Received: 14 February 2022 | Revised: 29 November 2022 | Accepted: 21 March 2024

DOI: 10.1002/ett.4965

RESEARCH ARTICLE

BlockSD-5GNet: Enhancing Security of 5G Network through Blockchain-SDN with ML-based Bandwidth Prediction

Anichur Rahman[1] | Md. Saikat Islam Khan[2] | Antonio Montieri[3] | Md. Jahidul Islam[4] | Md. Razaul Karim[2] | Mahedi Hasan[5] | Dipanjali Kundu[1] | Mostofa Kamal Nasir[2] | Antonio Pescapè[3]

[1]Department of Computer Science and Engineering, National Institute of Textile Engineering and Research (NITER), Constituent Institute of Dhaka University, Dhaka, Bangladesh

[2]Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Dhaka, Bangladesh

[3]Department of Electrical Engineering and Information Technologies, University of Napoli "Federico II", Napoli, Italy

[4]Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka, Bangladesh

[5]Department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore, Bangladesh

Correspondence
Antonio Montieri, Department of Electrical Engineering and Information Technologies, University of Napoli "Federico II", Via Claudio 21, Napoli, 80125, Italy.
Email: antonio.montieri@unina.it

Summary

The Fifth Generation (5G) of mobile communications is the most exciting emerging technology for researchers and scientists to get the full benefit of a network system. However, 5G networks confront massive threats and vulnerabilities including protection, privacy, and secrecy. To face these challenges in the increasingly interconnected Internet of Things (IoT) scenario, we aim to leverage state-of-the-art technologies as Software Defined Networking (SDN) in conjunction with Network Function Virtualization (NFV), Blockchain, and Machine Learning (ML). Indeed, these technologies convey a robust and secure setting in the networking platform enabling to manage several criticalities related to security, privacy, flexibility, and performance. In light of these considerations, in this paper, we propose the "BlockSD-5GNet" architecture to efficiently improve the security of a 5G network and to exploit the combined advantages of Blockchain, SDN, NFV, and ML. In the proposed architecture, the SDN helps to manage the network by dividing it into data plane and control plane, while the Blockchain guarantees improved security and confidentiality. Therefore, the "BlockSD-5GNet" architecture can both secure sensitive data and attain reliable data transfer within and between the 5G network-infrastructure planes. Additionally, an ML module is integrated into the SDN controller to estimate network bandwidth and assist the administrator in taking effective decisions and satisfying high-bandwidth demand. We assess the performance of the "BlockSD-5GNet" architecture via an experimental evaluation performed in a simulation environment, and show the effectiveness of the proposed solution in comparison with baseline schemes. Finally, we also demonstrate the capability of different ML models in bandwidth prediction.

KEYWORDS:
IoT, 5G Networks, SDN, NFV, Blockchain, Machine Learning, Security, Privacy, Bandwidth Prediction.

1 | INTRODUCTION

At the end of the 78^{th} Plenary in Lisbon in December 2017[1], the 3GPP approved the fifth generation of mobile communications New Radio (5G NR) in Non Standalone (NSA) operation, as well as the 5G NR in Standalone (SA) operation[2]. In more detail,

the 5G NR in NSA, which has partially benefited from 5G, was only the first implementation phase of 5G NR in SA, which conversely has fully benefited from 5G. 5G NR in SA—also called 5G core—includes:

- eMBB (enhanced Mobile Broadband);
- URLLC (Ultra Reliable Low Latency Communications);
- mMTC (massive Machine Type Communications).

Specifically, in the Internet of Things (IoT) era, the 5G is acknowledged as the enabler having the capability of changing the communication paradigm over the Internet. Moreover, when used in combination with Software Defined Networking (SDN), the 5G technology—even though it does not completely replace wired connections—allows rapid, ubiquitous, and on-demand access to fundamental resources, largely operating in the cloud environment. This provides improved capacity and Internet speed, faster response time, and personalized services[3].

Indeed, in 5G networks, the Network Slicing (NS) technique allows the creation of multiple sub-networks (viz. slices) with different properties, dedicated to specific applications. Specifically, the 5G network infrastructure leverages virtualization and cloud-shared technologies to create multiple slice types without dedicating a whole end-to-end network for each type of slice. Thus, since 5G mainly operates with cloud environments, security concerns such as privacy, safety, confidentiality, and data integrity also arise.

On the other hand, SDN has emerged as an approach to design, build, and manage networks by separating control and data (also referred to as forwarding) planes. Within the 5G infrastructure, SDN can be employed to make the network more stable and address security issues. Further, using the SDN technology, a 30% increase in bandwidth utilization and a 20% reduction in latency are estimated[4], which provide improved data flows and allow the 5G to operate across the control plane. On the other side, Network Function Virtualization (NFV) is used as a key enabler for the 5G infrastructure, helping to virtualize the different network appliances. Since NFV can enable network slicing[5] it can actually build the elements of the virtual network architecture. As anticipated before, such a virtual architecture allows the creation of several flexible and programmable networks, which share a common physical infrastructure.

However, the combined use of SDN and NFV with 5G introduces new security threats, such as vulnerabilities to Distributed Denial of Service (DDoS) attacks[6]. In this context, Blockchain is an emerging technology that can be used to solve these issues. The basic characteristic of Blockchain is that it contains a chain of blocks where data are stored. When a new block is added to the chain, a hash reference is created based on both the details of the record and the reference of the preceding block. These blocks and references are time-stamped and updated in every node of the network once verified. Once data are stored within the Blockchain, this procedure makes the alteration of a block after its creation extremely complicated[7,8]. Therefore, in 5G networks, Blockchain provides distributed trust models that allow 5G to protect itself against security breaches.

To face advanced persistent threats and improve data security, previous studies have already integrated SDN and NFV technologies into the 5G network[9,5]. However, as a consequence of this integration, new challenges arise. In more detail, NFV has to address decentralization and data interoperability issues, while SDN has introduced new security threats like vulnerabilities to DDoS attacks. To deal with these shortcomings, researchers have suggested the integration of Blockchain technology[10,11,12]. Indeed, Blockchain aims to alleviate these issues by providing distributed trust models and enhanced data security. Moreover, it can facilitate the deployment of decentralized 5G applications, services, and ecosystems by means of its core elements and supporting features (e.g., decentralized storage, smart contracts, and trusted oracles)[13]. Additionally, the joint usage of SDN, NFV, and Blockchain represents a solution to improve security, privacy, and confidentiality in an efficient way.

Finally, a clear knowledge of traffic characteristics is peculiar for the proper optimization of network resources (e.g., network planning, bandwidth allocation, and load balancing) especially in extremely dynamic and complex scenarios—as 5G networks—in which operators have recently experienced tremendous growth in mobile traffic. Indeed, 5G ultra-wideband networks can forward significantly more data than today's LTE networks, and such high bandwidth is necessary for tomorrow's most remarkable technologies to take off[14]. In particular, among other alternatives, Machine Learning-based regressors have proven to be reliable solutions for network bandwidth prediction tasks[15,16].

Motivated by these considerations, we propose the "BlockSD-5GNet" architecture which integrates SDN, NFV, and Blockchain technologies, along with network-bandwidth prediction capability via Machine Learning. "BlockSD-5GNet" is designed to specifically address the 5G-network challenges with a particular focus on IoT scenarios. Firstly, in a 5G network, bandwidth prediction is paramount as proper network operation depends on the reliability of data transfer from source to destination. This is particularly true in sensitive scenarios, such as attacks within the network and for applications demanding high and variable

throughput. Therefore bandwidth prediction is an essential component of a model aiming to provide a reliable data transfer medium. In addition, SDN and NFV—aided with the aforementioned prediction mechanism—are leveraged to improve bandwidth utilization and reduce latency in the network. In fact, we exploit SDN to maintain the full communication channel. In more detail, SDN and NFV integration manages the network planes through the distribution of loads within the network. Besides, SDN allows the management of the control plane via multiple controllers—which can significantly reduce packet loss—and identifies the desired path of a packet in advance via the OpenFlow protocol. Overall, among the several benefits of SDN and NFV integration for the network, the most important ones are load balancing, scalability and security of the system, and sustainability of network lifetime. For achieving the integrity of the system model we have considered 200–500 nodes. Finally, the security issues in the 5G network are addressed via the application of Blockchain. Specifically, Blockchain is employed to efficiently solve problems of decentralization, interoperability, data security, and privacy derived from the integration of SDN and NFV into the 5G network. In this way, our proposed "BlockSD-5GNet" architecture is capable of detecting drawbacks that have an impact on the bandwidth of the 5G network in order to secure sensitive data and attain reliable data transfer within and between the 5G network-infrastructure planes.

To summarize, the main contributions of this paper are as follows:

- we propose the "BlockSD-5GNet" architecture that provides strong security and reliable data transfer, resulting in enormous benefits for the 5G network, particularly in IoT scenarios;
- we integrate SDN and NFV into "BlockSD-5GNet", including multiple controllers that manage the network-infrastructure planes to efficiently distribute the load between the IoT devices and reduce (ideally eliminate) the packet loss;
- we employ a distributed Blockchain approach to guarantee decentralization, data security, and confidentiality to the "BlockSD-5GNet" architecture;
- finally, we enrich "BlockSD-5GNet" with a Machine Learning (ML) module integrated into the SDN controller, namely a Random Forest Regressor, for the prediction of network bandwidth.

For the sake of readability, the acronyms used in the present manuscript are listed in Tab. 1.

The rest of the paper is organized as follows. We discuss the literature review in Section 2. Then, Section 3 presents the "BlockSD-5GNet" architecture, describing also its components and functionalities. We report the experimental evaluation and the discussion of related findings in Section 4. Finally, Section 5 discusses the limitations and provides potential future improvements of our proposal, while Section 6 concludes the manuscript by giving the final remarks.

2 | RELATED WORK

Several works have recently investigated cutting-edge subjects related to increasingly emerging technologies considered in the present paper. In this section, we present a thorough literature review considering the joint combination of IoT, SDN, NFV, and Blockchain technologies along with their utilization in 5G networks. It is worth noting that the different subsections are meant to cover the integration in various flavors of considered technologies in interesting scenarios. Nevertheless, some works can overlap regarding the scenarios taken into account (e.g., by considering both IoT and 5G). In these cases, we categorize each work by referring to the most prominent scenario investigated.

2.1 | SDN in IoT Scenarios

Matheu et al. [17] considered the Manufacturer's Use Definition (MUD) model to enforce policies for data privacy, channel protection and authorization in IoT networks. They employed the SDN framework to efficiently access system information and resources, and leveraged the Blockchain to exchange data/information with IoT devices via Hyperledger[1]. Differently, Conti et al. [18] presented CENSOR, a platform providing a cloud-enabled IoT infrastructure via SDN. Specifically, the authors leveraged the SDN paradigm to efficiently manage big IoT-data in multiple stages. The work underlined also the need for facing several challenges such as advanced security threats, suitable routing algorithms, and proper network scalability. Molina et al. [19] presented an

[1] https://www.hyperledger.org/

TABLE 1 List of acronyms used in the manuscript in alphabetical order.

Acronym	Description
5G	Fifth generation of mobile communications
AAA	Authentication, Authorization, Accounting
ABR	Ada-Boost Regressor
AI	Artificial Intelligence
API	Application Programming Interface
(D)DoS	(Distributed) Denial of Service
DSSS	Direct Sequence Spread Spectrum
FHSS	Frequency Hopping Spread Spectrum
FL	Federated Learning
GBR	Gradient Boosting Regressor
HetNet	Heterogeneous Network
IoT	Internet of Things
IMSI	International Mobile Subscriber Identity
LLDP	Link Layer Discovery Protocol
LR	Linear Regressor
MITM	Man-In-The-Middle
ML	Machine Learning
mMTC	massive Machine Type Communication
NFV	Network Function Virtualization
NFVO	Network Function Virtualization Orchestration
PoW	Proof of Work
PPSS	Privacy-Preserving Slice Selection
QoE	Quality of Experience
QoS	Quality of Service
RFR	Random Forest Regressor
SC	Smart Contact
SDN	Software Defined Networking
SINR	Signal to Interference plus Noise Ratio
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
VANET	Vehicular Ad hoc Network
VNF	Virtual Network Function

on-demand modern security framework for the management of virtualized Authentication, Authorization, Accounting (AAA). The authors provided a comprehensive coverage of security aspects in the IoT ecosystem and related orchestration. Besides, they employed virtual AAA for bootstrapping and Datagram Transport Layer Security channel protection. However, they did not explicitly consider different intruders and attackers. Maksymyuk et al.[9] suggested a new approach for comprehensive monitoring of SDN-based 5G-ready mobile networks by using an IoT-based platform for the implementation of a monitoring system for mobile network operators, intending to be simple, data-agnostic, and interoperable. Liu et al.[20] proposed several techniques to handle different network attacks. The authors suggested using SDN for middlebox design and enforcing power constraints for flow tables. Their SDN-based security model for data transfer aimed at reducing network latency and improve the overall security. Reported findings showed that this model can effectively attain security and manage data-flow in an SDN-IoT-based networking system.

2.2 | Blockchain in SDN

To enhance network Quality of Service (QoS), Chaudhary et al.[21] jointly leveraged Blockchain and SDN technologies in the BEST framework, a Blockchain-based secure energy trading scheme for electric vehicles. BEST used Blockchain to distributedly validate vehicle requests avoiding the presence of a single point of failure, while SDN is employed at the network backbone to ensure low latency and real-time operations. Shao et al.[22] presented a novel consensus algorithm named Simplified Practical Byzantine Fault Tolerance (SPBFT) for securely communicating messages between controllers in the SDN network. Also, Blockchain is added to realize a distributed database in each SDN controller which stores updated system activities. The authors compared the SPBFT against the classic PBFT algorithm in terms of efficiency and security, showing superior performance of their proposal. El Houda et al.[23] proposed the Blockchain-based Cochain-SC architecture that offers both intra-domain and inter-domain DDoS mitigation in SDN. Specifically, the combination of intra entropy-based, intra Bayes-based, and intra-domain mitigation schemes is used to classify and mitigate the impact of illegitimate flows. In the inter-domain context, Cochain-SC leveraged smart contracts based on the Ethereum technology to simplify the collaboration among SDN-based Autonomous Systems against DDoS attacks. More recently, Navid et al.[24] developed a simple model for managing IoT issues via SDN, and added a Blockchain to enhance the security of 5G networks by integrating the Elliptic Curve Digital Signature (ECDS) cryptographic algorithm. The implementation of a distributed Blockchain-based SDN-IoT framework for smart cities is presented in[25]. The proposed framework took advantage of multiple controllers and NFV technology to assure accessibility, protection, and privacy, and to improve performance in terms of energy savings and load balancing. Finally, Basnet et al.[26] also investigated Blockchain security over SDN in an emulated network using an OpenDaylight controller integrated with the OpenStack one. They also added a distributed peer-to-peer system into OpenStack to manage information on the cloud repository for file assignment purposes.

2.3 | SDN-IoT with Blockchain

Yazdinejad et al.[27] proposed an IoT architectural model to deal with networking challenges (e.g., security, privacy, and confidentiality) by means of SDN and Blockchain. The focus was primarily on reliable and energy-efficient file transfer mechanisms between IoT devices. Similarly, Faizullah et al.[28] employed SDN to efficiently control the huge volume of data in an IoT network and used Blockchain to protect these data from intruders. However, they did not define the overall controlling process of such massive data and did not consider the attack management process. Muthanna et al.[29] introduced the concept of IoT-based fog network integrating Blockchain and SDN. By using the SDN framework, IoT-based applications can achieve high privacy, availability, and security, while Blockchain assures the distribution and decentralization of resources. The experimental evaluation considered different parameters like latency, network performance, and resource usage, demonstrating the applicability of the proposed architecture. More recently, Rahman et al.[30] proposed "SmartBlock-SDN", an energy-efficient and secure framework encompassing SDN and Blockchain for smart IoT networks. The authors devised a novel cluster head selection method for attaining low-energy utilization and reduced end-to-end delay among IoT sensors. The performance of the proposed architecture was evaluated in a simulation environment proving to outperform state-of-the-art cluster-head selection baselines.

2.4 | Blockchain for NFV

Regarding the integration of Blockchain and NFV, Fu et al.[31] presented a performance optimization procedure based on these leading technologies. The authors proposed a Blockchain-enabled NFV management and orchestration (NFV-MANO) framework that exploits multi-access edge computing instead of centralized cloud computing. The authors assessed the Blockchain throughput, computational delay, and operational costs, revealing the effectiveness of the proposed solution, but highlighting also additional challenges to be faced. Rebello et al.[32] proposed the BSec-NFVO model to provide security for Network Function Virtualization Orchestration (NFVO) by exploiting NFV-based Blockchain transaction model. The authors did not focus on parameter tuning to enhance BSec-NFVO performance but mainly focused on reducing the overhead on the cloud orchestrator. On the same line, the work[33] introduced the use of Blockchain to aid network slicing. The authors used the Hyperledger Fabric platform to define a prototype in which network slice runs on an isolated channel. Unfortunately, the study lacks an actual implementation and demonstrates that consensus and number of transactions required by the slices remain a challenge. Nag et al.[34] also presented a discussion on the relationship between Blockchain and Virtual Network Functions (VNFs), discussing the security issues related to VNF management in the context of 5G optical networks. They presented a high-level view of work-in-progress and proposed to use an over-optical Blockchain network to mitigate these problems. The BRAIN architecture, a Blockchain-based reverse auction, was devised in[35] as an auditable solution for infrastructure providers to host VNFs based on

user demand following an as-a-service paradigm. The authors evaluated the trade-off of using Blockchain via several parameters, namely comparing performance with extra costs and time.

2.5 | SDN-NFV through Blockchain in 5G Networks

To satisfy the demand of high mobility and low latency of 5G services, Yang et al.[36] proposed a combination of Blockchain and distributed multi-domain networks capable of achieving trusted cross-domain collaboration and topology privacy protection in heterogeneous mobile edge computing systems. The utilization of Blockchain made the system more trustworthy but the authors did not fully investigate threats and countermeasures specifically tailored to 5G networks. Barakabitze et al.[37] reviewed 5G network slicing based on SDN and NFV technologies. The authors discussed QoS and business requirements of 5G networks and how these can be attained via SDN, NFV, and mobile-edge/cloud/fog computing. Also, they reviewed various industrial initiatives toward the adoption of SDN and NFV in 5G networks. However, they focused only on the challenges of 5G network softwarization without taking into account the integration of Blockchain for security purposes. Xie et al.[38] presented a distributed Blockchain-based security and privacy model for IoT services in 5G vehicular ad-hoc networks (VANETs) enabled by SDN. The authors set up a model for secure and trustworthy 5G-VANETs with privacy preservation, demonstrating that malicious vehicular nodes can be detected with low overhead also in large-scale scenarios. Although the proposed solution guarantees security and trustworthiness, it has been specifically designed for 5G-VANETs. Gao et al.[39] also proposed the incorporation of SDN for effective network management of VANETs based on 5G and fog computing. Additionally, to ensure trust in such an Internet of Vehicles environment, Blockchain is considered to share management responsibilities with the SDN controllers while attaining efficient network performance. A scheme to ensure security and mobile user privacy in 5G networks was presented in[40]. User authentication and countermeasures against attacks were designed over an NFV-based SDN environment. A classification engine was also exploited to discriminate between malicious and benign traffic with the aim of protecting the network from authentication handover, flow table overloading, and DDoS attacks.

2.6 | Bandwidth Prediction using Machine Learning

Mei et al.[41] applied a Long Short-Term Memory (LSTM) and Bayesian Fusion for predicting the bandwidth of mobile applications such as video calls, games, and video on demand, with the aim of improving the user Quality of Experience (QoE). The results demonstrate that the proposed LSTM outperforms baseline prediction algorithms such as Recursive Least Squares recurrent neural network in terms of (lower) prediction error. Similarly, Labonne et al.[42] employed three ML-based methods, namely LSTM, MultiLayer Perceptron (MLP), and Auto-Regressive Integrated Moving Average (ARIMA), for predicting the bandwidth between different network links. The LSTM shows better performance than the other two approaches by achieving only 3% error rate. Khangura et al.[43] estimated the available bandwidth using a shallow neural network. They used vectors of packet dispersion as input features, which are characteristic of the available bandwidth. The authors train their neural network under challenging conditions as randomly generated network topologies with multiple bottleneck links and heavy cross-traffic burstiness, still achieving improved performance compared to state-of-the-art ML algorithms. Targeted to low-latency human-to-machine communications, Lihua et al.[44] proposed an MLP-based predictive dynamic bandwidth allocation algorithm. Simulation results show that prediction of human-to-machine packet bursts reaches $> 90\%$ accuracy. Yue et al.[45] developed *LinkForecast* a lightweight ML-based framework for predicting cellular link bandwidth in LTE networks. *LinkForecast* trained on both upper-layer (e.g., historical throughput, delay, loss rate, inter-packet arrival times) and lower-layer (e.g., reference signal received power and quality, channel quality indicator, block error rate) features achieves an average error rate ranging from 3.9% to 17.0% for predicting link bandwidth in real-time.

2.7 | Paper Positioning

In summary, the above literature review has shown that the dynamic requirements of 5G networks can be dealt with the capability offered by SDN and NFV technologies that guarantee a safe and manageable network environment. Additionally, Blockchain has emerged as a solution for improved security, privacy, and confidentiality of the large amount of data transferred within the 5G infrastructure. However, issues such as decentralization and data interoperability in 5G networks require an efficient and informed combination of such technologies. Motivated by these observations, in the following, we devise and analyze the "BlockSD-5GNet" architecture, providing both details on its design principles and architectural structure. Inspired by the

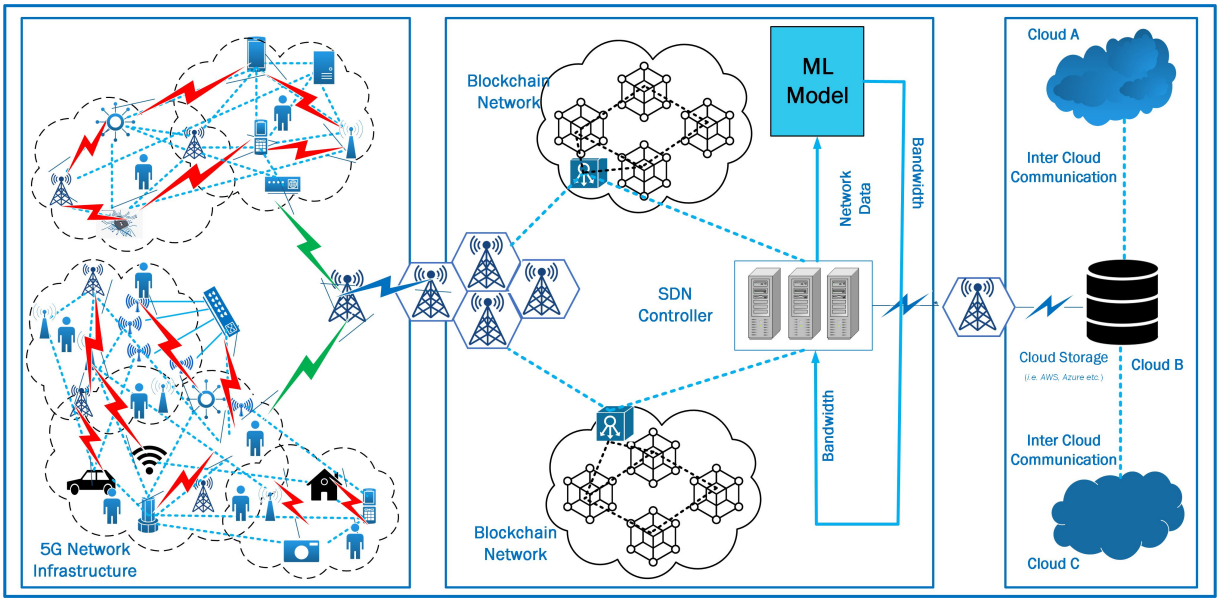


FIGURE 1 Overview of the proposed "BlockSD-5GNet" architecture for 5G networks.

successful application of ML to face 5G-network challenges—such as congestion control[46], fault detection[47], bandwidth sharing, route failure estimation, and energy supply[48]—"BlockSD-5GNet" also provides bandwidth prediction via ML-based regressors to aid the SDN/NFV management of the 5G network. Finally, we experimentally demonstrate that "BlockSD-5GNet" attains enhanced protection, confidentiality, reliability, and performance in 5G networks via the proper combination of state-of-the-art technologies discussed above aided by ML-based forecasting capability.

3 | PROPOSED "BLOCKSD-5GNET" ARCHITECTURE FOR 5G NETWORKS

In this section, we present the proposed "BlockSD-5GNet" secured architecture for 5G networks. As shown in Fig. 1, "BlockSD-5GNet" integrates SDN, NFV, Blockchain, and ML technologies in the 5G network providing connectivity to several IoT sensors, ranging from intelligent automotive systems to smart-home devices. In more detail, the dynamic deployment of network resources is achieved by using multiple SDN controllers enabled with NFV capabilities that enhance the scalability and dynamicity required by the 5G network architecture. Moreover, an ML module integrated in the SDN controller enables the effective prediction of network bandwidth. Indeed, since SDN provides separate control and data planes, specific bandwidth provisioning strategies can be deployed for both control and data traffic based also on the forecasting of ML-based bandwidth predictors. Additionally, "BlockSD-5GNet" leverages the public Ethereum Blockchain—despite being conceptually agnostic about the specific Blockchain technology as depicted in Fig. 1—to improve security with the aim of attaining immutability, decentralization, and transparency of data. These data are stored in cloud computing shared facilities on different Virtual Machines of a (public) cloud provider, with Blockchain guaranteeing security and confidentiality among data blocks in the 5G network. Overall, the 5G network itself constitutes the backbone communication infrastructure of "BlockSD-5GNet" and offers numerous services at the proposed architecture, such as low-cost, reduced network failures, ultra-low latency, and high mobility. The stakeholders that can benefit from the deployment of such an architecture are primarily mobile network operators on a large scale, and more in general, (mobile) network administrators, especially in smart contexts such as smart cities and condominiums, whose applications and services need strict requirements in terms of low failure rate, high performance, and confidentiality.

Hereinafter, we describe the "BlockSD-5GNet" architecture reporting the details of the IoT sensors network (Sec. 3.1), SDN data and control planes (Sec. 3.2), and SDN-IoT integration enabled with NFV capabilities (Sec. 3.3). Sec. 3.4 shows how ML techniques are utilized to provide further insights to properly manage the 5G network and improve its performance, considering bandwidth prediction as a notable use case. Successively, we discuss possible attacks against the 5G network and the related threat model (Sec. 3.5) and how these attacks can be mitigated by jointly exploiting SDN and Blockchain technologies (Sec. 3.6).

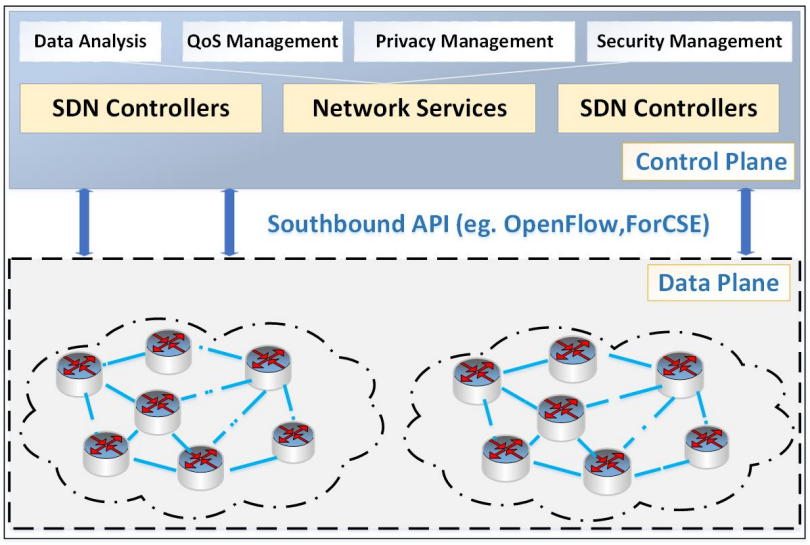


FIGURE 2 SDN architecture encompassing data and control planes.

Finally, in Sec. 3.7 we discuss how the "BlockSD-5GNet" architecture can help achieving the requirements of 5G-network use cases.

3.1 | IoT Sensors in 5G Networks

In our presented model "BlockSD-5GNet", IoT sensors within intelligent appliances (e.g., smart TVs, intelligent storage systems, smartwatches, etc.) transmit traffic data through SDN-enabled gateways, such as routers, switches, and firewalls. Given the multitude of smart appliances connected, the IoT sensors can be capable of producing a considerable amount of data within the networking system that should be efficiently managed. As shown in Fig. 1, the 5G network infrastructure accomplishes the forwarding of IoT data with the aides of the SDN platform enabled with NFV capabilities. In more detail, the IoT devices are connected together to exchange information keeping their communication links busy (red lightning in Fig. 1). Successively, all data generated by IoT sensors are collected through the data links into the SDN-NFV platform, while the 5G infrastructure offers the forwarding facilities. For instance, IoT services can be achieved via the 5G network leveraging a system-based slicing of the network based on IoT sensor data for efficiently establishing a dedicated IoT service-oriented architecture depending on user demands[49].

3.2 | Fundamentals of SDN Technology

SDN is a networking standard that aims to manage and configure networking applications by including fundamental networking system elements such as logically centralized management, a unified network view, the appropriation of dynamic control, and network programmability[50]. SDN permits better programmability and control of the network linked with traditional network management by disassociating the forwarding (in the data plane) and the routing (in the control plane) of network traffic[51]. Compared with the conventional networking model, it can also better deal with safety threats, new unseen threats, and different attacks[52]. Hence, the SDN plays a vital role within the 5G network and can be effectively exploited to enhance security, privacy, network stability, dynamic configuration, etc. Fig. 2 depicts the key components of the SDN technology highlighting its two conventional layers, i.e., the data plane and control plan (along with related network services) which are detailed hereinafter.

3.2.1 | Data Plane

As shown in Fig. 2, the data plane (also known as edge or infrastructure layer) is the lowest layer of the SDN platform and provides forwarding capabilities to network packets[30]. For instance, in our "BlockSD-5GNet" the data plane connects IoT sensors to other devices as a router, storage systems, etc. The data layer provides two types of switches: virtual and physical. The

former are virtualized components usually implemented with popular Linux-based operating systems [53]. The latter are hardware-based switches implemented either on open network hardware or dedicated hardware of networking vendors [54]. These network forwarding devices and SDN controllers (in the control plane) communicate via secure TLS-encrypted channels. Hence, the communication between control and data plane is established using well-known communication protocols, i.e. OpenFlow [55]. Protected data is then moved to the control plan.

3.2.2 | Control Plane

The control plan is the main backbone of the SDN platform and controls how data packets are forwarded, i.e., it is in charge of managing the routing process. The basic components of the control plane are logic and functional controllers applied to manage the control logic at different levels (e.g., to facilitate high network communication) and to provide controlling functionalities, respectively. The control plane is also tasked with the mapping between the data plane and the application layer and offers different types of networking services for the intended environment [54,56]. In more detail, the core of the control plane is implemented through established protocols such as OpenFlow, POX, Floodlight, OpenDayLight, OpenStack, and Beacon [55]. Furthermore, several interfaces are introduced for proper interaction with the other components of the SDN platform: (i) the southbound Application Programming Interface (API) for the communication between the SDN controllers and the switches and routers of the data layer; (ii) the northbound API (usually a RESTful API) for the communication between the SDN controllers and higher-level services and applications; and (iii) the east/westbound API for the communication between multiple distributed controllers. Finally, the SDN control plane provides several improved network services (e.g., data analysis and QoS, privacy, and security management) which offer high data protection and privacy in the smart IoT-5G network infrastructure.

3.3 | SDN-IoT with NFV Execution

NFV leverages virtualization technologies to virtualize network-node functions like load balancing, firewalling, and intrusion detection with the aim of effectively providing such services. In wireless IoT-sensor networks, NFV is usually leveraged also to improve the network lifetime. Despite being complimentary, NFV and SDN are not interdependent: SDN is the safest option for prompt control and orchestration of NFV. Indeed, SDN controllers can manage the virtual machines running network software and processes by decoupling the data and control planes via the standard OpenFlow protocol which provides the remote-management API to accomplish this task [57]. Additionally, NFV optimizes the implementation of network facilities in the SDN-IoT ecosystem by making it more efficient in terms of low power consumption, optimized performance, and reduction of safety concerns [58]. Moreover, through the proper combination of these technologies, the (IoT-5G) network environment becomes more efficient in terms of energy usage, data protection, and load balancing. In the proposed "BlockSD-5GNet" architecture, we have jointly adopted NFV with an SDN-IoT-based gateway instead of using a conventional gateway. The combination of these platforms, accordingly, helps to effectively improve the performance and safety of the 5G infrastructure.

3.4 | Machine Learning Model for Bandwidth Prediction

This section describes how ML algorithms can be integrated into "BlockSD-5GNet" to forecast network bandwidth. Such knowledge is essential for the proper optimization of network resources and suitable network administration, particularly in 5G networks constituting a highly-dynamic and challenging scenario [59]. In the latter, ML has proven to be an effective and reliable tool for prediction [16,60]. We underline that ML-based regressors can be effectively deployed into the SDN controllers being flexible and programmable devices. Hence, the regressor can predict network bandwidth and eventually notify the network administrator about a possible incoming demand of resources, or it can even adjust them automatically. In detail, the ML regressor is first trained offline and then utilized in conjunction with the SDN controller for bandwidth forecast and possible reaction. Figure 3 sketches the workflow of the proposed bandwidth prediction framework leveraged herein. The following paragraphs detail the relevant blocks of such a workflow.

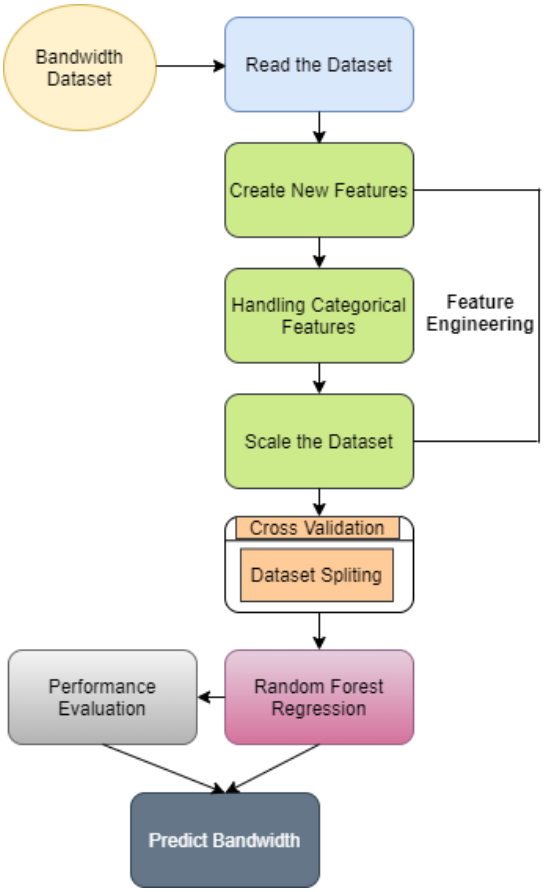


FIGURE 3 Workflow of the proposed framework for bandwidth prediction in 5G networks.

3.4.1 | Dataset Description

To foster reproducibility, we have employed the dataset collected for the "AIVIVN Predict Server Traffic" contest publicly available online[2]. Overall, the dataset encompasses 1048576 records collected from October 1^{st}, 2017 to March 9^{th}, 2019. Firstly, we perform dataset cleaning and feature extraction to remove noisy features and exploit only those related to network bandwidth prediction. In more detail, we use all the records in the dataset for training and testing the ML model (training-test splitting procedure is described hereinafter). A total of 4 features are available in the original dataset (the names refer to the dataset fields): UPDATE_TIME, ZONE_CODE, HOUR_ID, and MAX_USER. Additionally, the BANDWIDTH_TOTAL field represents the ground truth to be predicted. The description of each extracted record field is reported in the following:

- *UPDATE_TIME*: date (day, month, and year) of record collection;
- *ZONE_CODE*: region code number;
- *HOUR_ID*: hour (numerical) of record collection;
- *MAX_USER*: maximum number of users who have accessed the server within 1 hour;
- *BANDWIDTH_TOTAL*: bandwidth usage with 1 hour granularity.

3.4.2 | Feature Engineering

As shown in Fig. 3, before splitting the dataset into training and test set, we perform feature engineering preprocessing. Such a procedure makes the dataset machine-readable and helps to achieve higher prediction accuracy[61]. Firstly, since the dataset

[2]https://www.aivivn.com/contests/4

contains only 4 features for feeding the ML model, we generate additional features from existing ones to help the regressor accomplishing the bandwidth prediction task. Moreover, by increasing the number of features, we overcome the correlation issue between the dependent features. On the whole, the additional features are:

- *COUNT_DATE*: it is a numerical feature that represents the date of the first record in the dataset (October 1^{st}, 2017) as 0 and the last date (March 9^{th}, 2019) as 524.
- *DAY_OF_WEEK*: it is a numerical feature that represents the day of the week with a value comprised between 0 (Monday) and 6 (Sunday).

Then, we convert the categorical features to machine-readable (numerical) values that can be fed to the ML model. Finally, we perform feature scaling (i.e. normalization) to improve the numerical stability of the model and reduce training time[62]. These processes are described in more detail hereinafter.

- *Handling Categorical Features*: categorical features (i.e. UPDATE_TIME and ZONE_CODE) present in the dataset need to be converted into numerical values. For both features, we apply the *mean encoding*, which represents each feature based on the probability of the target variable (i.e. BANDWIDTH_TOTAL) in the dataset, conditional on each value of the features.
- *Feature Scaling*: we scale each feature such that no variable is overshadowed by the others. Scaling also makes the training faster and allows us to use less computational power. For this purpose, we use the *min-max scaler* that normalizes the data in the range from 0 to 1.

3.4.3 | Dataset Splitting

We evaluate the performance of network bandwidth prediction via the robust *five-fold cross-validation* technique that uses 80% of records for training and the remaining 20% for testing purposes. Consequently, the overall performance is obtained by performing the average of the results related to the five folds.

3.4.4 | Machine Learning Algorithm

We choose the Random Forest Regressor (RFR) for bandwidth prediction. The RFR is an ensemble of multiple decision trees (i.e. weak learners). The forest is built at training time leveraging the ideas of bagging and random-feature selection to mitigate overfitting. Each tree is trained to minimize the mean squared error between the predictions and the actual values. After training, the prediction is made by taking the (weighted) average of the responses of all the trees. It is worth noting that the RFR has been successfully employed in recent studies to accomplish prediction tasks related to network traffic at different granularities, and it has shown superior performance than both other ML-based regressors and statistical ones (e.g., Markovian models)[16,63]. Nevertheless, before coming to the final decision, different ML models, including Linear Regressor (LR), Gradient Boosting Regressor (GBR), and Ada-Boost Regressor (ABR), have been also tested on the considered dataset, showing lower performance than the RFR, despite having similar complexity in terms of both training and testing (cf. Sec. 4.2).

3.5 | Threat Model: Attacks in 5G Networks

As 5G promises more interconnected communities than ever[64], it becomes vulnerable to intruders[65]. To address their safety and security, we first model the possible ways of attacking 5G networks. In this regard, Fig. 4 depicts the threat model for 5G networks considered herein. Different types of attack from both inside and outside the network should be identified and neutralized. Hereinafter, we discuss the most notable active and passive attacks schematized in Fig. 4 aimed at reducing the dependability and availability of 5G networks.

3.5.1 | Eavesdropping

Eavesdropping is one of the most widely performed passive attacks against 5G networks[66]. It is also referred to as sniffing and represents the theft of data/information sent over a network by an illegal intruder device. Because of its passive nature, eavesdropping is very complex to detect. In 5G networks, broadcasting messages periodically sent by base stations are particularly subject to eavesdropping since they are not protected for confidentiality, authenticity, and integrity.

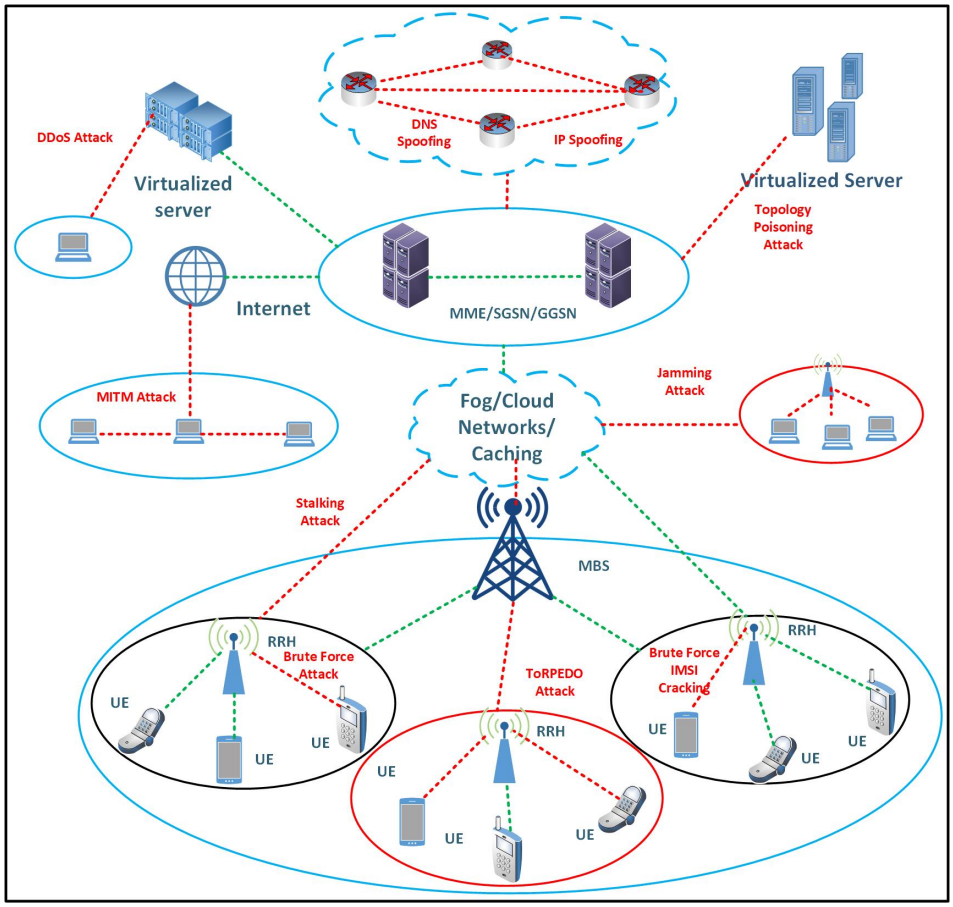


FIGURE 4 Threat model for 5G networks.

3.5.2 | Jamming Attack

In a jamming attack, an intruder device produces a noise signal which completely disrupts the communication channel between trustworthy users by decreasing the Signal to Interference plus Noise Ratio (SINR). Jamming attacks may also be exploited to launch DoS/DDoS attacks[66].

3.5.3 | DoS/DDoS Attack

In a DoS attack[67], an intruder keeps network resources busy and then unavailable for legitimate users by intentionally disrupting the network services. In an SDN-enabled 5G network, the intruder targets the flow table of an OpenFlow switch by requesting to open several connections without providing the credentials of client devices. Consequently, the OpenFlow switch flow table is overwhelmed with entities larger than its buffer, making legitimate traffic unable to traverse the switch. In a DDoS attack, compromised hosts (i.e. botnet) send a massive amount of these requests at the same time for keeping most of the network resources busy so that the service is negated to legitimate users. Since 5G utilizes much higher bandwidth than LTE and given the huge number of IoT devices connected, a DDoS attack may be more easily organized and has a greater effect against 5G networks. This constitutes a serious threat to 5G and, as a result, defenses stronger than traditional strategies must be implemented.

3.5.4 | Topology Poisoning Attack

Topology poisoning attack misleads the Link Layer Discovery Protocol (LLDP) service of the OpenFlow protocol[68]. Firstly, the intruder tracks the legitimate LLDP syntax, then it manipulates the propagation of LLDP packets by modifying specific information (e.g., port numbers) to inject fake links. Fake links can induce the controller to make incorrect routing choices and thus allow the intruder to re-route traffic flows toward compromised nodes.

3.5.5 | Side-Channel Attack

In a side-channel attack[68], an intruder initially collects information on the implementation of the network system, i.e. timing of traffic flows, power consumption, electromagnetic leaks, network monitoring information, etc. Then, the intruder can exploit this information to break a cryptosystem by reducing the number of attempts required by a blind brute-force attack. In an SDN, a side channel attack can disclose information on the network configuration, for instance: the OpenFlow protocol run on the controller, the size of switch forwarding tables, host configurations, or link properties (e.g., if they contain aggregate flows).

3.5.6 | Man-in-the-Middle (MITM) Attack

In a Man-in-the-Middle attack[49], an intruder intercepts and relays the traffic packets sent between two legitimate users opening independent connections with the victims. First, an intruder acts as a "middleman" between sender and receiver, then silently eavesdrops (or even sends) traffic packets toward the receiver by fakely impersonating the sender and vice versa. Therefore, the intruder can both alter the communication between the parties and steal confidential information (e.g., login, password, etc.). In 5G networks, the false base station is one of the most common variants of the MITM attack. The intruder broadcasts radio signals (after having eavesdropped on them) to impersonate legitimate base stations by using the same network identifier as a legitimate network but with a stronger signal to cheat users.

3.5.7 | Stalking Attack

The aim of a stalking attack[49] is to trace the location of legitimate (mobile) users or organizations. The ultimate intent is to threaten or harass a victim for controlling, scaring, or manipulating her.

3.5.8 | ToRPEDO Attack

The ToRPEDO (TRacking via Paging mEssage DistributiOn) attack has been designed in[69] to discover the coarse-grained location information of a victim by exploiting various information sources available in a 5G network, namely: the delay between the time when a call is made and when the paging message is observed, and the exact number of paging records in each frame. Successful ToRPEDO attacks enable the attacker to mount other threats such as DDoS (by intentionally injecting empty paging messages), eavesdropping (by detecting the presence of the victim in an area where the attacker has a sniffer), PIERCER, or brute-force IMSI cracking (described hereinafter). The attacker can also create a victim's mobility profile and breach her privacy by exposing the timing of the idle/active status of her Mobile Equipment (ME).

3.5.9 | PIERCER Attack

The same authors have also proposed the PIERCER (Persistent Information ExposuRe by the CorE netwoRk) attack which exploits the uncommon situation (in contrast with 3GPP recommendations) in which the service providers use the International Mobile Subscriber Identity (IMSI) instead of the Temporary Mobile Subscriber Identity (TMSI) in paging messages to register/identify MEs. Through the PIERCER attack, an intruder can become aware of the victim's IMSI, and using a sniffer and a fake base station in the victim's cell can associate the victim-device IMSI with its phone number while using ToRPEDO as a sub-attack. Furthermore, the intruder can instantiate other attacks in which the knowledge of the victim's IMSI and/or phone number is a prerequisite[5,9].

3.5.10 | Brute-Force IMSI Cracking Attack

Finally, in[69], it is shown how ToRPEDO can be exploited to obtain the IMSI of the victim via a brute-force attack. In the US, IMSIs are 49-bit binary numbers. The first 18 bits represent the country code and the mobile network code and can be obtained using lookup services. The ToRPEDO attack allows the attacker to obtain the trailing 7 bits which contain the victim's paging information. Therefore, the attacker should guess only the remaining 24 bits. In[69], the authors demonstrate an attacker can guess the victim's IMSI within 13 hours using a brute-force attack.

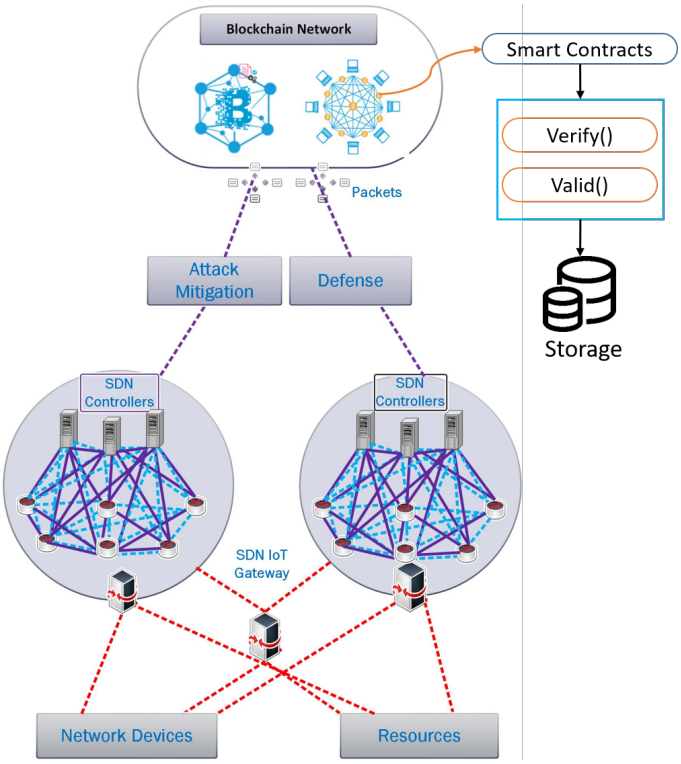


FIGURE 5 Process for attack mitigation and defense provided by "BlockSD-5GNet" in 5G networks.

3.6 | Attacks Mitigation Process in 5G Networks via SDN and Blockchain

To deal with the above-mentioned attacks, in the proposed "BlockSD-5GNet" architecture, we jointly leverage SDN and Blockchain technologies to properly manage the security and privacy of the 5G network. In a Blockchain, traffic data are transmitted as a chain of blocks that integrates mechanisms to protect these data. In more detail, Blockchain provides a distributed approach to attain such a goal by creating block-by-block hash connectors. The genesis block (i.e. the first block on the ledger) can be created in a distributed setting including multiple blocks, timestamps, hashing information, etc. Hash functions in a Blockchain seal each block of information and represent the current state of the chain. Each block is connected with the hash of the previous block. This hash chain can create the communication channel for securely connecting every smart IoT device in our "BlockSD-5GNet" architecture. Specifically, the integration of Blockchain permits to improve the security and privacy of the 5G network by providing several desired properties such as decentralization, privacy, immutability, traceability, and transparency.

Figure 5 shows how "BlockSD-5GNet" incorporates Blockchain for ensuring these properties in a 5G network and defending the network from third-party attacks. As seen in previous sections, network devices transfer data via SDN-IoT gateways. The SDN environment encompasses several SDN controllers (in the control plane) and switches (in the data plane) that manage the traffic flows. "BlockSD-5GNet" should guarantee confidentially to such a large amount of traffic data that need to be secured. Indeed, although SDN can mitigate common attacks (e.g., DoS/DDoS) within its domain, when deployed in a 5G network, SDN should deal with a significantly increased number of connected devices, higher data transfer rates, and extended attack domain. Thus, securing only one domain is not enough to ensure the security of the whole network. In such a case, combining SDN with Blockchain can facilitate attack detection and mitigation within the several domains that take advantage of the 5G network infrastructure[70].

Going into details, privacy, and confidentiality are obtained via public-key cryptographic schemes (e.g., RSA) in which the pair of public and private keys are generated in such a way that an attacker can not infer (i.e. it is computationally infeasible) the private key based only on knowledge of the public key. Furthermore, the Blockchain maintains a record of threats and mitigates the possibility of data breaches. Specifically, the Blockchain leverages transactions to immutably store (after confirmation) metadata about the services and requests made by the users. Hence, it actually realizes a distributed ledger (i.e. a database that is consensually shared and synchronized across multiple sites) which, as mentioned before, stores the hash values used for proper

authentication. This hash value depends on other blocks of the ledger, thus each time an inauthentic request is found in the 5G network, Blockchain warns and prevents the service requested, thus mitigating the possibility of data breaches. Moreover, in the considered IoT-5G scenario, involving a large number of device-to-device communications, Blockchain can be used to properly allocate network resources. In more detail, the IoT devices are considered nodes of the Blockchain which is exploited to verify the authenticity of the channel state information by implementing a consensus-based algorithm. Based on the latter decision, the other components of the "BlockSD-5GNet" architecture decide to allocate the network resources requested only after successful authentication. Therefore, the Blockchain can provide improved transparency and reliability to the system by marking as fraudulent the devices that intentionally advocate a higher value of the channel state information[71].

As illustrated in Fig. 5, the Blockchain also holds smart contracts as an executive block of program. In more detail, smart contracts contain verification and validation methods with different security algorithms. Namely, the usage of smart contracts allows the block pair to be verified and validated before the data are stored in the storage device. Figure 5 shows that to complete a transaction in the Blockchain, the two above-mentioned `verify()` and `valid()` methods are run by the smart contract which also contains a security algorithm to ensure the security of the transaction. Moreover, the Blockchain acts as a database for storing and managing 5G data through its secure distributed ledger. In fact, each block of the ledger immutably maintains the encrypted hash value and metadata related to the requested services (e.g., the cost of the transaction, the source and destination, etc.). Data indexes are also stored in the blocks and then employed for faster processing. Analogously, the information about the 5G network or the URLLC slices is maintained and managed in the distributed ledger. Overall, the latter provides a series of features (e.g., immutability, decentralization, transparency, and privacy) that allow "BlockSD-5GNet" to efficiently tackle security issues of modern 5G networks. On the other hand, SDN and NFV are the most suitable technologies jointly employed with Blockchain to enhance the security of 5G[32]. Overall, this suite of functionalities guarantees a solution to effectively tackle different threats in 5G networks, as briefly described hereinafter regarding the most common attacks.

3.6.1 | Eavesdropping Mitigation

As discussed in Sec. 3.5, eavesdropping is conducted via a mixture of passive attacks based on traffic monitoring for intercepting the message exchanged on the radio links of the 5G network. A viable solution to counter eavesdropping is designing a heterogeneous network (HetNet) encompassing nodes with different transmit powers and coverage sizes[66]. Indeed, HetNet introduces an advanced inference management system into the network that maximizes the secrecy of 5G-network users under eavesdropping attacks and adds possibilities for further computing and data analysis solutions. Moreover, given that an eavesdropping attack steals sensitive information without hampering the communication channel—it is commonly conducted when the communication is set up—the integration of Blockchain maintains the confidentiality of the communication, thus further securing the 5G network from such attacks.

3.6.2 | Jamming Attack Mitigation

The jamming attack is another threat that disrupts the communication channel by targeting the physical layer of 5G networks and can be the initial step of DDoS[66]. To secure the physical layer of 5G networks, we propose to leverage secure communication methods, namely Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) that spread the radio signals over a wider bandwidth mitigating the effect of jamming. Moreover, pseudo-random time-hopping anti-jamming schemes and detection mechanisms based on focused resource allocation and network monitoring can be added to FHSS to further improve its safety. In addition, novel two-phase Blockchain consensus protocols[72] have been also proposed to establish a jamming-resistant wireless communication in network environments where nodes have limited physical resources and fall short of well-established reliable channels.

3.6.3 | DoS/DDoS Attack Mitigation

DoS/DDoS attacks aim at exhausting network resources by exploiting vulnerabilities in the critical path. Although direct bandwidth exhaustion is the most common way to conduct a DDoS attack in a network, other vulnerabilities can be easily exploited. Indeed, on the one hand, the use of Blockchain eliminates single points of failure of centralized systems, on the other hand, it introduces other vulnerabilities exploitable for DDoS attacks. For instance, expensive back-end operations can be easily triggered in the Blockchain to halt the whole system. A common example to facilitate a DDoS attack is constraining the whole

network to fulfill PoW operations (i.e. block insertion) while simultaneously limiting the total transaction capacity (i.e. block size). More specifically, by sending spam transactions to the Blockchain, malicious attackers can fill the blocks and hinder legitimate transactions from being added to the chain, namely a transaction flooding attack. Given that several Blockchains have a fixed block size and limit how many transactions fit into a block, if any malicious attacker sends multiple transactions to the Blockchain network, he can fill the block with false or spam transactions causing legitimate transactions to stay in the memory pool for a long time, waiting for the next block.[3]

Additionally, in the 5G network, mMTC (massive Machine Type Communication) helps Blockchain operation to be faster and more reliable. However, DDoS attackers can exploit the advantage of the high bandwidth of mMTC to slow down the network. By proposing a secured 5G network we are exploiting the advantage of the high bandwidth of mMTC while blocking the attackers from taking the opportunities of mMTC.

In detail, to prevent such attacks, governing rules must be defined for the Blockchain. Hereinafter, we specifically refer to the Ethereum Blockchain being the one used in our experimental evaluation (cf. Sec. 4.1). In more detail, before adding new nodes to the network, the Ethereum Blockchain confirms their authenticity by interacting with smart contracts. Hence, in this way, Ethereum effectively verifies nodes' authenticity before actually adding them to the network, thus lowering the risk of attacks against the Blockchain. Moreover, Ethereum can further lower the likelihood of DDoS attacks at the application layer via advanced authentication procedure or via tracing and recording the IP addresses of malicious devices inside the Blockchain to prevent them from connecting and communicating with the network[73].

To proactively detect DDoS attacks, in[74] an IoT botnet detection system leveraging Hyperledger and Ethereum is proposed. More specifically, to connect to the network, an IoT device must meet the following criteria: (i) For communication to take place, a device must register. (ii) The functions of any IoT device are limited within a specified limit to guard against DDoS attacks. (iii) Whenever a failure of any type occurs or a limit is reached, the system has the ability to delete any device; additionally, the system sends the registered devices' addresses to all connected nodes and adds them to the trusted contact list. (iv) Every time any device initiates a new communication, the latter list is exploited to check the trustworthiness of the device.

3.6.4 | MITM Attack Mitigation

MITM is an attack that can affect various 5G network layers and undermines communication anonymity, integrity, and availability. To avoid a forged communication with the intruder (e.g., a false base station), the introduction of an authentication scheme between mobile devices and base stations provides an effective solution to mitigate a MITM attack. Specifically, the integration of Blockchain (e.g., based on smart contract) can provide mutual authentication and leads to a decentralized, reliable, and secure environment to protect the privacy and integrity of the communication against altered messages[75].

3.6.5 | Topology Poisoning Attack Mitigation

In Sec. 3.5, we have described how topology poisoning attacks mislead the LLDP service of OpenFlow to fabricate fake links between switches. To deal with this attack and offer real-time detection, the functionalities of the OpenFlow controller can be extended to automatically validate the update of the network topology. For instance, the *TopoGuard* extension[68] allows the SDN controller to check the legitimacy of host migrations and switch-port properties. In such a scenario, Blockchain restricts the access to the network by the attacker's device via its hashing security mechanism which provides confidentiality and authentication.

3.6.6 | Side Channel Attack Mitigation

On the other hand, side-channel attacks exploit timing information (e.g., processing time in the control plane) to gather knowledge on network infrastructure and configuration. A possible countermeasure is normalizing the control-plane delay to a configurable default responding time. For instance, to attain this goal the *FlowKeeper* framework[68] exploits a traffic agent for dynamically delaying selected traffic packets (without impacting perceived network performance) and confusing the response time used by side-channel attacks.

[3]For the Ethereum Blockchain, common values are between 15 and 20 transactions processed per second, namely a new block once every 12–14 seconds, on average.

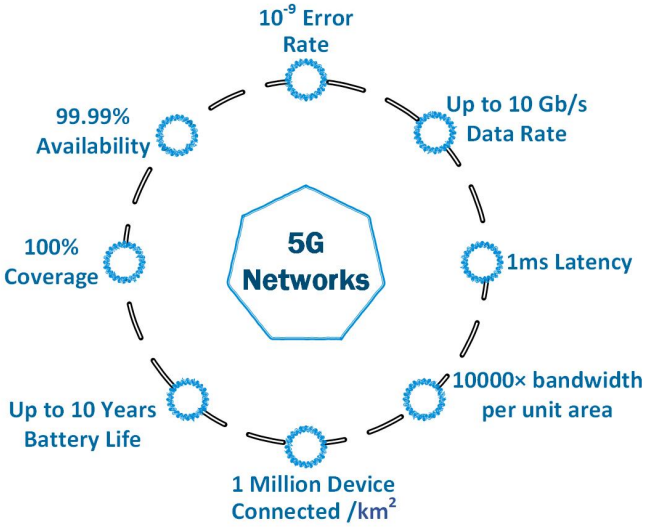


FIGURE 6 Requirements of 5G networks.

3.6.7 | Mitigation against Other Threats

Finally, to protect users in 5G IoT networks from major threats against privacy, authentication, integrity, and availability (e.g., eavesdropping, MITM, and stalking attacks, etc.) a suite of mitigation techniques can be jointly employed[76,49]: privacy-preservation of split selection aims to prevent user privacy leakages by unauthorized nodes; anonymous service-oriented authentication allows users to authenticate for IoT service access (without valid credentials an attacker cannot receive controller verification); service-oriented key agreement protects data by negotiating a unique service key among the IoT server, the controller, and the user which an attacker can not obtain.

To summarize, we propose the integration of cutting-edge technologies to attain greater privacy and attack protection in 5G networks, as well as higher data rates, reduced latency, large-scale system connectivity, diminished operating costs, and higher revenues[11,77]. In detail, with the support of innovative Blockchain, SDN, and NFV, "BlockSD-5GNet" can face the high-demand requirements of services and applications built on top of the 5G infrastructure.

3.7 | 5G-Network Requirements

Three essential use cases distinguish 5G networks compared to legacy mobile network technologies, namely the capability of supporting: (i) enhanced Mobile Broadband (eMBB) network access, (ii) massive Machine-Type Communications (mMTC), and (iii) ultra-reliable, low-latency communications (UR-LLC)[78]. To fulfill these needs, the 5G network has to guarantee a number of requirements—depicted in Fig. 6—which can be achieved by effectively exploiting the proposed "BlockSD-5GNet" architecture. In detail, the final goal of 5G technology is to provide up to 10 Gb/s throughput to mobile users, 1 Gb/s throughput in high-mobility scenarios, and up to 10000× bandwidth per unit area. Also, 5G should be flexible enough to control a variety of different applications (e.g., extended reality, autonomous vehicles, industrial automation, smart health, etc.) that demand high availability ($> 99.99\%$) and ultra-low latency ($< 1ms$). In addition to reduced latency of mobile services, 5G points to save network resources (e.g., battery life of network nodes) because of enhanced flexibility (e.g., network cutting and edge computing), with the consequent increase of QoS and providing the final users with a high degree of Quality of Experience (QoE). However, to fulfill these needs, mobile network operators have to build dense networks with a massive number of nodes (more than $1M$ devices connected for each km^2) that constitute the 5G infrastructure.

The management and security of such a complex infrastructure can be handled via the features offered by the "BlockSD-5GNet" architecture, which properly combines Blockchain, SDN, and NFV technologies to introduce strong security, high throughput, long network lifespan, cost-effective management, responsive interface, big-data accessibility, and data privacy. In detail, Blockchain allows key features for current and future applications and services of 5G networks, such as decentralization,

TABLE 2 Simulation environment parameters organized based on technology.

	Parameter	Value
General Parameters	Network emulator	Mininet-WiFi 2.2.1
	Packet analyzer	Wireshark
	Cloud storage platform	OpenStack
SDN Parameters	No. of SDN controllers	5
	No. of OpenFlow switches	6
	No. of SDN gateways	4
	Type of SDN controllers	Floodlight
	SDN routing protocol	OpenFlow
Blockchain Parameters	Blockchain platform	Ethereum
	No. of Ethereum Nodes	10
	Mode of Ethereum Nodes	Light
	Block size	4 B
	Block header	80 B
	Consensus algorithm	Proof of Work (PoW)
Network Parameters	Simulation area	2000 $m \times 2000$ m
	Simulation duration	600 s
	No. of IoT devices	200
	IoT devices speed	11 m/s
	Data rate	12 Mb/s
	Initial trust value	5 J
	Node transmitted packet sizes	$\{512, 700, 900, 1024\}$ B

immutability, transparency, protection, and privacy [10]. Besides, with the integration of SDN technology, it is possible to avoid the use of hardware by deploying "softwarized" network equipment that aids to reduce both capital and operating expenditure. SDN performs also a split between data and control planes, thus adding agility, adaptability, and control to the 5G network. On the other hand, NFV makes the life of 5G-network administrators even easier by simplifying a wide variety of network services, optimizing network performance, and delivering new revenue-generating services.

4 | EXPERIMENTAL EVALUATION

This section describes the experimental evaluation we have performed to assess the performance of proposed "BlockSD-5GNet" architecture. Firstly, in Sec. 4.1, we provide details on the experimental setup we have leveraged along with the parameters of the simulation environment and considered baselines. Then, in Sec. 4.2, we show the evaluation results in terms of different metrics related to both performance and robustness of "BlockSD-5GNet".

4.1 | Experimental Setup

In this section, we describe the performance evaluation setup, reporting details on the simulation tool, network setup, and simulation parameters.[4] Table 2 summarizes all the parameters of the simulation environment organized based on the reference technology. To set up the proposed architecture, we have chosen the Mininet-WiFi [79] for the emulation of the SDN environment, while the OpenFlow protocol is used for the control plane and the realization of the SDN routing capability.

[4] We exploit quantitative simulations that "execute" the model to replicate (viz. simulate) the real system's behavior. Indeed, simulations are commonly leveraged to forecast and explain how various configurations and situations affect the behavior of the system. As a result, simulations can be used to test new designs and rules and to answer "what-if" concerns, without having to stop the working system.

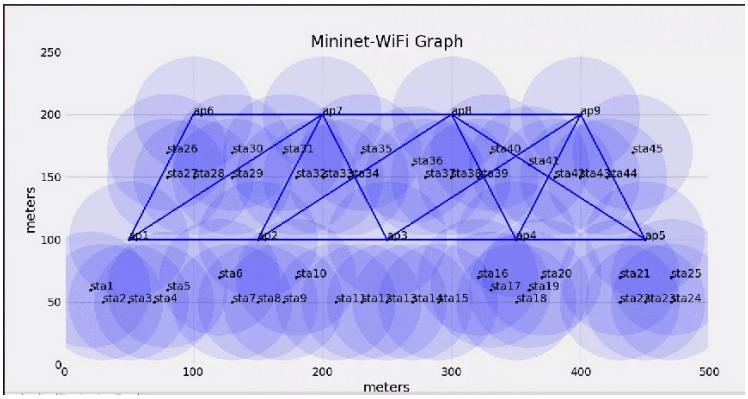


FIGURE 7 Network topology design (sample).

TABLE 3 Performance criteria and baselines.

Performance Criterion	**Baselines**
Achievable Bandwidth $[Mb/s]$	Conventional 5G network SDN-enabled 5G network
Throughput $[Mb/s]$	Simple IoT network
Node Failure Rate $[\%]$	SDN-based Controller Scheduling
Computational Delay $[s]$	Dual HMAC Model[80]
Bandwidth Prediction $[KB/s]$	Linear Regressor Ada-Boost Regressor Gradient Boosting Regressor

On the whole, the network encompasses 5 Floodlight controllers, 4 gateways, and 6 switches. For each communication, the source-destination pair is randomly chosen among 200 IoT devices in the network. The overall simulation time is set to 600 s. Each device transmits packets with sizes in the range: $\{512, 700, 900, 1024\}$ B with a data rate of 12 Mb/s. Nodes are spread in a 2000 $m \times 2000$ m rectangular region and are randomly located at the beginning of the simulation with an initial trust value of 5 J. Then, during simulation, the nodes move following a random waypoint model with a constant velocity of 11 m/s, namely they can shift randomly and without constraints within the region.

An example of the topological setup considered is depicted in Fig. 7, reporting the distance (in meters) among the nodes of the example topology (500 $m \times 250$ m). In such a sample, the network encompasses 55 nodes, more specifically, 9 access points (ap) and 46 stations (sta, namely simple IoT devices). The shadow circles around the nodes represent their communication range. Access points are interconnected to the stations and provide them with connectivity. The communication between nodes can be initiated by pinging them at the end of the design. Such topology graphs could be leveraged to make decisions to improve the performance and effectiveness of the network.

Regarding Blockchain, we leverage the Ethereum platform based on hashing and Proof of Work (PoW) consensus algorithm, with a block size of 4 B and a block header of 80 B. Specifically, we exploit 10 Ethereum nodes run by IoT devices. Each node is running light mode which only stores the block headers. Notably, the light mode allows IoT devices to participate in the Ethereum network without running powerful hardware and requiring high bandwidth. Indeed, in a real setting, IoT devices (e.g., sensors) would not have the proper computational power, storage, and energy to perform constant PoW validations on the whole Blockchain.

Finally, we use the Wireshark program to capture and analyze network packets generated by IoT devices running in such an SDN-IoT network. The experimental campaign is executed on an Ubuntu (GNU/Linux) x86 (2.20 GHz) server with 16 GB of RAM, 1 TB of SSD, and auxiliary storage to save the simulation output.

Table 3 reports the performance criteria considered to assess the proposed "BlockSD-5GNet" architecture and related unit of measurement. In more detail, we consider (i) the achievable bandwidth with respect to a target desired bandwidth, (ii) the average throughput (i.e. the number of transactions in Mb/s among IoT devices in the SDN), (iii) the percentage of node failures, and (iv) the computational delay (i.e. the average time in seconds that a node needs to wait to get the service it requested).

Regarding the bandwidth prediction task, performance is evaluated in terms of *R-squared* (R^2) averaged over the five folds and by comparing actual and predicted bandwidth (in KB/s). R^2 is a statistical metric that measures the proportion of variance of the dependent variable (in this case the network bandwidth) that the regression model is able to express. R^2 is defined as:

$$R^2(\hat{\mathbf{x}}) = \frac{ESS(\hat{\mathbf{x}})}{TSS(\hat{\mathbf{x}})} = 1 - \frac{RSS(\hat{\mathbf{x}})}{TSS(\hat{\mathbf{x}})} \tag{1}$$

where:

- $\hat{\mathbf{x}} = \hat{x}_1, \hat{x}_2, ..., \hat{x}_N$ is the sequence of values provided by the *prediction model*;
- $ESS(\hat{\mathbf{x}}) = \sum_{i=1}^{N}(\hat{x}_i - \bar{x})^2$ is the *Explained sum of squares*;
- $TSS(\hat{\mathbf{x}}) = \sum_{i=1}^{N}(x_i - \bar{x})^2$ is the *Total sum of squares*;
- $RSS(\hat{\mathbf{x}}) = \sum_{i=1}^{N} e_i^2 = \sum_{i=1}^{N}(\hat{x}_i - x_i)^2$ is the *Residual sum of squares*.

If $R^2 = 1$, there is a perfect match between observed and predicted data; $R^2 = 0$ occurs when the prediction corresponds to estimating the mean of the actual values; $R^2 < 0$ indicates that the average of the actual values is a better predictor than the considered method. Finally, for each performance criterion, Tab. 3 summarizes also the baselines against which we compare the performance of our "BlockSD-5GNet" architecture.

4.2 | Experimental Results

In the following, we assess the performance of the proposed "BlockSD-5GNet" architecture in terms of different performance criteria as shown in Tab. 3. In detail, we compare "BlockSD-5GNet" with considered baselines in terms of throughput, node failure rate, computational delay, and bandwidth prediction accuracy. The simulation results demonstrate that the integration of SDN-NFV with Blockchain allows *"BlockSD-5GNet" to outperform all the considered baselines* and properly react to events affecting network performance including failures and malicious attacks. Moreover, we show that *RFR can obtain satisfactory bandwidth prediction results* outperforming other ML-based regressors taken into account.

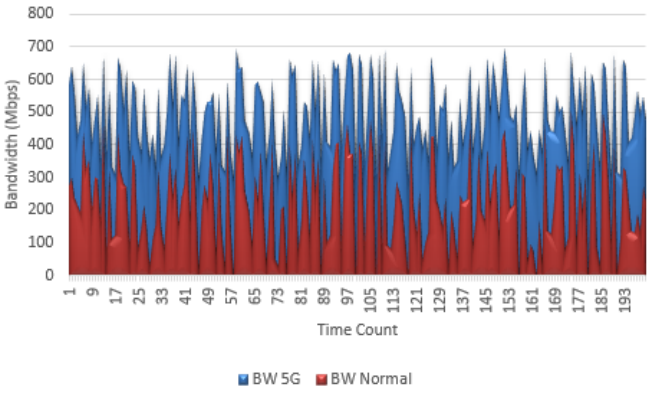
4.2.1 | Achievable Bandwidth Analysis

In Fig. 8, we depict the fluctuations of desired 5G network bandwidth (blue curve) in different time slots and compare them with the achievable bandwidth (red curve) (i) without deploying any of the emerging technologies included in "BlockSD-5GNet" (Fig. 8a), (ii) after exploiting only the SDN paradigm (Fig. 8b), and (iii) by applying our proposal for 5G network management and security (Fig. 8c).

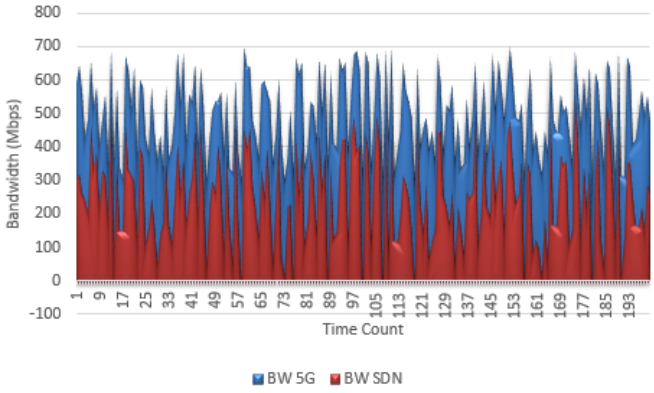
In Fig. 8a, we can notice that the actual achievable bandwidth without the integration of SDN and Blockchain is significantly lower when compared to the desired bandwidth of the 5G network. When the SDN management capability is added to the network, data are handled more uniformly and efficiently, partially preventing some security threats. Hence, as shown in Fig. 8b, the achievable bandwidth is slightly increased with respect to the one attained without SDN, though without reaching the same level of desired bandwidth. The proposed "BlockSD-5GNet" architecture exploits both SDN and Blockchain, providing enhanced security and confidentiality and improved network resource management. The effect of their combined advantages can be observed in Fig. 8c which shows an achievable bandwidth that follows almost perfectly the fluctuations of the desired bandwidth of the 5G network as no third party can interfere with the network.

4.2.2 | Throughput Analysis

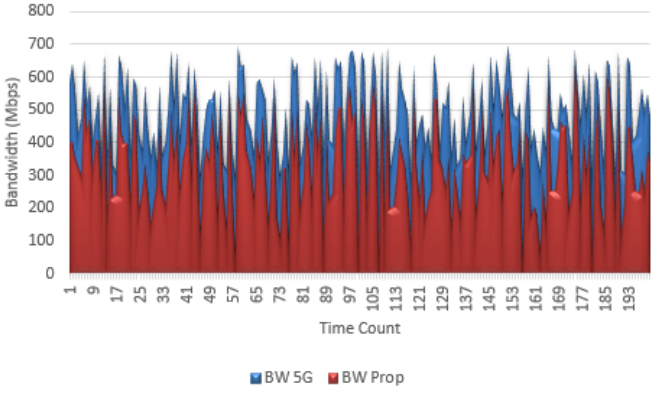
Figure 9 compares the throughput (in Mb/s) of proposed "BlockSD-5GNet" architecture with that attained in a simple IoT wireless network (i.e. without advanced capabilities provided by "BlockSD-5GNet", namely without integrating SDN, NFV, and Blockchain). The analysis is performed considering an IoT network simulated with the same network parameters reported in Tab. 2 and an increasing number of requests from IoT nodes.



(a) Desired vs. achievable bandwidth in a conventional 5G network.



(b) Desired vs. achievable bandwidth in a 5G network including SDN.



(c) Desired vs. achievable bandwidth in a 5G network when deploying "BlockSD-5GNet".

FIGURE 8 Comparison of desired bandwidth (blue line) with achievable bandwidth (red line) for different combinations of considered technologies deployed in a 5G network.

We can notice that with a low request rate (i.e. ≤ 50 requests), both systems exhibit similar throughput values. As expected, when the number of requests grows, the throughput value increases, being however far from an ideal linear trend. Nevertheless, the difference between the two approaches becomes sharper as the number of requests grows, with proposed "BlockSD-5GNet" always showing better performance starting from ≈ 60 requests. The maximum throughput improvement of $\approx 350\ Mb/s$ is obtained for ≈ 410 requests.

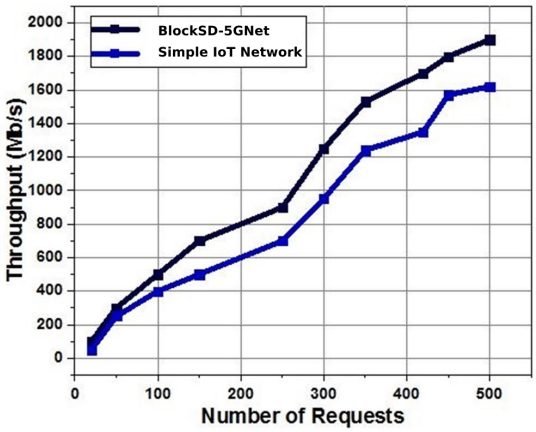


FIGURE 9 Throughput comparison of proposed "BlockSD-5GNet" with existing simple IoT network.

We can conclude that "BlockSD-5GNet" can properly handle increased request rate owing to security and consistency obtained via the integration of SDN-NFV and Blockchain that can help reduce processing overhead and react to unexpected events impacting network performance (e.g., unplanned reconfiguration, node and link failures, attacks, etc.).

4.2.3 | Node Failure Rate Analysis

Figure 10, to evaluate the robustness of a network enhanced with "BlockSD-5GNet", we have compared our proposal with a simple SDN-enabled controller scheduling (i.e. a baseline scheme that does not take advantage of NFV and Blockchain) in terms of node failure rate when varying the number of IoT devices deployed in the network. We consider a scenario in which an intruder undermines network operability by maliciously causing node failures. In detail, we simulate jamming and (D)DoS attacks with the aim of affecting network functionalities. During the simulation, we added extra noise (i.e. jamming) into the network system to cut off node communications. Also, some devices have been kept deliberately busy to simulate a DoS.

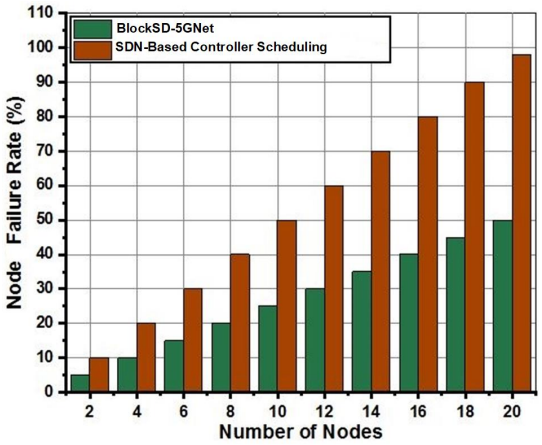


FIGURE 10 Comparison of node failure rate (due to network attack) of "BlockSD-5GNet" with a simple SDN-based controller scheduling.

Results show that, in presence of an intruder, the failure rate rises when the number of nodes subject to the attack increases. However, "BlockSD-5GNet" mitigates this detrimental effect compared to simple SDN-based scheduling. Indeed, our proposal approximately halves the node failure rate which in the worst-case reaches $\approx 50\%$ with 20 nodes deployed in the network region compared to $\geq 95\%$ obtained with simple scheduling (i.e. at most one node continues working). Therefore, we can conclude

that the integration of security-oriented Blockchain technology can significantly strengthen the network against attacks that aim to undermine its operability reducing the node failure rate up to a 2× factor.

4.2.4 | Computational Delay Analysis

Hereinafter, we analyze the computational delay of the proposed "BlockSD-5GNet" and the Dual homomorphic message authentication code (HMAC) scheme baseline [80].

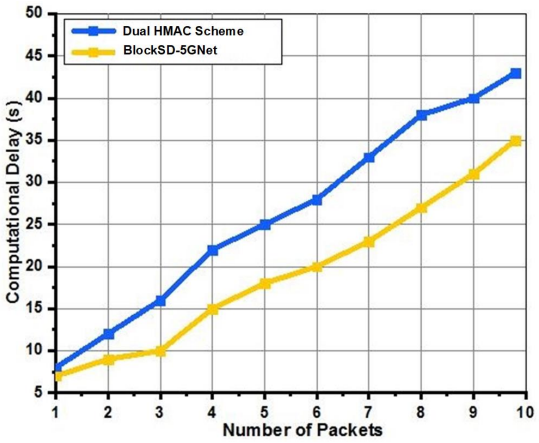


FIGURE 11 Comparison of computational delay of "BlockSD-5GNet" with Dual HMAC baseline [80].

The latter is a scheme used to secure wireless networks against attacks undermining the confidentiality and integrity of traffic packets (e.g., tag pollution attacks that maliciously modify tags appended at the end of the coded packets). Computational delay is defined as the average time in seconds that a node needs to wait to get the service it requested. Low computational delay is required for a 5G network system as the computation should be completed in real-time. Figure 11 compares the two approaches against a varying number of transmitted packets. We can observe that the Dual HMAC scheme presents a higher computational delay compared to our "BlockSD-5GNet" which proves to efficiently provide security and confidentiality to the 5G network. Moreover, "BlockSD-5GNet" is particularly effective when it has to deal with a greater number of packets (i.e. $\geq$ 7 packets) obtaining up to 10 *s* faster computation than the Dual HMAC scheme.

4.2.5 | Bandwidth Prediction Analysis

We now evaluate the performance of the bandwidth prediction capability of "BlockSD-5GNet". As discussed in Sec. 3.4, we propose to leverage ML models that have proven to be reliable solutions to fulfill this task [15,16].

TABLE 4 Performance of ML models for bandwidth prediction task.

Model	R^2
Linear Regressor	0.6290
Gradient Boosting Regressor	0.7340
Ada-boost Regressor	0.7002
Random Forest Regressor	0.8161

Firstly, we compare the prediction accuracy of various ML-based regressors, namely LR, ABR, GBR, and RFR. Table 4 shows the R^2 of these ML regressors averaged over the five folds. RF outperforms all state-of-the-art ML models attaining 0.8161 R^2. In detail, we have tuned the RFR by varying the number of decision trees in the range $\{10, 50, 100, 150, 200\}$, obtaining

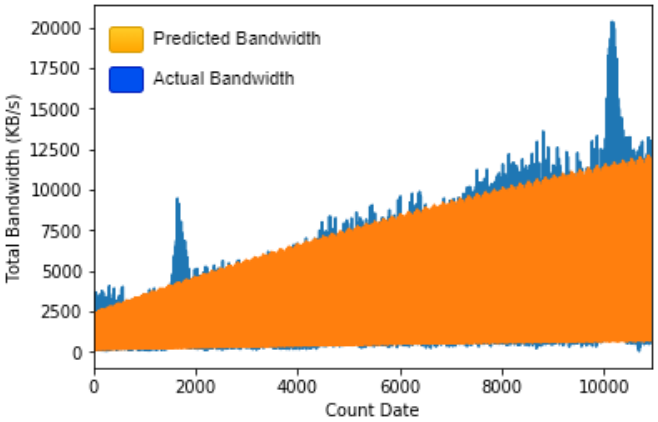


FIGURE 12 Actual vs. Predicted bandwidth using optimized RFR.

the best performance with 100 decision trees. Finally, in Fig. 12, we compare the bandwidth predicted with the optimized RFR against actual bandwidth measurements (with 1 hour granularity starting from October 1st, 2017, cf. Sec. 3.4). It is worth noting that, regardless of some spike outlier values, the RFR predictions follow the trend of actual values, thus demonstrating that the RFR is a reliable tool to assist network administrators in informed management and optimization of network resources. Indeed, since we consider the prediction of 5G-network bandwidth with such a fine granularity, it is expected that at certain hours of the day there may be temporary spikes due to the intense utilization of the network (this also depends on the particular dataset considered)[16]. However, the aim of our prediction is not to follow precisely such spikes but to forecast a demand for resources higher than normal to promptly alert the network administrator or adjust them automatically.

5 | LIMITATIONS, CHALLENGES, AND FUTURE PERSPECTIVES

The proposed "BlockSD-5GNet" integrates several technologies to provide effective management of 5G networks and security against attacks. In this regard, we have discussed the threat model and possible countermeasures to handle network vulnerabilities. On the one hand, simulation results have demonstrated the superiority of our proposal against different baselines when considering various performance criteria. On the other hand, there are still limitations and open challenges left by the present study. Hereinafter, we discuss such open issues and suggest possible directions that could be followed for further enhancements in the near future.

5.1 | Limitations and Challenges

One of the main limitations of our work is the reduced number of nodes considered when processing different evaluation parameters. Indeed, "BlockSD-5GNet" needs a scalable optimization algorithm that is in charge of promptly processing nodes' performance, particularly when their number grows significantly. Moreover, we have considered a first possible integration of emerging technologies, then advanced interaction of "BlockSD-5GNet" components should be taken into account. Similarly, we have investigated traditional ML algorithms fed with handcrafted features for network bandwidth prediction. In this regard, novel Deep Learning models could give even better performance than such traditional ML algorithms[81].

Finally, we have not evaluated a real-world implementation of "BlockSD-5GNet", having only demonstrated its functioning in a simulation environment. In an actual implementation, the scalability of the proposed architecture would be an open issue. In fact, if it is called for managing a considerable number of nodes, it may incur severe performance degradation or even failures. Moreover, since "BlockSD-5GNet" is agnostic with respect to the specific Blockchain implementation, its performance could be severely impacted by this choice since the most convenient platforms come at a huge cost in terms of implementation, processing, and energy costs: this is still an open challenge in both the research community and industry (e.g., finance and technology sectors). For instance, Ethereum Blockchain is able to handle as low as a few tens of transactions per second as opposed to legacy transaction processing systems that can process tens of thousands of transactions per second. This low transaction speed

limits its use as a viable solution for large-scale applications. Such a shortcoming is mainly due to the need for consensus on the network (e.g., via the PoW algorithm) to agree on the validity of a transaction in order for it to go through. On the one hand, this reduces the risk of malicious attacks but, on the other hand, increases the time needed for transactions to be completed. This challenge is further exacerbated in an IoT scenario, given that IoT devices are commonly power-constrained and thus require a lightweight (e.g., low-latency) consensus mechanism. Indeed, common Blockchain platforms (e.g., Bitcoin and Ethereum) can not be utilized as is, due to their high bandwidth demand and delays. Therefore, a suitable consensus algorithm should take into account the most urgent issues of the IoT environment, such as lack of security, different device standards, reduced device memory and computational capability, device power constraint, and transfer of large data amounts.

5.2 | Future Perspectives

This section describes possible lines of improvement of "BlockSD-5GNet". Firstly, the lifetime and reliability of the 5G network could be enhanced by adding mechanisms for *informed load balancing* to "BlockSD-5GNet" features. In more detail, we plan to take into account several optimization techniques to both *minimize the energy consumption of IoT devices* in the 5G network [82] and optimally allocate energy generators to *maximize the reliability of the energy distribution system* [83]. Energy-efficient cluster-head selection algorithms [30] would be also considered to reduce the power consumption and prolong the network lifetime by selecting a set of nodes that are used as optimal data transmitters to the base station.

Aimed at accelerating transaction speed, *enhanced consensus mechanisms* can be exploited in "BlockSD-5GNet" (it is not bounded to a specific Blockchain implementation). Specifically, we plan to adapt (lightweight) consensus algorithms based on the constraints of the considered environment mainly encompassing power-constrained IoT devices. These consensus mechanisms could be based on proof-of-stake [84]—where the consensus is reached by proving a certain stake ownership in the digital asset—on parallel proof-of-work [85]—based on parallel mining rather than solo mining—or hybrid consensus mechanism that combines proof-of-work mining with a proof-of-stake system—as done in Ethereum to motivate trustworthy behavior in the network. Blockchain designers continue also to explore newer consensus mechanisms such as proof-of-burn, proof-of-capacity, and proof-of-elapsed time to effectively ensure the validity and authenticity of the transactions [86].

Furthermore, as aforementioned, we plan to *improve the bandwidth prediction capability* by designing and evaluating more sophisticated ML-based regressors (e.g., based on hierarchical classification [76] or Deep Learning [81]). In this regard, on the one hand, *novel Deep Learning and advanced ML models* could give even better performance than traditional ML algorithms [81], on the other hand, they need proper tuning and (hyperparameter) optimization to avoid erroneous outcomes, for instance, due to biased inputs [62]. Also, without applying proper optimization, such more complex approaches would be costly and time-consuming, thus impacting "BlockSD-5GNet" effectiveness in managing the 5G network.

We plan to deploy "BlockSD-5GNet" in a *real-world scenario* to evaluate its effectiveness against large-scale threats such as DDoS and flooding attacks. However, to this end, a governance model should be defined for the *Decentralized Autonomous Organization (DAO)* resulting from the application of Blockchain for 5G networks. Such a governance model must adhere to national and international laws, regulations, and standards regulating 5G networks, as well as take into account operators' business logic. Therefore, defining a rule set compliant with the problem statement is needed to deploy "BlockSD-5GNet" in a real-world setting. More in detail, we plan to exploit smart contracts to build the DAO's rule set and allow any potential member to fully understand how the governing protocol operates. Indeed, since a DAO runs entirely autonomously, smart contracts would define the ground rules for the DAO's operations, and they can not be changed or manipulated without a consensus reached via a voting mechanism. The latter can be established based on novel consensus alternatives as discussed above in this section. Matters related to who has to construct the DAO's rule set and how, how to modify the participants of the DAO, and how to define voting rights (including veto power) must be also taken into account as fundamental design choices.

Finally, to face scalability issues, *Federated Learning* would be considered a novel learning paradigm applied to further improve bandwidth prediction capabilities and to fulfill advanced combinations such as Artificial Intelligence-Blockchain (briefly, AI-BC). Considering the components of the latter integration, AI would act as a security agent in the 5G network, while BC would ensure the confidentiality of the communications of these AI-secured network services.

6 | CONCLUSION

In this paper, we have investigated the integration of emerging leading technologies, namely SDN, NFV, Blockchain, and ML to enhance the performance, privacy, security, and management of 5G networks in an IoT scenario. These requirements should be addressed in the development phase of 5G networks and thus a proper combination of SDN, NFV, and Blockchain should be taken into account when deploying the network infrastructure. Therefore, we have provided the details of how these technologies can enhance the 5G services and how they can be jointly exploited via the proposed "BlockSD-5GNet" architecture. Moreover, to help administrators properly optimize network resources, we have proposed to integrate ML models into "BlockSD-5GNet" for bandwidth prediction and have found that RFR outperforms other state-of-the-art methods. Additionally, we have devised a threat model for 5G networks that takes into account several attacks and investigated possible countermeasures that "BlockSD-5GNet" can take for attack mitigation.

Extensive simulations have shown the effectiveness of the proposed architecture which betters various baselines both in terms of performance (i.e. achievable bandwidth, throughput, and computational delay) and robustness (i.e. node failure rate) owing to the effective integration of SDN-NFV with Blockchain and ML. Limitations and open challenges of the present work have also been discussed, which helped us outline possible future directions for the improvement of the "BlockSD-5GNet" architecture. These include, among others, mechanisms for optimized energy consumption and load balancing to prolong network lifetime, enhanced consensus mechanisms for improving transaction speed, advanced ML and DL bandwidth prediction approaches, and scalable real-world implementation of "BlockSD-5GNet".

Financial disclosure

None reported.

Conflict of interest

The authors declare no potential conflict of interests.

References

1. 3GPP . System architecture milestone of 5G Phase 1 is achieved. https://www.3gpp.org/news-events/3gpp-news/1930-sys_architecture; 2017. Accessed: 2021-09-06.
2. Patzold M. Countdown for the full-scale development of 5G new radio [mobile radio]. *IEEE Vehicular Technology Magazine* 2018; 13(2): 7–13.
3. Maksymyuk T, Klymash M, Jo M. Deployment strategies and standardization perspectives for 5G mobile networks. In: 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). IEEE. ; 2016: 953–956.
4. Panwar N, Sharma S, Singh AK. A survey on 5G: The next generation of mobile communication. *Physical Communication* 2016; 18: 64–84.
5. Ordonez-Lucena J, Ameigeiras P, Lopez D, Ramos-Munoz JJ, Lorca J, Folgueira J. Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. *IEEE Communications Magazine* 2017; 55(5): 80–87.
6. Abdulqadder IH, Zhou S, Zou D, Aziz IT, Akber SMA. Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. *Computer Networks* 2020; 179: 107364.
7. Goldstein AB, Sokolov N, Elagin V, Onufrienko AV, Belozertsev IA. Network characteristics of blockchain technology of on board communication. In: 2019 Systems of Signals Generating and Processing in the Field of on Board Communications. IEEE. ; 2019: 1–5.
8. Islam MJ, Rahman A, Kabir S, et al. Blockchain-SDN-Based Energy-Aware and Distributed Secure Architecture for IoT in Smart Cities. *IEEE Internet of Things Journal* 2022; 9(5): 3850-3864.

9. Maksymyuk T, Dumych S, Brych M, Satria D, Jo M. An IoT based monitoring framework for software defined 5G mobile networks. In: Proceedings of the 11th international conference on ubiquitous information management and communication. ACM. ; 2017: 1–4.

10. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5g and beyond networks: A state of the art survey. *Journal of Network and Computer Applications* 2020: 102693.

11. Chaer A, Salah K, Lima C, Ray PP, Sheltami T. Blockchain for 5G: opportunities and challenges. In: 2019 IEEE Globecom Workshops (GC Wkshps). IEEE. ; 2019: 1–6.

12. Yang H, Zheng H, Zhang J, Wu Y, Lee Y, Ji Y. Blockchain-based trusted authentication in cloud radio over fiber network for 5G. In: 2017 16th International Conference on Optical Communications and Networks (ICOCN). IEEE. ; 2017: 1–3.

13. Aceto G, Persico V, Pescapè A. A survey on information and communication technologies for Industry 4.0: state-of-the-art, taxonomies, perspectives, and challenges. *IEEE Communications Surveys & Tutorials* 2019; 21(4): 3467–3501.

14. Mei L, Gou J, Cai Y, Cao H, Liu Y. Realtime Mobile Bandwidth and Handoff Predictions in 4G/5G Networks. *arXiv preprint arXiv:2104.12959* 2021.

15. Zhou J, Yang X, Sun L, Han C, Xiao F. Network traffic prediction method based on improved echo state network. *IEEE Access* 2018; 6: 70625–70632.

16. Aceto G, Bovenzi G, Ciuonzo D, Montieri A, Persico V, Pescapé A. Characterization and Prediction of Mobile-App Traffic Using Markov Modeling. *IEEE Transactions on Network and Service Management* 2021; 18(1): 907-925.

17. Matheu SN, Robles Enciso A, Molina Zarca A, et al. Security architecture for defining and enforcing security profiles in dlt/sdn-based iot systems. *Sensors* 2020; 20(7): 1882.

18. Conti M, Kaliyar P, Lal C. CENSOR: Cloud-enabled secure IoT architecture over SDN paradigm. *Concurrency and Computation: Practice and Experience* 2019; 31(8): e4978.

19. Molina Zarca A, Garcia-Carrillo D, Bernal Bernabe J, Ortiz J, Marin-Perez R, Skarmeta A. Enabling virtual AAA management in SDN-based IoT networks. *Sensors* 2019; 19(2): 295.

20. Liu Y, Kuang Y, Xiao Y, Xu G. SDN-based data transfer security for Internet of Things. *IEEE Internet of Things Journal* 2017; 5(1): 257–268.

21. Chaudhary R, Jindal A, Aujla GS, Aggarwal S, Kumar N, Choo KKR. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. *Computers & Security* 2019; 85: 288–299.

22. Shao Z, Zhu X, Chikuvanyanga AM, Zhu H. Blockchain-Based SDN Security Guaranteeing Algorithm and Analysis Model. In: International Conference on Wireless and Satellite Systems. Springer. ; 2019: 348–362.

23. El Houda ZA, Hafid AS, Khoukhi L. Cochain-SC: An intra-and inter-domain Ddos mitigation scheme based on blockchain using SDN and smart contract. *IEEE Access* 2019; 7: 98893–98907.

24. Navid Rajabi JQ. SDIoBoT: A Software-Defined Internet of Blockchains of Things Model. *International Journal of Internet of Things* 2019; 8: 17-26.

25. Rahman A, Islam MJ, Sunny FA, Nasir MK. DistBlockSDN: A Distributed Secure Blockchain Based SDN-IoT Architecture with NFV Implementation for Smart Cities. In: 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET). IEEE. ; 2019: 1-6.

26. Basnet SR, Shakya S. BSS: Blockchain security over software defined network. In: 2017 International Conference on Computing, Communication and Automation (ICCCA). IEEE. ; 2017: 720–725.

27. Yazdinejad A, Parizi RM, Dehghantanha A, Zhang Q, Choo KKR. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Transactions on Services Computing* 2020.

28. Faizullah S, Khan MA, Alzahrani A, Khan I. Permissioned Blockchain-Based Security for SDN in IoT Cloud Networks. *arXiv preprint arXiv:2002.00456* 2020.

29. Muthanna A, A Ateya A, Khakimov A, et al. Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. *Journal of Sensor and Actuator Networks* 2019; 8(1): 15.

30. Rahman A, Islam MJ, Montieri A, et al. SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT. *IEEE Access* 2021; 9: 28361-28376.

31. Fu X, Yu R, Wang J, Qi Q, Liao J. Performance Optimization for Blockchain-Enabled Distributed Network Function Virtualization Management and Orchestration. *IEEE Transactions on Vehicular Technology* 2020.

32. Rebello GAF, Alvarenga ID, Sanz IJ, Duarte OCM. BSec-NFVO: A blockchain-based security for network function virtualization orchestration. In: ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE. ; 2019: 1–6.

33. Rebello GAF, Camilo GF, Silva LG, et al. Providing a sliced, secure, and isolated software infrastructure of virtual functions through blockchain technology. In: 2019 IEEE 20th International Conference on High Performance Switching and Routing (HPSR). IEEE. ; 2019: 1–6.

34. Nag A, Kalla A, Liyanage M. Blockchain-over-Optical Networks: A Trusted Virtual Network Function (VNF) Management Proposition for 5G Optical Networks. In: Asia Communications and Photonics Conference. Optical Society of America. ; 2019: M4A–222.

35. Franco MF, Scheid EJ, Granville LZ, Stiller B. BRAIN: blockchain-based reverse auction for infrastructure supply in virtual network functions-as-a-service. In: 2019 IFIP Networking Conference (IFIP Networking). IEEE. ; 2019: 1–9.

36. Yang H, Liang Y, Yuan J, Yao Q, Yu A, Zhang J. Distributed blockchain-based trusted multi-domain collaboration for mobile edge computing in 5g and beyond. *IEEE Transactions on Industrial Informatics* 2020.

37. Barakabitze AA, Ahmad A, Mijumbi R, Hines A. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks* 2020; 167: 106984.

38. Xie L, Ding Y, Yang H, Wang X. Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. *IEEE Access* 2019; 7: 56656–56666.

39. Gao J, Agyekum KOBO, Sifah EB, et al. A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. *IEEE Internet of Things Journal* 2019; 7(5): 4278–4291.

40. Abdulqadder I, Zou D, Aziz I, Yuan B, Dai W. Deployment of robust security scheme in SDN based 5G network over NFV enabled cloud environment. *IEEE Transactions on Emerging Topics in Computing* 2018.

41. Mei L, Hu R, Cao H, et al. Realtime mobile bandwidth prediction using LSTM neural network and Bayesian fusion. *Computer Networks* 2020; 182: 107515.

42. Labonne M, Chatzinakis C, Olivereau A. Predicting Bandwidth Utilization on Network Links Using Machine Learning. In: 2020 European Conference on Networks and Communications (EuCNC). IEEE. ; 2020: 242–247.

43. Khangura SK, Fidler M, Rosenhahn B. Machine learning for measurement-based bandwidth estimation. *Computer Communications* 2019; 144: 18–30.

44. Ruan L, Dias MPI, Wong E. Machine learning-based bandwidth prediction for low-latency H2M applications. *IEEE Internet of Things Journal* 2019; 6(2): 3743–3752.

45. Yue C, Jin R, Suh K, Qin Y, Wang B, Wei W. LinkForecast: cellular link bandwidth prediction in LTE networks. *IEEE Transactions on Mobile Computing* 2017; 17(7): 1582–1594.

46. Verma S, others . Machine Learning in 5G Wireless Networks. In: 5G and Beyond Wireless Systems. Springer. 2021 (pp. 391–410).

47. Mohamed A, Ruan H, Abdelwahab MHH, et al. An Inter-Disciplinary Modelling Approach in Industrial 5G/6G and Machine Learning Era. In: 2020 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE. ; 2020: 1–6.

48. Morocho-Cayamcela ME, Lee H, Lim W. Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions. *IEEE Access* 2019; 7: 137184–137206.

49. Ni J, Lin X, Shen XS. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. *IEEE Journal on Selected Areas in Communications* 2018; 36(3): 644–657.

50. Rahman A, Islam MJ, Rahman Z, et al. Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium. *IEEE Access* 2020; 8: 209594–209609.

51. Rahman A, Sara U, Kundu D, et al. DistB-SDoIndustry: Enhancing Security in Industry 4.0 Services based on Distributed Blockchain through Software Defined Networking-IoT Enabled Architecture. *International Journal of Advanced Computer Science and Applications* 2020; 11(9).

52. Pritchard SW, Hancke GP, Abu-Mahfouz AM. Security in software-defined wireless sensor networks: Threats, challenges and potential solutions. In: 2017 IEEE 15th International Conference on Industrial Informatics (INDIN). IEEE. ; 2017: 168–173.

53. Dargahi T, Caponi A, Ambrosin M, Bianchi G, Conti M. A survey on the security of stateful SDN data planes. *IEEE Communications Surveys & Tutorials* 2017; 19(3): 1701–1725.

54. Xie J, Yu FR, Huang T, et al. A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. *IEEE Communications Surveys & Tutorials* 2018; 21(1): 393–430.

55. Karakus M, Durresi A. A survey: Control plane scalability issues and approaches in software-defined networking (SDN). *Computer Networks* 2017; 112: 279–293.

56. Rahman A, Chakraborty C, Anwar A, et al. SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic. *Cluster Computing* 2022; 25(4): 2351–2368.

57. Rahman A, Montieri A, Kundu D, et al. On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives. *Journal of Network and Systems Management* 2022; 30(4): 1–44.

58. Ojo M, Adami D, Giordano S. A SDN-IoT architecture with NFV implementation. In: 2016 IEEE Globecom Workshops (GC Wkshps). IEEE. ; 2016: 1–6.

59. Megyesi P, Botta A, Aceto G, Pescapé A, Molnár S. Challenges and solution for measuring available bandwidth in software defined networks. *Computer Communications* 2017; 99: 48–61.

60. Islam N, Shamim S, Rabbi MF, Khan MSI, Yousuf MA. Building Machine Learning Based Firewall on Spanning Tree Protocol over Software Defined Networking. In: Proceedings of International Conference on Trends in Computational and Cognitive Engineering. Springer. ; 2021: 557–568.

61. Khan SI, Shahrior A, Karim R, Hasan M, Rahman A. MultiNet: A deep neural network approach for detecting breast cancer through multi-scale feature fusion. *Journal of King Saud University-Computer and Information Sciences* 2022; 34(8): 6217–6228.

62. Aceto G, Ciuonzo D, Montieri A, Pescapé A. Toward effective mobile encrypted traffic classification through deep learning. *Neurocomputing* 2020; 409: 306-315.

63. Yue C, Jin R, Suh K, Qin Y, Wang B, Wei W. LinkForecast: Cellular Link Bandwidth Prediction in LTE Networks. *IEEE Transactions on Mobile Computing* 2018; 17(7): 1582-1594.

64. Rossi MA. The advent of 5G and the non-discrimination principle. *Telecommunications Policy* 2021: 102279.

65. Khan JA, Chowdhury MM. Security Analysis of 5G Network. In: 2021 IEEE International Conference on Electro Information Technology (EIT). IEEE. ; 2021: 001–006.

66. Fang D, Qian Y, Hu RQ. Security for 5G mobile wireless networks. *IEEE Access* 2017; 6: 4850–4874.

67. Dainotti A, Pescapé A, Ventre G. A cascade architecture for DoS attacks detection based on the wavelet transform. *Journal of Computer Security* 2009; 17(6): 945–968.

68. Gao S, Li Z, Xiao B, Wei G. Security threats in the data plane of software-defined networks. *IEEE network* 2018; 32(4): 108–113.

69. Hussain SR, Echeverria M, Chowdhury O, Li N, Bertino E. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. *Network and Distributed Systems Security (NDSS) Symposium2019* 2019.

70. Rahman A, Nasir MK, Rahman Z, Mosavi A, Shahab S, Minaei-Bidgoli B. DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management. *IEEE Access* 2020; 8: 140008–140018.

71. Lin D, Tang Y. Blockchain consensus based user access strategies in D2D networks for data-intensive applications. *IEEE Access* 2018; 6: 72683–72690.

72. Xu M, Zhao F, Zou Y, Liu C, Cheng X, Dressler F. BLOWN: A Blockchain Protocol for Single-Hop Wireless Networks under Adversarial SINR. *arXiv preprint arXiv:2103.08361* 2021.

73. Ibrahim RF, Abu Al-Haija Q, Ahmad A. DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. *Sensors* 2022; 22(18): 6806.

74. Sajjad SM, Mufti MR, Yousaf M, et al. Detection and Blockchain-Based Collaborative Mitigation of Internet of Things Botnets. *Wireless Communications and Mobile Computing* 2022; 2022.

75. Razmjouei P, Kavousi-Fard A, Dabbaghjamanesh M, Jin T, Su W. Ultra-lightweight Mutual Authentication in the Vehicle Based on Smart Contract Blockchain: Case of MITM Attack. *IEEE Sensors Journal* 2020.

76. Bovenzi G, Aceto G, Ciuonzo D, Persico V, Pescapé A. A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios. In: GLOBECOM 2020 - 2020 IEEE Global Communications Conference. IEEE. ; 2020: 1-7.

77. Qiu J, Grace D, Ding G, Yao J, Wu Q. Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective. *IEEE Internet of Things Journal* 2019; 7(1): 451–466.

78. Agiwal M, Roy A, Saxena N. Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 2016; 18(3): 1617–1655.

79. Fontes R, Afzal S, Brito S, Santos M, Esteve Rothenberg C. Mininet-WiFi: Emulating Software-Defined Wireless Networks. In: 2nd International Workshop on Management of SDN and NFV Systems, 2015(ManSDN/NFV 2015). IEEE. ; 2015; Barcelona, Spain.

80. Esfahani A, Mantas G, Rodriguez J, Neves JC. An efficient homomorphic MAC-based scheme against data and tag pollution attacks in network coding-enabled wireless networks. *International Journal of Information Security* 2017; 16(6): 627–639.

81. Montieri A, Bovenzi G, Aceto G, Ciuonzo D, Persico V, Pescapè A. Packet-level prediction of mobile-app traffic using multitask Deep Learning. *Computer Networks* 2021; 200: 108529.

82. Iwendi C, Maddikunta PKR, Gadekallu TR, Lakshmanna K, Bashir AK, Piran MJ. A metaheuristic optimization approach for energy efficiency in the IoT networks. *Software: Practice and Experience* 2020.

83. Selim A, Kamel S, Jurado F. Efficient optimization technique for multiple DG allocation in distribution networks. *Applied Soft Computing* 2020; 86: 105938.

84. Latif S, Idrees Z, Huma eZ, Ahmad J. Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. *Transactions on Emerging Telecommunications Technologies* 2021; 32(11): e4337.

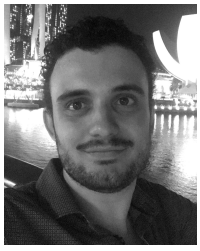
85. Hazari SS, Mahmoud QH. A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE. ; 2019: 0916-0921.

86. Aggarwal S, Kumar N. Chapter Eleven - Cryptographic consensus mechanisms - Introduction to blockchain. In: Aggarwal S, Kumar N, Raj P., eds. *The Blockchain Technology for Secure and Smart Applications across Industry Verticals*. 121 of *Advances in Computers*. Elsevier. 2021 (pp. 211-226).

AUTHORS' BIOGRAPHY

Anichur Rahman received the B.Sc. and M.Sc. degree in Computer Science and Engineering from Mawlana Bhashani Science and Technology University (MBSTU), Tangail, Bangladesh in 2017 and 2020 respectively. Currently, he is working as a Lecturer at Computer Science and Engineering (CSE), National Institute of Textile Engineering and Research (NITER), Constituent Institute of Dhaka University, Savar, Dhaka, Bangladesh since January 2020 to the present. His research interests include Internet of Things (IoT), Blockchain (BC), Software Defined Networking (SDN), Image Processing, Machine Learning, 5G, Industry 4.0, and Data Science.

Md. Saikat Islam Khan received the B.Sc. degree in Computer Science and Engineering from Mawlana Bhashani Science and Technology University (MBSTU), Tangail, Bangladesh in 2020. His research interests are Machine Learning, Computer Vision, Bioinformatics. He is also into some emerging technologies like IoT, SDN and Blcokchain.



Antonio Montieri is an Assistant Professor at DIETI of the University of Napoli Federico II. He has received his Ph.D. degree in Information Technology and Electrical Engineering in April 2020 from the same University. His work concerns network measurements, (encrypted and mobile) traffic classification, traffic modeling and prediction, and monitoring of cloud network performance. Antonio has co-authored more than 50 papers in international journals and conference proceedings.

Md. Jahidul Islam received the B.Sc. and M.Sc. degrees in Computer Science and Engineering from Jagannath University (Jnu), Dhaka, in 2015 and 2017 respectively. Currently, he is working as an Assistant Professor and Program Coordinator at Computer Science and Engineering (CSE), Green University of Bangladesh (GUB), Dhaka, Bangladesh since May 2017 to present. He is a member of Computing and Communication and Human-Computer Interaction (HCI) research groups, CSE, GUB. His research interests include Internet of Things (IoT), Blockchain, Network Function Virtualization (NFV), Software Defined Networking (SDN), 5G, Industry 4.0, Machine Learning, HCI, and Wireless Mesh Networking (WMN).

Md. Razaul Karim received the B.Sc. degree in Computer Science and Engineering from Mawlana Bhashani Science and Technology University (MBSTU), Tangail, Bangladesh in 2020. The main interests of his research are Machine Learning, Computer Vision, and Image Processing. He is also keen on Blockchain.

Mahedi Hasan received M.Sc. in Database Technology from Saint Petersburg State University, Russia in 2016 and the B.Sc. (Engg.) degree in Information and Communication Technology from Mawlana Bhashani Science and Technology University (MBSTU), Tangail, Bangladesh in 2012. Currently, he is working as a Lecturer at Computer Science and Engineering (CSE), Jashore University of Science and Technology University (JUST), Jashore, Bangladesh since March 2020 to present. His research interests are Bayesian Inference, Data Science, Machine Learning (ML) and Natural Language Processing (NLP).

Dipanjali Kundu received the B.Sc. degree in Computer Science and Engineering from Chittagong University of Engineering and Technology (CUET), Bangladesh in 2018. Currently, she is working as a Lecturer at Computer Science and Engineering (CSE), National Institute of Textile Engineering and Research (NITER), Savar, Dhaka, Bangladesh since January 2020 to present. Her research interests include Machine Learning, Human Computer Interaction, Internet of Things (IoT), Blockchain (BC), Software Defined Networking (SDN) 5G, Industry 4.0 and Robotics.

Mostofa Kamal Nasir is a Professor of Computer Science and Engineering of Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. He has completed his PhD from University of Malaya, Kuala Lumpur, Malaysia in the field of Mobile Adhoc Technology in 2016. Before that he has completed his BSc and MSc in Computer Science and Engineering from Jahangirnagar University, Bangladesh. His current research interest includes VANET, IoT, SDN and WSN.

Antonio Pescapè is a Full Professor of computer engineering at the University of Napoli Federico II. His work focuses on measurement, monitoring, and analysis of the Internet. He has co-authored more than 200 conference and journal papers, he is the recipient of a number of research awards. Also, he has served as an independent reviewer/evaluator of research projects/project proposals co-funded by a number of governments and agencies.

How to cite this article: Rahman A., Khan Md. S. I., Montieri A., Islam Md. J., Karim Md. R., Hasan M., Kundu D., Nasir M. K., and Pescapè A. (2024). BlockSD-5GNet: Enhancing Security of 5G Network through Blockchain-SDN with ML-based Bandwidth Prediction. *Trans Emerging Tel Tech. 2024;35(4):e4965*. doi: 10.1002/ett.4965.