# Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions

**Syed Hussain Ali Kazmi**
Universiti Kebangsaan Malaysia
**Faizan Qamar**
Universiti Kebangsaan Malaysia
**Rosilah Hassan** ( rosilah@ukm.edu.my )
Universiti Kebangsaan Malaysia
**Kashif Nisar**
Universiti Malaysia Sabah
**Bhawani Shankar Chowdhry**
Mehran University of Engineering & Technology

**Research Article**

**Keywords:** SDN, 5G, Security, Networks, Virtualization

**Posted Date:** June 14th, 2022

**DOI:** https://doi.org/10.21203/rs.3.rs-1648186/v1



**Version of Record:** A version of this preprint was published at Wireless Personal Communications on April 19th, 2023. See the published version at https://doi.org/10.1007/s11277-023-10402-7.

## Abstract

Modern communication systems are probable to surface new challenges while introducing innovative fronts concerning context consciousness in wireless networks. The main outcome behind this expected technological jump will be a whole novel set of intuiting aptitudes forecasted for Fifth Generation (5G) enabled devices. In line with 5G, Software Defined Networking (SDN) is also rising as an intrinsically novel phenomenon. SDN is an unconventional methodology and key technology in modern communication. SDN maintains favorable novelty about network programmability, where network administration is permitted with extraordinary intellections. SDN architecture has the prospective to allow, simplify or augment security implementations in network through instantly reprogrammable centralized view of the data plane. In the near future, 5G and SDN will ripe mobile communication through the development of state-of-the-art implementations such as a smart city, advanced military security, modern national defense, intelligent traffic, etc.; thereby, these emerging mobile communication concepts invoke various significant topics, where security is a paramount implication. Therefore, we initiate our focus from basic architecture of 5G and SDN. Next, we analyze security requirements, solutions and challenges in joint paradigm of 5G and SDN. Further, considering the modern communication technological shift, we discuss future trends and research directions in the joint era of 5G and SDN technologies.

## 1. Introduction

The unremitting growth in the capacity and aspects of data apprehended by technological advancements has shaped diversified flow of data in either organized or unorganized format such as the rise of social media, Internet of Things (IoTs) for Healthcare [1] and huge multimedia communications. Indeed, the rapid expansion of the Internet industry is considerably dependent on communication system speed, which has emerged as a critical steering factor for the advancement in computer networks [2]. Scientific advancements are rapidly changing the information technology; thereby computer networks are expanding towards incorporation, dissemination, modification and intelligence [3]. The pillar behind this anticipated technological hop will be an entire novel set of aptitudes forecasted for Fifth Generation (5G) communication [4]. 5G is encapsulating all advanced emerging technologies like Artificial Intelligence (AI) [5]. Within the near future, 5G will reap portable communication organized through the advancement of inventive executions such as smart city, smart grid system, advanced military security etc. So, it is considered fundamental to boost the organized engineering of 5G technology. Likewise, Software Defined Networking (SDN) technology is expanding eminently everywhere globally due to its programmable [6], economical, agile, robust and consolidated networking. 5G is more complex and harder to manage as compared to conventional computer telecommunications and satellite communication systems. SDN is a potential organized design that abridges the operational complexities of the Conventional Networking (CN) worldview by isolating the control plane and information plane. Network Architecture, agility and security are major stack holders among several significant fundamentals for emerging future networks as per the technological engagement of 5G and SDN [7]. Extremely pertinent and challenging requirements are emerging in line with the advancement in network communication technologies, whereas introducing innovative approaches towards setting awareness within the networks. The provision of huge traffic is invoking various significant topics, where security is of paramount significance in modern networks [8]. The gathering of these advanced characteristics can give development to an unusual type of security protocols and architectures. From the security perception, SDN parts security concerns into the control and information plane, thereby this innovative re-composition brings fortifying openings and challenges. Virtualization-based concepts such as Network Function Virtualization (NFV), Cloud Computing (CC), Mobile Edge Computing (MEC), Network Slicing (NS) and Virtual Machine (VM) framework are widely presented as foundation for success in 5G communication [9]. The general understanding is that SDN proficiencies will inevitably result in updated security usage in advanced portable devices in 5G. Concurring to [10], the progressing procedures of Distributed Denial of Service (DDoS) threats in SDN-based advances amid the enormous communication activity in cutting edge applications permit us to understand the potential security requirement of 5G innovations [11]. It is exceptionally critical to analyze the restrictions of conventional and SDN-based systems with respect to the 5G based network engineering, issues and challenges of securing SDN controllers [12]. Attacks on SDN and SDN-based defense operation to counter cyber threats are extensively pursued research topics. Optimized SDN controller placement in SDN-enabled Integrated Satellite-Terrestrial Networks (ISTNs) can minimize the average failure probability of Satellite-based SDN (SSDN) control paths [13]. Various opportunities and challenges will arise in the joint era of 5G and SDN technologies, as depicted in Fig. 1.

## 1.1 Related Previous Works

According to our knowledge, most recent works in the research publications contain various comparisons and discussion on SDN-based 5G technologies but rarely contain security perspectives as well. However, none has presented a focused review on the joint security paradigm emerging in 5G and SDN. For example, NFV security and threat analysis is presented in [14], but 5G elements require further detailed deliberations. [10] presented a detailed survey on DDoS attacks and related threats in SDN-related emerging era where as aspects related to 5G networking are not discussed. 5G interference Management: Requirement, Challenges and future direction are discussed in [15]. However, security perspective-based implementation and corresponding challenges are not discussed. [16] discussed 5G mm-wave challenges, but Security aspects with respect to SDN and IoTs need to be addressed primarily regarding millimeter Wave (mm-Wave) challenges. 5G applications are discussed in [17, 18]; however, all related elements in emerging commination need further discussion, especially security elements and SDN. The study in [12] discussed SDN fundamental architectural elements, challenges and solutions but the security perspective

and SDN relation with the emerging 5G paradigm needs further deliberation. The survey [19] covers security aspects with respect to SDN, however, detailed security analysis and impact of 5G paradigm require further discussion. Likewise, discussion in [20] covers SDN architecture, challenges, and security aspects focusing on SDN, but corresponding issues with 5G are also required to be discussed. SDN scalability, reliability and security of SDN controller in covered in [21], but the survey does not provide impact, requirement, challenges and solutions for SDN with respect to 5G. Similarly, an overview of SDN-based Cyber defense along with SDN-based security solutions is discussed in [22] however, key emerging player i.e. 5G security is discussed in [23] but fundamental emerging technologies requires focus with respect to security in SDN. [24] only explains the essential and underlying concept of SDN with structural design by separating the data plan and control plan from each other, giving a flexible environment to both the vender and network operators, but aspects related to 5G are not included. [25] presented a detailed comprehensive survey on NS in 5G; however, review on SDN-related common areas, architectural elements and security perspectives are lacked. Thereby, none of the previously referenced literature work presents a comprehensive security perspective with respect to all primary fundamental architectural elements in emerging mobile communication networks. Various survey papers and research articles cover the subject aspects with partial focus on selective areas.

## 1.2 Scope and Contributions

The aim of this survey is to present a security centric assessment of emerging joint technological paradigm in 5G and SDN. Therefore, we comprehensively review 5G architectural elements, security and progression in the course of network virtualization through SDN. We initiate our discussions from the advancements and key elements in 5G mobile communication. Thereafter, we present a Confidentiality, Integrity, Authentication, Availability and Access Control ($CIA^3$) centric foundational security analysis [26] of 5G technology. With a similar proposition, we inline a similar systematic review on SDN. Further, we analyze SDN-based mechanisms against dominant security situations in networks. We provide a review on the enhancements in network operations due to different high-tech integrated essentials of 5G and SDN. Moreover, this paper contains a detailed analysis of 5G security based on emerging network technology concepts. We also present the open-ended problems and future research prospects in the joint era of 5G and SDN technologies. Table 1 provides a comparative overview of previous related works with respect to the scope of this survey. We summarize our contributions as follows:

- We provided a comprehensive introduction of 5G communication concepts. Further, we provided an overview of emerging trends in primary architectural areas related to the implementation of 5G technology. We provided a summarized overview of our 5G review in Table 3.
- We discussed the 5G security paradigm through $CIA^3$ based analysis. We reviewed the prevailing threats and solutions in 5G regarding each security fundamental element in $CIA^3$. We summarized our review of $CIA^3$ analysis on 5G as Table 4.
- We described the latest research in SDN basic architectural elements through discussion as well as a pictorial overview of primary elements and concepts related to SDN implementation. For a brief, we summarized our discussion in Table 5.
- We reviewed the latest security trends in SDN regarding the $CIA^3$ based security analysis model. We discussed the latest solutions and challenges of SDN with respect to $CIA^3$ requirements. Moreover, we also summarized our review as Table 6.
- We discussed the implementation and solution related to the joint paradigm of 5G and SDN. We discussed the merger of the $CIA^3$ security domain of SDN and 5G through a graphical overview in Fig. 5.
- We discussed the latest research for joint implementation of SDN and 5G in the security domain. We provided as a pictorial overview of the prevailing research scenario as Fig. 6. We also summarized our discussion of this portion in Table 7.
- We reviewed the research works related to joint implementation of 5G and SDN with emerging communication technology related concepts, including NVF, MEC and NS. Moreover, we discussed security issues related to these emerging trends. We summarized this portion in Table 8.
- Finally, we provided a brief discussion on the latest research directions related to 5G and SDN, along with a summary in Table 9.

Table 1
A comparative overview of related previous works and Scope of this Survey

| Contributions and Covered Scope | | [14] 2018 | [10] 2019 | [12] 2019 | [19] 2019 | [25] 2019 | [17] 2020 | [20] 2020 | [23] 2020 | [24] 2020 | [22] 2021 | [21] 2021 | [16] 2021 | [16] 2021 | [15] 2021 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5G Architecture | | X | X | X | X | 0 | √ | X | X | X | X | X | √ | √ | √ |
| 5G Fundamental Features | | X | X | X | X | √ | √ | X | 0 | 0 | X | X | √ | √ | √ |
| 5G Security Analysis | | X | X | X | X | 0 | 0 | X | 0 | 0 | X | X | 0 | X | 0 |
| 5G CIA$^3$ Security Analysis | | X | X | X | X | X | X | X | X | X | X | X | 0 | X | X |
| SDN Architecture | | √ | √ | √ | √ | √ | 0 | √ | X | √ | √ | √ | 0 | X | X |
| SDN Primary Features | | √ | √ | √ | √ | 0 | X | √ | 0 | √ | √ | √ | X | X | X |
| SDN Security Analysis | | √ | 0 | 0 | √ | X | X | √ | 0 | √ | √ | √ | X | X | X |
| SDN CIA$^3$ Security Analysis | | X | X | X | X | X | X | X | X | 0 | X | X | X | X | X |
| Joint effects of 5G and SDN technologies | | X | X | X | X | 0 | 0 | X | 0 | 0 | 0 | X | 0 | X | X |
| Joint security of 5G and SDN technologies | | X | X | X | X | 0 | X | X | 0 | 0 | 0 | X | 0 | X | X |
| 5G and SDN related technologies | NVF | X | X | X | √ | X | 0 | X | X | X | X | 0 | X | X | X |
| | MEC | X | X | X | √ | X | 0 | X | X | X | X | 0 | X | X | X |
| | CC | X | X | X | √ | X | 0 | X | X | X | X | 0 | X | X | 0 |
| | NS | X | X | X | √ | X | 0 | X | X | X | X | 0 | X | X | X |
| 5G and Security in SDN related technologies | NVF | X | X | X | 0 | X | X | X | X | X | X | 0 | X | X | X |
| | MEC | X | X | X | 0 | X | X | X | X | X | X | 0 | X | X | X |
| | CC | X | X | X | 0 | X | X | X | X | X | X | 0 | X | X | 0 |
| | NS | X | X | X | 0 | X | X | X | X | X | X | 0 | X | X | X |
| Research Directions in joint era of 5G and SDN | | X | X | X | X | 0 | 0 | X | 0 | 0 | 0 | X | 0 | X | X |

Annotations:

"√" indicates that concepts are covered comprehensively

"0" indicates that scope is partially covered

"X" indicates that scope is not covered

## 1.3 Paper Structure and Organization

The rest of this survey is organized as follows: We start our review with a discussion on architectural elements and primary concepts of 5G technology along with CIA$^3$ based 5G security analysis in Section 2. Section 3 contains a review on SDN technology in the lines as for 5G in Section 2. In Section 4 we elaborate the joint paradigm of SDN and 5G security. Section 5 contains a discussion on SDN-related modern concepts in 5G networks such as NFV, MEC, CC and NS. In the second last Section 6 we presented the latest trends, challenges and research directions in the joint era of 5G and SDN. Thereby, the survey is concluded in Section 7. Therefore, we adapted a systematic parallel research approach with stage-wise merger of 5G and SDN. Figure 2 depicts the overall structure and organization of this paper. Table 2 provides commonly used acronyms in this paper.

Table 2
A list of commonly used acronyms in this paper.

| Abb. | Definition | Abb. | Definition |
|---|---|---|---|
| 5G | Fifth Generation | MNA | Mobile Network Application |
| SDN | Software-Defined Networking | API | Application Program Interface |
| IoTs | Internet of Things | OpenPATH | Open aPplication Aware software-defined swiTcHing |
| AI | Artificial Intelligence | ONOS | Open Network Operating System |
| CN | Conventional Networking | MitM | Man in the Middle |
| NFV | Network Function Virtualization | HTTP | Hyper Text Terminal Protocol |
| CC | Cloud Computing | SSL | Secure Socket Layer |
| MEC | Mobile Edge Computing | THP | The Hidden Pattern |
| NS | Network Slicing | ADS | Anomaly Detection schemes |
| VM | Virtual Machine | E-ABAC | Extended Attributes Based Access Control |
| DDoS | Distributed Denial of Service | COTS | Common Commercial Off The Shelf |
| SSDN | Satellite-based SDN | Intel SGX | Intel Software Guard Extensions |
| mm-Wave | millimeter Wave | NSFV | Network Security Function Virtualization |
| PAPR | Peak to Average Power Ratio | E2E | End to End |
| NR | New Radio | D2D | Device to Device |
| 6G | Sixth communications | FMEC | Fog and Mobile-Edge Computing |
| 3GPP | 3rd Generation Partnership Project | MCC | Mobile Cloud Computing |
| LTE | Long Term Evolution | P2P | Peer to Peer |
| eMBB | enhanced Mobile Broad Band | RAN | Radio Access Network |
| MIMO | Multiple Input Multiple Output | NGMN | Next Generation Mobile Network |
| mMTC | massive Machine Type Communication | THz | Tera-Hertz |
| QoS | Quality of Service | GoS | Grade-of-Service |
| RFID | Radio Frequency Identification Device | IoV | Internet of Vehicle |
| URLLC | Ultrareliable Reliable Low Latency | TDMA | Time Division Multiple Access |
| UAV | Unmanned Aerial Vehicle | GFA | Grant Free Access |
| CI | Close-In | ML | Machine Learning |
| FI | Floating Intercept | RLF | Radio Link Failure |
| UEs | User Equipment's | SVM | Support Vector Machine |
| RAT | Radio Access Technology | LSTM | Long Short Term Memory |
| AHP | Analytical Hierarchical Approach | NAS | Non-Access Stratum |
| AS | Adaptive-Sleep | AS | Access Stratum |
| NOMA | Non Orthogonal Multiple Access | uMTC | ultra-reliable Machine Type-Communication |
| B5G | Beyond 5G | SaaS | Security-as-a-Service |
| $CIA^3$ | Confidentiality, Integrity, Authentication, Availability and Access Control | ABA-IDS | Abnormal Behavior Analysis-Intrusion Detection System |
| EUA | Edge User Allocation | ONF | Open Network Foundation |
| SDH | Synchronous Digital Hierarchy | LTs | Light-trails |

## 2. Fifth Generation Communication

Rapid expansion in the digital transformation of communication segments is driven by the 5G mobile communication among diverse sectors, including finance, transport, health etc. Freeze of 3rd Generation Partnership Project (3GPP) Release 15 and the conclusion of the first phase of 5G until the end of 2018 are counted as an essential milestone as per business necessities, New Radio (NR), network framework, and network composition. The next inline, Release 17 and Release 18 are concerned with protocol, improvements in service and placement pragmatics [27], transforming to the Next Generation of mobile communications (6G). 3GPP Release 18 would impact earlier features after 5G expands and establishes around the world. Initial services associated with 5G are enhanced Mobile Broadband (eMBB) services [28] that also simultaneously exist with Long Term Evolution (LTE) for coverage requirements with Network Radio. Radios with Artificial Intelligence (AI) and the main network can create centralized intelligence to enhance diversified wireless networks utilization [29]. 5G would require reducing delay and improving consistency for services extending ahead of edge or private networks. 5G may also boost a tighter integration with diverse network sections containing edge framework and accelerate network coverage, allowing a simpler structure and management of new applications and services. 5G is anticipated to augment Network Radios and mm-Wave manipulating a broader spectrum of frequencies from sub-6 GHz to 300 GHz. An outline of Network Radio implementation schemes, involving innovative waveform, frame configurations and improved radio elements are described in [30]. 5G will overlay centralized cell-less coverage related to users and investigate beyond the use of virtual radio control, non-line-of-sight ecosystems of mm-Wave and optical technology in wireless networks.

3GPP Release 17 creates augmentations to Network Radios for unlicensed frequency band, massive Multiple Input Multiple Output (MIMO), and a low data rate communication in industry, mentioned as NR-Light [27]. The scenarios evolving with 5G emergence as depicted in Fig. 3 are 1) “enhanced Mobile Broad Band (eMBB)” that supplements 4G broadband competencies, attainment of 100 Mbps characteristic data rates and ultimate data rates well above 1 Gbps. 2) “massive Machine Type Communication (mMTC)” that signifies IoT utilization in emergent paradigm currently with 4G LTE, but at relatively highly dense levels. It also aims to handle enormous applications span in 4G LTE that surfaced several demanding Quality of Service (QoS) requirements [31]. Likewise, the generally familiar characteristics of 5G are the ability to serve up to 1 million / km² devices, 10 times enhanced compared to 4G. The types and quantity of all these devices is dependent on expansion in IT development; however, smart cities are a common case. 5G also contains a 100-times improvement in energy efficacy, resulting in appreciably extended life for battery-based devices, like environmental sensors or fitness bands and Radio Frequency Identification Device (RFID) tags [32]. 3) “Ultrareliable Reliable Low Latency” (URLLC) that transforms applications time framework in a way that was previously unachievable. It is also revolutionizing mobile networks through autonomous transport systems, industrial automation, innovative mobile telemedicine system, etc.

5G technological modern aims are associated with certain key requirements. 5G technology is being designed to have the potential for compliance with all use cases of modern communication scenarios. Therefore, 5G is gaining considerable momentum from multiple domains like governments, industry, academia and researcher [33]. Several solutions and implantation are emerging on the surface through literature, projects, informal ideas, etc. Prominent elements in this area, including mm-Wave utilization, efficient handover, bandwidth management, massive connectivity and ultra-low latencies, are discussed in subsequent paragraphs. Similarly, these reviewed primary elements of 5G technology are summarized in Table 3.

## 2.1 mm-Wave Utilization

Several implementations are suggested by various researchers regarding the utilization of mm-Wave for 5G. The primary challenge faced by mm-Wave in 5G is path loss. Various models of Close-In (CI) and Floating Intercept (FI) can be utilized for comparative analysis of 5G mm-wave path loss [34]. 5G can enable 100kmph transmission and beam tracking through a beam tracking algorithm-based RF front architecture [35]. Moreover, 5G provisions use of congestion control algorithm to handle massive application data through mm-Wave [36]. Unmanned Aerial Vehicles (UAV) mm-Wave communication challenge can be counter through 5G based MIMO system [37]. However, mm-Wave utilization surfaces several constraints such as coverage problems and hardware utilization. Hybrid beam forming unconventional antenna and is a potential solution to counter coverage problem in Base Station and User Equipment’s (UEs) [38]. Employment of advanced baseband algorithms in 5G architecture can improve software/hardware performance [39].

## 2.2 Efficient Handover

Efficient handover is a primary requirement in 5G network employment for selection and shift among stations. Various techniques and algorithms can be used for challenging 5G scenarios in handover. Handover control is dependent on thresholding limits at signal level received by mobile devices; therefore, efficient thresholding algorithms are employable for improved handover performance in Radio Access Technology (RAT) selection in 5G [40]. Similarly, Analytical Hierarchical Approach (AHP) [41] and analysis algorithms [42] for RAT selection outperform the traditional A2A4 RAT selection with improved efficiency, reduced latency and less packet loss. Likewise, [43] proposed two distinct energy-saving schemes called, Adaptive-Sleep (AS), sectorization Adaptive Hybrid (AH) partitioning schemes for localized mobile networks using smart antenna systems. In this solution, a spatial Poisson process-based generic base model reduces the system intricacy and enhances the adaptive antenna's beam angle adjustment flexibility, termed a Smart Antenna (SA).

## 2.3 Bandwidth Management

One of the key functional challenge in ultra-dense 5G communication is efficient interference centric bandwidth management [44]. 5G also has the capacity to utilize the Visible Light Communication framework for the handover process to avoid saturation issues of Radio Frequencies [45]. Non Orthogonal Multiple Access (NOMA) based approaches are considered suitable for addressing the increased receiver complexity due to successive interference cancellation requirements. Simulations show that cooperative NOMA substantially improves the diversity gain and data rates in Beyond 5G (B5G) networks [46]. Similarly, a pre-coded NOMA system outperforms the conventional NOMA through Peak to Average Power Ratio (PAPR) minimization [47].

## 2.4 Massive Connectivity

Massive connectivity is considered a hallmark characteristic of 5G technology. This area has created various unconventional approaches along with several challenges and opportunities. Edge User Allocation (EUA) is one the challenges faced by 5G [48]. Unconventional approaches like decentralized game theory are suitable for baseline architecture in EUA based massive connectivity handling issues [49]. Other linked areas of massive connectivity handling are efficient and robust routing mechanisms and beamforming schemes [50]. The evolving and extensively related research concept for efficient routing is the MEC-based routing algorithm in 5G for improved resource and access management. This strategy outperforms the Time Division Multiple Access (TDMA) as well.

## 2.5 Low Latencies

The outstanding impact of 5G has attracted several advanced and mission-critical scenarios into a common sphere. In a wholistic scenario, the integrated performance of URLLC and eMBB is critically dependent on attaining low latency communication [51]. 5G low latencies requirements are pursued in literature through various techniques such as Grant Free Access (GFA), caching\ edge computing, dynamic multiplexing, intelligent scheduling and Machine Learning (ML) [52]. Similarly, zero downtime edge computing techniques are emerging to address the ultra-low latency streaming challenges in 5G communication [53]. Likewise, edge caching is emerged as a potent solution to address the data requests of mobile users at a first end to efficiently minimize latencies and improve the QoS of mobile users [54, 55].

## 2.6 Link Reliability

It is evident that seamless adoption of 5G technology is extremely dependent on the maintenance of network-wide link reliability. The emerging approaches in this regard are data replication, finite block length, multi-connectivity, multicast, network coding and channel control [51]. Deep learning-based link adaptation is one of the latest techniques in this domain. [56] presents a novel mapping method to compress highly multi-dimensional 5G transmissions into low multi-dimensions with bearable information loss to improve link reliability. One of the challenging associated problems of link reliably in 5G is Radio Link Failure (RLF). [57] proposed employment of ML for RLF prediction through correlation of Support Vector Machine (SVM) and Long Short Term Memory (LSTM).

Table 3
5G Challenges, Solutions & Outcome

| Ref. | Year | Area | Challenges | Solutions | Outcome |
|---|---|---|---|---|---|
| [35] | 2020 | mm-Wave utilization | RF Front End Architecture design | Beam-tracking Algorithm | A beam Tracking Technique |
| [36] | 2020 | | Integration with 3GPP | Congestion Control Algorithm | Execution Estimation of E2E communication |
| [39] | 2019 | | Bidirectional channeled performance | Baseband Algorithm | Software & hardware Compatibility and better flexibility |
| [50] | 2018 | | Path Loss | Beam forming | High data rates & improved massive connectivity |
| [38] | 2019 | | Coverage Problem | Hybrid beam forming | Unconventional antenna solution for Base Station and UEs |
| [37] | 2021 | | UAV mm-Wave communication | UAV MIMO System | Delivers massive assistance in steadiness, robustness, and spectral efficiency |
| [40] | 2019 | Efficient Handover | A new RAT without any thresholding is unfavorable to the system resources | A thresholding approach for RAT selection | Improves the performance of the system and reduces the handover |
| [41] | 2018 | | Selection criteria of RATs | AHP | The scheme outperforms the traditional A2A4 selection process of RAT |
| [42] | 2020 | Bandwidth Management | Time distribution in channel selection | Analysis Algorithm | Higher efficiency, reduced latency and packet loss |
| [45] | 2016 | | Saturation issues of Radio Frequencies | Visible Light Communication framework | Improved handover process |
| [46] | 2021 | Massive Connectivity | NOMA Complexity | Cooperative relaying scheme | The scheme shows higher diversity gain and improved data rate with cooperative NOMA system |
| [47] | 2019 | | PAPR minimization | Pre-coded NOMA system | Improved the performance of conventional NOMA |
| [49] | 2021 | | EUA | Decentralized game-theoretic approach | Suggestively outpaces several advanced and baseline methods |
| [58] | 2021 | | Resource and access management | MEC-based routing algorithm | Outperforms the TDMA based scheme |
| [53] | 2020 | Low Latencies | Zero downtime | Edge computing technique | Ultra-low latency streaming in 5G |
| [54, 55] | 2018 2014 | | Data requests of mobile users | Edge caching | Minimized latencies and improved the QoS |
| [56] | 2021 | Link Reliability | Link Adaptation | Deep Learning | Improve link reliability |
| [57] | 2021 | | RLF | ML | RLF prediction |

## 2.7 Security in Fifth Generation Communication

Wireless technology classifications are not primarily restricted to classic phone-based audio and video communication. In the same fashion, phreaking is not restricted to the theft of general data [59]. Currently, it is transformed into immense cybercrime nexuses with distinct monetary, political and personal objectives [60]. 5G paradigm has opened up widespread research challenges for developers [61]. Moreover, 5G network has substantial security challenges due to numerous connections between the devices [62]. Subsequently [63, 64], the researchers have unified content perceptibility and centrally control policy to improve security and fortify vital data related to applications, users, and network functionality. $CIA^3$ is a widely adopted security analysis model for categorizing threats and corresponding solutions. $CIA^3$ based threat landscape of modern 5G mobile communication is shown in Figure 4. In subsequent paragraphs, we cover 5G security related research landscape into $CIA^3$ segments along with summary in Table 4.

## 2.7.1 Confidentiality in 5G

Confidentiality of user data is one of the primary security goals in the 5G security model. It is the attribute that can guard data communication from getting exposed to malicious elements and from passive security occurrences. In both the security schemes of 4G-LTE and 5G architectures, users must be restricted to authorized data only [65]. We categories confidentiality related threats in thirteen types, which includes, Man-in-the-Middle (MitM) Threat [66], parallel session Threat [67], replay Threat [68], eavesdropping Threat [69], collaborated Threat [70], distributed threat [71], tracing Threat [72], spoofing Threat [73], privacy Threat [74], adaptive chosen text Threat [75], impersonation Threat [76], stalking Threat [77], sniffing threat [78] and disclosure Threat [79]. In 5G compatible data applications (e.g., autonomous vehicles [80], real-time health monitoring [81], etc.), the standard data encryption algorithms are generally employed to ensure data confidentiality. In standard practice, one private key is used to perform encryption and decryption functions of 5G data through symmetric key algorithms. According to [82], high reliance on large-scale deployed sensors has significantly increased the security risk due to IoT integration with 5G. To guarantee the privacy of user's data gathered by cloud and improved data streaming, both linear and nonlinear models are recommended to be addressed by implementing a private Unscented Kalman filter [82].

## 2.7.2 Integrity in 5G

Integrity is generally defined as the prevention of altering and forfeiture of information during communication from one point to another. Integrity-related threats can be segregated into five types: Message append threats[83], message alteration threats [84], Selective message hampering threat [85], tampering threat [86] and spam related threats [87]. Non-Access Stratum (NAS) and Access Stratum (AS) are used for 4G LTE integrity protection [88]. Non-Access Stratum (NAS) and Access Stratum (AS) are used for 4G LTE integrity protection [88]. However, the major distinction of 5G NR is integrity protection entailment at the user plane as well. This is noteworthy since integrity fortification of the application plane is not provisioned in 4G. It is one of the desired features of resource-constrained 5G enabled IoT devices.

## 2.7.3 Authentication in 5G

This category includes five types of threats:, smart card based threats [89], partial collision based threats [90], forgery based threats [91], dictionary based threats [92] and parameters reuse based threats [93]. With the focus on authentication mechanism, [94] have suggested an authenticated key formation system founded on signatures for 5G enabled IoTs. The suggested method is analogous to some of the other techniques and certified for security by resorting to Burrows-Abadi-Needham logic, conventional and unofficial security evaluation via automated validation of application tools and internet security protocol. [95] proposed the requirement of the necessary security factor in IoT for ensuring authentication and authorization. Moreover, integrity-protected signaling is used in the 5G authentication mechanism. This guarantees that no unauthorized entity can alter or access the data transported wirelessly [96].

## 2.7.4 Availability in 5G

This categorization contains Seven types of threats, which includes, Redirection threat [97], physical threat [98], Distributed Denial of Service (DDoS) [99], Denial of Service (DoS [100]), First In First Out (FIFO) threat [101], Free riding threat [102] and skimming threat [103]. 5G paradigm ensures that legitimate users are provided with uninhibited network availability, thereby it established reputation on service provider. It simultaneously estimates the reliability of the network infrastructure to counter active security incidents, e.g., Denial of Service (DoS) attack. Network performance is seriously affected by a DoS attack. [72] indicated that 95–99.99% network availability can be ensured through the primary specifications bench marks of 5G, including eMBB and ultra-reliable Machine Type-Communication (uMTC). 5G based Network architecture is expected to ensure availability at a high probability of effectiveness.

## 2.7.5 Access Control in 5G

It is pertinent to discuss that the existing 3GPP 4G security scheme cannot seamlessly meet requirements of the modern 5G ecosystem as they are based on the traditional trust model of operators and subscribers. Thus, modern novelties necessitate a centralized security policies architecture to empower users to access network resources and applications conveniently. This category includes phishing [104], cloning [105], birthday [106] and social engineering [107]. [108] suggested a security-centric policy management framework to assist centralized security policy implementation scheme in 5G. Moreover, Security-as-a-Service (SaaS) can be enabled by operators as a prospective service to a number of IoT customers. A centrally controlled policy for assessing susceptibilities and lightly secured areas is desirable for the concerns of privacy, reliance and secrecy in distributed 5G based IoT networks [109]. The traditional requirement of secure network environment can be substantially addressed through centralized access control. Therefore, implementation of wide-ranging End-to-End security strategies are dominating security requirements in 5G networks. Further, these strategies should include the network architecture at all levels like signaling, data, and application levels [110]. Comprehensive access control and check at all levels in the network are the foundation to instrument a flawless security scheme. 5G necessitates a state or the art implementation of security framework like Abnormal Behavior Analysis-Intrusion Detection System (ABA-IDS) [93].

Table 4
Focused areas & Solutions for 5G Security

| Ref. | Year | Focused Areas | Solutions |
|---|---|---|---|
| [65] | 2020 | Confidentiality | Restricted user access to authorized data only |
| [80] [81] | 2021, 2018 | | Standard data encryption algorithms |
| [82] | 2018 | | Private Unscented Kalman filter |
| [88] | 2019 | Integrity | Integrity protection at the user plane. |
| [95] | 2020 | Authentication | Definite Requirement of security factor |
| [94] | 2020 | | Key formation system |
| [96] | 2018 | | Integrity-protected signaling approach |
| [111] | 2018 | Availability | Assurance of availability |
| [110] | 2020 | Access Control | Centralized visibility End-to-End security strategies |
| [108] | 2020 | | Security centric policy management framework |
| [81] | 2018 | | ABA-IDS in IoT smart water system |

## 3. Software Defined Networking

Software Defined Network was officially recommended by Stanford University in 2009 [112, 113]. It is a way forward for network structural design and functional mode. Currently, the SDN framework [114] suggested by the Open Network Foundation (ONF) comprises three components: application layer, control layer, and facilities layer. In order to make the network control programmable and more flexible, the concept of OpenFlow [115] was introduced that provides proper interfacing between the planes. In SDN design, as shown in Fig. 5, the highest component is the application layer, which includes a range of distinct commercial and private applications. The middle layer, i.e. control layer, is liable for apportioning assets [38], providing the network details and state data. In the entire scheme, the SDN controller has the global vision of the network to control the network terminals and the software information [116]. The lowest layer is the infrastructure layer that accomplishes data handing, forwarding and state collection. Two types of Application Program Interface (API) are used between the three mentioned SDN layers. North bound API is between application layer and control layer. Similarly, South bound API is used between the control and infrastructure layers. The API interfaces between these layers are also a significant fragment of the SDN design. Network infrastructure equipment can help extract state information acquisition using the southbound controller interface. OpenFlow is a prominent south bound API protocol. Moreover, it utilizes Open Standard Interface to provision services to the control layer. This scheme assistances the infrastructure layer equipment to accept control information. ONF has been introduced as an open OpenFlow standard interface at the bottom layer [117]. Functionality of middle layer, i.e. Control Layer, is to supply Mobile Network Application (MNA) resource information of the lower layer to the top layer [20, 118, 119]. SDN architecture and routing is suitable for highly dynamic scenarios in vehicular communication due to flexibility, programmability and scalability [120]. The emerging requirements related to SDN design, employment and various corresponding solutions are discussed in subsequent paragraphs and same is summarized in Table 5.

## 3.1 Switching Efficiency

SDN framework called Open aPplication Aware software-defined swiTcHing framework (OpenPATH) is evolving with the claim of cost-effective scalability, higher throughput and reduced latency [121]. Network splitting techniques are employed for efficient load balancing in SDN controllers [122]. Likewise, another dominating challenge is hardware processing power for massive switching in Virtual Network Functions (VNFs) [123]. Traditional concept of keep alive message potentially reduces the redundant traffic between SDN and switches [124].

## 3.2 Processing Power

Computing power is one of the prevailing limitations in the modern communication paradigm [125]. Hardware performance and scalability can be addressed through programmable rules distribution schemes among independent SDN controllers [126]. A lightweight SDN controller combined with an external SDN controller can be employed to address the processing limitation of embedded devices [127]. Virtualized Network Tomography (NT) in the combination of SDN and In-band network telemetry [128] can be an efficient network monitoring tool with low overhead [126, 129].

## 3.3 Global Network View

It is one of the most appreciated properties of SDN-based networks where a complete global view of all devices is available, resulting in an efficient next-generation communication era. In this novel SDN-based networking topology, it is imperative to develop new routing schemes and algorithms [130] and especially, the employment of broadcast schemes is challenging in SDN [131].

## 3.4 Backward Compatibility

Technological advancement and modern requirements are facing deficiency of a high maturity level in SDN-based standards; therefore, multiple opensource projects like Open Network Operating System (ONOS) are initiated by organizations [132]. Conceptualization of SDN is a kind of middleware system that translates commands into the required configuration in legacy networking [133].

Table 5
SDN Challenges, Solutions & Outcomes

| Ref. | Year | Area | Challenges | Solutions | Outcomes |
|---|---|---|---|---|---|
| [121] | 2021 | Switching Efficiency | Overloading of SDN controller | *OpenPATH* | Cost-effective scalability, greater throughput, and reduced latency |
| [122] | 2021 | | Load balancing among SDN controllers | Network dataflow splitting technique | Effective balanced network flow and reduced overhead |
| [126] | 2021 | Processing Power | Intensive packet processing | Programmable rules distributed SDN controllers | Improves VNF capacity and saves virtualization resources |
| [127] | 2021 | | Embedded low-power devices | Lightweight SDN controllers on embedded hardware | Quantification of the requirement for employing an external controller |
| [129] | 2021 | | Efficient monitoring | NT | NT together with SDN yields accurate estimations with low overhead |
| [128] | 2021 | | Timely network verification | In-band network telemetry | Six times reduced overhead |
| [132] | 2020 | Backward Compatibility | Deficiency of a high maturity level in SDN-based standards | SDN-IP and ONOS SDN controller | Minimum control path latency using optimal path routing |
| [133] | 2020 | | Vendor lock-in legacy devices | Middleware system | Translation of OpenFlow commands into legacy networking |

## 3.5 Security in Software Defined Networking

SDN technology has seamless potential to empower modern networking through various revolutionized concepts. However, this new SDN-based era has opened various security domains, challenges and opportunities. We cover SDN security scenarios related to the research landscape into following CIA3 segments and summary in Table 6.

### 3.5.1 Confidentiality in SDN

Any kind of communication without confidentiality is susceptible to various unintentional or intentional threats to user data. Confidentiality bench marks the quality of secrecy and encryption in communication among endpoints, sensors and readers. Implementation of advanced security mechanisms is critical for confidentiality in next modern network technologies like SDN. Various innovative front-like blockchain technology-based confidentiality mechanisms are surfacing in SDN [134]. SDN-based security infrastructure has the potential to counter Man in the Middle (MitM) attacks in wireless networks [135]. Links with SDN controllers are kept at dedicated lines to ensure confidentiality [136]. Global view and improved network management of SDN provisions solutions for ensuring confidentiality in devices that are only Hyper Text Terminal Protocol (HTTP) capable [137]. Moreover, the global view of SDN enables network wide centralized control of encryption and key management schemes [138]. The link between wireless SDN controllers and mobile switches must remain confidential and secure [139]. Due to no embedded security in north-bound API protocols, SDN is susceptible to sniffing attacks. Thereby provisioning attacker with information about network architecture. Therefore, Secure Socket Layer (SSL) encryption and public key certificate infrastructure are desired for connection between controller and switches[140]. Similarly, Due to multi-vendor approaches and no standard or opens specification for North bound APIs, third-party services at the applications layer pose serious threat to user data and network confidentiality in SDN [141]. SDNs provide Context-based security mechanisms for enhancing network security and guaranteeing counters to MitM attacks [142]. In the SDN paradigm, MitM attack is considered susceptible because of the subsidiary connection between the controller and switches; therefore, the controller to switches communication is exposed. Thus, an invader can posture a representative node in the middle of the controller and switches to perform various assaults such as hijacking a complete session, spoofing in DNS, black hole attack, and eavesdropping [143]. Similarly, In [144], various advanced fog computing scenarios are highlighted, which will create several new security requirements. Therefore, IoT-Fog framework threat analysis mechanisms are suitable for SDN security. Likewise, OpenFlow channel control can be used for countering the potential risks of MitM attacks in SDN architecture [94].

## 3.5.2 Integrity in SDN

Data integrity is an absolute requirement in all communication scenarios. SDN has provisioned various unconventional implementations for guaranteeing data integrity in modern computer communication. [145] proposed a blockchain-based solution for ensuring integrity and tamper resistance of logfiles for SDN-based forensic analysis. [146] proposed SDN-based contextual data integrity model where SDN application gathers context information from storage partitions to verify the context required. To detect the data integrity attacks in IoTs, roll forward validation-based decision tree classification is employed in [147]. However, SDN infrastructure has vulnerabilities related to compromised third-party apps at application plan that can cause network malfunction and manipulation of network flow. Therefore, flawless monitoring of network data records is extremely necessary for the integrity of the network in an SDN environment [143]. Likewise, the south-bound API protocol, OpenFlow, is also susceptible to degradation in data integrity, especially in wireless networks [148].

## 3.5.3 Authentication in SDN

The modern communication paradigm faces serious privacy concerns due to unauthorized smart gadgets and plain text-based authentication schemes. SDN, a centralized and high-power computational architecture, can facilitate modern networks to successfully overcome the challenges related to computational and processing requirements of strong authentication schemes [149]. SDN can potentially overcome computing challenges in MEC-enabled resource-contained nodes [150]. SDN-based framework reduces overhead communication issues in critical application related to smart grid system [151]. Global view of SDN provisions implementation of hierarchical authentication with in large network [152, 153]. Software-based architecture of SDN has the ability to absorb all the traditional cryptographic solutions like hash tables, hash functions etc. [154]. Flawless, heterogenous, backward compatible, and a global authentication scheme must be visualized for the SDN-based network. Whereas, keeping in view the centrality of SDN controller, it is extremely mandatory to incorporate a strong authentication scheme. [155] presented an unconventional authentication scheme called The Hidden Pattern (THP), a unified implementation of graphics-based password and digital challenge value to counter several authentication attacks in SDN. SDN is potential solution for security and authentication in wireless body area networks due to distinct robustness centralized control and flexibility [156].

## 3.5.4 Availability in SDN

Availability is directly dependent on network ability to sustain all types of DoS. Global view of SDN provision implementation of various novel DDoS detection schemes in combination with both traditional and unconventional technologies such as Information theoretic, ML and AI [157]. [158] proposed an ML-based DDoS detection scheme in an SDN environment. Devices have limited ability to apply standard security schemes in mMTC communication, likewise, rouge nodes or the attacker can flood wireless SDN controller with random forged packets. Therefore, various Anomaly Detection schemes (ADS) are proposed to ensure the security of SDN controllers [159]. DDoS attack discovery in SDN is proposed in [160] to secure and evaluate the evolving network design inspired by SDN layer topology through utilizing SVM model. As per [161, 162], SDN controllers' discovery methods where expanding DDoS assaults can be caught on through deep learning and other ML approaches for interruptive discovery in software-defined architectures. Presently, SDN supports moving forward the emerging technologies and novel networking system [163–165] where different techniques are concentrating on identifying DDoS. SDN architecture characterizes security threats into three categories: the threats related to the application, control, and data layers [20, 166]. In the SDN data layer, a huge number of packets are sent to switches to perform the DoS attack through overflowing the buffer and the flow table. In consequence, it will overload the buffer flow and the valid incoming packets will start dropping [167]. [168] suggests Counter-based DDoS Attack Detection (C-DAD) application for efficient DDOS attack detection in minimum time and reduced hardware resources. [169] suggests hybrid SDN approach through combined utilization of flow-based and packet based routing for minimizing false positive rate for DoS attack detection.

## 3.5.5 Access control in SDN

SDN-based architecture systematically provisions access control mechanisms. SDN is suitable for implementing static as well as dynamic access control in mobile and IoT-based applications [170]. SDN provision dynamic modification of flow rules in the network switches to incorporate robust centralized network access control [171]. However, the centralized architecture of SDN poses serious security issues especially related to north-bound API and corresponding interfaces. [172] suggested a broadcast encryption scheme so that the network control resources are encrypted and accessible only to legitimate users. [172] presents a role-based access control model for SDN applications that segregates secure and no secure communication sessions. Network providers, operators and application developers require control over shared resources through north bound interface[173]. SDN is expanding as a revolutionary approach to implement central access control and IDS due to the global view network. [174] have proposed a lightweight blockchain-based IDS for SDN cloud for improved attack mitigation with respect to detection probability. Utilization of SDN architecture for URLs based detection of phishing attacks with 99.5% detection accuracy [175]. [176] proposed an Extended Attributes Based Access Control (E-ABAC) model to ensure integrity and confidentiality in the access control process. SDN incorporates dynamic firewall management for secure access control, mitigation of DoS attacks and prevention of malicious traffic [177].

Table 6
Focused areas & Solutions for SDN Security

| Ref. | Year | Focused Areas | Solutions |
|---|---|---|---|
| [134] | 2020 | Confidentiality | Block chain technology base confidentiality mechanism |
| [137] | 2020 | | Confidentiality in devices that are only HTTP |
| [138] | 2021 | | Centralized control of encryption and key management |
| [94] | 2020 | | OpenFlow channel control to counter threats |
| [145] | 2019 | Integrity | Blockchain-based solution for tamper resistance of logfiles |
| [146] | 2021 | | Contextual data integrity model |
| [147] | 2019 | | Forward validation based decision tree |
| [151] | 2018 | Authentication | Computational power for MEC enabled resource contained nodes |
| [116] | 2019 | | Hierarchical region-wise authentication |
| [154] | 2019 | | Ability to absorb all the traditional cryptographic solutions |
| [158] | 2020 | Availability | ML based DDoS detection scheme |
| [121] | 2020 | | DDoS attack discovery with SVM model |
| [123] | 2019 | | Deep learning and other ML approaches |
| [170] | 2018 | Access Control | Dynamic access control in mobile and IoTs |
| [171] | 2019 | | Dynamic modification of flow rules |
| [172] | 2018 | | Broadcast encryption scheme |
| [173] | 2019 | | Control over shared resources |
| [174] | 2021 | | Light weight block chain based IDS |
| [175] | 2021 | | URLs based detection of phishing attacks |
| [176] | 2019 | | Extended Attributes Based Access Control (E-ABAC) model |
| [177] | 2021 | | dynamic management of firewall |

## 4. Fifth Generation Communication In Sdn Environment

The network equipment manufacturers typically formulate a private description of the interface configuration; they require a multifaceted control protocol to execute the configuration function. Moreover, the interface scheme, configuration optimization, and network administration are all complex tasks. Therefore, it becomes challenging for operators to intelligently organize networks as conventional schemes are inadequate for handling network modernization. Consequently, the idea of SDN is presented in the modern 5G network design. The SDN-based 5G networking scheme is primarily distributed into three portions: control layer, access layer, and forward layer [178]. In SDN-based 5G network architecture, an intelligent centralized network control entity resides at the control layer. In contrast, User data is separated from the control plane. Access layer provisions several wireless technologies and network types such as service data flow with guaranteed high dependability, ultra-fast speed and average load of the service data flow. At the same time, COTS hardware-based forward layer can assure low latency, extraordinary reliability and average load balancing of the service data flow. In the meantime, well-organized network control and resource utilization is provided to users through combined attributes of 5G and SDN.

SDN modernization is realized through the network function, where each function is linked with software level control based on virtualization technology like wireless virtualization [179]. In standard format, the network controller may contain inter-system coordination, radio resource management [180, 181], policy management, information center, path management, mobility management[182], compatibility for the conventional network adapter, network resource organization module [183] and so on. Similarly, API provides report state information from to control cloud from forwarding cloud and access cloud. The control cloud directs 5G cloud architecture. Therefore, network topology contains service factors and forwarding units. The control cloud selects mainly services-related paths on the basis of user data, service information and administration policy. Resultantly, user experience and capacity of service networks are improved with cache management. The control cloud achieves intelligent network traffic scheduling through the flexible deployment of the forwarding cloud. However, 5G network design will provision local changes at the intermediary level that will have a constructive influence on the expansion of the whole modernized network and

the evolution of the existing mobile network. Similarly, 5G architecture reins the complications instigated by data flux, latencies, energy efficacy and quantity of connections in varied business scenarios. The incessant area coverage, huge volume, low power operations, minima latencies [17, 184–189] and high dependability are key application scenarios of mobile networks and the internet.

New orchestration framework and flexible network at the edge can be realized through novel functionalities of modern programming languages at the data plane [190]. [191] presents a traffic prediction model based on a Long Short-Term Neural network for dynamic resource allocation for SDN and Edge computing in 5G. SDN-based location aware network virtualization minimizes network load and resource cost by efficiently selecting VMs, VNF nodes, applications and resources [192]. [193] present an Entropy-based simple additive weighting decision-making method for multi-criteria handover in SDN-based 5G. Light-trails (LTs) architecture-based dynamic bandwidth communication, sub-wavelength optical grooming and optical layer multicasting are novel implementations in 5G backhaul [194]. [195] proposed a metaheuristic approach for optimal performance with low complexity for the joint controller and gateway placement in 5G-Satellite SDN. NS's QoS framework in SDN has provided key QoS indicators for fundamental 5G scenarios [196]. Before the discussion on the joint security paradigm in next paragraph, we provide Fig. 6 as a joint visualization through the number of security solutions of our review in Section 2 and Section 3, which illustrates the broader security strength in the modern network through the combined implementation of various security solution in both the emerging g technologies of 5G and SDN. It is also deducible that SDN based security solution are directed towards strong access control due to centralized architecture.

## 4.1 5G Security in SDN

The fast expansion of network innovations and radically rationalized management of huge networks is the well-known promise of SDN technology. Basically, SDN achieves packet forwarding inside the network through centralized monitoring and control of the whole network through the implementation of control plane architecture [197]. Likewise, 5G encompasses various modern key technologies, but improved security and high throughput management is attributed to SDN [198, 199]. The study in [200] presented a relative comparison between conventional and SDN network architecture, focusing on primary network resources essential in traditional networks. [201] used multiple approaches to achieve synchronization in a data model for the simultaneity of inheritance in SDN networks. The concept of the maximized cluster in the 5G control plane is proposed by [202] for implanting a security framework in big data analysis. It further deliberates upon various authentication mechanisms for optimization of control plane and organization of cluster arrangement. [203] have introduced a layered security architecture for 5G Software Defined Mobile Networking (SDMN) and cloud computing. The presented method covers five mechanisms: occurrence supervision, policy-controlled communication, security statistics, secure channel, and scrutinized SDMN security for control and data levels. The deep learning-based IDS approach [121] and multi-layered AI-based IDS solution [163] for SDN-enabled 5G networks effectively detect and prevent threats. The joint manifestation of 5G and SDN has revolutionized the modern networking security concept. The joint paradigm of 5G and SDN can be visualized though additional wireless plane as depicted in Fig. 7. The overall emerging concepts with the integration of 5G and SDN are summarized in Table 7.

Table 7
Joint Paradigm of 5G & SDN with Solutions and Outcomes

| Ref. | Year | Emerging Concepts | Solution | Outcomes |
|---|---|---|---|---|
| [190] | 2021 | Disruptive functionalities of P4 language | Novel functionalities at the data plane level in SDN enabled 5G | New orchestration frameworks at the edge |
| [13] | 2020 | SDN controller placement | Optimized SDN control placement in ISTNs | Minimized the average failure probability of SSDN control paths |
| [191] | 2021 | Neural Network-based resource allocation | Long Short-Term Neural network for dynamic resource allocation for SDN and Edge computing in 5G | Improved prediction accuracy |
| [192] | 2020 | Location-aware network | Location-aware network virtualization method | Minimized network load and resource cost |
| [193] | 2021 | Entropy-based decision making | Entropy-based simple additive weighting decision-making | Enhancement in handover mechanism |
| [194] | 2021 | Dynamic bandwidth control | LTs architecture of light-trails for micro cells, pico cells, and femto cells | Realized coordinated multipoint using light-trails |
| [195] | 2020 | Metaheuristic Approaches | Joint controller and gateway placement in 5G-Satellite SDN | Improved accuracy and lesser computational intricacy |
| [196] | 2020 | QoS framework for NS | QoS framework of NS in 5G and beyond networks based on SDN | Provide reliable E2E QoS |
| [201] | 2019 | SDN based synchronization | Synchronization in the data model | The simultaneity of inheritance in SDN networks. |
| [202] | 2021 | Analysis framework | Security framework in dig data analysis | Maximized cluster in the 5G control plane |
| [203] | 2021 | SDN based authentication | Authentication mechanisms for control plane | Policy-controlled communication |

## 5. 5g Security And Emerging Networking Concepts

This survey portion covers the utmost prevailing implementations known as NVF, MEC and NS in 5G and SDN-based modern emerging communication concepts. Likewise, several 5 G-based security solutions are related to these technologies. The implementation of such technologies is widely suggested in joint SDN and 5G environments. Moreover, the effect of these technologies on network security is also deliberated in this segment. It can be observed from prevailing research solutions that these technologies are primarily implemented in close integration with SDN. The reviewed areas are further summarized in Table 8 as well.

# 5.1 Network Function Virtualization in 5G

Conventional network operations are achieved through specific hardware and software implementation. Each hardware node performs an explicit network functionality [204] communication. However, the multifold advancements in mobile computer networks are being hampered due to distributed conventional network architecture. Primarily conventional mobile network architecture includes a complicated foundational structure with an enormous diversity of proprietary hardware nodes. Moreover, this traditional network architecture depicts resistance in implementing revisions in-network services. Similarly, complicated and costly proprietary hardware machines are making the task more challenging [205]. However, the modern concepts of networking are quickly resolving these issues. Hence, it is necessary to renovate the network infrastructure in line with technological advancement systematically. Therefore, independence from hardware limitations has become a focused area of network providers. The resultant of all these limitations is the conception of Network Virtualization Function (NVF) to redefine the network equipment architecture. The implementation of NVF is achieved through trademarked hardware of various organizations. Network services hosted on virtual platforms are termed as NVF[206]. However, currently all NFV are incorporated through cloud based software application. Common Commercial Off The Shelf (COTS) hardware is utilized for the implementation of NVF in network infrastructure. Elimination of proprietary hardware substantially reduces infrastructure costs. NFV, being a novel technology, is creating tremendous opportunism for the industry to incorporate various business models. However, it also surfaces challenging security paradigms. Software defined NVF fairly optimized the traffic matrix for essential endeavors such as model, measure, maintain and augment heterogeneous network architectures [207].

5G network quality of services is seriously undermined due to security imitations. The security vulnerabilities are spread across hardware as well as virtual architecture. Particularly, vulnerable NFV renders all other network elements compromised. [208–211] have presented all-inclusive

surveys of security vulnerabilities in the NFV environment. However, it is suggested that virtualization through SDN and NFV in 5G communication are expected to fill the gap of programmable control and management of network [25]. [212] highlighted the security requirements in NFV mobile cloud architectures. Similarly, NVF vulnerabilities are also discussed [213]. An Intel Software Guard Extensions (Intel SGX) based novel scheme to counter stealing and manipulation of internal management is discussed by [214]. Intel SGX is also suitable for SDN controllers to secure network virtualization implementation [175]. Similarly, [215–217] suggested building security management architecture on this modern NFV. Openflow infrastructure is also utilized for evaluation and analysis through the concept of Network Security Function Virtualization (NSFV) [201, 218]. Security concerns associated with network service infrastructure, network surveillance and 5G networks End to End (E2E) security can be addressed through NSFV. Moreover, several NVF security schemes are also suggested by [219].

## 5.2 Mobile Edge Computing in 5G

Utilization of network edge for cloud computing implementation in mobile networks is known as MEC or Multi Access Edge Computing [220]. Several SDN-based MEC implementations are available, especially for several solutions related to the 5G network. [221] suggest SDN-based performance for efficient control of distributed resources in MEC. SDN-based MEC in 5G provides adaptive control for the initial congestion window through deep enforcement learning [222]. MEC-based operations are performed close to the user interface and relatively distant from the network administrator. Therefore, physical attacks are more susceptible to edge devices. The most vulnerable functionalities of edge computing are billing and management or data route. [223] suggests that logging of periodic polling by edge user to another UE provisions data tracking by the core 5G network. Several articles have discussed different measures to curtail security vulnerabilities related to MEC. Services related to multimedia content and multi-shared data are to be potentially secured through Zero-watermarking and visual cryptography [224]. [225] suggests a biometric security solution for facial pictures through the above-mentioned method with unharmed image quality. The same mechanism is also suggested for copyright protection in multimedia content. Device to Device (D2D) communication with edge nodes has been proposed as a secure mobile edge computing framework by [226]. Security vulnerabilities in Vehicular Edge Computing (VEC) are countered through a non-centralized management system [227]. For suitable security scheme implementation in real-time multi-conditional 5G network ecosystem, [228] presented virtualized fuzzy logic-based Fog and Mobile-Edge Computing (FMEC). [229] suggests a mechanism for authentication-dependent MSNs with MEC for improving the trust level for Mobile Social Networks (MSNs). The information of social relations is utilized to refine security and effectiveness at the edge in the 5G network. [230] examines security concerns for supporting MEC in IoT applications.

Cloud-based architecture is a necessity for handling huge streams of continuous data in the modern era of Beyond 5G technology. Limited storage, energy and dependability are primary restraining factors in mobile end devices. Mobile Cloud Computing (MCC) is recognized as a potential solution to this problem due to mobile computing and cloud computing integration. This also provides unhampered data access to the mobile user. This scheme has introduced various security vulnerabilities associated with privacy, data integrity and authentication. Several secure MCC systems has been discussed by [231]. Likewise in [232] proposes protected and effective data distribution in MCC. It is an independent of 3rd party mechanism for ensuring data integrity, authentication, privacy, access control and manageability. A chaotic fuzzy transformation technique has been proposed for incorporating the search route of user's encrypted data on the cloud in MCC to guarantee confidentiality and privacy. Similarly, a low processing requirement-based data distribution process for MCC is suggested by [233]. [142, 234] offer Ciphertext-Policy an appropriate access control configuration to ensure cloud security. [235] designed proxy encryption and a ciphertext-policy framework for Peer to Peer (P2P) storage in the cloud combined with practical and precise handling of cipher text.

Several generic MEC-based security implementations are suggested in the literature that can be optionally employed in 5G Networks. Fog and cloud computing-based manageable, effective and protected recovery system is presented by [236]. For workflow applications on centralized clouds, [237] have presented an extension of the Bell-LaPadula Multi-Level security model-based algorithm. This model introduced an entropy computing technique for the utmost dependable workflow placement. A preventive scheme is suggested by [238] to protect the information of data interchange amongst different data owners from an untruthful cloud server. Another novel implementation is a time-based self-vanishing mechanism for data security [239]. This scheme employs a Key-Policy with Time-Specified Attributes (KP-TSA) for cloud architecture. For data flow administration of smart grids based on big data, [196] suggested that Smart-Frame offer a less vulnerable cloud computing architecture.

## 5.3 Network Slicing in 5G

A traditional methodology of divide and rule has been utilized in 5G networks. Therefore, 5G networks are managed for security services through NS. NS is built on the foundation of SDN and NVF technologies [240]. [241] suggested SDN-based NS in 3GPP network slice management for fundamental operations specific federated control. In order to get executed on the upper layer of specific shared physical network services, various logical/virtual networks are deployed as a unique form of NFV. Global configuration of the network resources, isolation of Adhoc-users and optimization in distinct traffic clusters are primary functions of NS [242]. Particularly desired functionalities in the form of a case/field are segregated as slices. A solo physical network is distributed virtually, each recognized as a comprehensive E2E network. All fundamental services like access, transport, device and core network are entirely isolated from each other to function independently in various dedicated services and scenarios. Security, QoS and resource management are completely optimized through NS-based division. Thus, E2E NS is employed to manage

computing, network and storage resources. Enhanced compatibility, network infrastructure management, and asset dissemination are considered primary functionalities of NS in 5G. Similarly, NS security is an essentially focused requirement for effective NS functionality. Similarly, several requirements necessitate a robust controlling scheme, such as unplanned communication among operational applications, network operator, signaling, and management level communication. Therefore, an efficient scheme is mandatory for the security of connections between operations, slices, and edges to meet the operator's security criteria.

NS concept is considered substantially vulnerable without a secure communication mechanism among various distributed slices. Attack on communication in NSs can cause underutilization of resources due to hampered slices management services [243]. NSs are loaded in the host machine dynamically by the slice manager. Therefore, an authentication mechanism between the network slice manager and the physical host is deemed essential for safe and secure communication [244]. Especially, the virtual entities in the slice are more vulnerable as they can be vanished, changed, or modified with another fresh request by a malevolent or non- malevolent actor. This kind of attack can disrupt all network slices' functionalities, which can be avoided through a strong authentication mechanism for network slices. There are diverse properties of network slices related to performance and latency due to application-oriented protocols and network services. However, this diversity must not be a challenge if a baseline security level universal for all layers is implemented without any exception. Similarly, all level must contain evenly characterized security infrastructure in case the baseline scheme unavailable.

A hierarchical authentication mechanism is suggested by [245]. In this scheme, users are first required to link with the less secure slice by authentication and then access the fully secured slice—a famous vulnerability in any communication system a the denial of service. Similarly, network slicing is also vulnerable in case common resources are exhausted. For assured maximum and minimum recommended levels of resources, network slicing must-have functionalities of capping resources and optionally ring-fencing resources. Ring-fencing embeds competence in NS managers to initiate security protocols even in case of resource exhaustion [243]. There are also several other vulnerabilities like leakage of any cryptographic information through the side-channel attack. Mainly, side-channel attacks are more probable during slice share primary hardware. Side-channel attacks can be countered through the segregation of virtual machines that averts the code disclosure of one virtual element due to the code compromise of some other virtual entity. Hence, it is mandatory to incorporate resilient security mechanism is both UEs and network for competent safety [243]. There is expectedly an elevated possibility of new security threats due to many linked devices in 5G networks. [246–249] have discussed the demands and requirements of system security Next Generation Mobile Network (NGMN) and solutions to some probable threats. NGMN is emerging as a model of innovative methods, authentication for network slicing, network delays, access network, and reliable user experience for most security threats. [250] proposed cross payer control based on SDN for network management through NS-enabled Radio Access Network (RAN) in 5G network.

Table 8
Issues in Emerging Networking Technologies related to 5G

| Ref. | Year | Technology / Domain | Issues | Recommendation |
|---|---|---|---|---|
| [218] | 2020 | NFV | Stealing and manipulation of internal management Data | Intel SGX for secure SDN controller in NVF |
| [201] | 2019 | | Securing resources and dynamic control functionality | Evaluation and analysis through the concept of NSFV |
| [224] | 2017 | MEC | Multimedia content and multi shared data security | Zero-watermarking and visual cryptography |
| [225] | 2017 | | Copyright protection in multimedia | Biometric security solution |
| [228] | 2019 | | VEC | Real-time multi-conditional network ecosystem based on FMEC |
| [229] | 2021 | | The trust level for Mobile Social Networks | Authentication dependent MSNs with MEC |
| [232] | 2019 | | Confidentiality and privacy | Chaotic fuzzy transformation technique |
| [233] | 2018 | | Low processing requirement | Data distribution process for MCC |
| [235] | 2021 | | Handling cipher text | A proxy encryption and a cipher text-policy framework |
| [236] | 2020 | | Effective and protected recovery system | A fog and cloud computing-based solution |
| [237] | 2018 | | Workflow applications security on centralized clouds | Extension of the Bell-La Padula Multi-Level security model |
| [239] | 2019 | | Data interchange amongst different data owners | Time-based self-vanishing mechanism for data security |
| [251] | 2019 | | Data flow administration of smart grids | Smart-Frame to offer a less vulnerable cloud computing architecture. |
| [244] | 2020 | NS | Attack for underutilization of resources | Authentication mechanism between network slice manager |
| [245] | 2020 | | Evenly characterized security infrastructure | A hierarchical authentication mechanism |
| [243] | 2019 | | Vulnerable in case common resources are exhausted | Ring-fencing |

## 6. Research Directions

Current network infrastructure has huge expansion in various dimensions like the enormous quantity of user's data and eased network operations. However, several limiting factors simultaneously prevail even when there is substantial capacity in terms of spectrum utilization and data rates. 5G network have visible enhancement certainly in conveying a lot of ease to communication services in terms of enactment, competence and QoS specifications. However, this modernization is also surfacing various challenging issues; we will deliberate certain utmost prevailing complications confronted in the joint paradigm of SDN and 5G network along with a summary in Table 9.

## 6.1 mm-Wave or Tera-Hertz Spectrum

Several limiting factors exist for employing mm-Wave or THz technology in 5G “beachfront spectrum” [252]. However, the performance gains in bandwidth are worthy of such limiting factors [15, 245]. The primary problem of mm-Wave and THz is the properties related to signal fading and distortion problems during the propagation process in Beyond 5G networks [252]. SDN management architecture can optimize TH spectrum and network resources in the 5G era [253]. Dynamic beamforming control services management through SDN architecture is possible in 5G networks [254]. SDN along with NVF has potential to virtualize the mm-Wave beamforming concepts in RANs for handling massive flux of connections in 5G communication [255].

## 6.2 Un-availability of Universal Channel

A major challenge of 5G is more channels [256]. While mm-Wave still contains room for research to avoid the delay and blocking issues [257]. The resolution of these complications is valuable to promote research in designing air interfaces and multiple access mechanisms. In [258], joint optimization of fronthaul Grade-of-Service (GoS) for minimized power consumption is proposed. [259] suggests a novel SDN-based handover approach for advance channel allocation in a 5G SDN-based network. SDN based mobility management can optimize MEC-enabled 5G vehicular networks [260].

## 6.3 Transmission Latency

Millimeter-wave is highly sensitive to the surrounding atmosphere of transmitter and receiver hardware [261]. Thus, the design of RF hardware is also a key area of research for improved performance of 5G infrastructure. This area seems quite lagging compared to evolution and research in modern networking concepts. Slicing in the SDN core network can achieve ultra-low latencies for 5G-based autonomous systems [262]. Similarly, adaptive clustering for traffic aggregation can substantially reduce the bit error rate in SDN-enabled 5G networks [263]. [264] presented a queuing model-based analysis to reduce overall network congestions and latencies in SDN-enabled 5G networks. 5G has extremely challenging delay management or real-time operations requirements. Current literature shows that 5G is still waiting for further research to reduce network time below one millisecond [265].

## 6.4 Energy Efficiency

The modern IoT paradigm and mobile ecosystem are increasing stress on energy efficiency in 5G design. Presently, the increased concentration of base stations is the primary power-consuming element in the 5G architecture. Similarly, massive data consumption will push the spectrum capacity to limits [266]. Moreover, the user handing over among base stations will also boost the power consumption. Although a lot of effort is in the pipeline, there is still a requirement if research in devising energy-saving techniques. Currently, edge computing, renewable energy technologies, and energy-aware technology are prevailing as potential solutions to this challenge. [267] proposed a novel efficient energy consumption approach at the expense of the processing power of the SDN controller. SDN provides a management architecture in 5G Internet of Vehicle (IoV) architecture to effectively handle resources [268]. [269] suggested using NVF and SDN as enablers for efficient energy consumption by network resources. SDN/NVF enables joint routing and function placement scheme for energy efficiency, the simulation-based results show up to 70% energy economy through the proposed algorithm [270].

## 6.5 Scalability

Centralized management architecture of 5G may produce network congestion among switches and controllers [271, 272]. Hence, it is necessary to keep scalability a paramount requirement [273–276]. Similarly, a dramatic increase in UEs is a concerning factor [266]. Therefore, a focused researcher is necessary for optimizing resource consumption, such as network data aggregation technologies [277]. [278] presented a hybrid SDN-based 5G core network for efficient path computation and reduced synchronization overhead. Likewise, an SDN-based synchronization mechanism for the 5G core network is considered optimal for achieving scalability [279].

## 6.6 Mobility and Routing

Communication services are primarily influenced by the mobility of devices in the wireless network. In 5G, the centralized network controller SDN can effectively address positional changes in both horizontal and vertical dimensions through sensors and geodata [266, 275]. Moreover, this centralized control architecture also reduces link failures and unplanned route changes in static network devices [271, 274]. However, these factors have gained only limited attention in the literature. [280] addresses mobility management through SDN, NFV and MEC in 5G network. [281] presents feasibility for implementation of SDN OpenFlow for 5G mobile network. [282] suggests SDN based routing optimization for network load balancing and energy efficient routing in 5G enabled mobile networks.

## 6.7 Interoperability

The functionality of SDN in the 3GPP framework is still debatable as there is a contradictory perception in this domain, such as certain groups propose that additional adjustments should be incorporated in the protocol while others argue for developing a novel universal design from basics [266, 275, 283]. [272] and [273] suggest incorporation of interoperability among various network controller software. But this concept requires in-depth analysis and further research to verify hardware and software compatibility. 5G heterogeneous IoT can be handled using semantic technologies in combination with that of SDN [284]. [285] proposed a novel Synchronous Digital Hierarchy (SDH) achieve interoperability with higher-level protocol in the 5G network.

## 6.8 Performance Evaluation

Integrated LTE-SDN operations are discussed in the literature; however, practical evaluation of performance parameters requires further formal research [271, 272, 275, 277, 283, 286–288]. Virtual scenarios of the LTE-SDN combination are built by [266, 275–277]. But these scenarios are focused on specific functionalities; therefore, an inclusive and general verification mechanism should be offered to authenticate modern concepts.

## 6.9 Virtual Machine Employment

SDN can support network operations attain excellent outcomes regarding VM employment, but it also has certain security issues especially related to data privacy and availability [289]. Therefore, Research for safe, resilient and continuous availability VM is crucial and very limited literature is available in this domain.

## 6.10 Security

5G has revolutionized wireless networks [288, 290]. The traditional wireless network contained several shortcomings; however, SDN in 5G has a completely new scheme, but several open-ended issues and unknown challenges require enormous research. Such as DDoS discovery counter mechanism [291], MitM attack Counters [292], 5G-SDN ecosystem-based IDS, IPS [293].

Table 9
5G & SDN research trends and challenges

| Ref. | Research Area | Challenges & Trends |
|---|---|---|
| [252] | mm-Wave or Tera-Hertz Spectrum | Signal fading and distortion problem during the propagation process |
| [245, 261] | | Performance gains in bandwidth |
| [253] | | SDN management architecture for joint optimization of 5G TH spectrum |
| [254] | | Dynamic beamforming control services in 5G networks |
| [256] | Un-availability of Universal Channel | Extra number of channels |
| [257] | | Avoidance of the delay and blocking issues |
| [258] | | Joint optimization for minimized power consumption |
| [259] | | SDN based advance channel allocation in 5G SDN based network |
| [261] | Transmission Latency | Millimeter-wave high sensitivity to the surrounding atmosphere |
| [262] | | 5G slicing in SDN for ultra-low latencies in autonomous systems |
| [263] | | Adaptive clustering in SDN enabled 5G |
| [264] | | A queuing model-based analysis to reduce network congestions |
| [265] | | Reduce network time below one millisecond |
| [266] | Energy Efficiency | Energy efficiency in 5G mobile ecosystem |
| [267] | | Efficient energy at the expense of processing power of SDN controller |
| [268] | | SDN based 5G IoV architecture |
| [269] | | NVF and SDN as enablers for efficient energy consumption |
| [271, 272] | Scalability | Management architecture of 5G for congestion control |
| [277] | | Optimizing resource consumption in network data aggregation technologies |
| [278] | | Hybrid SDN based 5G core network for efficient path computation |
| [279] | | SDN based synchronization mechanism for scalable 5G core network |
| [266, 275] | Mobility and Routing | Positional changes in 3 dimensions |
| [271, 274] | | Handling of link failures |
| [280] | | Mobility management |
| [281] | | Implementation of SDN OpenFlow for 5G mobile network |
| [266, 275, 283] | Interoperability | Additional adjustments in the protocol for developing a universal design in 5G |
| [272, 273] | | Verification of hardware and software compatibility |
| [284] | | 5G heterogeneous IoT using the semantic technologies in combination with SDN |
| [285] | | SDH to achieve interoperability in 5G network |
| [271, 272, 275, 277, 283, 286–288] | Performance Evaluation | Formal evaluation of performance parameters |
| [266, 275–277] | | Virtual scenarios of LTE-SDN combination |
| [283] | Virtual Machine Employment | SDN operations and VM employment |
| [291] | Security | DDoS discovery, the counter mechanism |
| [292] | | MitM attack Counters |
| [293] | | 5G-SDN ecosystem-based IDS, IPS |

## 7. Conclusion

In this paper, we presented a detailed survey on the joint paradigm of 5G and SDN emerging mobile technologies focusing on architecture and security. The leading portion was regarding the 5G evolution, foundational technologies and security. We presented a comprehensive review of the latest $CIA^3$ based security analysis and threat categorization related to 5G employment in the modern network environment. We provided a similar methodical outline of SDN with this premise. Further, we discussed the advantages, security and improvement in network architecture related to joint implementation of 5G and SDN. We also presented pictorial overview of all the inferences of our review regarding combined employment of 5G and SDN. Moreover, we also reviewed the 5G security solutions and challenges in emerging network technologies, including NVF, MEC and NS. Finally, we discussed the open-ended problems, unaddressed factors and future research directions of 5G and SDN network technologies. Our survey conclusively advocates revolution in modern network communication due to the joint paradigm of 5G and SDN. It can be imperatively concluded that modern network communication will be definitely revolutionized in terms of architecture and security due to joint implementation of 5G and SDN.

## Declarations

The authors have NO affiliations with or involvement in any organization or entity with any financial interest (such as honoraria; educational grants; participation in speakers' bureaus; membership, employment, consultancies, stock ownership, or other equity interest; and expert testimony or patent-licensing arrangements), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

# ACKNOWLEDGEMENT

The authors would like to acknowledge Universiti Kebangsaan Malaysia Geran Galakan Penyelidik Muda

## References

1. Anwar, S., B.S. Chowdhry, and R. Prasad. *Smart pharma: Towards efficient healthcare ecosystem*. in *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures*. 2017. Springer.
2. Javaid, M., et al., *Progressive schema of 5G for Industry 4.0: features, enablers, and services.* Industrial Robot: the international journal of robotics research and application, 2022.
3. Prathiba, S.B., et al., *SDN-assisted safety message dissemination framework for vehicular critical energy infrastructure.* IEEE Transactions on Industrial Informatics, 2021.
4. Sun, P., *5GtoB Evolution Path*, in *Unleashing the Power of 5GtoB in Industries*. 2021, Springer. p. 273-279.
5. Rahman, M.M., M. Manavalan, and T.K. Neogy, *Artificial Intelligence in 5G Technology: Overview of System Models.* Asia Pacific Journal of Energy and Environment, 2021. **8**(1): p. 17-26.
6. Ren, C., et al., *Achieving Near-Optimal Traffic Engineering Using a Distributed Algorithm in Hybrid SDN.* IEEE Access, 2020. **8**: p. 29111-29124.
7. Hussain, R., et al., *On the Adequacy of 5G Security for Vehicular Ad Hoc Networks.* IEEE Communications Standards Magazine, 2021. **5**(1): p. 32-39.
8. Fourati, H., R. Maaloul, and L. Chaari, *A survey of 5G network systems: challenges and machine learning approaches.* International Journal of Machine Learning and Cybernetics, 2021. **12**(2): p. 385-431.
9. Khan, A., et al., *An End-to-End (E2E) Network Slicing Framework for 5G Vehicular Ad-hoc Networks.* IEEE Transactions on Vehicular Technology, 2021.
10. Dong, S., K. Abbas, and R. Jain, *A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments.* IEEE Access, 2019. **7**: p. 80813-80828.
11. Haque, M.R., et al., *Automated controller placement for software-defined networks to resist DDoS attacks.* Computers, Materials & Continua, 2021. **68**(3): p. 3147-3165.
12. Singh, S. and S. Prakash, *A Survey on Software Defined Network based on Architecture, Issues and Challenges*, in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*. 2019, IEEE.
13. Torkzaban, N., et al., *Joint Satellite Gateway Placement and Routing for Integrated Satellite-Terrestrial Networks*, in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. 2020, IEEE.
14. Pattaranantakul, M., et al., *NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures.* IEEE Communications Surveys & Tutorials, 2018. **20**(4): p. 3330-3368.

15. Siddiqui, M.U.A., et al., *Interference management in 5G and beyond network: requirements, challenges and future directions.* IEEE Access, 2021. **9**: p. 68932-68965.
16. Busari, S.A., et al., *5G Millimeter-Wave Mobile Broadband: Performance and Challenges.* IEEE Communications Magazine, 2018. **56**(6): p. 137-143.
17. Erunkulu, O.O., et al., *5G Mobile Communication Applications: A Survey and Comparison of Use Cases.* IEEE Access, 2021. **9**: p. 97251-97295.
18. Shanmugam, H.M. and S. Srinivasan, *A Review on Future Security Challenges in 5G: Future Security Challenges in 5G.* Asia-Pacific Journal of Management and Technology, 2020. **1**(2): p. 8-12.
19. Pohrmen, F.H., R.K. Das, and G. Saha, *Blockchain-based security aspects in heterogeneous Internet-of-Things networks: A survey.* Transactions on Emerging Telecommunications Technologies, 2019. **30**(10).
20. Nisar, K., et al., *A survey on the architecture, application, and security of software defined networking: Challenges and open issues.* Internet of Things, 2020. **12**: p. 100289.
21. Ahmad, S. and A.H. Mir, *Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers.* Journal of Network and Systems Management, 2020. **29**(1).
22. Yurekten, O. and M. Demirci, *SDN-based cyber defense: A survey.* Future Generation Computer Systems, 2021. **115**: p. 126-149.
23. Hassan, R., et al., *Internet of Things and its applications: A comprehensive survey.* Symmetry, 2020. **12**(10): p. 1674.
24. Alam, T., *Cloud-MANET and its Role in Software-Defined Networking*. 2020, Center for Open Science.
25. Barakabitze, A.A., et al., *5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges.* Computer Networks, 2020. **167**: p. 106984.
26. Thandeeswaran, R., et al., *Managing Security Services in Heterogenous Networks: Confidentiality, Integrity, Availability, Authentication, and Access Control*. 2020: CRC Press.
27. Ghosh, A., et al., *5G Evolution: A View on 5G Cellular Technology Beyond 3GPP Release 15.* IEEE Access, 2019. **7**: p. 127639-127651.
28. Attaran, M., *The impact of 5G on the evolution of intelligent automation and industry digitization.* Journal of ambient intelligence and humanized computing, 2021: p. 1-17.
29. Banumathi, J., S. Sangeetha, and R. Dhaya, *Robust Cooperative Spectrum Sensing Techniques for a Practical Framework Employing Cognitive Radios in 5G Networks.* Artificial Intelligent Techniques for Wireless Communication and Networking, 2022: p. 121-138.
30. Nidhi, A. Mihovska, and R. Prasad, *Overview of 5G New Radio and Carrier Aggregation: 5G and Beyond Networks*, in *2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC)*. 2020, IEEE.
31. Qamar, F., et al., *A comprehensive review on coordinated multi-point operation for LTE-A*. Computer Networks, 2017. **123**: p. 19-37.
32. Ibrahim, A.A.A., et al. *Review and analyzing RFID technology tags and applications*. in *2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT)*. 2019. IEEE.
33. Santos, G.L., et al., *When 5G meets deep learning: a systematic review.* Algorithms, 2020. **13**(9): p. 208.
34. Qamar, F., et al., *Outdoor Propagation Channel Investigation at 26 GHz for 5G mmWave Communication*, in *2020 IEEE Student Conference on Research and Development (SCOReD)*. 2020, IEEE.
35. Chen, W.C., *5G mmWAVE Technology Design Challenges and Development Trends*, in *2020 International Symposium on VLSI Design, Automation and Test (VLSI-DAT)*. 2020, IEEE.
36. Zugno, T., et al., *Toward Standardization of Millimeter-Wave Vehicle-to-Vehicle Networks: Open Challenges and Performance Evaluation.* IEEE Communications Magazine, 2020. **58**(9): p. 79-85.
37. Zhang, C., et al., *Research Challenges and Opportunities of UAV Millimeter-Wave Communications.* IEEE Wireless Communications, 2019. **26**(1): p. 58-62.
38. Lee, J., et al., *Spectrum for 5G: Global Status, Challenges, and Enabling Technologies.* IEEE Communications Magazine, 2018. **56**(3): p. 12-18.
39. Yang, X., et al., *Hardware-Constrained Millimeter-Wave Systems for 5G: Challenges, Opportunities, and Solutions.* IEEE Communications Magazine, 2019. **57**(1): p. 44-50.
40. Gaur, G., et al., *Application specific thresholding scheme for handover reduction in 5G Ultra Dense Networks.* Telecommunication Systems, 2020. **76**(1): p. 97-113.
41. Habbal, A., S.I. Goudar, and S. Hassan, *A Context-aware Radio Access Technology selection mechanism in 5G mobile network for smart city applications.* Journal of Network and Computer Applications, 2019. **135**: p. 97-107.
42. Feng, W., et al., *Millimetre-Wave Backhaul for 5G Networks: Challenges and Solutions.* Sensors (Basel, Switzerland), 2016. **16**(6): p. 892.

43. Qamar, F., et al., *Robust Schemes to Enhance Energy Consumption Efficiency for Millimeter Wave-Based Microcellular Network in Congested Urban Environments.* International Journal of Electronics and Telecommunications, 2021. **67**(3): p. 417-424.
44. Gu, X., et al., *A hybrid game method for interference management with energy constraint in 5G ultra-dense HetNets.* Journal of computational science, 2018. **26**: p. 354-362.
45. Inn, A.i., et al., *Framework for Handover process using Visible Light Communications in 5G*, in *2019 Symposium on Future Telecommunication Technologies (SOFTT)*. 2019, IEEE.
46. Ahmed, A., et al., *Cooperative Non-Orthogonal Multiple Access for Beyond 5G Networks.* IEEE Open Journal of the Communications Society, 2021. **2**: p. 990-999.
47. Kaba, V.B. and R.R. Patil, *A Precoding Based PAPR Minimization Schemes for NOMA in 5G Network.* SN Computer Science, 2021. **2**(4).
48. Lai, P., et al., *Cost-Effective User Allocation in 5G NOMA-based Mobile Edge Computing Systems.* IEEE Transactions on Mobile Computing, 2021.
49. Lai, P., et al., *Cost-Effective User Allocation in 5G NOMA-based Mobile Edge Computing Systems.* IEEE Transactions on Mobile Computing, 2021: p. 1-1.
50. Li, G., et al., *Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities.* Entropy (Basel, Switzerland), 2019. **21**(5): p. 497.
51. Yang, W., et al. *Dynamic URLLC and eMBB multiplexing design in 5G new radio*. in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*. 2020. IEEE.
52. Mutalemwa, L.C. and S. Shin, *A Classification of the Enabling Techniques for Low Latency and Reliable Communications in 5G and Beyond: AI-Enabled Edge Caching.* IEEE Access, 2020. **8**: p. 205502-205533.
53. Vasilakos, X., et al. *Towards Zero Downtime Edge Application Mobility for Ultra-Low Latency 5G Streaming*. in *2020 IEEE Cloud Summit*. 2020. IEEE.
54. Li, X., et al., *Hierarchical edge caching in device-to-device aided mobile networks: Modeling, optimization, and design.* IEEE Journal on Selected Areas in Communications, 2018. **36**(8): p. 1768-1785.
55. Bastug, E., M. Bennis, and M. Debbah, *Living on the edge: The role of proactive caching in 5G wireless networks.* IEEE Communications Magazine, 2014. **52**(8): p. 82-89.
56. Huang, Y., Y.T. Hou, and W. Lou. *A deep-learning-based link adaptation design for eMBB/URLLC multiplexing in 5G NR*. in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*. 2021. IEEE.
57. Boutiba, K., M. Bagaa, and A. Ksentini, *Radio Link Failure Prediction in 5G Networks.*
58. Bai, L., et al., *Multi-Satellite Relay Transmission in 5G: Concepts, Techniques, and Challenges.* IEEE Network, 2018. **32**(5): p. 38-44.
59. Sharma, B. and P. Singh, *A Review of Anti-phishing Techniques and its Shortcomings*, in *Lecture Notes on Data Engineering and Communications Technologies*. 2021, Springer Singapore. p. 273-288.
60. Khidzir, N.Z., et al., *Social engineering (SoE) attacks towards network security in higher learning institute: The partial least squares path modeling approach*, in *PROCEEDINGS OF 8TH INTERNATIONAL CONFERENCE ON ADVANCED MATERIALS ENGINEERING & TECHNOLOGY (ICAMET 2020)*. 2021, AIP Publishing.
61. Dzik, S., *COVID-19 Convalescent Plasma: Now Is the Time for Better Science.* Transfusion medicine reviews, 2020. **34**(3): p. 141-144.
62. Gundogan, C., et al., *Content Object Security in the Internet of Things: Challenges, Prospects, and Emerging Solutions.* IEEE Transactions on Network and Service Management, 2021: p. 1-1.
63. Zhao, G., et al., *Network slice selection in softwarization-based mobile networks.* Transactions on Emerging Telecommunications Technologies, 2019. **31**(1).
64. Ben Jaballah, W., M. Conti, and C. Lal, *Security and design requirements for software-defined VANETs.* Computer Networks, 2020. **169**: p. 107099.
65. Olimid, R.F. and G. Nencioni, *5G Network Slicing: A Security Overview.* IEEE Access, 2020. **8**: p. 99999-100009.
66. Zhao, H., et al., *A fast physical layer security-based location privacy parameter recommendation algorithm in 5G IoT.* China Communications, 2021. **18**(8): p. 75-84.
67. Lee, J., et al. *A Multi-Server Authentication Protocol Achieving Privacy Protection and Traceability for 5G Mobile Edge Computing*. in *2021 IEEE International Conference on Consumer Electronics (ICCE)*. 2021. IEEE.
68. Mo, J. and Z. Hu, *Comments on A Remote User Authentication Scheme for Multi-server 5G Networks.* International Journal of Network Security, 2021. **23**(5): p. 878-882.
69. Kwon, S., et al., *Towards 5G-based IoT security analysis against Vo5G eavesdropping.* Computing, 2021. **103**(3): p. 425-447.

70. Sedjelmaci, H., *Cooperative attacks detection based on artificial intelligence system for 5G networks.* Computers & Electrical Engineering, 2021. **91**: p. 107045.
71. Rahman, M. and H. Jahankhani, *Security vulnerabilities in existing security mechanisms for iomt and potential solutions for mitigating cyber-attacks*, in *Information Security Technologies for Controlling Pandemics*. 2021, Springer. p. 307-334.
72. Jiang, H., et al., *Location privacy-preserving mechanisms in location-based services: A comprehensive survey.* ACM Computing Surveys (CSUR), 2021. **54**(1): p. 1-36.
73. Park, J.H., et al., *A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions.* Hum.-Centric Comput. Inf. Sci, 2021. **11**(3).
74. Wang, Y., Z. Zhang, and Y. Xie. *Privacy-Preserving and Standard-Compatible {AKA} Protocol for 5G*. in *30th {USENIX} Security Symposium ({USENIX} Security 21)*. 2021.
75. Noura, H.N., R. Melki, and A. Chehab, *Efficient data confidentiality scheme for 5g wireless NOMA communications.* Journal of Information Security and Applications, 2021. **58**: p. 102781.
76. Zhang, J., et al., *Is Today's End-to-End Communication Security Enough for 5G and Its Beyond?* IEEE Network, 2021.
77. Gupta, R., S. Tanwar, and N. Kumar, *Blockchain and 5G integrated softwarized UAV network management: Architecture, solutions, and challenges.* Physical Communication, 2021. **47**: p. 101355.
78. Mani Sekhar, S., et al., *Security and Privacy in 5G-Enabled Internet of Things: A Data Analysis Perspective*, in *Blockchain for 5G-Enabled IoT*. 2021, Springer. p. 303-322.
79. Holtrup, G., et al., *5G System Security Analysis.* arXiv preprint arXiv:2108.08700, 2021.
80. Qi, L., et al., *Privacy-Aware Data Fusion and Prediction With Spatial-Temporal Context for Smart City Industrial Environment.* IEEE Transactions on Industrial Informatics, 2021. **17**(6): p. 4159-4167.
81. Chen, Z., et al., *Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control.* Future Generation Computer Systems, 2018. **87**: p. 712-724.
82. Wang, J., R. Zhu, and S. Liu, *A differentially private unscented Kalman filter for streaming data in IoT.* IEEE Access, 2018. **6**: p. 6487-6495.
83. Irshad, A., et al., *A Secure Blockchain-Oriented Data Delivery and Collection Scheme for 5G-enabled IoD environment.* Computer Networks, 2021: p. 108219.
84. Junejo, M.H., et al., *Location Closeness Model for VANETs with Integration of 5G.* Procedia Computer Science, 2021. **182**: p. 71-79.
85. Fonyi, S., *Overview of 5G security and vulnerabilities.* The Cyber Defense Review, 2020. **5**(1): p. 117-134.
86. Kim, H., *5G core network security issues and attack classification from network protocol perspective.* J. Internet Serv. Inf. Secur., 2020. **10**(2): p. 1-15.
87. Hussain, B., et al., *Deep learning-based DDoS-attack detection for cyber–physical system over 5G network.* IEEE Transactions on Industrial Informatics, 2020. **17**(2): p. 860-870.
88. Choi, S., et al., *5G K-SimNet: End-to-End Performance Evaluation of 5G Cellular Systems*, in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. 2019, IEEE.
89. Ayub, M.F., et al., *Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology.* Digital Communications and Networks, 2021. **7**(2): p. 235-244.
90. Nkenyereye, L., C.H. Liu, and J. Song, *Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles.* Future Generation Computer Systems, 2019. **95**: p. 488-499.
91. Hu, Y., et al. *Fuzzing Method Based on Selection Mutation of Partition Weight Table for 5G Core Network NGAP Protocol*. in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. 2021. Springer.
92. Choi, V.K., et al., *When danger strikes: A linguistic tool for tracking America's collective response to threats.* Proceedings of the National Academy of Sciences, 2022. **119**(4).
93. Rathee, A. and J.K. Chhabra, *Feature-based critical components identification in multimedia software.* Multimedia Tools and Applications, 2022: p. 1-24.
94. Wang, F. and X. Zhang, *Secure Resource Allocation for Polarization-Based Non-Linear Energy Harvesting Over 5G Cooperative CRNs.* IEEE Wireless Communications Letters, 2020: p. 1-1.
95. Li, J., X. Yang, and R. Sitzenfrei, *Rethinking the Framework of Smart Water System: A Review.* Water, 2020. **12**(2): p. 412.
96. Gupta, S., B.L. Parne, and N.S. Chaudhari, *Security Vulnerabilities in Handover Authentication Mechanism of 5G Network*, in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*. 2018, IEEE.
97. Kim, J., P.V. Astillo, and I. You, *DMM-SEP: Secure and efficient protocol for distributed mobility management based on 5G networks.* IEEE Access, 2020. **8**: p. 76028-76042.

98. Wang, N., et al., *Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities.* IEEE Internet of Things Journal, 2019. **6**(5): p. 8169-8181.
99. Haque, M.R., et al., *Unprecedented smart algorithm for uninterrupted SDN services during DDoS attack.* Computers, Materials & Continua, 2022. **70**(1): p. 875-894.
100. Sakthibalan, P. and K. Devarajan, *DFMS: Differential flow management scheme for denial of service impact mitigation in 5G communications.* Journal of King Saud University-Computer and Information Sciences, 2020.
101. Chen, C.-Y., G.-L. Hung, and H.-Y. Hsieh. *A study on a new type of DDoS attack against 5G ultra-reliable and low-latency communications*. in *2020 European Conference on Networks and Communications (EuCNC)*. 2020. IEEE.
102. Seok, B., et al., *Secure D2D communication for 5G IoT network based on lightweight cryptography.* Applied Sciences, 2020. **10**(1): p. 217.
103. Atapoor, S. *Security for 4G and 5G cellular networks*. in *Report for the Course Research Seminar in Cryptography (MTAT. 07.022), Institute of Computer Science, University of Tartu*. 2018.
104. Estrada, C.A., W. Fuertes, and H.O. Cruz, *An implementation of an artifact for security in 5G networks using deep learning methods.* Periodicals of Engineering and Natural Sciences, 2021. **9**(3): p. 603-614.
105. Wang, E.K., et al., *Voice-transfer attacking on industrial voice control systems in 5G-aided IIoT domain.* IEEE Transactions on Industrial Informatics, 2020.
106. Braeken, A. and M. Liyanage, *Highly efficient key agreement for remote patient monitoring in MEC-enabled 5G networks.* The Journal of Supercomputing, 2021. **77**(6): p. 5562-5585.
107. Mashtalyar, N., et al. *Social Engineering Attacks: Recent Advances and Challenges*. in *International Conference on Human-Computer Interaction*. 2021. Springer.
108. Sun, Y., et al., *Automated Attack and Defense Framework toward 5G Security.* IEEE Network, 2020. **34**(5): p. 247-253.
109. Iqbal, W., et al., *An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security.* IEEE Internet of Things Journal, 2020. **7**(10): p. 10250-10276.
110. Velasco, L., et al., *End-to-End Intent-Based Networking.* IEEE Communications Magazine, 2021. **59**(10): p. 106-112.
111. Larsen, L.M.P., M.S. Berger, and H.L. Christiansen, *Fronthaul for Cloud-RAN Enabling Network Slicing in 5G Mobile Networks.* Wireless Communications and Mobile Computing, 2018. **2018**: p. 1-8.
112. Long, Q., et al., *Software Defined 5G and 6G Networks: a Survey.* Mobile Networks and Applications, 2019.
113. Moorthy, V., R. Venkataraman, and R. Gururajan, *Bayesian trust analysis of flooding attacks in distributed software defined networking nodes.* Journal of Ambient Intelligence and Humanized Computing, 2020. **12**(7): p. 7489-7498.
114. *Redundant rule Detection for Software-Defined Networking.* KSII Transactions on Internet and Information Systems, 2020. **14**(6).
115. Correa Chica, J.C., J.C. Imbachi, and J.F. Botero Vega, *Security in SDN: A comprehensive survey.* Journal of Network and Computer Applications, 2020. **159**: p. 102595.
116. Kim, J., G. Caire, and A.F. Molisch, *Quality-Aware Streaming and Scheduling for Device-to-Device Video Delivery.* IEEE/ACM Transactions on Networking, 2016. **24**(4): p. 2319-2331.
117. Chen, K.-Y., et al., *SDNShield: NFV-Based Defense Framework Against DDoS Attacks on SDN Control Plane.* IEEE/ACM Transactions on Networking, 2021: p. 1-17.
118. Alonso, R.S., et al., *Deep Reinforcement Learning for the management of Software-Defined Networks in Smart Farming*, in *2020 International Conference on Omni-layer Intelligent Systems (COINS)*. 2020, IEEE.
119. Adebayo, A. and D.B. Rawat, *Deceptor-in-the-Middle (DitM): Cyber Deception for Security in Wireless Network Virtualization*, in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*. 2020, IEEE.
120. Islam, M.M., et al., *Software-defined vehicular network (SDVN): A survey on architecture and routing.* Journal of Systems Architecture, 2021. **114**: p. 101961.
121. Krishnan, P., S. Duttagupta, and R. Buyya, *OpenPATH: Application aware high-performance software-defined switching framework.* Journal of Network and Computer Applications, 2021. **193**: p. 103196.
122. Rawal, B.S., et al., *Network Augmentation by Dynamically Splitting the Switching Function in SDN*, in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. 2021, IEEE.
123. Park, T. and S. Shin, *Mobius: Packet re-processing hardware architecture for rich policy handling on a network processor.* Journal of Network and Systems Management, 2021. **29**(1): p. 1-26.
124. Awan, I.I., et al., *An improved mechanism for flow rule installation in-band SDN.* Journal of Systems Architecture, 2019. **96**: p. 1-19.
125. Ibrahim, M.Z. and R. Hassan, *The implementation of Internet of Things using test bed in the UKMnet environment.* Asia Pac. J. Inf. Technol. Multimed, 2019. **8**: p. 1-17.

126. de Oliveira, J.V.G., et al., *Virtualizing Packet-Processing Network Functions over Heterogeneous OpenFlow Switches.* IEEE Transactions on Network and Service Management, 2021: p. 1-1.
127. Kulkarni, M., M. Baddeley, and I. Haque, *Embedded vs. External Controllers in Software-Defined IoT Networks*, in *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*. 2021, IEEE.
128. Haxhibeqiri, J., et al., *In-Band Network Monitoring Technique to Support SDN-Based Wireless Networks.* IEEE Transactions on Network and Service Management, 2021. **18**(1): p. 627-641.
129. Kakkavas, G., et al., *Network Tomography for Efficient Monitoring in SDN-Enabled 5G Networks and Beyond: Challenges and Opportunities.* IEEE Communications Magazine, 2021. **59**(3): p. 70-76.
130. Todorov, D., H. Valchanov, and V. Aleksieva. *Simple routing algorithm with link discovery between source and destination hosts in SDN networks*. in *2021 International Conference Automatics and Informatics (ICAI)*. 2021. IEEE.
131. Bhatia, J., et al., *SDN-Enabled Adaptive Broadcast Timer for Data Dissemination in Vehicular Ad Hoc Networks.* IEEE Transactions on Vehicular Technology, 2021. **70**(8): p. 8134-8147.
132. Dawadi, B.R., et al., *Legacy Network Integration with SDN-IP Implementation towards a Multi-Domain SoDIP6 Network Environment.* Electronics, 2020. **9**(9): p. 1454.
133. Sokappadu, B. and A. Mungur. *A Middleware for Integrating Legacy Network Devices into Software-Defined Networking (SDN)*. in *International Conference on e-Infrastructure and e-Services for Developing Countries*. 2020. Springer.
134. Rahman, A., et al., *Distb-sdoindustry: Enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture.* arXiv preprint arXiv:2012.10011, 2020.
135. Sarkunavathi, A. and V. Srinivasan. *A Scrutinized study on DoS attacks in Wireless Sensor Networks and need of SDN in Mitigating DoS attacks*. in *2021 International Conference on Computer Communication and Informatics (ICCCI)*. 2021. IEEE.
136. Bak, D., et al. *Logical Network Separation and Update Inducing Techniques of Non-updated Vaccine Host by Creating Flow Rule in SDN*. in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. 2020. Springer.
137. Al Hayajneh, A., M.Z.A. Bhuiyan, and I. McAndrew, *Improving Internet of Things (IoT) security with software-defined networking (SDN).* Computers, 2020. **9**(1): p. 8.
138. Iqbal, W., et al., *PCSS: Privacy Preserving Communication Scheme for SDN Enabled Smart Homes.* IEEE Sensors Journal, 2021.
139. Wang, H. *Authentic and confidential policy distribution in software defined wireless network*. in *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*. 2014. IEEE.
140. Chica, J.C.C., J.C. Imbachi, and J.F.B. Vega, *Security in SDN: A comprehensive survey.* Journal of Network and Computer Applications, 2020. **159**: p. 102595.
141. Neto, E.P., et al., *Seamless MANO of multi-vendor SDN controllers across federated multi-domains.* Computer Networks, 2021. **186**: p. 107752.
142. Gonzaga, R. and P.N.M. Sampaio. *Mitigating Man In The Middle attacks within Context-based SDNs*. in *8th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2020)*. 2020.
143. Pradhan, A. and R. Mathew, *Solutions to vulnerabilities and threats in software defined networking (SDN).* Procedia Computer Science, 2020. **171**: p. 2581-2589.
144. Abdali, T.-A.N., et al., *Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues.* IEEE Access, 2021. **9**: p. 75961-75980.
145. Duy, P.T., et al. *Sdnlog-foren: Ensuring the integrity and tamper resistance of log files for sdn forensics using blockchain*. in *2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*. 2019. IEEE.
146. Karimi, M. and P. Krishnamurthy. *Software defined ambit of data integrity for the internet of things*. in *2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*. 2021. IEEE.
147. Madhawa, S., P. Balakrishnan, and U. Arumugam, *Roll forward validation based decision tree classification for detecting data integrity attacks in industrial internet of things.* Journal of Intelligent & Fuzzy Systems, 2019. **36**(3): p. 2355-2366.
148. Dave, D. and A. Nagaraju. *A pragmatic analysis of security and integrity in software defined networks*. in *Proceedings of International Conference on Communication and Networks*. 2017. Springer.
149. Iqbal, W., et al., *ALAM: Anonymous Lightweight Authentication Mechanism for SDN-Enabled Smart Homes.* IEEE Internet of Things Journal, 2020. **8**(12): p. 9622-9633.
150. Cao, J., et al., *CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets.* IEEE transactions on dependable and secure computing, 2019.

151. Aydeger, A., et al. *Assessing the overhead of authentication during SDN-enabled restoration of smart grid inter-substation communications*. in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. 2018. IEEE.
152. Nife, F. and Z. Kotulski. *New SDN-Oriented Authentication and Access Control Mechanism*. in *International Conference on Computer Networks*. 2018. Springer.
153. Liang, X. and H. Chen. *A SDN-Based Hierarchical Authentication Mechanism for IPv6 Address*. in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*. 2019. IEEE.
154. Mahboob, T., et al. *Authentication Mechanism to Secure Communication between Wireless SDN Planes*. in *2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*. 2019. IEEE.
155. Fang, L., et al., *THP: A novel authentication scheme to prevent multiple attacks in SDN-based IoT network*. IEEE Internet of Things Journal, 2019. **7**(7): p. 5745-5759.
156. Narwal, B. and A.K. Mohapatra, *A survey on security and authentication in wireless body area networks.* Journal of Systems Architecture, 2021. **113**: p. 101883.
157. Singh, J. and S. Behal, *Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions.* Computer Science Review, 2020. **37**: p. 100279.
158. Benzaïd, C., M. Boukhalfa, and T. Taleb. *Robust self-protection against application-layer (D) DoS attacks in SDN environment*. in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*. 2020. IEEE.
159. Wang, B., Y. Sun, and X. Xu, *A Scalable and Energy-efficient Anomaly Detection Scheme in Wireless SDN-based mMTC Networks for IoT.* IEEE Internet of Things Journal, 2020. **8**(3): p. 1388-1405.
160. Sahoo, K.S., et al., *An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks.* IEEE Access, 2020. **8**: p. 132502-132513.
161. Tang, T.A., et al., *DeepIDS: Deep Learning Approach for Intrusion Detection in Software Defined Networking.* Electronics, 2020. **9**(9): p. 1533.
162. Dey, S.K. and M.M. Rahman, *Effects of Machine Learning Approach in Flow-Based Anomaly Detection on Software-Defined Networking.* Symmetry, 2019. **12**(1): p. 7.
163. Shakil, M., et al., *A novel dynamic framework to detect DDoS in SDN using metaheuristic clustering.* Transactions on Emerging Telecommunications Technologies, 2019: p. e3622.
164. Virupakshar, K.B., et al., *Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud.* Procedia Computer Science, 2020. **167**: p. 2297-2307.
165. Bhushan, K. and B.B. Gupta, *Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment.* Journal of Ambient Intelligence and Humanized Computing, 2018. **10**(5): p. 1985-1997.
166. Iqbal, M., et al., *Security Issues in Software Defined Networking (SDN): Risks, Challenges and Potential Solutions.* International Journal of Advanced Computer Science and Applications, 2019. **10**(10).
167. Abdulkarem, H.S. and A. Dawod, *DDoS Attack Detection and Mitigation at SDN Data Plane Layer*, in *2020 2nd Global Power, Energy and Communication Conference (GPECOM)*. 2020, IEEE.
168. Bhayo, J., S. Hameed, and S.A. Shah, *An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)*. IEEE Access, 2020. **8**: p. 221612-221631.
169. Latah, M. and L. Toker, *Minimizing false positive rate for DoS attack detection: A hybrid SDN-based approach.* ICT Express, 2020. **6**(2): p. 125-127.
170. Al-Shaboti, M., et al. *Towards secure smart home IoT: Manufacturer and user network access control framework*. in *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*. 2018. IEEE.
171. Li, H., F. Wei, and H. Hu. *Enabling dynamic network access control with anomaly-based IDS and SDN*. in *Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*. 2019.
172. Weng, J.-S., et al., *BENBI: Scalable and dynamic access control on the northbound interface of SDN-based VANET.* IEEE Transactions on Vehicular Technology, 2018. **68**(1): p. 822-831.
173. Paladi, N. and C. Gehrmann, *Sdn access control for the masses.* Computers & Security, 2019. **80**: p. 155-172.
174. Abdulqadder, I.H., et al. *An Effective Lightweight Intrusion Detection System with Blockchain to Mitigate Attacks in SDN/NFV Enabled Cloud*. in *2021 6th International Conference for Convergence in Technology (I2CT)*. 2021. IEEE.
175. Wazirali, R., R. Ahmad, and A.A.-K. Abu-Ein, *Sustaining Accurate Detection of phishing URLs Using SDN and Feature Selection Approaches.* Computer Networks, 2021: p. 108591.
176. Chang, D., et al. *An E-ABAC-based SDN access control method*. in *2019 6th International Conference on Information Science and Control Engineering (ICISCE)*. 2019. IEEE.

177. Ramprasath, J. and V. Seethalakshmi, *Secure access of resources in software-defined networks using dynamic access control list.* International Journal of Communication Systems, 2021. **34**(1): p. e4607.
178. Liu, Z. and Z. Zou, *Analysis of network topology and deployment mode of 5G wireless access network.* Computer Communications, 2020. **160**: p. 34-42.
179. Sapavath, N.N. and D.B. Rawat, *Wireless virtualization architecture: Wireless networking for Internet of Things.* IEEE Internet of Things Journal, 2019. **7**(7): p. 5946-5953.
180. Wang, X., et al., *DRL-Based Energy-Efficient Resource Allocation Frameworks for Uplink NOMA Systems.* IEEE Internet of Things Journal, 2020. **7**(8): p. p. 7279-7294.
181. Zhang, H., et al., *Incomplete CSI Based Resource Optimization in SWIPT Enabled Heterogeneous Networks: A Non-Cooperative Game Theoretic Approach.* IEEE Transactions on Wireless Communications, 2018. **17**(3): p. 1882-1892.
182. Li, Y., et al., *NDN Producer Mobility Management Based on Echo State Network: A Lightweight Machine Learning Approach*, in *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*. 2018, IEEE.
183. Zhang, X., et al., *Hybrid Communication Path Orchestration for 5G Heterogeneous Ultra-Dense Networks.* IEEE Network, 2019. **33**(4): p. 112-118.
184. Devyatkin, E.E., et al., *Российское оборудование для сетей 5G/IMT-2020.* Электросвязь, 2019(12).
185. Osseiran, A., et al., *Relaying for IMT-Advanced*, in *Mobile and Wireless Communications for IMT-Advanced and Beyond*. 2011, John Wiley & Sons, Ltd. p. 157-179.
186. Campos, L.M., et al., *Reference Scenarios and Key Performance Indicators for 5G Ultra-dense Networks*, in *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*. 2020, IEEE.
187. *4G Radio Network Planning and Optimisation*, in *Fundamentals of Network Planning and Optimisation 2G/3G/4G*. 2018, John Wiley & Sons, Ltd. p. 235-265.
188. Yosuf, B.A., et al., *Energy Efficient Distributed Processing for IoT.* IEEE Access, 2020. **8**: p. 161080-161108.
189. Benalia, E., S. Bitam, and A. Mellouk, *Data dissemination for Internet of vehicle based on 5G communications: A survey.* Transactions on Emerging Telecommunications Technologies, 2020. **31**(5).
190. Paolucci, F., et al., *Enhancing 5G SDN/NFV Edge with P4 Data Plane Programmability.* IEEE Network, 2021. **35**(3): p. 154-160.
191. Selvi, K.T. and R. Thamilselvan, *Dynamic Resource Allocation for SDN and Edge Computing based 5G Network*, in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. 2021, IEEE.
192. Kim, Y.h., J.M. Gil, and D. Kim, *A location-aware network virtualization and reconfiguration for 5G core network based on SDN and NFV.* International Journal of Communication Systems, 2020. **34**(2).
193. Cicioğlu, M., *Multi-criteria handover management using entropy-based SAW method for SDN-based 5G small cells.* Wireless Networks, 2021. **27**(4): p. 2947-2959.
194. Sharma, S., et al., *Light-Trail Design for 5G Backhaul: Architecture, SDN Impact and Coordinated Multipoint.* Journal of Lightwave Technology, 2021. **39**(17): p. 5383-5396.
195. Luong, D.K., et al., *Metaheuristic Approaches to the Joint Controller and Gateway Placement in 5G-Satellite SDN Networks*, in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. 2020, IEEE.
196. Shu, Z. and T. Taleb, *A Novel QoS Framework for Network Slicing in 5G and Beyond Networks Based on SDN and NFV.* IEEE Network, 2020. **34**(3): p. 256-263.
197. Braeken, A., et al., *Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks.* IEEE Access, 2019. **7**: p. 64040-64052.
198. Z. Ibrahim, A.A. and F. Hashim, *An architecture of 5G based on SDN NV wireless network.* Indonesian Journal of Electrical Engineering and Computer Science, 2019. **14**(2): p. 725.
199. Subedi, P., et al., *Network slicing: a next generation 5G perspective.* EURASIP Journal on Wireless Communications and Networking, 2021. **2021**(1).
200. Haji, S.H., et al., *Comparison of Software Defined Networking with Traditional Networking.* Asian Journal of Research in Computer Science, 2021: p. 1-18.
201. Lin, G., et al., *Security Function Virtualization Based Moving Target Defense of SDN-Enabled Smart Grid*, in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. 2019, IEEE.
202. Rathore, S., J.H. Park, and H. Chang, *Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT.* IEEE Access, 2021. **9**: p. 90075-90083.

203. Abdulqadder, I.H., et al., *Deployment of Robust Security Scheme in SDN Based 5G Network over NFV Enabled Cloud Environment.* IEEE Transactions on Emerging Topics in Computing, 2021. **9**(2): p. 866-877.
204. Abdulqadder, I.H., et al., *Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms.* Computer Networks, 2020. **179**: p. 107364.
205. Kato, N., et al., *Ten Challenges in Advancing Machine Learning Technologies toward 6G.* IEEE Wireless Communications, 2020. **27**(3): p. 96-103.
206. Kaur, K., V. Mangat, and K. Kumar, *A comprehensive survey of service function chain provisioning approaches in SDN and NFV architecture.* Computer Science Review, 2020. **38**: p. 100298.
207. Fiore, U., et al., *Traffic matrix estimation with software-defined NFV: Challenges and opportunities.* Journal of computational science, 2017. **22**: p. 162-170.
208. Lata, M. and V. Kumar, *Standards and Regulatory Compliances for IoT Security.* International Journal of Service Science, Management, Engineering, and Technology, 2021. **12**(5): p. 133-147.
209. Ponmagal, R.S., et al., *Optimized virtual network function provisioning technique for mobile edge cloud computing.* Journal of Ambient Intelligence and Humanized Computing, 2020. **12**(6): p. 5807-5815.
210. Van Dinh, D., et al., *ICT Enabling Technologies for Smart Cities*, in *2020 22nd International Conference on Advanced Communication Technology (ICACT)*. 2020, IEEE.
211. Van Rossem, S., et al., *Introducing Development Features for Virtualized Network Services.* IEEE Communications Magazine, 2018. **56**(8): p. 184-192.
212. Bouras, C., A. Kollia, and A. Papazois, *SDN & NFV in 5G: Advancements and challenges*, in *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*. 2017, IEEE.
213. Moustafa, N., *A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets.* Sustainable Cities and Society, 2021. **72**: p. 102994.
214. Islam, M.S., et al., *Secure IoT Data Analytics in Cloud via Intel SGX*, in *2020 IEEE 13th International Conference on Cloud Computing (CLOUD)*. 2020, IEEE.
215. Masiuk, A., et al., *Resource management method in LTE heterogeneous networks*, in *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*. 2018, IEEE.
216. Song, H., et al., *Design of a Security Service Orchestration Framework for NFV*, in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. 2020, Springer International Publishing. p. 37-52.
217. Islam, M.J., et al., *SDoT-NFV: A Distributed SDN Based Security System with IoT for Smart City Environments.* GUB Journal of Science and Engineering, 2021: p. 27-35.
218. Youssef, Q., M. Yassine, and A. Haqiq, *Secure Software Defined Networks Controller Storage using Intel Software Guard Extensions.*
219. Yao, M., et al., *Artificial Intelligence Defined 5G Radio Access Networks.* IEEE Communications Magazine, 2019. **57**(3): p. 14-20.
220. Islam, A., et al., *A survey on task offloading in multi-access edge computing.* Journal of Systems Architecture, 2021. **118**: p. 102225.
221. Kiran, N., et al., *Joint resource allocation and computation offloading in mobile edge computing for SDN based wireless networks.* Journal of Communications and Networks, 2019. **22**(1): p. 1-11.
222. Xie, R., X. Jia, and K. Wu, *Adaptive online decision method for initial congestion window in 5G mobile edge computing using deep reinforcement learning.* IEEE Journal on Selected Areas in Communications, 2019. **38**(2): p. 389-403.
223. Ahmed, E., et al., *Bringing Computation Closer toward the User Network: Is Edge Computing the Solution?* IEEE Communications Magazine, 2017. **55**(11): p. 138-144.
224. Ali, Z., et al., *Chaos-based robust method of zero-watermarking for medical signals.* Future Generation Computer Systems, 2018. **88**: p. 400-412.
225. Aydin, I. and N.A. Othman, *A new IoT combined face detection of people by using computer vision for security application*, in *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*. 2017, IEEE.
226. Garg, S., et al., *Edge Computing-Based Security Framework for Big Data Analytics in VANETs.* IEEE Network, 2019. **33**(2): p. 72-81.
227. Huang, X., et al., *Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks.* IEEE Access, 2017. **5**: p. 25408-25420.
228. Sonmez, C., A. Ozgovde, and C. Ersoy, *Fuzzy Workload Orchestration for Edge Computing.* IEEE Transactions on Network and Service Management, 2019. **16**(2): p. 769-782.
229. Garg, S., et al., *Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities.* IEEE Network, 2021. **35**(5): p. 298-305.

230. Trakadas, P., et al., *Hybrid Clouds for Data-Intensive, 5G-Enabled IoT Applications: An Overview, Key Issues and Relevant Architecture.* Sensors (Basel, Switzerland), 2019. **19**(16): p. 3591.
231. Jamal, F., et al., *Reliable Access Control for Mobile Cloud Computing (MCC) With Cache-Aware Scheduling.* IEEE Access, 2019. **7**: p. 165155-165165.
232. Qiu, T., et al., *SIGMM: A Novel Machine Learning Algorithm for Spammer Identification in Industrial Mobile Cloud Computing.* IEEE Transactions on Industrial Informatics, 2019. **15**(4): p. 2349-2359.
233. Olufemi Olakanmi, O. and S.O. Oke, *MASHED: Security and privacy-aware mutual authentication scheme for heterogeneous and distributed mobile cloud computing services.* Information Security Journal: A Global Perspective, 2018. **27**(5-6): p. 276-291.
234. Liu, H. and B. Wang, *Mitigating File-Injection Attacks with Natural Language Processing*, in *Proceedings of the Sixth International Workshop on Security and Privacy Analytics*. 2020, ACM.
235. Gao, J., et al., *Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption.* IEEE Systems Journal, 2021: p. 1-12.
236. Sun, P., *Security and privacy protection in cloud computing: Discussions and challenges.* Journal of Network and Computer Applications, 2020. **160**: p. 102642.
237. Stasiak, A. and Z. Zieliński, *Multi-level Security System Verification Based on the Model*, in *Advances in Intelligent Systems and Computing*. 2018, Springer International Publishing. p. 69-85.
238. Le, T.T.N. and T.V.X. Phuong, *Privacy Preserving Jaccard Similarity by Cloud-Assisted for Classification.* Wireless Personal Communications, 2020. **112**(3): p. 1875-1892.
239. Bentajer, A., et al., *An IBE-based design for assured deletion in cloud storage.* Cryptologia, 2019. **43**(3): p. 254-265.
240. Ahmed, T., et al. *On-demand network slicing using SDN/NFV-enabled satellite ground segment systems*. in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. 2018. ieee.
241. Taleb, T., et al., *On multi-domain network slicing orchestration architecture and federated resource control.* IEEE Network, 2019. **33**(5): p. 242-252.
242. Le, L.-V., et al., *SDN/NFV, Machine Learning, and Big Data Driven Network Slicing for 5G*, in *2018 IEEE 5G World Forum (5GWF)*. 2018, IEEE.
243. Kuklinski, S. and L. Tomaszewski, *Key Performance Indicators for 5G network slicing*, in *2019 IEEE Conference on Network Softwarization (NetSoft)*. 2019, IEEE.
244. Addad, R.A., et al., *Network Slice Mobility in Next Generation Mobile Systems: Challenges and Potential Solutions.* IEEE Network, 2020. **34**(1): p. 84-93.
245. Ko, H., et al., *Hierarchical Identifier (HID)-based 5G Architecture with Backup Slice*, in *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*. 2020, IEEE.
246. Fang, D., Y. Qian, and R.Q. Hu, *Security for 5G Mobile Wireless Networks.* IEEE Access, 2018. **6**: p. 4850-4874.
247. Ziani, A. and A. Medouri, *A Survey of Security and Privacy for 5G Networks*, in *Emerging Trends in ICT for Sustainable Development*. 2021, Springer International Publishing. p. 201-208.
248. Park, S., et al., *5G Security Threat Assessment in Real Networks.* Sensors (Basel, Switzerland), 2021. **21**(16): p. 5524.
249. Ksentini, A. and P.A. Frangoudis, *Toward Slicing-Enabled Multi-Access Edge Computing in 5G.* IEEE Network, 2020. **34**(2): p. 99-105.
250. Barmpounakis, S., et al., *Network slicing-enabled RAN management for 5G: Cross layer control based on SDN and SDR.* Computer Networks, 2020. **166**: p. 106987.
251. Mu, H. and Y. Li, *An assured deletion scheme for encrypted data in Internet of Things.* Advances in Mechanical Engineering, 2019. **11**(2): p. 168781401982714.
252. Boulogeorgos, A.-A.A., et al., *Terahertz Technologies to Deliver Optical Network Quality of Experience in Wireless Systems Beyond 5G.* IEEE Communications Magazine, 2018. **56**(6): p. 144-151.
253. Costa-Requena, J., et al. *SDN-Enabled THz Wireless X-Haul for B5G*. in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. 2021. IEEE.
254. Muñoz, R., et al. *Sdn/nfv control and orchestration of dynamic optical beamforming services for beyond 5G fronthaul networks*. in *2020 European Conference on Optical Communications (ECOC)*. 2020. IEEE.
255. Rahimi, P., et al., *Joint Radio Resource Allocation and Beamforming Optimization for Industrial Internet of Things in Software-Defined Networking-Based Virtual Fog-Radio Access Network 5G-and-Beyond Wireless Environments.* IEEE Transactions on Industrial Informatics, 2022. **18**(6): p. 4198-4209.
256. Fourati, H., R. Maaloul, and L. Chaari, *A survey of 5G network systems: challenges and machine learning approaches.* International Journal of Machine Learning and Cybernetics, 2020. **12**(2): p. 385-431.

257. Jijo, B.T., et al., *A Comprehensive Survey of 5G mm-Wave Technology Design Challenges.* Asian Journal of Research in Computer Science, 2021: p. 1-20.
258. Datsika, E., et al., *SDN-enabled resource management for converged Fi-Wi 5G Fronthaul.* IEEE Journal on Selected Areas in Communications, 2021.
259. Lee, J. and Y. Yoo. *Handover cell selection using user mobility information in a 5G SDN-based network.* in *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*. 2017. IEEE.
260. Shah, S.D.A., et al., *SDN-based Service Mobility Management in MEC-enabled 5G and Beyond Vehicular Networks.* IEEE Internet of Things Journal, 2022.
261. Reinhardt, A., et al., *Remote Measurement of Particle Streams with a Multistatic Dual Frequency Millimeter Wave Radar Sensor*, in *2018 IEEE/MTT-S International Microwave Symposium - IMS*. 2018, IEEE.
262. Chekired, D.A., et al., *5G-Slicing-Enabled Scalable SDN Core Network: Toward an Ultra-Low Latency of Autonomous Driving Service.* IEEE Journal on Selected Areas in Communications, 2019. **37**(8): p. 1769-1782.
263. Duan, X., Y. Liu, and X. Wang, *SDN Enabled 5G-VANET: Adaptive Vehicle Clustering and Beamformed Transmission for Aggregated Traffic.* IEEE Communications Magazine, 2017. **55**(7): p. 120-127.
264. Mathew, A., M. Srinivasan, and C.S.R. Murthy. *Packet generation schemes and network latency implications in SDN-enabled 5G C-RANs: Queuing model based analysis*. in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. 2019. IEEE.
265. Nasrallah, A., et al., *Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research.* IEEE Communications Surveys & Tutorials, 2019. **21**(1): p. 88-145.
266. Ahmed, A.H., et al., *Energy Efficiency in 5G Massive MIMO for Mobile Wireless Network*, in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. 2020, IEEE.
267. Oliveira, T.F., S. Xavier-de-Souza, and L.F. Silveira, *Improving Energy Efficiency on SDN Control-Plane Using Multi-Core Controllers.* Energies, 2021. **14**(11): p. 3161.
268. Cao, B., et al., *Resource Allocation in 5G IoV Architecture Based on SDN and Fog-Cloud Computing*. IEEE Transactions on Intelligent Transportation Systems, 2021. **22**(6): p. 3832-3840.
269. Tipantuna, C. and X. Hesselbach, *NFV/SDN Enabled Architecture for Efficient Adaptive Management of Renewable and Non-Renewable Energy.* IEEE Open Journal of the Communications Society, 2020. **1**: p. 357-380.
270. Moosavi, R., et al., *Energy efficiency through joint routing and function placement in different modes of SDN/NFV networks.* Computer Networks, 2021. **200**: p. 108492.
271. Aujla, G.S., et al., *Data Offloading in 5G-Enabled Software-Defined Vehicular Networks: A Stackelberg-Game-Based Approach.* IEEE Communications Magazine, 2017. **55**(8): p. 100-108.
272. Barakabitze, A.A., et al., *A Novel QoE-Centric SDN-Based Multipath Routing Approach for Multimedia Services over 5G Networks*, in *2018 IEEE International Conference on Communications (ICC)*. 2018, IEEE.
273. Escolar, A.M., J.M.A. Calero, and Q. Wang, *Scalable Software Switch Based Service Function Chaining for 5G Network Slicing*, in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*. 2020, IEEE.
274. Behravesh, R., et al., *Time-Sensitive Mobile User Association and SFC Placement in MEC-Enabled 5G Networks.* IEEE Transactions on Network and Service Management, 2021. **18**(3): p. 3006-3020.
275. Salva-Garcia, P., et al., *Scalable Virtual Network Video-Optimizer for Adaptive Real-Time Video Transmission in 5G Networks.* IEEE Transactions on Network and Service Management, 2020. **17**(2): p. 1068-1081.
276. Preciado Rojas, D.F. and A. Mitschele-Thiel, *A scalable SON coordination framework for 5G*, in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*. 2020, IEEE.
277. Zafeiropoulos, A., et al., *Benchmarking and Profiling 5G Verticals' Applications: An Industrial IoT Use Case*, in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*. 2020, IEEE.
278. Chekired, D.A., M.A. Togou, and L. Khoukhi, *HybCon: A Scalable SDN-Based Distributed Cloud Architecture for 5G Networks.* IEEE Transactions on Cloud Computing, 2021.
279. Botez, R., et al., *SDN-Based Network Slicing Mechanism for a Scalable 4G/5G Core Network: A Kubernetes Approach.* Sensors, 2021. **21**(11): p. 3773.
280. Akkari, N. and N. Dimitriou, *Mobility management solutions for 5G networks: Architecture and services.* Computer Networks, 2020. **169**: p. 107082.
281. Alghamdi, K. and R. Braun, *Software defined network (SDN) and OpenFlow protocol in 5G network.* Communications and Network, 2020.

282. Alidadi, A., S. Arab, and T. Askari, *A novel optimized routing algorithm for QoS traffic engineering in SDN-based mobile networks.* ICT Express, 2022. **8**(1): p. 130-134.
283. Sodhro, A.H., et al., *Towards 5G-Enabled Self Adaptive Green and Reliable Communication in Intelligent Transportation System.* IEEE Transactions on Intelligent Transportation Systems, 2021. **22**(8): p. 5223-5231.
284. Prasad, J.R., S.P. Bendale, and R.S. Prasad, *Semantic Internet of Things (IoT) Interoperability Using Software Defined Network (SDN) and Network Function Virtualization (NFV).* Semantic IoT: Theory and Applications. Studies in Computational Intelligence, 2021. **941**.
285. Dubey, D., T.P. Singh, and A. Bhattacharjee. *Design of ATM Network Architecture that interoperate with Higher Level Protocols in 5G environment.* in *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*. 2021. IEEE.
286. Leinonen, M.E., et al., *Radio Interoperability in 5G and 6G Multiradio Base Station*, in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*. 2020, IEEE.
287. Dubey, D., T.P. Singh, and A. Bhattacharjee, *Design of ATM Network Architecture that interoperate with Higher Level Protocols in 5G environment*, in *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*. 2021, IEEE.
288. Apostolakis, K.C., et al., *Cloud-Native 5G Infrastructure and Network Applications (NetApps) for Public Protection and Disaster Relief: The 5G-EPICENTRE Project*, in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. 2021, IEEE.
289. Ahmad, I., et al., *Overview of 5G security challenges and solutions.* IEEE Communications Standards Magazine, 2018. **2**(1): p. 36-43.
290. Magsi, H., et al., *Evolution of 5G in Internet of medical things*, in *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. 2018, IEEE.
291. Gaba, G.S., et al., *Secure Device-to-Device communications for 5G enabled Internet of Things applications.* Computer Communications, 2021. **169**: p. 114-128.
292. Hasan, M.K., et al., *A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things.* IET Communications, 2021.
293. Iavich, M., et al., *The Novel System of Attacks Detection in 5G*, in *Advanced Information Networking and Applications*. 2021, Springer International Publishing. p. 580-591.

## Figures


**Figure 1**

Joint 5G and SDN security paradigm

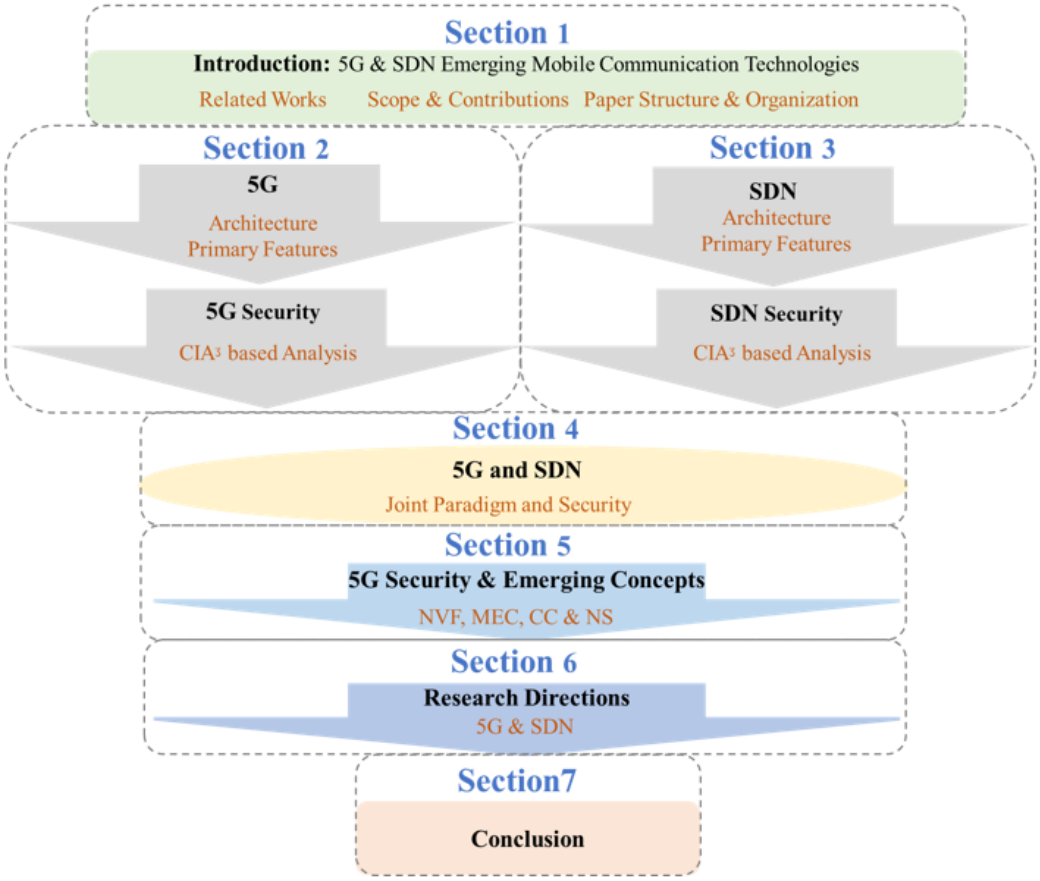


**Figure 2**

Structure and Organization of this paper

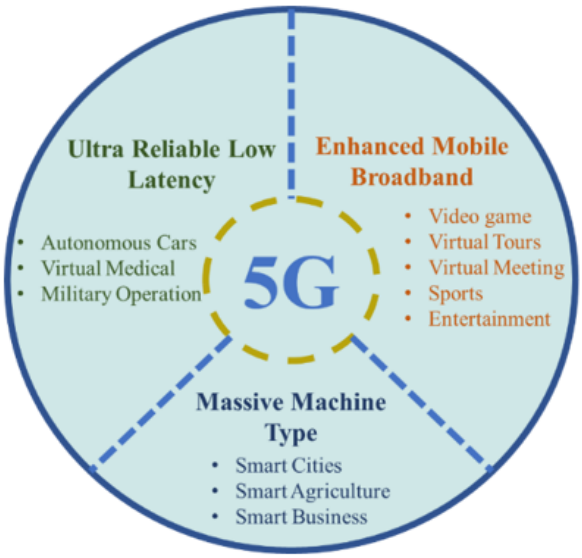


**Figure 3**

5G scenarios

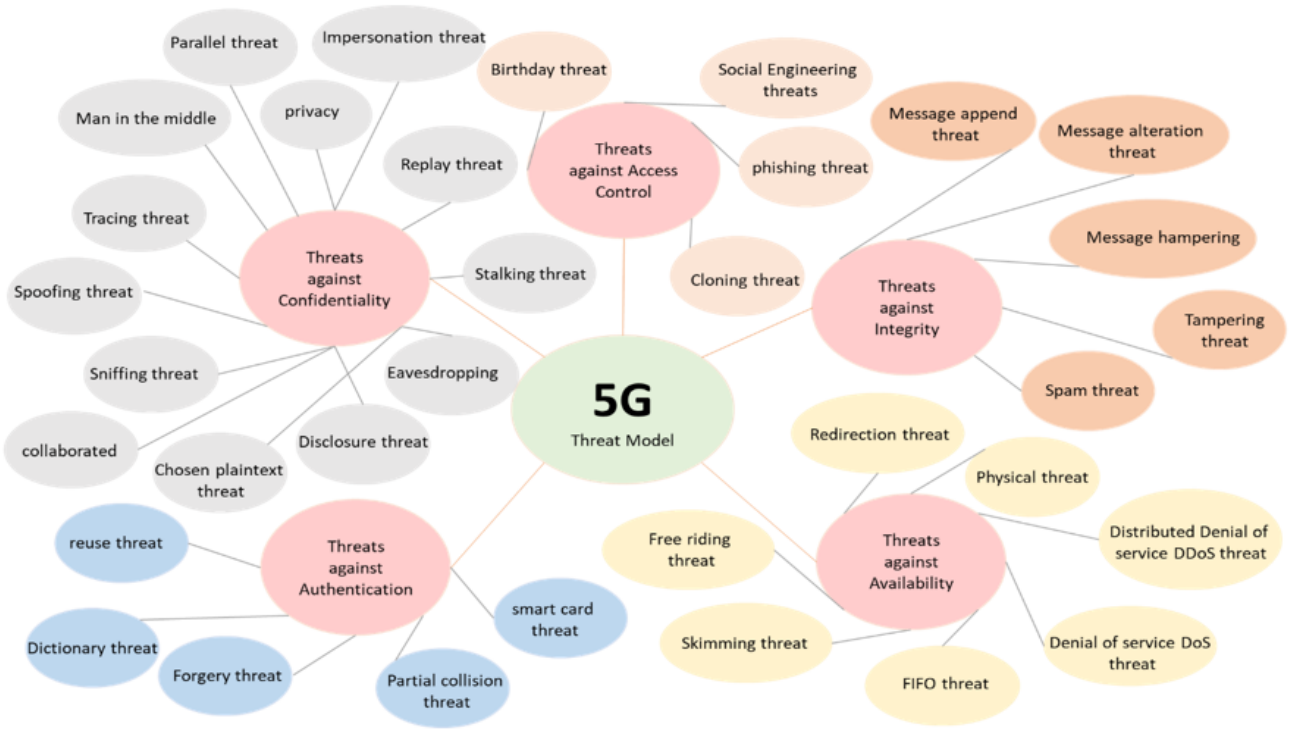


**Figure 4**

CIA[3] based Threat landscape of 5G communication

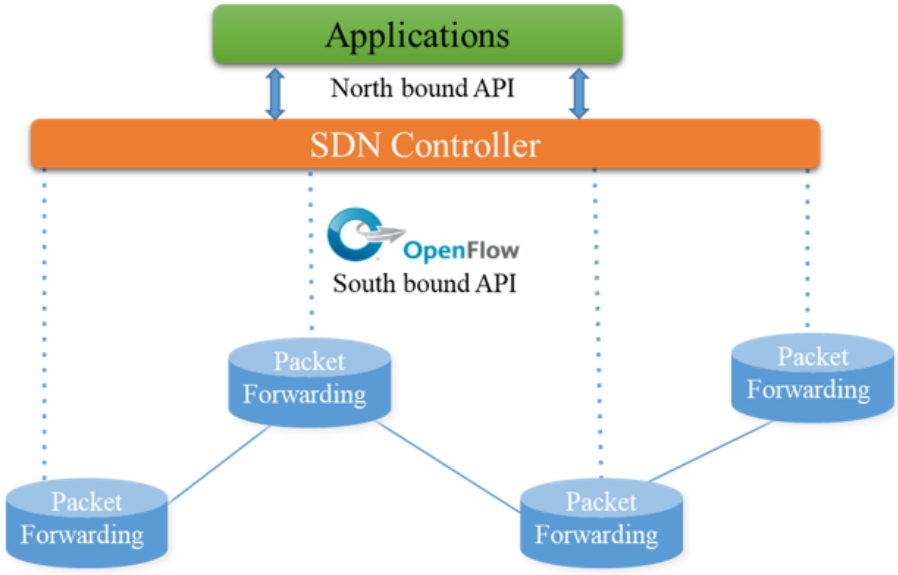


**Figure 5**

SDN Controller and OpenFlow

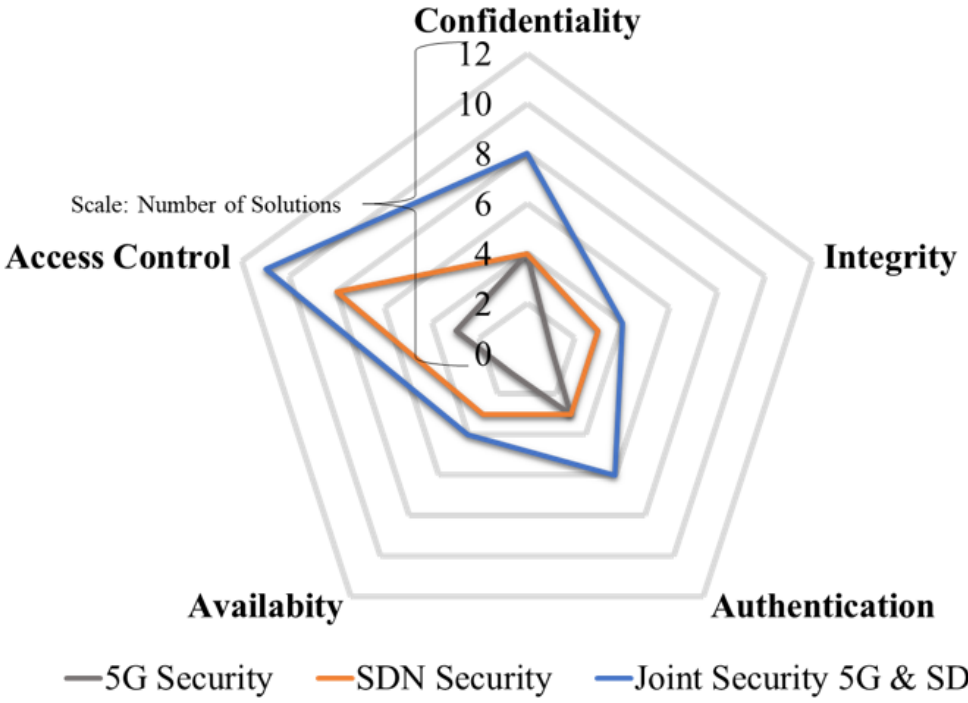


**Figure 6**

Security solutions in Joint CIA$^3$ of 5G and SDN

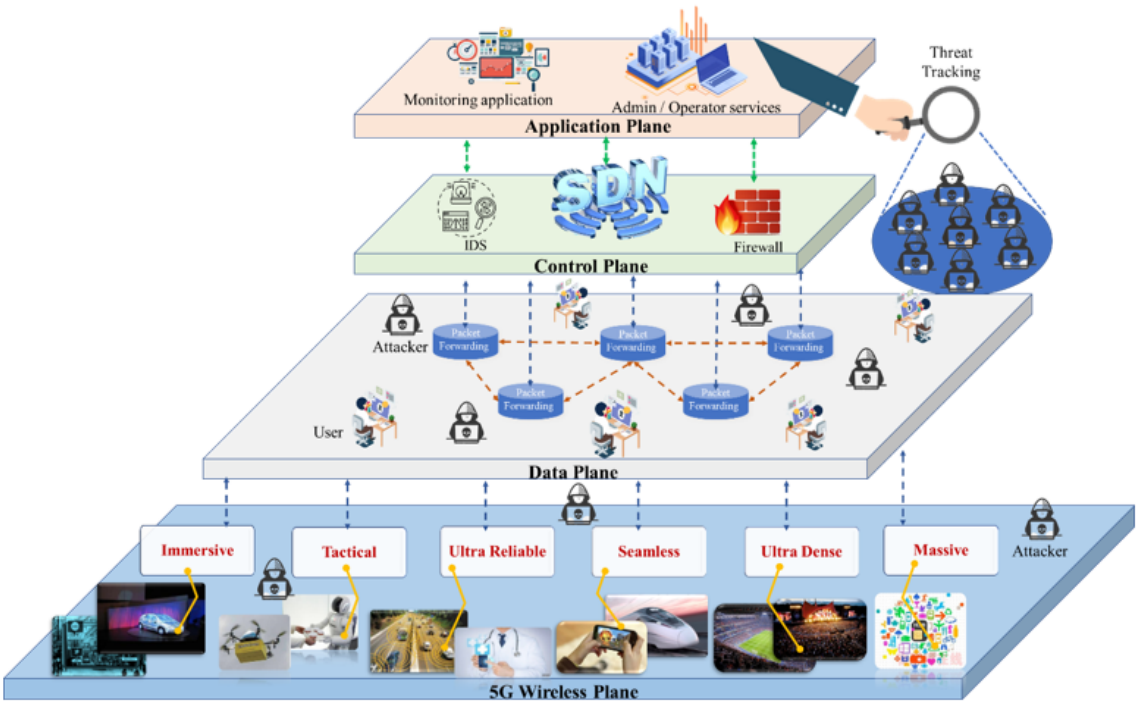


**Figure 7**

Joint security paradigm of SDN & 5G