and Workshops (NetSoft), Seoul, Korea, 6–10 June 2016.
177. He, M.; Kalmbach, P.; Blenk, A.; Kellerer, W.; Schmid, S. Algorithm-data driven optimization of adaptive communication networks. In Proceedings of the 2017 IEEE 25th International Conference on Network Protocols (ICNP), Toronto, ON, Canada, 10–13 October 2017.

178. Blenk, A.; Kalmbach, P.; Kellerer, W.; Schmid, S. CO'zapft is: Tap your network algorithm's big data! In Proceedings of the Workshop on Big Data Analytics and Machine Learning for Data Communication Networks, Los Angeles, CA, USA, 21 August 2017.
179. Kakiz, M.T.; Öztürk, E.; Çavdar, T. A novel SDN-based IoT architecture for big data. In Proceedings of the 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, Turkey, 16–17 September 2017.
180. Nguyen, C.; Hoang, D. Software-Defined Virtual Sensors for Provisioning IoT Services on Demand. In Proceedings of the 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15–18 May 2020; pp. 796–802.
181. Bakshi, K. Network considerations for open source based clouds. In Proceedings of the 2015 IEEE Aerospace Conference, Big Sky, MT, USA, 7–14 March 2015.
182. Munir, A.; Kansakar, P.; Khan, S.U. IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things. *IEEE Consum. Electron. Mag.* **2017**, *6*, 74–82. [[CrossRef](#)]
183. Alli, A.A.; Alam, M.M. The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications. *Internet Things* **2020**, *9*, 100177. [[CrossRef](#)]
184. Wen, Z.; Yang, R.; Garraghan, P.; Lin, T.; Xu, J.; Rovatsos, M. Fog orchestration for internet of things services. *IEEE Internet Comput.* **2017**, *21*, 16–24. [[CrossRef](#)]
185. Bansal, S.; Kumar, D. IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 1–25. [[CrossRef](#)]
186. Omnes, N.; Bouillon, M.; Fromentoux, G.; le Grand, O. A programmable and virtualized network and IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges. In Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, Paris, France, 17–19 February 2015.
187. Wen, Z.; Liu, X.; Xu, Y.; Zou, J. A RESTful framework for Internet of things based on software defined network in modern manufacturing. *Int. J. Adv. Manuf. Technol.* **2016**, *84*, 361–369. [[CrossRef](#)]
188. Mohammed, A.H.; Khaleefah, R.M.; Abdulateef, I.A. A Review Software Defined Networking for Internet of Things. In Proceedings of the 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 26–28 June 2020; pp. 1–8.
189. Bekri, W.; Jmal, R.; Fourati, L.C. Internet of things management based on software defined networking: a survey. *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 385–410. [[CrossRef](#)]
190. Boussard, M.; Bui, D.T.; Ciavaglia, L.; Douville, R.; le Pallec, M.; le Sauze, N.; Noirie, L.; Papillon, S.; Peloso, P.; Santoro, F. Software-defined lans for interconnected smart environment. In Proceedings of the 2015 27th International Teletraffic Congress, Ghent, Belgium, 8–10 September 2015.
191. Hakiri, A.; Berthou, P.; Gokhale, A.; Abdellatif, S. Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications. *IEEE Commun. Mag.* **2015**, *53*, 48–54. [[CrossRef](#)]
192. Nisar, K.; Welch, I.; Hassan, R.; Sodhro, A.H.; Pirbhulal, S. A Survey on the Architecture, Application, and Security of Software Defined Networking. Internet of Things. *Internet Things* **2020**, *12*, 100289. [[CrossRef](#)]
193. Anadiotis, A.-C.G.; Galluccio, L.; Milardo, S.; Morabito, G.; Palazzo, S. Towards a Software-Defined Network Operating System for the IoT, In Internet of Things (WFIoT). In Proceedings of the 2015 IEEE 2nd World Forum, Milan, Italy, 14–16 December 2015; pp. 579–584.
194. Wani, A.; Revath, S. Ransomware protection in IoT using software defined networking. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 3166–3175.
195. Jararweh, Y.; Al-Ayyoub, M.; Benkhelifa, E.; Vouk, M.; Rindos, A. SDIoT: A software defined based internet of things framework. *J. Ambient. Intell. Humaniz. Comput.* **2015**, *6*, 453–461. [[CrossRef](#)]
196. Rahouti, M.; Xiong, K.; Xin, Y. Secure Software-Defined Networking Communication Systems for Smart Cities: Current Status, Challenges, and Trends. *IEEE Access.* **2020**, *9*, 12083–12113. [[CrossRef](#)]
197. Zhou, L.; Chiu, A.; Satterlee, M.; Mahar, D.; Zhang, Q.; Palacharla, P.; Tadashi, I. IoT Gateway Edge VNFs on uCPE. In Proceedings of the 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Verona, Italy, 27–29 November 2018.
198. Czaja, S.; Gawron, Z.; Kaczmarek, P. Virtualized SD-WAN: Practical Implementation of NFV. *Przegląd Telekomunikacyjny+Wiadomości Telekomunikacyjne* **2018**, *12*, 911–919.
199. Shi, Z.; Tian, Y.; Wang, X.; Pan, J.; Zhang, X. Po-Fi: Facilitating innovations on WiFi networks with an SDN approach. *Comput. Netw.* **2021**, *187*, 107781. [[CrossRef](#)]
200. Zhang, Q.; Liu, A. An unequal redundancy level-based mechanism for reliable data collection in wireless sensor networks. *EURASIP J. J. Wirel. Commun. Netw.* **2016**, *2016*, 1–22. [[CrossRef](#)]
201. Anbalagan, S.; Kumar, D.; Raja, G.; Ejaz, W.; Bashir, A.K. SDN-assisted efficient LTE-WiFi aggregation in next generation IoT networks. *Future Gener. Comput. Syst.* **2020**, *107*, 898–908. [[CrossRef](#)]
202. Holik, F.; Roedig, U.; Race, N. LoRa-SDN: Providing Wireless IoT Edge Network Functions via SDN. In Proceedings of the 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 28 September–2 October 2020.
203. Dawaliby, S.; Bradai, A.; Pousset, Y. Network slicing optimization in large scale Lora wide area networks. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019.

204. Ray, P.P.; Kumar, N. SDN/NFV architectures for edge-cloud oriented IoT: A systematic review. *Comput. Commun.* **2021**, *169*, 129–153. [[CrossRef](#)]
205. Vilalta, R.; Ciungu, R.; Mayoral, A.; Casellas, R.; Martinez, R.; Pubill, D.; Serra, J.; Munoz, R.; Verikoukis, C. Improving security in Internet of Things with software defined networking. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016.
206. Sivanathan, A.; Sherratt, D.; Gharakheili, H.H.; Sivaraman, V.; Vishwanath, A. Low-cost flow-based security solutions for smart-home IoT devices. In Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, Bangalore, India, 6–9 November 2016.
207. Salman, O.; Elhadj, I.; Chehab, A.; Kayssi, A. IoT Survey: An SDN and Fog Computing Perspective. *Comput. Networks* **2018**, *143*, 221–246. [[CrossRef](#)]
208. Tomovic, S.; Yoshigoe, K.; Maljevic, I.; Radusinovic, I. Software-defined fog network architecture for IoT. *Wirel. Pers. Commun.* **2017**, *92*, 181–196. [[CrossRef](#)]
209. Sharma, P.K.; Chen, M.; Park, J.H. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* **2017**, *6*, 115–124. [[CrossRef](#)]
210. Cerroni, W.; Buratti, C.; Cerboni, S.; Davoli, G.; Contoli, C.; Foresta, F.; Callegati, F.; Verdona, R. Intent-based management and orchestration of heterogeneous openflow/IoT SDN domains. In Proceedings of the IEEE Conference on Network Softwarization (NetSoft), Bologna, Italy, 3–7 July 2017; pp. 1–9. [[CrossRef](#)]
211. Khakimov, A.; Ateya, A.A.; Muthanna, A.; Gudkova, I.; Markova, E.; Koucheryavy, A. IoT-fog based system structure with SDN enabled. In Proceedings of the International Conference on Future Networks and Distributed Systems, Amman, Jordan, 26–27 June 2018.
212. Tahaei, H.; Ko, K.; Seo, W.; Joo, S. A QoE Based Trustable SDN Framework for IoT Devices in Mobile Edge Computing. In Advances in Computer Science and Ubiquitous Computing; Park, J., Loia, V., Yi, G., Sung, Y., Eds.; CUTE 2017; CSA 2017; Lecture Notes in Electrical Engineering; Springer: Singapore, 2017; Volume 474.
213. Nguyen, B.; Choi, N.; Thottan, M.; van der Merwe, J. SIMECA: SDN-based IoT mobile edge cloud architecture. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017.
214. Maksymyuk, T.; Dumych, S.; Brych, M.; Satria, D.; Jo, M. An IoT based monitoring framework for software defined 5G mobile networks. In Proceedings of the 11th International Conference On Ubiquitous Information Management And Communication, Beppu, Japan, 5–7 January 2017.
215. Hernando, A.B.G.; Da Silva Farina, A.; Triana, L.B.; Pinar, F.J.R.; Cambronero, D.F. Virtualization of residential IoT functionality by using NFV and SDN. In Proceedings of the 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 8–10 January 2017.
216. Muthanna, A.; Gimadinov, R.; Kirichek, R.; Koucheryavy, A.; Muthanna, M.S.A. Software development for the centralized management of iot-devices in the “smart home” systems. In Proceedings of the 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIconRus), St. Petersburg and Moscow, Russia, 1–3 February 2017.
217. Han, G.; Guizani, M.; Bi, Y.; Luan, T.H.; Ota, K.; Zhou, H.; Guibene, W.; Rayes, A. Software-defined vehicular networks: Architecture, algorithms, and applications: Part 1. *IEEE Commun. Mag.* **2017**, *55*, 78–79. [[CrossRef](#)]
218. Al-Rubaye, S.; Kadhum, E.; Ni, Q.; Anpalagan, A. Industrial internet of things driven by SDN platform for smart grid resiliency. *IEEE Internet Things J.* **2017**, *6*, 267–277. [[CrossRef](#)]
219. Volkov, A.; Muhathanna, A.; Pirmagomedov, R.; Kirichek, R. SDN approach to control internet of thing medical applications traffic. In *International Conference on Distributed Computer and Communication Networks*; Springer: Cham, Switzerland, 2017.
220. Sallabi, F.; Naeem, F.; Awad, M.; Shuaib, K. Managing IoT-based smart healthcare systems traffic with software defined networks. In Proceedings of the 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, Italy, 19–21 June 2018.
221. Walport, M. *The Internet of Things: Making the Most of the Second Digital Revolution*; UK Government Office for Science: London, UK, 2020.
222. Lai, S.; Zhao, R.; Tang, S.; Xia, J.; Zhou, F.; Fan, L. Intelligent secure mobile edge computing for beyond 5G wireless networks. *Phys. Commun.* **2020**, *45*, 299–327.
223. Salam, A. *Internet of things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends*; Springer: Cham, Switzerland, 2020; pp. 299–327.
224. AWS IoT Services Overview-Amazon Web Services. Available online: <https://aws.amazon.com/iot/> (accessed on 13 August 2020).