IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON BLOCKCHAIN TECHNOLOGY: PRINCIPLES AND APPLICATIONS

Received July 11, 2020, accepted July 28, 2020, date of publication August 5, 2020, date of current version August 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3014356

Block5GIntell: Blockchain for AI-Enabled 5G Networks

ABIR EL AZZAOUI[1], SUSHIL KUMAR SINGH[1], YI PAN[2], (Senior Member, IEEE), AND JONG HYUK PARK[1], (Member, IEEE)

[1]Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul 01811, South Korea
[2]Department of Computer Science, Georgia State University, Atlanta, GA 30302-5060, USA

Corresponding author: Jong Hyuk Park (jhpark1@seoultech.ac.kr)

This work was supported by the Advanced Research Project funded by the Seoul National University of Science and Technology (SeoulTech).

ABSTRACT Nowadays, 5G network is considered to be one of the main pillars of various industries, including the Internet of Things (IoT), smart cities, virtual reality, and many more. Unlike previous network generations, 5G utilizes complex digital technologies such as massive Multiple Input Multiple Output (mMIMO) and runs over higher radio frequencies. The introduction of new technologies and advanced features in the 5G network raises new challenges for network operators, and merging Artificial Intelligence (AI) is one of the effective solutions to address these complexities. However, AI-enabled 5G network engenders security concerns and requires improvement to meet the standardization and qualification of the new network generation. To mitigate these dilemmas, Blockchain must be integrated. Blockchain, as a decentralized methodology provides a secure sharing of information and resources among various nodes of 5G environments. Blockchain can support other technologies, such as AI-based 5G, to create smarter, more efficient, and secure cellular networks. In this article, we present a comprehensive intelligence and secure data analytics framework for 5G networks based on the convergence of Blockchain and AI named ''Block5GIntell''. We depict the applications of Blockchain and AI on 5G networks separately and we argue on the support that Blockchain can provide for AI to create smart and secure 5G networks relying on our proposed framework. To support our proposition, we present an energy-saving case study using Blockchain for AI-enabled 5G. The simulation shows an overall 20% decrease in energy consumption at the RAN level.

INDEX TERMS 5G networks, artificial intelligence, blockchain, smart contract, security, and privacy.

I. INTRODUCTION

Compared with earlier generations of wireless communication technology, the rationale for 5G development is to expand mobile networks' broadband capability and allow the migration of all the services depending on a fixed connection, into ubiquitous mobile connectivity. The new generation of networking enhances mobile broadband, supports massive machine type communication, and provides an ultra-reliable and low latency communications [1], [2]. 5G networks adopt five key technologies, including massive multiple-input multiple-output, radio access technology, Ultra-Dense Network (UDN), channel coding and decoding, and millimeter-wave access [3]–[5]. These technologies improve the notion of network slicing and virtualization to fit into the feasibility of operating different services on the same infrastructure. 5G networks certainly revolutionize networking technology and successfully embrace large-scale applications such as IoT, smart cities, virtual reality, and many more. However, the advancement of 5G networks raises multiple concerns. The massive number of Machine-Type-Communication (MTC) devices adds more intricacy to the UDN as it requires the achievement of high availability, reliability, security, and a very low latency [6]–[9]. Besides, 5G radio technology operates on higher frequencies, which creates a convoluted antenna configuration and uses more sophisticated connectivity mechanisms. Additionally, at the level of network and service design, unlike the previous generations, 5G new radio has new layers of complexity that require analytical capabilities and fast responsiveness, which goes beyond what human power can provide. Conjointly, assuring the performance of different applications such as the Industrial Internet of Things

The associate editor coordinating the review of this manuscript and approving it for publication was Wenbing Zhao.

(IIoT), e-Health systems, and smart cities require continuous network monitoring and optimization.

To mitigate these problems, numerous researches propose to merge Artificial Intelligence (AI) and its subcategories such as Reinforcement Learning (RL), Deep Learning (DL), supervised and unsupervised learning, and Natural Language Processing (NLP) with 5G networks.

In fact, 70% of network operators are testing AI's feasibility for 5G networks and planning to fully integrate it by the end of 2020 [91]. The merge of AI creates a smart and optimized 5G network; however, the centralized nature of AI brings up numerous security concerns and complications. AI is designed to collect and analyze a massive amount of data generated by the network's components. Hence, it creates more considerable computational complexity and makes it arduous to be applied to the real-word latency-intolerant 5G-based applications. Moreover, the collected data embrace sensitive personal information (i.e.; user's identification, user's location). The above-mentioned information and many others are subject to various attacks, and it must be securely protected from any possible leaking. Fortunately, Blockchain as a distributed ledger is capable to unscrambling these obstacles. Abundant states-of-art examined the benefits of Blockchain on 5G networks such as security, reliability, immutability, and permanence. Still, only a few of them have considered merging Blockchain with AI for a smart and secure 5G network.

Our paper focuses on the integration of three leading-edge technologies of today. We review the studies conducted on Blockchain for 5G and AI for 5G separately alongside our vision of merging Blockchain with AI for 5G networks. We analyze the benefits of this convergence on 5G networks and beyond to create a smart, optimized, and secure network that is a pillar of the digital transformation of millions of applications and businesses around the globe.

To this end, we have examined and studied 150 papers and articles regarding Blockchain for AI, Blockchain for 5G, and AI for 5G. We tried to eliminate old publications and focus more on 5G related solutions and challenges, which lead us to 90 states-of-art and literature reviews. To organize and structure our study, we formed six Research Questions (RQ) depicted as follows:

RQ1: What are the significant challenges facing 5G networks?

RQ2: How can these challenges be approached by AI?

RQ3: How can these challenges be approached by Blockchain?

RQ4: What are the concerns of only using AI to approach these challenges?

RQ5: What are the concerns of only using Blockchain to approach these challenges?

RQ6: How can Blockchain support AI to efficiently mitigate these challenges and create a smart and secure 5G network?

Based on the above-mentioned questions, we organized the collected papers and articles into four categories:

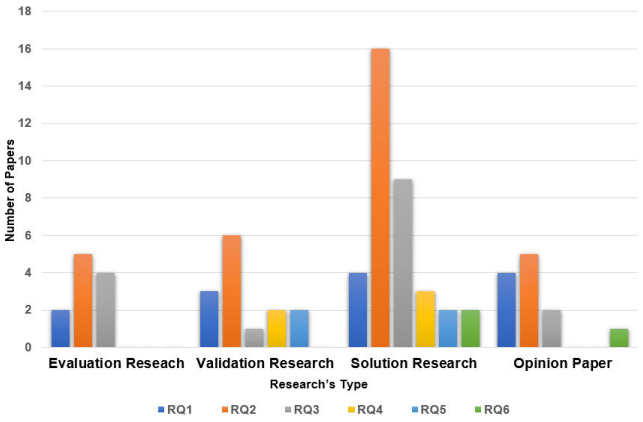


FIGURE 1. Visualization of a Systematic Mapping Study.

1) Evaluation research: Researches that practically measure the implementation of Blockchain for 5G and/or AI for 5G networks and show its consequences and drawbacks.

2) Validation research: Researches that investigate novel techniques on 5G networks and validate them through experiments.

3) Solution research: Researches that propose a solution to existent problems regarding 5G. These solutions can be either novel or significant extension of an existing technique.

4) Opinion research: Researches that review and survey other state-of-art works and presents a summarized technical opinion.

Tables 1, 3, and 4 summarize those papers and categorize them based on their contribution. Figure 1 presents a visualization of the systematic mapping study used in our paper.

Research contribution: The main contributions of our paper are as follows:

1) We present a comprehensive intelligence and secure data analytic framework named "Block5GIntell" on the convergence of Blockchain and AI for 5G networks, which supports the development of a novel methodology for decentralized, distributed, and immutable smart applications.
2) This article presents high-level taxonomies of Blockchain and AI for 5G with existing state-of-art techniques and applications.
3) We discuss the benefits of Blockchain and AI for 5G networks separately while covering performance and security issues. We argue as well in this article on the support of Blockchain for AI-Enabled 5G networks.
4) We demonstrate the potency of our concept by providing an overview framework and an energy-saving study-case to evaluate the proposal.
5) We discuss the open research challenges of using Blockchain and AI for 5G in terms of security and performance issues.

The rest of the paper is organized as follows: In Section 2, we present a general overview of Blockchain, Artificial Intelligence, and 5G networks as well as the related works regarding Blockchain and AI for 5G networks. Section 3 discusses

TABLE 1. Contribution of our study related to existing research.

Research Work	Year	AI for 5G	Blockchain for 5G	AI and Blockchain for 5G	Key Technologies	Consideration
Porambage et al. [19]	2019	Yes	Limited	Limited	EdgeAI, Beyond5G	Security
Chen et al. [20]	2018	No	Yes	No	Improved Byzantine Fault Tolerance Algorithm	Security, Latency, and Authentication
Ortega et al. [21]	2018	No	Yes	No	Permissioned Blockchain and Smart Contract	Security, Privacy and Latency
Nour et al. [22]	2019	No	Yes	No	Smart Contract	Security and Privacy
Li et al. [23]	2017	Yes	No	No	Kalman Filtering, K-means, Markov Chain, and Reinforcement Learning	Enhance Self-Organization, and Reduce Latency
Yang et al. [24]	2017	No	Yes	No	Zero-Knowledge Proof, Public Blockchain	Trust access, Privacy, Credibility, Low Network Cost, and Enhance Radio Frequency
Jangirala et al. [25]	2019	No	Limited	Limited	Lightweight Blockchain	Security, Immutability, Traceability, QoS
Balevi et al. [26]	2017	Yes	No	No	Unsupervised Learning and K-mean Soft Algorithm	Reduce Latency
Sciancalepore et al. [27]	2019	Yes	No	No	Reinforcement Learning, Unsupervised Learning	Optimization and Resources Management
Ibarrola et al. [28]	2018	Yes	No	No	Supervised and Unsupervised Learning,	Enhancing QoE, QoS Management Model, Detecting Anomalies, and Enhancing Channel Selection
Valtanen et al. [52]	2018	No	Yes	No	Consensus Algorithms, Smart Contract	Supporting 5G' Network Slice Broker, Continuous Testing, Resource-Crowd Sourcing, Sorting, Prospecting, Grafting and Streamlining
Bogale et al. [29]	2018	Yes	No	No	Machine Learning, NLP, Graph Theory and Markov Chain Model	Network Planning Optimization, Energy Efficient, Security, and Context Aware-Data Transmission
Prez-Romero et al. [59]	2016	Yes	No	No	Classification, Prediction, and Clustering	Self-Organized Network (SON)
Jiang et al. [55]	2016	Yes	No	No	Supervised and unsupervised learning, Unsupervised Bayesian Learning, and K-means Clustering	Energy Prediction, Channel Estimation, and Resource Allocation
Kafle et al. [61]	2018	Yes	No	No	Reinforcement Learning	Planning and Design, Network Slicing, and Security
Lee et al. [33]	2019	No	Yes	No	Proof-of-Work	Security and Performance
Messié et al. [34]	2019	No	Yes	No	Proof-of-Bandwidth	Enhance QoS and QoE
Dinesh et al. [35]	2019	No	Yes	No	Consensus Protocols	Security of Communication
Zhang et al. [36]	2019	Yes	Yes	Yes	Deep Reinforcement Learning and Blockchain	Resource Scheduling and Resource optimization
Dai et al. [37]	2019	Yes	Yes	Yes	Deep Reinforcement Learning and Content Caching Blockchain	Resource Management and Network Flexibility
Our Contribution	2019	Yes	Yes	Yes	Blockchain Techniques and AI Techniques	Network Performance, Security and Privacy

the convergence of Blockchain and AI into 5G separately. Section 4 presents our contribution identified as Blockchain for AI-enabled 5G networks. In this section, we include a comprehensive framework, an analyzed discussion supported by a summarized taxonomy, a qualitative, and a quantitative analysis to evaluate our proposed framework. Section 5 discusses some open research challenges. Finally, we conclude this work with a summary in Section 6.

II. BACKGROUND

In this section, firstly we cover an overview of Blockchain, 5G, and Artificial Intelligent. Secondly, we present a comprising table summarizing the related works.

A. BLOCKCHAIN

Blockchain is a chain data structure. Each data composes a block where all the created blocks are sequentially connected in chronological order. Blockchain is a cryptographically guaranteed neither non-falsified nor modified distributed ledger technology. Blockchain networks have a small-world model that can maintain network stability in case of node changes, integrity, and consistency of the transacted data. Despite its short history, blockchain has been rapidly developed and gained the trust of various applications. The investment in blockchain is expected to reach 2.3 billion in 2021. Apart from its financial uses such as Bitcoin and similar applications, Blockchain has proved its role as a secure

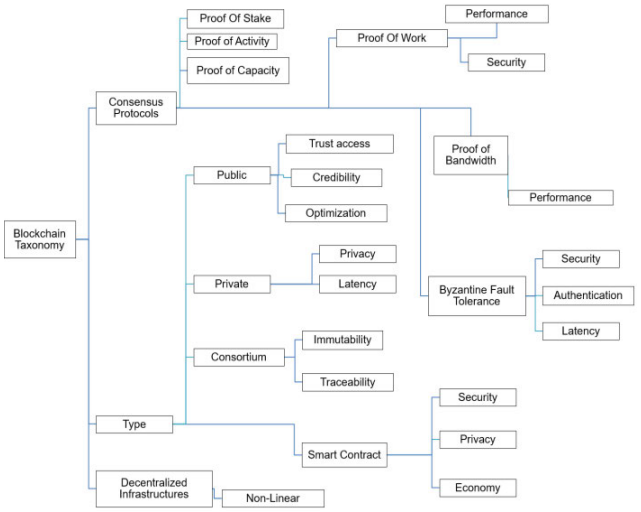


FIGURE 2. High-Level Taxonomy of Blockchain for 5G networks.

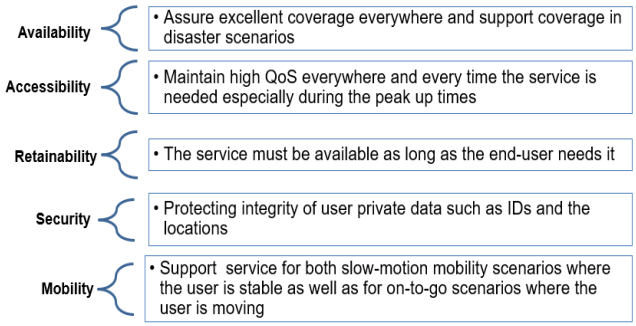


FIGURE 3. Key Performance Indicators in 5G.

and decentralized database. Blockchain technology can be merged into numerous non-financial applications, including networking. The decentralized storage in blockchain is used for storing a large amount of data, which links the current block to the previous one by smart contract code [13]. The decentralized and secure nature of blockchain makes it a promising solution for the 5G network. Blockchain protocols, including proof-of-work, proof-of-bandwidth, Byzantine Fault of Tolerance, and many more can improve the performance and security of 5G networks as we will discuss in the third section. Moreover, Blockchain technology engenders four main types that could enhance privacy, security as well as optimization for 5G networks. Figure 2 presents the taxonomy of feasible Blockchain categories that could be applied to 5G networks.

1) CONSENSUS PROTOCOLS

The key contribution of Blockchain is the consensus algorithm. It decides how the agreement will be made to append a new block between all nodes in the network [14].

2) DECENTRALIZED INFRASTRUCTURES

Blockchain was originally designed as a linear infrastructure based on the linked data structures and hashing strategies [15]. However, recently, the non-linear infrastructures are being used for real-time applications as it can handle big databasing on graph theory and queuing information models, which makes it perfect for the 5G network's latency-intolerant applications.

3) TYPES OF BLOCKCHAIN

We can distinguish four types of Blockchain; public or permission-less Blockchain, where anyone can join the network and participate as any other node. Private or permissioned Blockchain where a certain entity makes a restriction. The smart contract that executes the acts included automatically once the conditions are fulfilled without the intervention of a third party. And finally, the consortium Blockchain or semi-decentralized Blockchain; unlike the private Blockchain, the consortium Blockchain is controlled by a group of approved entities and not just one, thus ensuring the privacy of the network as well as its security.

In 5G networks, each type of Blockchain is deployed differently for several reasons and has different outcomes.

B. 5G NETWORK

5G network is evolving rapidly across a broad technological environment, including virtualization, IoT, and Industry 4.0 [12]. The number of connected devices in 2018 reached 22 billion devices, and this number is expected to increase up to 50 billion by 2030 [16]. Alongside the continuous growth of applications and devices relying on the telecommunication network, a need to evolve the concept of wireless connectivity to the fifth generation of mobile technology was created. 5G enables new ways to define performance monitoring and assurances as well as enhancing Quality of Service (QoS) and Quality of Experience (QoE).

The QoS/QoE of the advertised service should be consistent with the QoS/QoE of the delivered service and should be the same for each user [17-18]. To achieve the QoS/QoE required from the 5G network, five main Key Performance Indicators (KPI) shall be considered, including availability, accessibility, retainability, security, and mobility. Figure 3 summarizes 5G's KPI. With those considerations, 5G will be able to support various real-world applications and enhance their performance. Assuring the KPI requirements allows fast and secure real-time data transmission. Thus, making 5G a fundamental technology for the development of smart city applications [38] Machine-to-Machine communication, virtual reality as well as mission-critical applications such as V2X and e- Healthcare systems.

C. ARTIFICIAL INTELLIGENT

Artificial Intelligence (AI) is the science that aims to develop machine systems toward the same intelligence as a human mind [39]. It is used to solve complex problems automatically and undependably from human intervention [40]. The taxonomy in Figure 4 presents two main AI's subcategories that can be deployed to enhance 5G networks. We briefly explain in this section the role of each method.

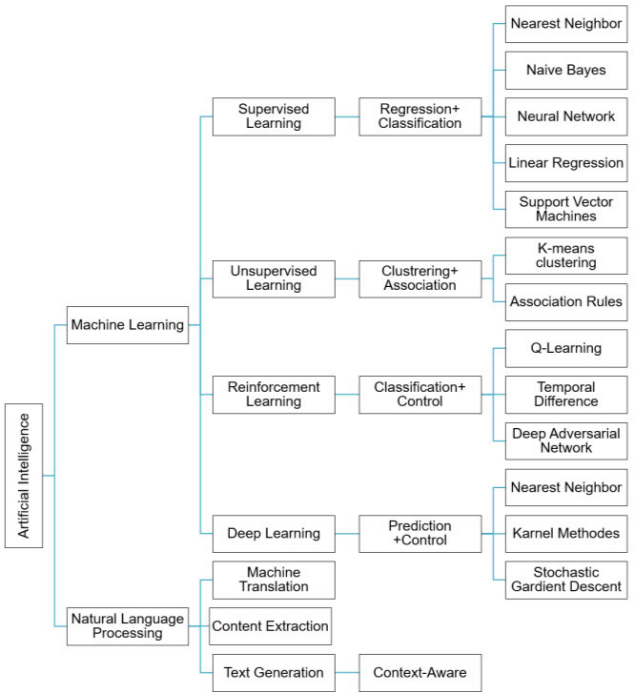


FIGURE 4. High-Level Taxonomy of AI techniques for 5G.

1) SUPERVISED LEARNING

The supervised learning can be used to explain the relationship between a giving input and output to deduct the primary function [41] This function can be used to make future predictions based on the learned patterns.

2) UNSUPERVISED LEARNING

Unsupervised Learning aims to find similarities between input values and a similar group of data into clusters [42].

3) REINFORCEMENT LEARNING

In reinforcement learning, there is no input nor output data; the learning is consummated through experience relying on a trial-and-error model to learn to obtain a reward.

4) DEEP LEARNING

Deep learning can conduct unsupervised learning from unstructured and unlabeled data, imitating by that the human brain functions [93]. Because of the interventional optimization of deep learning algorithms, artificial intelligence has made great breakthroughs in many aspects [43].

5) NATURAL LANGUAGE PROCESSING

Natural Language Processing (NLP) makes it possible for computers to interact with a human using a natural language, NLP can understand, decipher and make sense of human language in a valuable way [44]. The summary of existing papers is shown in Table 1.

III. THE CONVERGENCE OF BLOCKCHAIN AND AI FOR 5G

This section covers the applications of Blockchain for 5G and AI for 5G separately. We discuss the convergence as well of Blockchain with AI-enabled 5G networks. Our concept is supported by an overview framework named Block5GIntell that explains the way Blockchain can support AI to create a full endorsement to 5G networks. We describe the benefits of this framework in our provided taxonomy.

A. BLOCKCHAIN FOR 5G NETWORKS

Blockchain techniques can fully assist 5G's authentication security, communication security, and network coding security as well as establishing new economic benefits for 5G operators and providers [45]. We explain those points in detail in this section.

1) SECURE AUTHENTICATION

5G networks face several authentication issues, from the frequent authentication applied in Ultra-Dense Network (UDN) to the authentication vulnerability such as key derivation scheme [10]–[11]. These dilemmas expose the network to attackers and increase the latency. Fortunately, Blockchain can mitigate these problems. Blockchain Byzantine Fault tolerance consensus protocol mechanism can generate a group of trusted Access Points to share the authentication result with [20]. Hence, reducing the authentication frequency and securely enhancing the response time. Since, the User Equipment (UE) will be moving between different APs and knowing that the physical security environment of AP is complex and different. The risk of connecting to a malicious or illegal AP is higher. Thus, securing the fast authentication to the AP is critical in the UDN environment. The approach presented by Chen *et al.* [20] tried to solve this problem by performing an optimized Byzantine fault Tolerance algorithm with a reverse screening method to enhance the accuracy of joined APs and improve access efficiently.

In a supply chain environment, real-time transmitted data between different departments need to be secured. 5G- enabled IoT in mobile edge computing is intended to cover this issue. Jangirala *et al.* [25] propose a lightweight Blockchain-Enabled RFID based authentication. RFID enabled devices to deal with sensitive information such as passports and identity documents. These data are exposed to cyberattacks threats in the case of real-time applications and health care monitoring systems. The proposed scheme called LBRAPS is based on bitwise exclusive-or (XOR), one-way cryptographic hash, and bitwise rotation operations only.

LBRAPS will provide a secure, shared authentication between different departments, all while considering different threat models such as:

1) Dolev-Yao: An adversary can eavesdrop the communicated messages as well as modify, delete, or insert fake messages in between the messages [46].

2) Impersonation Attack: An adversary can successfully impersonate one of the legitimate parties in a communication protocol using their identity.

3) Replay Attack: A valid data transmission is maliciously repeated or delayed.

4) Man-in-the-Middle Attack: The attacker gets between two parties in a communication scenario and reads, modifies, or deletes the communicated messages. While those two parties believe that they are directly communicating with each other.

5) Ephemeral Secret Leakage Attack: Compromises the private keys of clients and the session key by an adversary from eavesdropped messages [47].

The authentication protocol proposed will handle the problems related to blockchain-enabled RFID based authentication for supply chains in the 5G mobile edge computing environment. It is proved to be efficient in communication and computation as well as supporting security and functionality features. Moreover, the centralized access authentication in a cloud radio access network is performed in the mobile core network. This fact causes an extremely high operating and capital expenditure for the network. To mitigate this problem, Blockchain-based Trusted Authentication (BTA) architecture for 5G using the Blockchain-based Anonymous Access (BAA) scheme in cloud radio over fiber network can be used [24]. This approach is based on the public blockchain platform and Zero-knowledge proof protocol for reference in C-RoFN. The proposed solution can eliminate the unified authentication in the core network and introduce decentralized tripartite agreement with the blockchain consensus platform. As a result, radio resources can be optimized, access and authentication can be secured, and the cost can be lowered.

2) SECURE COMMUNICATION

5G network, with its ultra-low latency, comes to support new use cases such as the sully autonomous vehicle [48]. However, the cybersecurity of V2V communication is not fully covered, as the risk of losing control over a vehicle is possible. Creating a Permissioned Blockchain can mitigate this issue [21]. In this approach, when a new vehicle enters the network, it can immediately start sending information and communicate with other vehicles by using its private key to add a digital signature to all its transmitted messages. The receivers by their role will verify the accuracy of the information by comparing their estimation with the provided information and add their review to the shared ledger. Hence, if a vehicle has received different reviews from different participants, which confirm its validity, this confirmation could be added as a secure node in the blockchain. Thus, the blocks of generated transactions are affirmed to be trustable, and the 5G-based Vehicle-to- everything (v2x) and vehicle-to-vehicle (V2V) communication and is conducted anonymously and securely.

3) SECURE NETWORK CODING

A scalable bandwidth offers a high data rate and meets end-to-end QoS requirements [49]. Network Coding is a key enabler for scaling bandwidth and optimizing energy consumption in the UDN environment. However, before moving to the phase of network coding and adaptation in 5G network deployment, the security vulnerabilities need to be considered [50]. Adat *et al.* [51] considered this issue and proposed a blockchain-based message authentication scheme, which can minimize the delay and signaling costs, all while studying the performance of Random Linear Network Coding for wireless mobile networks. Network coding is vulnerable to pollution attacks, threatening the correct reconstruction of the original information and deteriorate the overall 5G network performance. To this end, the authors suggested the use of homomorphism hash function and signature of each block. They eliminated the polluted nodes with the help of Blockchain distributed ledger of immutable encrypted values.

4) RESOURCE CONFIGURATION FRAMEWORK

The resource configuration framework is designated for organizing, designing, and orchestrating the firm's resources regarding 5G's sub-slicing. Valtanen *et al.* [52] presented an analyzed study about the value creation process by describing resource configuration micro-processes and explaining the way Blockchain could facilitate the implementation of these processes based on previous studies. As a case study, they assessed the features of the broker/ledger concept against the blockchain capabilities to find the most appropriate values creation micro-processes and roles for the broker/ledger. According to this study, Blockchain can potentially be beneficial in the following areas:

- *Continuous Testing:* Firms should continuously test their offerings for 5G sub-slices and adjust them accordingly; Blockchain can be used to automate offer modifying processes based on the parameters stored in a shared ledger.
- *Resource Crowdsourcing (RC):* RC creates value by collecting distributed under-utilized resources to reach a scale. Blockchain facilitates the resource crowd-sourcing process by providing a trusted environment with lower transaction costs. Based on that, 5G's network operators can manage to get the best offer from the network's sub-slices' service offers.
- *Sorting:* Sorting brings value by categorizing resources to enable effective matching between 5G networks' needs and offered resources. However, the sorted data is exposed to security risks such as leaking of stakeholders' identity. To mitigate this issue Blockchain, homomorphic encryption can be used to allow data analytics and computations to be run over encrypted data without revealing data's sensitive information. Homomorphic encryption technology includes partially homomorphic and fully homomorphic; however, the fully homomorphic encryption is not practical [53].
- *Prospecting:* Firms try to predict the 5G network's resource needs and controllers' expectations, the prediction made is based on previously generated data, and at this point, Blockchain can be used to securely store those data and provides it to an AI system to analyze it and extract future predictions from it.

TABLE 2. Summary of Blockchain applications on 5G networks.

Area of use	Description	Solution	References
Secure Authentication	Frequent authentication and authentication' security vulnerabilities make the network prone to latency and exposed to security threats	Blockchain Byzantine Fault of Tolerance consensus algorithm, lightweight Blockchain-Enabled RFID based authentication, Zero-knowledge proof protocol	[20], [24]
Secure communication	Due to 5G heterogeneous nature, communication between connected entities should be secure from any potential attack and sensitive information' leaking	Permissioned Blockchain	[21]
Secure Network Coding	Network Coding is vulnerable to *pollution attacks*	Blockchain homomorphic hash function	[51]
Economy	Network slicing procedure and data generation and storage costs are relatively expensive	Smart contract, Blockchain homomorphic encryption	[52]

- *Grafting:* Grafting tries to couple hetero unconnected resources and 5G network operators' needs to produce novel complementarities. Large datasets can help in finding unique business combinations and crowd-sourcing of human intelligence in business process development can produce valuable results, and as it is known, Blockchain can efficiently enhance the crowd-sourcing process by generating a reward mechanism; those who contribute the most get the bigger reward.
- *Streamlining:* Streamlining is a method used by firms to reduce the incompatibilities and uncertainties that the grafting process may create. Blockchain can contribute by facilitating rapid experiments.

Based on this analysis, blockchain proves to have a huge impact on the network's economic system. Especially, in the 5G area where the notion of network slicing is a key performance to the network. Blockchain can enable the storage of various needs from vertical industries and applications. Moreover, a smart contract can automate negotiation, which will efficiently reduce transaction costs. The data stored in the blockchain can be used anonymously later to streamlining the services created in the Grafting process.

Blockchain's smart contract can be used as well to secure contract negotiation between 5G network slice providers and the network provider; Nour *et al.* [22] proposed a Blockchain-Based network slice broker for 5G services. The scheme presented will announce an anonymous request to receive the necessary resources to build an end-to-end network slice. The approach promised secure auctions and trading, secure end-to-end slicing, and anonymous transactions using smart contracts. Table 2 presents a summary of the above-mentioned related works.

B. ARTIFICIAL INTELLIGENT FOR 5G NETWORKS

A fully operating network ought the support of AI; 5G can benefit from the assistance that AI could generate to enhance the network performance and security. We present in this section a detailed explanation about the impact of AI on 5G network components, performance, security, and privacy.

1) MASSIVE-MIMO

Massive MIMO or (mMIMO) is a key 5G network's enabler as it allows the base station to be equipped with numerous antennas, which are several orders of magnitude higher than the number of antennas in the previous network generations. The mMIMO grants the service to multiple users simultaneously on the same time-frequency resources [54]. Since the mMIMO system is associated with hundreds of antennas, detection and channel estimation can lead to a high-dimensional search problem [55]. In a wireless system, all communications pass by a channel between the sender (base station, access point) and the receiver (user equipment). The communication signals are coded, and a noise is added by the channel. The characteristics of the channel where the signal has passed through must be revealed using channel estimation techniques to decode the signals without errors. And to enhance transmission efficiency, avoiding repeated channel estimation is highly required. To mitigate this problem, Principal Component Analysis (PCA) and Independent Component Analysis (ICA) are used to reducing channel estimation during the transmission scenarios between smart utility meters and power utility stations [56].

PCA and ICA are capable of blindly separating signals before the decoding phase, which will enhance efficiency and security by eliminating wideband interference and Jamming signals [55]. Furthermore, the Hierarchical version of Support Vector Machine (H-SVM), a powerful binary classification mechanism, can be deployed [32]. Using this function, even the simplest information will be enough to perform the task of estimation due to the capability of H-SVM to transform the various types of network information into the feature space.

The authors also used a parallel learning algorithm to reduce memory space and computational power to make it easily adopted by high mobility users. A pilot contamination problem happens when two terminals use the same reference signal known as the pilot, to solve this dilemma. Bayesian Learning technique can be used to detect the channel parameters of the desired links in a target cell, and the sparse channel components can be reconstructed using a small number of observations [57].

2) NETWORK PLANNING

In 5G networks, one of the most effective costs saving way is to automate network designs by applying software planning tools. AI can be very advantageous in this case, Poon *et al.* [58] proposed an AI-based system that can automate and optimize the planning process using graph theory-based problem formulation, Mixed Integer Linear Programming (MILP), Ant Colony Optimization (ACO) and Genetic Algorithms (GA). In other approaches, AI can be used to fix 5G's Radio Access Network (RAN) complexity. AI's classification, prediction, and clustering models can be deployed to create a Self-Organizing 5G Network (SON) [59]. SON mainly has three functions: Automating the resource's allocation decision in Self-Planning function, improving and maintaining the network performance in terms of coverage using the Self-Optimization function. It is keeping the network operational and preventing disruptive problems from arising using the Self-Healing function.

3) NETWORK OPTIMIZATION

AI techniques could efficiently serve network optimization, notably AI-Natural Language Processing NLP. Understanding network context will help reducing radio resources used for information transition. For example, a base station can transmit only the coded information's contextual data instead of full-text information to the user equipment, and the UE, by its turn, decodes the text and extract the exact information [29]. Generally, they are two approaches to summarize the data context: using new expressions to express the context in the Abstractive approach, or deploying only the original context in the Extractive approach. However, summaries generated by these approaches may lack logical coherence [60].

Pellet reasoner can be deployed as well to support debugging for ontology [30]. Using NLP can intensively reduce network traffic and improve the Quality of Service desired. Towards another approach and to optimize the network, reinforcement learning methods can be used as well to decrease the number of resources and determine the value of parameters for an optimal network slice setup [61].

4) LATENCY OPTIMIZATION

Predicting computational resources based on historical data using machine learning will permit the network to schedule the resources in advance, hence reducing global latency. Furthermore, in fog enabled wireless systems, numerous machine learning techniques including incremental learning, divide-and-conquer, parallelization, sampling, granular computing, feature selection, and hierarchical classes for big data analytics can be used to achieve awareness at edge network [62]. Deploying AI can allow the smart use of different Radio Access Technology; the base station can learn when to transmit and on which type of frequency band based on the network condition. While heterogeneous learning models can be used to identify the unused spectral slot, elect from it a sub-channel and configure the terminals [63]. Other methods, including Support Vector Machine (SVM), gradient boosting decision tree, and spectral clustering, can be used as well to meet latency and bandwidth requirements for 5G [61]. These methods will noticeably reduce the latency and enhance the Quality of Service.

5) ENERGY EFFICIENT

The RAN consumes over 80% of wireless network power. Especially at the base station as it stays active regardless of the variation of traffic loads. The continuous growth of IoT devices in both numbers and requirements makes current energy planning incompetent for future applications such as smart cities [60]. The need to create a green communication rises, and AI can fulfill it [65]. Autonomous network equipment controlling such as servers based on AI can be used to optimize energy consumption [31]. Using predictive models, including neural network and Markov decision, can create wireless power transfer for IoT devices in smart cities [64]. In contrast, Li *et al.* [23] merged the prediction and reasoning modules to propose a traffic-aware greener cellular networks by using Markov chain to model possible traffic load variation and applied branch-and-bound algorithm to determine the appropriate base station's switching policy. The proposal module can estimate traffic load based on the online experience, and then select the feasible base station switching operation. Based on SDN controllers' feedbacks, the reciprocal cost will be acknowledged, and the AI center would learn which base station's switching operation to be used for one specific traffic load profile. Similarly, Trivedi *et al.* [66] proposed an energy harvesting for a communication network that relies on SDN.

To realize the same goal and to optimize energy consumption in mobile devices, linearization techniques are used to remove the complex computations and reduce energy consumption [67]. Moreover, supervised machine learning techniques including variants of linear discriminant analysis, linear logistic regression, non-linear logistic regression with neural networks, k-nearest neighbor, and support vector machines can be used to predict device wireless data and location interface configurations. The results prove that AI can improve an average of 24% of energy-saving [68].

6) NETWORK MANAGEMENT

To achieve a high throughput of packet processing, controlling heterogeneous network traffic is fundamental. In this case, Deep Learning can be very effective [69]. Based on the number of configurable parameters (over 2000), reinforcement learning must be adopted to create a smart network reconfiguration [61].

7) SECURITY

Wireless communication systems have been prone to security vulnerabilities from the very inception;

Therefore, it is crucial to highlight the security challenges and propose vigorous solutions [70]. Fortunately, AI can bring its benefits to secure the 5G network. Using

TABLE 3. Summary of artificial intelligent for 5G networks.

5G Network related problem	Description	Solution	References
Massive-MIMO	Channel Estimation and High-Dimensional Search Problems	PCA, ICA, H-SVM and Parallel Learning Algorithm	[54-56]
	Pilot Contamination Problem	Bayesian Learning Technique	[57]
Network Planning	Automate and Optimize the Planning Process	Graph Theory, MILP, ACO, GA	[58]
	Fix RAN Complexity	Classification, Prediction, and Clustering	[59]
Network Optimization	Understanding Network Context	NLP, Pellet Reasoner	[29-30]
	Optimal Network Slice	Reinforcement Learning	[61], [85]
Latency Optimization	Predicting Computational to Schedule the Resources in Advance	Incremental Learning, Divide-and-Conquer, Parallelization, Sampling, Granular Computing, Feature Selection, and Hierarchical Classes	[62], [86-87]
	Smart Use of RAT	heterogeneous learning models	[63]
Energy Efficient	Create a Green Communication	Neural Network and Markov Decision	[23],[31], [64]
	Predict Device Wireless Data and Location Interface Configurations	Variants of Linear Discriminant Analysis, Linear Logistic Regression, Non-Linear Logistic Regression with Neural Networks, K-nearest Neighbor, and Support Vector Machines	[68]
Network Management	Controlling Heterogeneous Network Traffic	Machine learning, and Deep learning	[69], [84], [88]
	Smart Network Reconfiguration	Reinforcement Learning	[61]
Security	Detection of Instruction and Spoofing Attacks	Unsupervised Learning, Random Key Distribution, and AIS	[61], [71]
Quality of Experience	Understanding User's Behavior and Enhancing QoE	Supervised Learning, Unsupervised Learning	[42], [28]

unsupervised learning techniques to analyze the traffic can help in the detection of instruction and spoofing attacks by statistically identifying unusual behavior from the system operation data [61]. Following the same context, a random key distribution based Artificial Immune System (AIS) has been proposed to create a spoofing attack detection scheme with a rate above 90%. The technique used is a random key hopping based approach. The randomness creates difficulty in altering the network operation by spoofing unwanted packets as the malicious nodes will be unaware of it [71]. The security issues arise in the context of Mobile Ad-hoc Network (MANET) in 5G, which is a radio system aimed at extremely high data rates and lower latency, energy, and cost [72].

Barani [73] proposes an approach based on the Genetic Algorithm (GA) and AIS called (GAAIS). This solution can secure the network by creating dynamic intrusion detection in MANET. Applying this approach can be efficiently beneficial for 5G-MANET as it will provide a secure environment for the networks.

8) QUALITY OF EXPERIENCE

It exists three Quality of Experience aspects that should be considered, as shown in Figure 5.

Since the QoE is mainly affected by the user's behavior and other factors that cannot be controlled. Understanding the user's behavior becomes a critical point to achieve the expected QoE. In this context, unsupervised machine-learning can be used to find the user's context influence factors through big data analyzing while learning can be used to deduce the rules to determine the Quality of Service norms related to users [28].

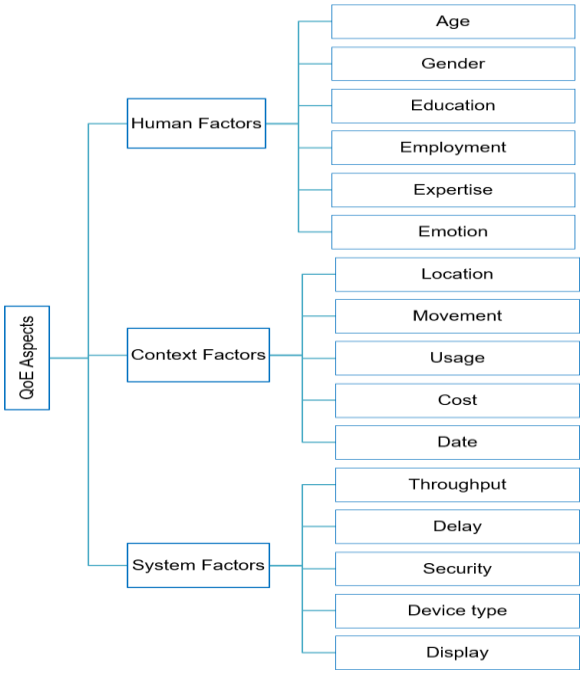


FIGURE 5. Quality of Experience Aspects.

A survey study was conducted to generate the needed data. AI can apply machine learning techniques (supervised and unsupervised learning) on these data to enhance the network by learning about the user's behavior and detecting

anomalies [42]. Semi-supervise learning can support the benefits of both supervised and unsupervised learning [74].

IV. BLOCKCHAIN FOR ARTIFICIAL INTELLIGENT-ENABLED 5G NETWORKS

We solely reviewed the applications of Blockchain and AI on 5G networks separately. In this section, we present our vision of merging Blockchain with AI-enabled 5G. we provide an overview Framework named Block5GIntell along with a detailed taxonomy. We argue as well on the support provided by Blockchain for AI to create a smart and secure 5G network.

A. BLOCKCHAIN FOR ARTIFICIAL INTELLIGENT-ENABLED 5G NETWORKS

Following our analysis of the applications of each technology into 5G separately, in this section, we present a further discussion about the convergence of Blockchain with AI-enabled 5G. 5G necessitates the endorsement of AI to meet its requirements. However, without the assistance of Blockchain, AI cannot bring its all benefits to 5G.

We present an overview of the proposed framework illustrated in Figure 6. The framework is mainly composed of four hierarchical layers: (1) Device Layer, (2) Access Layer, (3) Fog Layer, and (4) Cloud Layer. The device layer consists of four slices subsequently made of heterogeneous IoT devices, smart transportation and infrastructure, smart homes and sensors, and e-health systems. The device layer produces a tremendous amount of data. Thus, we integrated Blockchain in the device layer to collect and store the data generated securely and privately. Blockchain is integrated at the access layer as well for the same intentions. The access layer contains macro and small base stations, core network, cloud/centralized radio access network, and base station controllers. The access layer yields information about the network's status, resources, and performance. The data generated at the device layer and access layer is stored in it relevant Blockchain at each layer and sent to the cloud layer where it would be organized and stored and forwarded to the fog layer. The fog layer, by its turn, contains AI-powered fog nodes and computation resources. The fog nodes have two main roles, including Performing Learning methods and Acting methods. The learning modules use the data stored at the Blockchain-cloud layer and process the data to extract acting results, which can optimize, plan, manage and secure the network, as we discussed in the third section. These results are applied to the network's access layer. AI's successful learning algorithms and knowledge discovery are sent back to the Blockchain-cloud layer and stored in smart contracts to be executed directly on the access layer depending on the next-time network status.

1) DEVICE LAYER

The device layer in this framework contains heterogeneous 5G network slices; this layer generates a tremendous amount of data regarding human statistics. Such as user's age and expertise, context's information, for instance, location, movement and usage, and system's information essentially device type, security, and delay.

This information includes private individual data that need to be secured and protected [83] are collected locally in the relevant Blockchain ledger and sent to the Blockchain-cloud layer where it will be organized and stored for the AI learning module. As an example of how AI can learn from these data to improve the network is explained in section 3. Unsupervised machine learning can be used to find the user's context influence factors through big data analyzing, while supervised learning can be used to deduce the rules to determine the Quality of Service norms related to users. Correspondingly, AI's acting module can enhance the Quality of Service and Quality of Experience as well as preventing future errors from occurring.

2) ACCESS LAYER

The next layer in proposed framework Block5GIntell is the Access layer. It generates data about base stations, core network, and C-RAN's condition and status. The Blockchain in access layer stores these data as well as enables secure peer-to-peer communication between different base stations to share status information. The data generated is sent as well to the Blockchain-cloud layer to be organized and AI in the fog layer can use it for its learning modules. The data produced in the access layer are mandatory for AI's acting modules to bring its solutions to the massive-MIMO dilemma, network planning, and optimization, energy efficiency as well as enhancing the network security.

3) FOG LAYER

The third layer in our Intelligence and Secure Data Analytic framework Block5GIntell is the fog layer. The fog layer is where AI's learning modules and acting modules are integrated with its relevant computational resources. Learning modules use the data stored in the Blockchain-cloud layer to perform the necessary learning algorithms on it such as Linear Regression, Decision Tree, SVM, KNN, K-Means, Q-Learning, Naïve Bayes and so on. The results are forwarded to the acting modules, which by its turn, apply it directly to the network. Successful results such as searching results are sent back to the Blockchain-cloud layer and stored in the form of a smart contract. The smart contract will be executed automatically on the network without passing by the fog layer.

4) CLOUD LAYER

The last layer in our Intelligence and Secure Data Analytic framework Block5GIntell is the cloud layer or Blockchain-cloud layer. As the last name indicates in this layer, Blockchain will be able to store in an organized way all the data forwarded by the previous three layers. The AI in this layer is integrated to provide decentralized and secure data organization and clustering in Blockchain so it can be used by the fog layer easily and efficiently. We joined a Blockchain

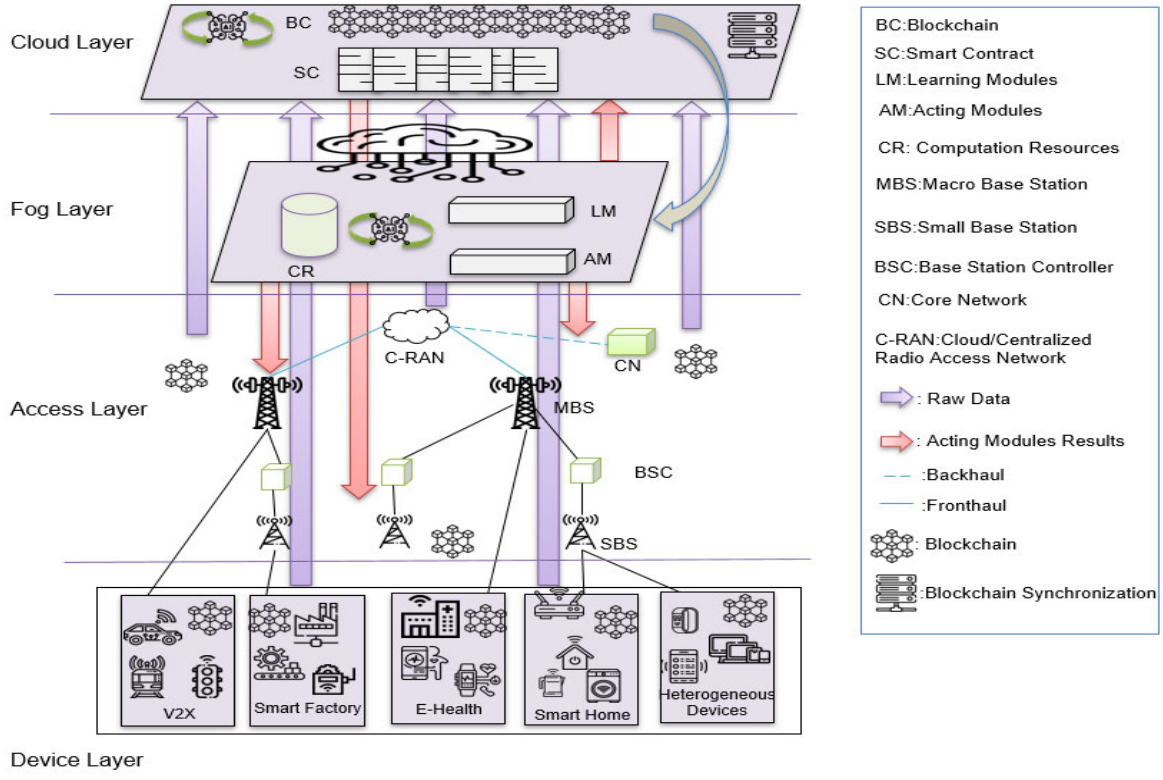


FIGURE 6. Overview of The Secure Data Analytic framework Block5GIntell for 5G networks.

synchronization module in this layer to maintain a real-time raw data update from the device and access layer.

B. EVALUATION OF THE PROPOSED INTELLIGENCE AND SECURE DATA ANALYTIC FRAMEWORK FOR 5G

In this section, we discuss the evaluation of the proposed Intelligence and Secure Data Analytics Framework for 5G. Our evaluation is divided into 2 parts: Qualitative analysis and Quantitative analysis. In qualitative analysis, a high-level taxonomy is presented to explain the framework overview and discuss in detail how can Blockchain support AI to create smart and secure 5G networks. In the second part, in quantitative analyses, a case study is presented to give an example of how our Intelligence and Secure Data Analytics Framework for 5G is working.

C. QUALITATIVE ANALYSES

In this section, we present a detailed taxonomic discussion about key concepts of AI-based Blockchain and its applications for 5G networks. We explain the deficiency of AI's deployment on 5G and demonstrate possible solutions based on Blockchain technology. Figure 7 presents a classification tree based on Salah *et al.* [15] taxonomy; we extend it to be applied for 5G networks.

1) AUTONOMIC COMPUTING

The Blockchain architecture can ensure operational decentralization and keep permanent footprints of interactions

FIGURE 7. Blockchain for AI-enabled 5G networks Classification Tree.

between users and user/network provider. This autonomous decentralized system not only can automate the 5G network design, but it can help in solving the automatic billing problems between users and 5G network providers as all the interactions are kept in a secure Blockchain ledger.

Network Optimization: Network optimization can be achieved efficiently with the enablement of decentralized

AI's optimization strategies using Blockchain. Blockchain enables highly relevant data processing for AI algorithms by collecting, storing, and organizing data in a secure and trusted ledger. AI-based Blockchain can enhance the efficiency of 5G network optimization.

2) PERCEPTION

In a heterogeneous 5G network environment, AI applications will continuously collect and analyze data using centralized perception strategies, these methods generally lead to a monolithic data collection [75]. Blockchain can be mitigated to this problem by decentralizing perception strategies. Blockchain decentralized nature facilitates secure, immutable, and permanent data collection. This feature brings magnificent support to AI to perform learning algorithms on user's behaviors and network traffics. Predicting computational resources and identifying unused spectral slots using the data collected and stored in Blockchain. Considering the permanent nature of Blockchain, only the footprints of successful perceptions should be stored to optimize AI's performance. Perception can achieve awareness for the 5G network's latency optimization.

3) 5G NETWORK'S SMART CONTRACT

Blockchain-enabled
smart contracts can support AI by enabling learning algorithms and knowledge discovery to be executed automatically depending on the network status. However, since the smart contracts are permanent, they should be implemented carefully and only after training and testing it.

4) CHANNEL ESTIMATION AND DETECTION

In channel estimation, AI's searching algorithms are applied to detect the right channel to use. However, implementing searching methods intermittently can affect the performance of the algorithm, reduce the performance of the network, and increase the latency. Moreover, the statistical knowledge on the channel should be available all the time [76]. To solve these issues, Blockchain can be used to store permanently and securely successful search traces and traversal paths which will optimize the search solutions for future operations.

5) SELF-ORGANIZED NETWORK

To realize a self-organized network, AI reasoning methods can be deployed. However, the centralized nature of AI's reasoning methods leads toward generalized behavior that could be spread across the network [77]. Using Blockchain distributed reasoning strategies can be beneficial to develop personalized reasoning strategies for network Self-planning, Self-optimization, and Self-healing separately. In addition to permanently storing the successful reasoning methods for future deployment using smart contracts. Decentralized reasoning strategies can efficiently create a self-organized 5G network.

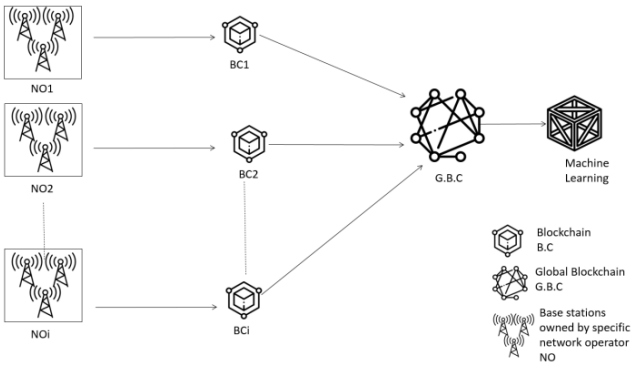


FIGURE 8. Global Blockchain for an Accurate Machine Learning Results.

D. QUANTITATIVE ANALYSIS

In this section, a case study is proposed as an example to measure the performance of our framework. In 5G networks, RAN consumes over 80% of wireless network power. Especially, the base station as it stays active regardless of the network traffic, thus consuming more gas to cover the amount of demanded energy. This will make the network incompatible with future applications such as smart cities. In this context, the need to create a smart and secure green network communication rises. Vodafone partnered with Ericsson to reduce network operating costs using Machine Learning [90]. This method is surely effective; however, the learned patterns are provided by one network operator, which means that each network operator has to collect and learn from its available data on-site separately. The more data a machine learning algorithm is fed, the more accurate the learned patterns are, and the better the results are. Thus, we suggest creating a Global Blockchain located on the cloud as our framework shows. Each Network Operator (NO) collects its data from its relevant base stations in every site using its private Blockchain. Those data are shared globally between other network operators in the Global Blockchain and used for the learning phase, as shown in Figure 8.

Every NO has its consortium Blockchain that collects the information sent by the relevant base stations. However, to make sure that all the participated base stations are legal and not fake nodes that trie to send false and misleading data to the Global Blockchain; we refers to the study in [20]. Chen *et al.* [20] presented a secure authentication scheme based on the Blockchain-Improved Practical Byzantine Fault-Tolerance (PBFT) algorithm; the PBFT is derived from the Byzantine Generals problem, that is, how to reach consensus on an untrustworthy distributed network.

According to the paper proposed in 1982 by Lamport [89], to tolerate f traitors or less, we need $3f + 1$ generals and f+1 rounds of information exchange. The BGP has been extended to Fault-tolerant theory in the field of network computing. We extend and develop the proposed version of the algorithm to be sure that only legal base stations are participating in our proposed system and all the data sent are accurate and none falsified.

Algorithm 1 Legal Base Station's Selection (LBSS)

1:**Input:** Base station ID and the request message to join the Blockchain
2:**Output:** Decision and final consensus result (If the base station can join
and participate in the Blockchain or not)
3:**Process:**
4: BSk.Send(<BSID, Msg, *t*>, *request, LSC);*
//with BSID: Base station identify, t: timestamp
5: LSC.Verify (<BSID, *h, Msg, t*>, *BS0); //h : the Msg high*
6: *BS0.Prepare(<v, h, d>, Msg); //d : the Msg digest, v : view* identity
7: *BS0.Broadcast(<v, h, d, s>, BSn*); *//s : the digest signature* of *BS0*
8: *for i= 1 to n*
{
9: *BSi.Receive(<v, h, d, s>);*
10: *Bsi.Verify(<v, h, d, s>, f, n);*
11: *Bsi.Prepare(<v, h, d, s>);*
12: *Bsi.Broadcast(<v, h, d, s>, BS|n-i|);*
13: *BSi.count(<f: fault d>, count m);*
}
//if m > f+1, broadcast commit, mark and reply to LSC(*BS0).*
14: w*hile count: m*> $(f + 1)$ *then*
{
// add a marking function to determine whether it is consistent with the final result.
//r : the result of the request operation
15: *BSi.Mark(<v, in : d, out : d, t, Mark: k>);*
16: *BSi.Commit(<v, h, d, s, t>, Result : k, BS0);*
}
17: *BS0.Receive(<v, h, d, s, t>, Msg: r, count m);*
18: *while* count: m>(2f+1) *then*
{
19: BS0.Compute(<*v, h, d, s* >, *Msg*: r, BSk=0.Mark = *r*);
}
20: *for* k=1 to n
{
21: BS0. *finalCheck*(BSk.*Mark* = *r*);
22: *if* BSk.*Mark* == *BS0.Mark then*
{
23: addBSToBlockhain (BC, BSID, 0, BSk);
}
24: else
25: skip;
}

The Legal Base Station's Selection (LBSS) to join the Blockchain can be described as follows:

1) If a base station BSk wants to join the Blockchain and participate with its data, it has to send a request message to the networks Local Service Center (LSC), the LSC is considered as the root in this algorithm and assigned BS0.
2) LSC verifies the identity of the base station that sent the request. If the identity is accurate BS0 prepare and broadcasts the verification message to other peers. Since we are using a consortium Blockchain, we assume that the peer that will verify the accuracy of the message are pre-selected by the network operator and are trusted base stations.
3) Each peer receives the message from BS0, verifies it, and prepare to broadcast it between the other peers.
4) The peers continue to forward and receive the message from each other and at the same time begin to accumulate the number of messages in their memory.
5) When the prepare message reaches f+1 rounds, the peers broadcast the commit status, mark the result, and send a reply to the BS0. Marking the result will help in the final checking phase to determine whether it is consistent with the final result.
6) Each peer keeps returning the results to BS0 until the retuned results equal to 2f+1.
7) After that, the final checking function is executed to compare the BSk result with the final result marked in BS0. If both results are consistent, the BSk is considered a legal base station and can join the Blockchain and participate with its data as well, if not then the request will be canceled.

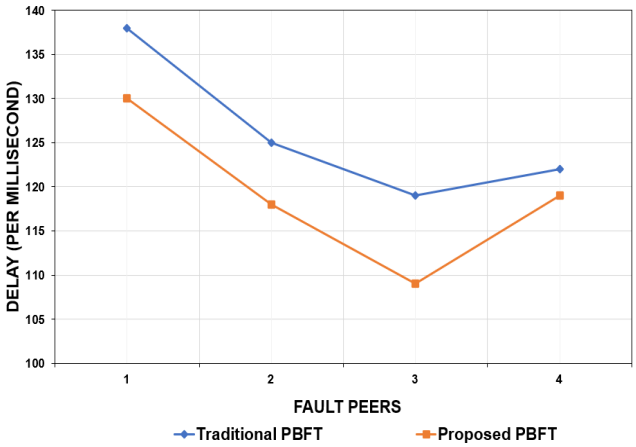


FIGURE 9. Performance of the PBFT based on the delay of transaction.

This algorithm makes a noticeable improvement on the traditional PBFT algorithm. The procedure *mark* is added before the *commit* procedure, which improves the efficiency of the final check. Moreover, we chose consortium Blockchain to use in our extended version of the algorithm, the thing that reduces the number of nodes participating in the consensus phase and reduces the computation time. Figure 9 represents the performance of the improved PBFT algorithm. As it shows, the algorithm scores less delay time per millisecond compared to the traditional PBFT algorithm.

Using this algorithm, we can be sure of the accuracy of data collected as all the participants base stations are legal, thus creating a safe environment for machine learning to learn from. Moreover, the collected data are securely stored in a shared Global Blockchain, which creates a tremendous amount of data for machine learning algorithms, the thing that will lead to more accurate results and notably reduce the energy consumption. Improving the efficiency at each site using machine learning and Blockchain makes a significant reduction in the overall energy consumption. All the network operators will be able to participate and share accurate information related to base station status and the best time to switch off and on the base station, thus creating a global 5G green communication, saving energy, and thereof saving gas and creating a green environment for 5G networks.

In order to simulate our proposed idea, we used Network Simulator-3 (ns-3) which relies on C++ to implement the network models and Python for network topology. The machine-learning algorithm was implemented using Python and GO-Ethuriem was deployed to implement the Global and private Blockchain. The simulation was performed on an intel core-i7 computer with 16 GB of RAM running under Ubuntu Linux. Using our virtual environment, we created four BS (BS1, BS2, BS3, BS4) belonging to four differents NO denoted recursively as (NO1, NO2, NO3, NO4) and located at four different locations (LO1, LO2, LO3, LO4) in a square topology of 500m X 500m. We configured 50 UEs randomly distributed between the four locations. At an initial state, we measure the Physical Resource Block (PRB) which is used to determine the usage of time and frequency resources [92] at every BS and fed the collected data to the machine learning algorithm for four weeks for training. The results were anonymously stored in the Global Blockchain. The machine-learning algorithm was trained during four weeks on site-specific data by each NO to learn the patterns of local UE's activities, daily high and low traffic times, and the time at which the base station can be switched on or off all while keeping the Quality of Experience needed and without any human intervention. The results show a 14% decrease in energy consumption as the machine learning algorithm was able to precisely predict when usage would peak and decline, and how to optimize energy allocation to automatically control the BS's switching (on/off).

After four weeks, we added another new base station BS5 belonging the NO1 in the location LO2 (notice that NO1 has been operating only in LO1) which belongs to NO2. Using the knowledge stored in the Global Blockchain, the BS5 was able to learn the patterns of UEs and the traffic times in the LO2. During two more weeks, we notice that BS5 has fastly adapted to the energy consumption in that area and recorded an energy decrease of 20%. Figure 10 represents the numerical results of our simulation.

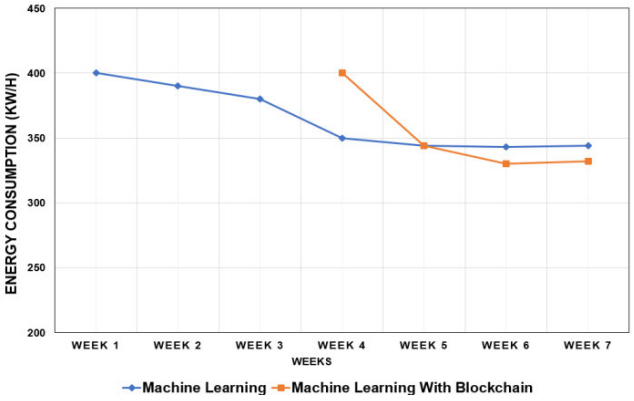


FIGURE 10. Network Energy Consumption.

V. DISCUSSION AND OPEN RESEARCH CHALLENGES

5G networks and beyond (6G) require the integration of AI to meet the demands of users and network providers. Yet, the continuously growing number of connected devices and the heterogeneous nature of networks restrain AI from bringing the optimization and smart solution to 5G networks and beyond. The tremendous amount of data generated from diverse parties can even worsen the network performance when applying AI algorithms on it as it consumes massive computational power and time to analyze the data generated. Moreover, security issues rose with the centralized nature of AI. However, with the use of Blockchain, these problems can be solved. Blockchain is not only able to store organized data for AI, but it can apply AI acting modules directly on the network using smart contracts and lighten the use of AI for networks. Thus, we firmly believe that Blockchain and AI should not be separated and must be considered together in future researches for scalable, smart, and secure 5G networks and Beyond.

A. DISCUSSION ABOUT BLOCKCHAIN FOR AI-ENABLED 5G

AI and its subcategories can bring an adequate improvement to the 5G network, enhance network planning and organization, augment Quality of Service and Quality of Experience as well as energy efficiency. However, the merge of AI with a cellular network is accompanied by security complications as well. The cybercriminals are using AI, in the same way, to profuse the threats rapidly and find more network vulnerability points, hence creating more victims. The centralized nature of AI exposes the data collected for the learning phase to different security threats. Furthermore, since 5G is a heterogeneous network, and it is designed to support a range variety of IoT devices, user equipment, and smart vehicles, the amount of data communicated and generated is tremendous. The amount of data can provoke a heavyweight on AI to analyze, hence, limiting its performance [78]. Nevertheless, Blockchain can partially, if not completely solve those problems. Blockchain alone can bring security and economic benefits to the 5G network, but the network performance's issues will still be untreated. Thus we strongly advocate the convergence of both technologies for a better outcome to cover security and performance of 5G networks. Blockchain

can securely store 5G' generated data in a real-time shared ledger, organize and sort it in categories while keeping the data anonymous without revealing sensitive information such as identity or location using homomorphic encryption. AI can make use of this organized and secured data ledger to perform learning algorithms, optimizing the performance of the network, predicting and preventing future errors from occurring.

Moreover, Blockchain can host an AI advanced enough to works on its own, which introduces the concept of decentralized AI [15]. Applied on the 5G network, decentralized AI applications will be able to operate autonomously and execute network planning, network optimization, user behaviors, and network traffic learning and knowledge management strategies. All without the intervention of a third party, thus remarkably enhancing network performance, tightening security, and reducing cost both on network operators and providers.

With the support of Blockchain and the use of its protocols, AI can fully bring its benefits and create an optimized, secure 5G network. Thus, we believe that both technologies are not separable and should be studied wildly together for a truly smart 5G and beyond 5G networks.

B. OPEN RESEARCH CHALLENGES

We have discussed the advantages of using AI and Blockchain on 5G networks. We have argued on the implementation of these technologies as it can notably enhance the network performance and optimize it all while maintaining a secure environment for the network user. However, combining AI with blockchain can have its drawbacks that could affect 5G networks as well. In this section, we cite some of the issues that could occur with the convergence of AI and Blockchain and how they can disturb 5G networks.

1) PRIVACY

Collecting data in a public blockchain can help improving AI algorithms and network performance.

However, it does impose a user's sensitive information at risk of privacy leaking as the public blockchain nature is accessible to anyone. Using private blockchain can be secure, but it does not help AI as it will limit the data generation process from 5G heterogeneous environments, thus affecting AI performance and narrowing its benefits. Subsequently, existing privacy-preserving approaches such as [79]–[81] can be used to protect the privacy of compressive data and location data in the 5G network.

2) SCALABILITY

Blockchain scalability is still one of the biggest challenges that face Blockchain developers, and it is one of the main reasons why implementing a large-scale AI into Blockchain is still considerate as a risky move for many researchers. Especially in 5G network environment where the amount of data collected from various parties can create a scalability problem. However, optimizing consensus algorithms used and choosing the right ones can partly solve this problem and improve the performance of blockchain. Further works are highly needed to increase the scalability of Blockchain.

3) SECURITY

Although the secure nature of blockchain, the public blockchain ledger is still prone to cyber-attacks as that of a 51% attack [82]. This fact is treating for AI's collected data from the network as it affects AI performance and leads to false learning which can severely damage 5G networks and its components. For this case using a private blockchain seems to be the only solution at the moment even though it will decrease AI abilities to support 5G networks [94]–[96].

4) SMART CONTRACTS

Since the smart contracts are permanent and non-modifiable, it is necessary to ensure the integrity and security of AI applications before implementing it into a smart contract. Any falsified data or security vulnerability can severely damage the network [97]–[99]. Thus, training and testing AI applications is a crucial phase. Moreover, the cost of generating and executing a smart contract is still considered very expensive in terms of money and time.

VI. CONCLUSION

In this article, we presented a comprehensive overview framework on the convergence of Blockchain with AI-enabled 5G networks named Block5GIntell. The framework supports the development of a novel methodology for decentralized, distributed, and immutable smart applications. This article presented a high-level taxonomy of Blockchain and AI for 5G separately based on recent related studies as well as Blockchain for AI-enabled 5G network. We have proposed as well a case study using Blockchain and AI to create a green 5G network environment and save the gas and energy consumption at the level of RAN. Following our proposition, Blockchain can fully support AI to reduce energy consumption and enhance the security and accuracy of collected data in 5G network. Moreover, different Network Operators will be able to share their knowledge about energy consumption at each location securely, which will lead to a noticeably overall, global and effective energy saving and reduction of gas consumption and cost as well.

REFERENCES

[1] W. Chen, C.-T. Lea, S. He, and Z. XuanYuan, "Opportunistic routing and scheduling for wireless networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 320–331, Jan. 2017.

[2] S. He, K. Xie, K. Xie, C. Xu, and J. Wang, "Interference-aware multisource transmission in multiradio and multichannel wireless network," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2507–2518, Sep. 2019.

[3] E. Mohyeldin, "Minimum technical performance requirements for IMT-2020 radiointerface(s)," in *Proc. ITU-R Workshop IMT-Terrestrial Radio Interfaces*. Munich, Germany: Nokia, 2017.

[4] L. Li, D. Wang, X. Niu, Y. Chai, L. Chen, L. He, X. Wu, F. Zheng, T. Cui, and X. You, "mmWave communications for 5G: Implementation challenges and advances," *Sci. China Inf. Sci.*, vol. 61, Jan. 2018, Art. no. 021301, doi: 10.1007/s11432-017-9262-8.

[5] C.-X. Wang, S. Wu, L. Bai, X. You, J. Wang, and C.-L. I, "Recent advances and future challenges for massive MIMO channel measurements and models," *Sci. China Inf. Sci.*, vol. 59, no. 2, pp. 1–16, Feb. 2016, doi: 10.1007/s11432-015-5517-1.

[6] R. El Hattachi and J. Erfanian, "5G white paper," NGMN Alliance, Frankfurt, Germany, White Paper, 2015.

[7] W. B. Daoud, M. S. Obaidat, A. Meddeb-Makhlouf, F. Zarai, and K.-F. Hsiao, "TACRM: Trust access control and resource management mechanism in fog computing," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, p. 28, Dec. 2019, doi: 10.1186/s13673-019-0188-3.

[8] F. Concone, G. L. Re, and M. Morana, "SMCP: A secure mobile crowd-sensing protocol for fog-based applications," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–23, Dec. 2020, doi: 10.1186/s13673-020-00232-y.

[9] M. Weiner, M. Jorgovanovic, A. Sahai, and B. Nikolić, "Design of a low-latency, high-reliability wireless communication system for control applications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 3829–3835, doi: 10.1109/ICC.2014.6883918.

[10] S. Chen, F. Qin, B. Hu, X. Li, Z. Chen, and J. Liu, *User-Centric Ultra-Dense Networks for 5G*. Cham, Switzerland: Springer, 2017.

[11] Z. Chen, S. Chen, H. Xu, and B. Hu, "Security architecture and scheme of user-centric ultra-dense network (UUDN)," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 9, p. e3149, Sep. 2017.

[12] *The 5G Infrastructure Public Private Partnership: The Next Generation of Communication Networks and Services*. Accessed: Dec. 2, 2019. [Online]. Available: http://www.5g-ppp.eu

[13] S. K. Singh, S. Rathore, and J. H. Park, "Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2019, doi: 10.1016/j.future.2019.09.002.

[14] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018, doi: 10.3745/JIPS.01.0024.

[15] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019, doi: 10.1109/ACCESS.2018.2890507.

[16] *Strategy Analytics Research*. Accessed: Oct. 21, 2019. [Online]. Available: https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where

[17] Y. Luo, K. Yang, Q. Tang, J. Zhang, P. Li, and S. Qiu, "An optimal data service providing framework in cloud radio access network," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, p. 23, Dec. 2016, doi: 10.1186/s13638-015-0503-2.

[18] T. Hossfeld, P. Tran-Gia, and M. Fiedler, "Quantification of quality of experience for edge-based applications," in *Proc. Int. Teletraffic Congr.*, vol. 4516, 2007, pp. 361–373, doi: 10.1007/978-3-540-72990-7_34.

[19] P. Porambage, T. Kumar, M. Liyanage, J. Partala, L. Loven, M. Ylianttila, and T. Seppanen, "Sec-EdgeAI: AI for edge security vs security for edge AI," in *Proc. 1st 6G Wireless Summit*, At Levi, Finland, 2019. Accessed: May 16, 2019.

[20] Z. Chen, S. Chen, H. Xu, and B. Hu, "A security authentication scheme of 5G ultra-dense network based on block chain," *IEEE Access*, vol. 6, pp. 55372–55379, 2018.

[21] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 121–127, Jun. 2018.

[22] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Netw. Lett.*, vol. 1, no. 3, pp. 99–102, Sep. 2019.

[23] R. Li, Z. Zhao, X. Zhou, G. Ding, Y. Chen, Z. Wang, and H. Zhang, "Intelligent 5G: When cellular networks meet artificial intelligence," *IEEE Wireless Commun.*, vol. 24, no. 5, pp. 175–183, Oct. 2017.

[24] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, "Blockchain-based trusted authentication in cloud radio over fiber network for 5G," in *Proc. 16th Int. Conf. Opt. Commun. Netw. (ICOCN)*, Wuzhen, China, Aug. 2017, pp. 1–3.

[25] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 7081–7093, Nov. 2020.

[26] E. Balevi and R. D. Gitlin, "Unsupervised machine learning in 5G networks for low latency communications," in *Proc. IEEE 36th Int. Perform. Comput. Commun. Conf. (IPCCC)*, San Diego, CA, USA, Dec. 2017, pp. 1–2.

[27] V. Sciancalepore, X. Costa-Perez, and A. Banchs, "RL-NSB: Reinforcement learning-based 5G network slice broker," *IEEE/ACM Trans. Netw.*, vol. 27, no. 4, pp. 1543–1557, Aug. 2019.

[28] E. Ibarrola, M. Davis, C. Voisin, C. Close, and L. Cristobo, "A machine learning management model for QoE enhancement in next-generation wireless ecosystems," in *Proc. ITU Kaleidoscope, Mach. Learn. 5G Future (ITU K)*, Santa Fe, Argentina, Nov. 2018, pp. 1–8.

[29] T. E. Bogale, X. Wang, and L. B. Le, "Machine intelligence techniques for next-generation context-aware wireless networks," 2018, *arXiv:1801.04223*. [Online]. Available: http://arxiv.org/abs/1801.04223

[30] L. Nachabe, M. Girod-Genet, and B. El Hassan, "Unified data model for wireless sensor network," *IEEE Sensors J.*, vol. 15, no. 7, pp. 3657–3667, Jul. 2015.

[31] K. Awahara, S. Izumi, T. Abe, and T. Suganuma, "Autonomous control method using AI planning for energy-efficient network systems," in *Proc. 8th Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Compiègne, France, Oct. 2013, pp. 628–633.

[32] V.-S. Feng and S. Y. Chang, "Determination of wireless networks parameters through parallel hierarchical support vector machines," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 3, pp. 505–512, Mar. 2012.

[33] H. Lee and M. Ma, "Blockchain-based mobility management for 5G," *Future Gener. Comput. Syst.*, vol. 110, pp. 638–646, Sep. 2020.

[34] V. Messié, G. Fromentoux, X. Marjou, and N. L. Omnes, "BALAdIN for blockchain-based 5G networks," in *Proc. 22nd Conf. Innov. Clouds, Internet Netw. Workshops (ICIN)*, Paris, France, 2019, pp. 201–205.

[35] B. Dinesh, B. Kavya, D. Sivakumar, and M. R. Ahmed, "Conforming test of blockchain for 5G enabled IoT," in *Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI)*, Tirunelveli, India, Apr. 2019, pp. 1153–1157.

[36] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things," *IEEE Netw.*, vol. 33, no. 5, pp. 12–19, Sep. 2019.

[37] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Netw.*, vol. 33, no. 3, pp. 10–17, May 2019.

[38] J. H. Jo, P. K. Sharma, J. C. S. Sicato, and J. H. Park, "Emerging technologies for sustainable smart city network security: Issues, challenges, and countermeasures," *J. Inf. Process. Syst.*, vol. 15, no. 4, pp. 765–784, 2019, doi: 10.3745/JIPS.03.0124.

[39] F. Wang, L. Zhang, S. Zhou, and Y. Huang, "Neural network-based finite-time control of quantized stochastic nonlinear systems," *Neurocomputing*, vol. 362, pp. 195–202, Oct. 2019.

[40] F. Kuang, S. Zhang, Z. Jin, and W. Xu, "A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection," *Soft Comput.*, vol. 19, no. 5, pp. 1187–1199, May 2015.

[41] G. Zhu, J. Zan, Y. Yang, and X. Qi, "A supervised learning based QoS assurance architecture for 5G networks," *IEEE Access*, vol. 7, pp. 43598–43606, 2019.

[42] S. Aroussi and A. Mellouk, "Survey on machine learning-based QoE-QoS correlation models," in *Proc. Int. Conf. Comput., Manage. Telecommun. (ComManTel)*, Da Nang, Vietnam, 2014, pp. 200–204.

[43] C. Yin, S. Ding, and J. Wang, "Mobile marketing recommendation method based on user location feedback," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, p. 14, Dec. 2019, doi: 10.1186/s13673-019-0177-6.

[44] E. Cambria and B. White, "Jumping NLP curves: A review of natural language processing research [review article]," *IEEE Comput. Intell. Mag.*, vol. 9, no. 2, pp. 48–57, May 2014.

[45] J. Zhang, S. Zhong, T. Wang, H. C. Chao, and J. Wang, "Blockchain-based systems and applications: A survey," *J. Internet Technol.*, vol. 21, no. 1, pp. 1–14, 2020.

[46] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[47] C.-L. Liu, W.-J. Tsai, T.-Y. Chang, and T.-M. Liu, "Ephemeral-secret-leakage secure id-based three-party authenticated key agreement protocol for mobile distributed computing environments," *Symmetry*, vol. 10, no. 4, p. 84, 2018, doi: 10.3390/sym10040084.

[48] Z. Xia, Z. Hu, and J. Luo, "UPTP vehicle trajectory prediction based on user preference under complexity environment," *Wireless Pers. Commun.*, vol. 97, no. 3, pp. 4651–4665, Dec. 2017.

[49] S. Ou, K. Yang, and H.-H. Chen, "Integrated dynamic bandwidth allocation in converged passive optical networks and IEEE 802.16 networks," *IEEE Syst. J.*, vol. 4, no. 4, pp. 467–476, Dec. 2010, doi: 10.1109/JSYST.2010.2088750.

[50] S. K. Singh, M. M. Salim, M. Cho, J. Cha, Y. Pan, and J. H. Park, "Smart contract-based pool hopping attack prevention for blockchain networks," *Symmetry*, vol. 11, no. 7, p. 941, Jul. 2019, doi: 10.3390/sym11070941.

[51] V. Adat, I. Politis, C. Tselios, P. Galiotos, and S. Kotsopoulos, "On blockchain enhanced secure network coding for 5G deployments," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–7, doi: 10.1109/GLOCOM.2018.8647581.

[52] K. Valtanen, J. Backman, and S. Yrjölä, "Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2018, pp. 185–190, doi: 10.1109/WCNCW.2018.8368983.

[53] P. Zhang, W. Li, and H. Sun, "Cost-efficient and multi-functional secure aggregation in large scale distributed application," *PLoS ONE*, vol. 11, no. 8, Aug. 2016, Art. no. e0159605, doi: 10.1371/journal.pone.0159605.

[54] J. Wu, "Research on massive MIMO key technology in 5G," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 466, Dec. 2018, Art. no. 012083.

[55] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 98–105, Apr. 2017.

[56] R. C. Qiu, Z. Hu, Z. Chen, N. Guo, R. Ranganathan, S. Hou, and G. Zheng, "Cognitive radio network for the smart grid: Experimental system architecture, control algorithms, security, and microgrid testbed," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 724–740, Dec. 2011.

[57] C.-K. Wen, S. Jin, K.-K. Wong, J.-C. Chen, and P. Ting, "Channel estimation for massive MIMO using Gaussian-mixture Bayesian learning," *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1356–1368, Mar. 2015.

[58] K. F. Poon, A. Chu, and A. Ouali, "An AI-based system for telecommunication network planning," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage.*, Hong Kong, Dec. 2012, pp. 874–878.

[59] J. Perez-Romero, O. Sallent, R. Ferrus, and R. Agusti, "Knowledge-based 5G radio access network planning and optimization," in *Proc. Int. Symp. Wireless Commun. Syst. (ISWCS)*, Sep. 2016, pp. 359–365.

[60] T. Hirao, M. Nishino, Y. Yoshida, J. Suzuki, N. Yasuda, and M. Nagata, "Summarizing a document by trimming the discourse tree," *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 23, no. 11, pp. 2081–2092, Nov. 2015.

[61] V. P. Kafle, Y. Fukushima, P. Martinez-Julia, and T. Miyazawa, "Consideration on automation of 5G network slicing with machine learning," in *Proc. ITU Kaleidoscope, Mach. Learn. 5G Future (ITU K)*, Santa Fe, Argentina, Nov. 2018, pp. 1–8.

[62] X. Wang and Y. He, "Learning from uncertainty for big data: Future analytical challenges and strategies," *IEEE Syst., Man, Cybern. Mag.*, vol. 2, no. 2, pp. 26–31, Apr. 2016.

[63] G. Alnwaimi, S. Vahid, and K. Moessner, "Dynamic heterogeneous learning games for opportunistic access in LTE-based macro/femtocell deployments," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 2294–2308, Apr. 2015.

[64] W. Ejaz, M. Naeem, A. Shahid, A. Anpalagan, and M. Jo, "Efficient energy management for the Internet of Things in smart cities," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 84–91, Jan. 2017.

[65] C. M. S. Magurawalage, K. Yang, L. Hu, and J. Zhang, "Energy-efficient and network-aware offloading algorithm for mobile cloud computing," *Comput. Netw.*, vol. 74, pp. 22–33, Dec. 2014.

[66] H. Trivedi, S. Tanwar, and P. Thakkar, "Software defined network-based vehicular adhoc networks for intelligent transportation system: Recent advances and future challenges," in *Proc. Int. Conf. Futuristic Trends Netw. Commun. Technol.* Singapore: Springer, 2018, pp. 325–337.

[67] Y. Shen, J. Li, Z. Zhu, W. Cao, and Y. Song, "Image reconstruction algorithm from compressed sensing measurements by dictionary learning," *Neurocomputing*, vol. 151, pp. 1153–1162, Mar. 2015, doi: 10.1016/j.neucom.2014.06.082.

[68] B. K. Donohoo, C. Ohlsen, S. Pasricha, Y. Xiang, and C. Anderson, "Context-aware energy enhancements for smart mobile devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1720–1732, Aug. 2014.

[69] N. Kato, Z. M. Fadlullah, B. Mao, F. Tang, O. Akashi, T. Inoue, and K. Mizutani, "The deep learning vision for heterogeneous network traffic control: Proposal, challenges, and future perspective," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 146–153, Jun. 2017.

[70] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[71] E. S. Kumar, S. M. Kusuma, and B. P. V. Kumar, "A random key distribution based artificial immune system for security in clustered wireless sensor networks," in *Proc. IEEE Students Conf. Electr., Electron. Comput. Sci.*, Bhopal, India, Mar. 2014, pp. 1–7.

[72] V. K. Quy, V. N. Education, N. T. Ban, and N. D. Han, "An advanced energy efficient and high performance routing protocol for MANET in 5G," *J. Commun.*, vol. 13, no. 12, pp. 743–749, 2018, doi: 10.12720/jcm.13.12.743-749.

[73] F. Barani, "A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system," in *Proc. Iranian Conf. Intell. Syst. (ICIS)*, Bam, Iran, Feb. 2014, pp. 1–6.

[74] Y. Tu, Y. Lin, J. Wang, and J.-U. Kim, "Semi-supervised learning with generative adversarial networks on digital signal modulation classification," *Comput. Mater. Continua*, vol. 55, no. 2, pp. 243–254, 2018.

[75] H. Lu, Y. Li, M. Chen, H. Kim, and S. Serikawa, "Brain intelligence: Go beyond artificial intelligence," *Mobile Netw. Appl.*, vol. 23, no. 2, pp. 368–375, Apr. 2018.

[76] S. Maghsudi and S. Stanczak, "Channel selection for network-assisted D2D communication via no-regret bandit learning with calibrated forecasting," *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1309–1322, Mar. 2015.

[77] S. Banerjee, P. K. Singh, and J. Bajpai, "A comparative study on decision-making capability between human and artificial intelligence," in *Nature Inspired Computing*. Singapore: Springer, 2018, pp. 203–210.

[78] J. Wang, Y. Yang, T. Wang, R. S. Sherratt, and J. Zhang, "Big data service architecture: A survey," *J. Internet Technol.*, vol. 21, no. 2, pp. 393–405, 2020.

[79] K. Xie, X. Ning, X. Wang, S. He, Z. Ning, X. Liu, J. Wen, and Z. Qin, "An efficient privacy-preserving compressive data gathering scheme in WSNs," *Inf. Sci.*, vol. 390, pp. 82–94, Jun. 2017.

[80] W. Zeng, P. Chen, H. Chen, and S. He, "PAPG: Private aggregation scheme based on privacy-preserving gene in wireless sensor networks," *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 9, pp. 1–25, 2016.

[81] K. Gu, L. Yang, and B. Yin, "Location data record privacy protection based on differential privacy mechanism," *Inf. Technol. Control*, vol. 47, no. 4, pp. 639–654, Dec. 2018.

[82] S. V. Akram, P. K. Malik, R. Singh, G. Anita, and S. Tanwar, "Adoption of blockchain technology in various realms: Opportunities and challenges," *Secur. Privacy*, vol. 3, p. e109, Apr. 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.109

[83] S. He, W. Zeng, K. Xie, H. Yang, M. Lai, and X. Su, "PPNC: Privacy preserving scheme for random linear network coding in smart grid," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 3, pp. 1510–1532, 2017, doi: 10.3837/tiis.2017.03.015.

[84] Y. Fu, S. Wang, C.-X. Wang, X. Hong, and S. McLaughlin, "Artificial intelligence to manage network traffic of 5G wireless networks," *IEEE Netw.*, vol. 32, no. 6, pp. 58–64, Nov. 2018.

[85] D. Wang, B. Song, D. Chen, and X. Du, "Intelligent cognitive radio in 5G: AI-based hierarchical cognitive cellular networks," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 54–61, Jun. 2019.

[86] D. Pliatsios and P. Sarigiannidis, "Resource allocation combining heuristic matching and particle swarm optimization approaches: The case of downlink non-orthogonal multiple access," *Information*, vol. 10, no. 11, p. 336, Oct. 2019.

[87] M. Chen, Y. Miao, H. Gharavi, L. Hu, and I. Humar, "Intelligent traffic adaptive resource allocation for edge computing-based 5G networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 2, pp. 499–508, Jun. 2020.

[88] C. Benzaid and T. Taleb, "AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions," *IEEE Netw.*, vol. 34, no. 2, pp. 186–194, Mar. 2020.

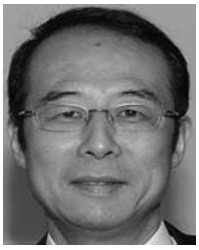
[89] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982, doi: 10.1145/357172.357176.

[90] *Automating MIMO Energy Management With Machine Learning, Ericsson With Vodafone, 1/213 31-FGC 101 3362 Uen*, Ericsson, Stockholm, Sweden. Accessed: Jan. 20, 2020.

[91] *How Will AI Enable the Switch to 5G*. Accessed: Feb. 16, 2020. [Online]. Available: https://www.ericsson.com/en/networks/offerings/network-services/ai-report
[92] *LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Layer 2—Measurements*, document TS 36.314, Version 8.1.0, Release 8, 3GPP, 2009.
[93] S. K. Singh, Y.-S. Jeong, and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart city," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102252.
[94] C. Yin, B. Zhou, Z. Yin, and J. Wang, "Local privacy protection classification based on human-centric computing," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, p. 33, Dec. 2019.
[95] F. Peng, L. Qin, and M. Long, "Face presentation attack detection using guided scale texture," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8883–8909, Apr. 2018.
[96] J.-L. Zhang, W.-Z. Wang, X.-W. Wang, and Z.-H. Xia, "Enhancing security of FPGA-based embedded systems with combinational logic binding," *J. Comput. Sci. Technol.*, vol. 32, no. 2, pp. 329–339, Mar. 2017.
[97] F. Peng, Z.-X. Lin, X. Zhang, and M. Long, "Reversible data hiding in encrypted 2D vector graphics based on reversible mapping model for real numbers," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2400–2411, Sep. 2019.
[98] Y.-S. Luo, K. Yang, Q. Tang, J. Zhang, and B. Xiong, "A multi-criteria network-aware service composition algorithm in wireless environments," *Comput. Commun.*, vol. 35, no. 15, pp. 1882–1892, Sep. 2012.
[99] M. Liu, L. Cheng, K. Qian, J. Wang, J. Wang, and Y. Liu, "Indoor acoustic localization: A survey," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, p. 2, Dec. 2020.

ABIR EL AZZAOUI received the B.S. degree in computer science from the University of Picardie Jules-Verne, Amiens, France. She graduated from the National School of Higher Education Hassan II in Development of Information Systems, Marrakech, Morocco. She is currently pursuing the master's degree in computer science and engineering with the Ubiquitous Computing Security (UCS) Laboratory, Seoul National University of Science and Technology, Seoul, South Korea, under the supervision of Prof. Jong Hyuk Park. Her current research interests include blockchain, the Internet-of-Things (IoT) security, and post-quantum cryptography. She is also a Reviewer of IEEE Access journal. She has received the Quarterly Franklin Membership from the *London Journal of Engineering Research* (LJER), London, GB.

SUSHIL KUMAR SINGH received the M.E. degree in information technology from Karnataka State University, Mysore, India, in 2011, and the M.Tech. degree in computer science and engineering from Uttarakhand Technical University, Dehradun, India, in 2018. He is currently pursuing the Ph.D. degree with the UCS Laboratory, Seoul National University of Science and Technology, Seoul, South Korea, under the supervision of Prof. Jong Hyuk Park. He has more than nine-year experience of teaching in the field of computer science. His current research interests include blockchain, artificial intelligence, big data, and the Internet of Things. He is also a Reviewer of the IEEE Systems Journal, FGCS, *Computer Networks*, HCIS, JIPS journal, and others.



YI PAN (Senior Member, IEEE) received the B.Eng. and M.Eng. degrees in computer engineering from Tsinghua University, China, in 1982 and 1984, respectively, and the Ph.D. degree in computer science from the University of Pittsburgh, PA, in 1991. He is currently the Chair of and a Professor with the Department of Computer Science and a Professor with the Department of Computer Information Systems, Georgia State University, Atlanta. He has published more than 100 journal articles with 38 articles published in various IEEE journals. In addition, he has published more than 100 papers in refereed conferences. He has also authored/edited 34 books (including proceedings) and contributed many book chapters. His research interests include parallel and distributed computing, networks, and bioinformatics. He has also served as a Program Committee Member for several major international conferences, such as BIBE, BIBM, ISBRA, INFOCOM, GLOBECOM, ICC, IPDPS, and ICPP. He has organized several international conferences and workshops. He has delivered more than ten keynote speeches at many international conferences. He is also a Speaker for several distinguished speaker series. He is listed in Men of Achievement, Who's Who in Midwest, Who's Who in America, Who's Who in American Education, Who's Who in Computational Science and Engineering, and Who's Who of Asian Americans. He has served as the Editor-in-Chief or an Editorial Board Member for 15 journals, including six IEEE Transactions, and a Guest Editor for ten journals, including the IEEE/ACM Transactions on Computational Biology and Bioinformatics and the IEEE Transactions on NanoBioscience.

JONG HYUK (JAMES J.) PARK (Member, IEEE) received the Ph.D. degrees from the Graduate School of Information Security, Korea University, South Korea, and the Graduate School of Human Sciences, Waseda University, Japan. From December 2002 to July 2007, he was a Research Scientist with the Research and Development Institute, Hanwha S&C Company Ltd., South Korea. From September 2007 to August 2009, he was a Professor with the Department of Computer Science and Engineering, Kyungnam University, South Korea. He is currently a Professor with the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), South Korea. He has published about 200 research papers in international journals and conferences. His research interests include the IoT, human-centric ubiquitous computing, information security, digital forensics, vehicular cloud computing, and multimedia computing. He is a member of the IEEE Computer Society, KIPS, and KMMS. He got the best paper awards from ISA-2008 and ITCS-2011 conferences and the outstanding leadership awards from IEEE HPCC-2009, ICA3PP-2010, IEE ISPA-2011, PDCAT-2011, and IEEE AINA-2015. Furthermore, he got the outstanding research awards from the SeoulTech, in 2014. He has been serving as the Chair, the Program Committee, or the Organizing Committee Chair for many international conferences and workshops. He is also the Steering Chair of international conferences–MUE, FutureTech, CSA, CUTE, UCAWSN, and World IT Congress-Jeju. He is the Editor-in-Chief of *Human-Centric Computing and Information Sciences* (HCIS) (Springer), the *Journal of Information Processing Systems* (JIPS) (KIPS), and the *Journal of Convergence* (JoC) (KIPS CSWRG). He is an Associate Editor/Editor of 14 international journals, including JoS, JNCA, SCN, CJ, and so on. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford University Press, Emerald, Inderscience, and MDPI.