IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS. 2020.Doi Number

Deep Learning and Blockchain-empowered Security Framework for Intelligent 5G-enabled IoT

Shailendra Rathore[1], Jong Hyuk Park [2], Hangbae Chang[3,*]

[1] Blockchain Service Research Center, Chung-Ang University, 84, Heukseok-ro, Dongjak-gu, Seoul, Republic of Korea
[2] Department of Computer Science and Engineering, Seoul National University of Science and Technology, (SeoulTech) Seoul 01811, Korea
[3] Department of Industrial Security, Chung-Ang University, 84, Heukseok-ro, Dongjak-gu, Seoul, Republic of Korea
Email id: a91203@cau.ac.kr, jhpark1@seoultech.ac.kr, hbchang@cau.ac.kr

ABSTRACT Recently, many IoT applications, such as smart transportation, healthcare, and virtual and augmented reality experiences, have emerged with fifth-generation (5G) technology to enhance the Quality of Service (QoS) and user experience. The revolution of 5G-enabled IoT supports distinct attributes, including lower latency, higher system capacity, high data rate, and energy saving. However, such revolution also delivers considerable increment in data generation that further leads to a major requirement of intelligent and effective data analytic operation across the network. Furthermore, data growth gives rise to data security and privacy concerns, such as breach and loss of sensitive data. The conventional data analytic and security methods do not meet the requirement of 5G-enabled IoT including its unique characteristic of low latency and high throughput. In this paper, we propose a Deep Learning (DL) and blockchain-empowered security framework for intelligent 5G-enabled IoT that leverages DL competency for intelligent data analysis operation and blockchain for data security. The framework's hierarchical architecture wherein DL and blockchain operations emerge across the four layers of cloud, fog, edge, and user is presented. The framework is simulated and analyzed, employing various standard measures of latency, accuracy, and security to demonstrate its validity in practical applications.

INDEX TERMS Internet of Things, Security Attack Detection, Edge Computing, Fog Computing, Blockchain, Software-Defined Networking

I. INTRODUCTION

The recent development in communication and networking applications gives rise to a massive demand for a next -generation communication paradigm. Unlike past generation communications (i.e., Second-Generation (2G) to Fourth -Generation (4G)), Fifth-Generation (5G) communication has become prominent in recent years due to its distinct competencies of higher scalability, low latency, high reliability, and high throughput [1]. The competencies of 5G support pervasive connectivity solutions in many Internet of Things (IoT) applications, such as smart healthcare, smart grid, smart home, and smart cities, and give rise to a new phenomenon known as 5G-enabled IoT. A 5G-enabled IoT can facilitate the operations of a massive number of devices and improve user satisfaction, quality of service, and quality of experience in IoT applications [2]. To enable flexible operation and heterogeneous IoT services, the 5G-enabled IoT technologies support emerging technologies and orchestrations including network function virtualization, massive multiple inputs–multiple outputs, mobile edge computing, and ultra-dense networks [3].

MarketsandMarkets [4] reported a 55.4% Compound Annual Growth Rate (CAGR) of the global 5G-enabled IoT market and an estimated increment from $0.7 billion to $6.3 billion by 2025. In addition, 5G-enabled IoT is being deployed from manufacturing industries to autonomous system, including connected cars and consumer wearable devices. However, such deployment of 5G-enabled IoT leads to the generation of massive amounts of data by connected devices and IoT sensors. According to Ericsson Mobility Report [5], the use of 5G will account for 65% of the total population globally, and this will further lead to a significant growth in data traffic (i.e., approx. 45% of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3077069, IEEE Access

mobile data traffic globally) by year 2025. The escalation in the connected IoT devices and data generation by end of 2025 are estimated to be 41.6 billion and 79.4 zettabytes (ZB), respectively, according to the International Data Corporation (IDC) report [6]. The significant surge in data makes data analytics a forethought, giving rise to the need for intelligent services and applications to handle massive data in 5G-enabled IoT. On the other hand, security and privacy are also major concerns as a consequence of significant data growth. Various data breaches and losses, including sensitive and personal data, health data, and financial data, are likely. Several critical complications such as social trust, personal safety, monetary penalty, and consumer confidence can occur due to security and privacy risks [7]. Examples include Untethered Virtual Reality (VR) employing 5G to support ultra-low-latency communications, which gives rise to the data privacy issue such as virtual identity theft in VR. The 5G security market report [8] expects IoT services to account for approximately 30% of the 5G security market from 2019 to 2024 and privacy and security of data to be critical issues in 5G-enabled IoT.

State-of-the-art security solutions have emerged to provide secure services and data-intensive applications in traditional 4G-enabled IoT. These solutions support either centralized approach, novel paradigms, architecture, or framework for efficient, secure data management (i.e., processing, analysis, and storing) in the cloud [9-11]. However, the distinct characteristics of 5G-enabled IoT, including low latency, high speed, high throughput, and high capacity, make traditional 4G-enabled IoT security solutions less efficient compared to the 5G-enabled IoT security. The large number of devices supported by 5G-enabled IoT, unlike 4G-enabled IoT, gives rise to challenges in processing and analysis of the generated massive data. In particular, the extraction of substantial information from massive data is challenging in terms of supporting data caching (i.e., content distribution and content placement), classification, and prediction of future incidents in 5G-enabled IoT [12]. In addition, excessive overhead on network bandwidth due to data generated by more devices and more locations gives rise to supplementary security threats (such as Denial of Service (DoS) attack) that in turn cause delay or failure of services in terms of availability and delivery. The deployment of fragile security policies and global access of 5G devices anytime, anywhere may also give rise to different security threats [13]. Adversaries may maliciously control and abuse the communication infrastructure of the connected system, including nuclear facilities and vehicular network [14]. Thus, there is a need for the design and development of efficient solutions to support security and data analytics for intelligent 5G-enabled IoT. Recently, deep learning (DL) has become a promising analytic paradigm due to its excellent operation in analyzing huge amounts of data. Unlike the traditional machine learning approach, DL supports efficient feature engineering by managing reliable and automatic feature extraction and representation [15, 16]. As a strong analytic tool, DL can deliver state-of-the-art accuracy and latency than the traditional machine learning approach, and it can be deployed to analyze massive data in 5G-enabled IoT. Such DL deployment can support the prediction of future event and detection of attacks and provide substantial information for content caching and placement in dynamic scenarios of 5G-enabled IoT [17, 18].

As an emerging technology, blockchain is becoming a promising choice for handling security and privacy in next-generation communication infrastructure. It creates a peer-to-peer (P2P) transactions platform wherein the information is recorded, validated, and exchanged in a decentralized manner to deliver data security and verification independent from a centralized authority [19]. The critical features of blockchain including decentralization, security, and anonymity can implement secure transactions of data and overcome the centralized server dependency to support security in 5G-enabled IoT [20]. Furthermore, the unique properties of distributed data storage, asset tracking, and smart contracts make blockchain technology desirable for 5G-enabled IoT [21].

The aforementioned discussion suggests that the development of DL and blockchain-based mechanisms can be combined to overcome data analytic and security challenges in 5G-enabled IoT. In addition, fog and edge computing can process the data nearer to the data source instead of the cloud layer to help overcome the constraints of bandwidth and computation and high latency challenges. The actionable intelligence supported by the distributed computing of fog and edge enhances the capability of translating big data-at-rest and data-in-motion into instantaneous process [22]. Thus, secure orchestration and intelligent services can be developed in 5G-enabled IoT by developing machine learning and blockchain-based solutions at the fog and edge computing layers [24].

Research contribution: The main contributions of the research work are as follows:

- This paper identifies the design and development requirements of 5G-enabled IoT and presents the required design principle for emerging networks and services.
- Based on the required design principle, we propose a DL and blockchain-empowered security framework for intelligent 5G-enabled IoT that employs DL and blockchain's capability to support intelligent data and security operations across the 5G-enabled IoT network.
- The framework's hierarchical architecture wherein

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3077069, IEEE Access

DL and blockchain operations are described along with the four layers of cloud, fog, edge, and user is presented.

- To demonstrate the feasibility of the proposed framework in the practical application, we simulated it. The performance was evaluated on an object detection application using various standard measures of latency, accuracy, and security.

II. REQUIRED DESIGN PRINCIPLES

The proposed security framework considers some fundamental aspects of design and development in the 5G-enabled IoT environment to handle the existing and evolving network and service requisites. These aspects can be described as follows:

Scalability: The scalability of an information and communication system is described by its potential to handle a growing number of devices associated with it. The service overhead, i.e., communication bandwidth, latency, energy efficiency, security, and data analytics, can be impacted by the number of associated devices in the commination system. As 5G-enabled IoT supports a higher number of devices than traditional IoT, the factor of scalability should be considered to design security and data analytic solutions for it.

Reliability and Performance: The total consistency of measurement by a system is defined by its reliability and performance aspects. A highly reliable system delivers identical performance outcomes in a definite environment and a consistent situation. Since security and data analytic are critical features in 5G-enabled IoT, the proposed security and intelligent design should be reasonably reliable and considerable in terms of performance. Low reliability and performance can lead to the failure of overall 5G-enabled IoT operations, causing financial losses and allowing gains for attackers. The performance outcomes of the proposed design need to be precise, reliable, and re-implementable in the dynamism of the testing environment. To ensure reliable measurement, the proposed design is tested repeatedly over a definite time period in a certain experimental and testbed setup that enables achieving accurate performance outcomes in 5G-enabled IoT.

Quality of Service (QoS): The overall performance of a system is measured by QoS that demonstrates how a newly proposed design is feasible in a practical environment. It relies on various factors, including accuracy, latency, computation overhead, availability, security, and privacy, to measure the overall performance. Our development of new secure and intelligent solutions for 5G-enabled IoT also considers QoS factors to validate real-time application feasibility.

Computational Complexity: It improves the efficiency of a system by measuring the computational feasibility of operation. It supports the measurement of additional overhead by supplementary applications that are added for the emergence and advancement of the system. Since the proposed security framework employs blockchain technology as well as a machine learning paradigm that can provide additional overhead, it is essential to measure the computational complexity of the framework to validate its efficiency and real-time deployment. We consider CPU and memory overhead to measure the computational complexity of the proposed framework.

Security measurement: The data-intensive applications of 5G-enabled IoT, such as autonomous driving, virtual reality, and augmented reality, require the security and privacy measurement of the data circulating in the entire network system to ensure autonomous and instantaneous services. Our proposed design reflects security measurement as a core consideration that relies on security's fundamental aspects, including confidentiality, integrity, and availability.

Quality of Experience (QoE): It describes the user's experiences and satisfaction level (i.e., annoyance or delight) with a service or a system. A number of factors related to data (privacy), network (bandwidth), and communication (latency) are considered to perceive the QoE of a service. For instance, the user satisfaction ratio of content caching is measured by employing various standard parameters, such as traffic intensity, storage size, and backhaul capacity.

III. Design Overview of the Proposed Framework

The proposed framework aims to support intelligent and secure data analytic services by deploying DL and blockchain technologies in 5G-enabled IoT. It delivers secure orchestration and flexible networking by configuring a hierarchical architecture as illustrated in Fig. 1, wherein DL and blockchain mechanisms are deployed on four layers of cloud, fog, edge plane, and device. The configuration and operation of each layer are described below.

A. Cloud Plane

Servers with high-performance computing, processing, and caching capabilities are configured to design the cloud layer. A large-capacity storage space equipped with advanced operations, such as estimation algorithms (i.e., collaborative filtering), DL, and big data mining, is leveraged to assist in the pre-allocation of services or forecasting and estimation of future incidents to transform networking and computing tasks from reactive state to proactive state. Robust computing capability and adequate caching resources at the cloud server aid in additional services, including the processing of delay-tolerant services and log-less strategic content and huge volume of data. The management of security keys and parameters of entities at the lower layers (i.e., fog nodes, Macro Base Station (MBS), Small Base

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3077069, IEEE Access

Station (SBS), and IoT devices) is carried out by deploying a central authority equipped with tamper-resistant hardware in the cloud layer. The data analytic task is carried out on a cloud layer that consists of the following major components:

Raw Data Collection: The data analytic operation starts with the collection and management of raw data consisting of different types (such as videos, images, and text) from diverse sources, including Social Networking Services (SNSs), mobile devices, IoT devices, wearable devices, and many more. These data can be collected and managed by existing applications or by developing innovative applications that rely on the types of data sources. For instance, SNSs employ various application programming interfaces (APIs), such as Twitter API and Facebook API, to collect and manage their data for near-real-time data analysis purposes [25]. Our research [26] developed a mobile application to accumulate mobile data (i.e., values of mobile's sensors) for caching management.
Data preprocessing: It is performed to eliminate noisy, unnecessary, or inappropriate data from the raw data. Here, data is properly structured and processed proficiently to support efficient data mining and feature extraction. Data processing relies on various aspects, including real-time processing of data, different types of data from different sources, and huge quantity of data (i.e., in order of petabytes). Various data processing engines, such as Apache Spark, a high-performance relational or distributed database, are used to do away with the immense processing effort.

Feature extraction: Features play a significant role in data analysis in the cloud layer. The selection of relevant and appropriate features can support effective and robust data analytic operation. In a broad sense, we can divide the relevant features into three types. Intrinsic features signify the inherent aspects of entities, such as personality, gender, and age. Actional features represent the ideological or behavioral aspects produced by users, such as patterns of the content generated or viewed by an entity. Finally, societal features represent the social contexts of entities within the social circle, such as discriminative network characteristics. The choice of the relevant features relies on the following fundamentals:

- *Differentiability:* It defines the capability of a feature to differentiate multiple entities. An entity can be evidently differentiated by a type of feature or a combination of multiple types of features. Among all the features, actional feature shows high differentiability due to its reliance on unique patterns (i.e., behavioral or content access).
- *Tenacity:* The extracted features could be erratic and sporadic patterns, which further make them inconsistent and less effective for use in data analytic operation.
- *Adaptability*: Due to technological advancements, a malicious entity can imitate the patterns of an ordinary entity and falsify the whole data analytic process by implanting false data. Intrinsic and actional features are more vulnerable to adaptability and can be easily adapted by a malicious user to pose as an ordinary user. Societal features, however, are more robust against adaptability because they rely on social contexts of entities within the social network, which cannot be dynamically changed by a malicious user. Table 1 summarizes the different features based on their substances and significance for essential fundamentals.
- *Estimation algorithm:* It refers to an automatic learning method that supports the execution of process data (i.e., data with extracted features known as training data) to estimate future events or decisions. Collaborative filtering [27] is a widely used estimation technique that estimates unknown patterns based on direct experience or sample data. [SEP]

Table 1. Different types of features and their characteristics

	Intrinsical	Actional	Societal
Entity metaphor	What do they seem like?	How do they act?	With whom do they connect?
Substance	Intrinsic facts about an entity such as personality, gender, age.	Activity facts about an entity in the context of content generation patterns	Social connection of an entity, such as friend list of an social network user
Adaptability	Weak	Moderate	Strong
Tenacity	Moderate	Strong	Moderate
Differentiability	Moderate	Strong	Weak

B. Fog Plane

The cloud layer allocates storage and computation load to many fog nodes at the fog layer to improve real-time applications' performance and overcome the issues of large data analysis and fast response in 5G-enabled IoT. The fog computing paradigm delivers massive parallelism that settles throughput and load among various computing nodes. Each fog node is deployed with blockchain and SDN controller that allows dynamic and distributed network configuration programmatically to support data monitoring and network performance. The machine learning is programmed in the SDN controller for analyzing and classifying network data to recognize various data patterns, such as malicious data. The blockchain provides secure, decentralized, Peer-to-Peer transactions of data among the fog node and its connected edge nodes to support secure participation of edge nodes and increase data availability

for efficient data analysis. Due to incompetent resource management, the fog node could be vulnerable to various security attacks and exploitation of "zero-day" vulnerabilities. Considering security and service management as key aspects, we designed an SDN-based fog node wherein an SDN controller consists of the following components:

Traffic flow analyzer: The data traffic from various edge nodes is analyzed at the fog node to improve resource management and security. The traffic flow analyzer supports the analysis task wherein patterns of data traffic such as frequency of data sending and receiving by an edge device, bandwidth utilization, and many more are accumulated and employed as training data for analysis purposes. Besides, several known patterns of malicious data traffic, such as blacklisted IP addresses of source and destination, TCP flooding patterns, etc. are also added to the training data to identify attacks and malicious behaviors across the network.

Traffic flow classifier: The data traffic classification delivers the seizure or stoppage of unnecessary and malicious data traffic to speed up the data processing task and reduce the latency delay by processing only valued data. The traffic flow classifier aids in data traffic classification, wherein Machine Learning (ML) paradigms are employed over the training data to prepare the classification model (i.e., trained model). The selection of an ML paradigm depends on the structure of training data (i.e., ratio of labeled and unlabeled data). For instance, supervised learning is employed for a sufficient amount of labeled data. In contrast, an unsupervised learning approach is used in case of a lack of labeled data or when only unlabeled data are available.

Service Management: The management of the services relies on dynamic and distributed policies to support flexible fog infrastructure and services. The policy manager at the fog node supports policy-driven services that include the registered device's status, service orchestration, and service directory. Software-defined protection is maintained by the service orchestration that enables flexibility and dynamic configuration across the network to handle different types of threat patterns, including existing and new ones.

Context Awareness Module and Distributed Database: The 5G-enabled IoT supports a higher number of sensors that lead to a massive amount of raw sensor data. To understand and add value to the sensor data, contextual computing plays a significant role. It implies context awareness, including location awareness and activity awareness, to help recognize different activities and identify the movement of 5G-enabled IoT devices in a specific territory or a specific region. On the other hand, the increment in fault tolerance and scalability due to massive data is managed by the distributed database that supports smart storage and retrieval of data (i.e., faster), unlike centralized storage. All the application data, policies, and metadata are logged by the distributed database to facilitate fog management.

C. Edge Plane

Several edge nodes contribute to distributing the load of the fog node at the edge layer, wherein network entities, including SDN switches, MBSs, and SBSs, are geo-distributed and configured with blockchain application and MEC server. These network entities can support instant wireless communication and seamless coverage to deliver radio interfaces for 5G-enabled IoT devices. The computing resources are configured in MEC servers that perform computing tasks intelligently to carry out computation-intensive jobs and operate delay-sensitive applications, including caching strategic content (i.e., recent videos) and DL for data analysis. An SDN controller updates the flow rules to the associated SDN switches to detect and mitigate malicious activates at the network edge. All edge nodes are associated with a fog node connected via a blockchain network to carry out the secure sharing of data and resources among them.

SDN-based edge node: Each edge node (i.e., base station) is a configured local edge controller enabled with SDN. It consists of several components, including cache management, switches information, channel monitoring, network resources, traffic monitoring, and radio resources. The local controller facilitates the flow table at each network switch, wherein specific rules are defined and implemented by translating the network policies employing ternary content addressable memory (TCAM). Due to the limited TCAM, only a few hundred entries can be logged in the flow tables. It further enforces reactively caching rules by switches, resulting in packet delays and large buffers in case of cache misses. Many approaches can be employed to facilitate efficient flow rules management in SDN. Huang, *et al* [28] partitioned the flow rules in the heterogeneous flow table distribution considering the characteristics, including the allocation scheme, dependency, and same policies. Mosherf, *et al* [29] employed a vCRIB algorithm to minimize traffic redirection and mitigate the issue of resource constraints on switches. In our proposed framework, we employed "RPAL," our recently presented flow rules partition algorithm that leverages the advantage of that of Huang, *et al* [28] (i.e., dependency and policy-enabled partition mechanism) and Mosherf, *et al* [29] (i.e., traffic and resource-conscious allocation mechanism).

Blockchain network: To enable less resource-intensive blockchain operation (i.e., blockchain mining task), a private blockchain is configured in the proposed framework. Unlike the public blockchain, it foregoes the need for an economic incentive mechanism. The blockchain application is deployed on fog nodes and their associated edge nodes. Here, as a full blockchain node, a fog node performs resource-intensive tasks, including generating and propagating blocks and monitoring the transactions. In contrast, as a light blockchain node, an edge node communicates and logs its transactions. To facilitate

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3077069, IEEE Access

blockchain deployment, a lightweight consensus, for instance, Practical Byzantine Fault Tolerance (PBFT) [96]

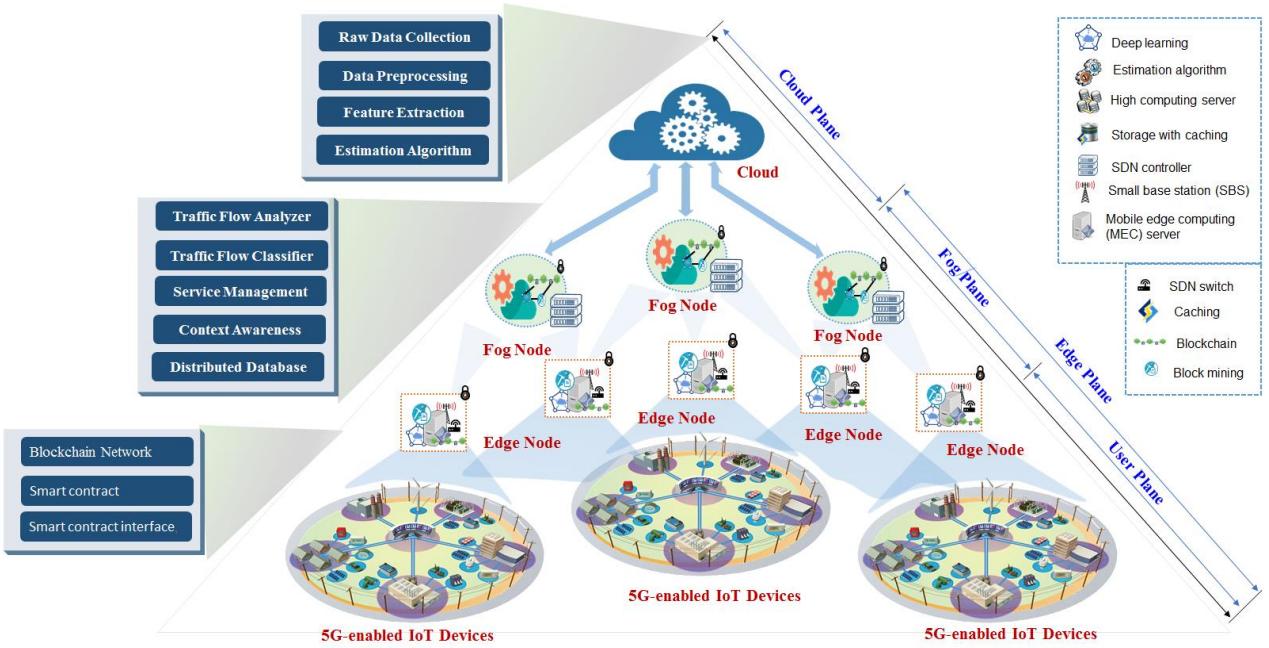


Fig.1 Design overview of the proposed security framework

that supports no proof-of-work and resource constraints mining, is used.

Smart contract: It defines service contracts (i.e., rules and policies) among all nodes, including the fog node and its associated node across the blockchain network, to operate and govern the data services. The contracts consist of data contract and processing contract. The data contract describes the rules and policies to facilitate data transactions at the edge nodes in the blockchain network (i.e., delivery of data from each edge node to its associate fog node), while processing contract liable for data processing at the fog node from its associated edge nodes and block generation and mining.

Smart contract interface: The smart contract interaction among fog node and edge nodes is set up and executed via a smart contract interface. It facilitates the various important tasks of smart contracts' operations such as registration whenever a new node participates in the blockchain network, uploading (i.e., data from edge nodes to their associated fog node), and requesting (i.e., request processed data by an edge node from an associated fog node). It can be configured using the JavaScript-based Application Programming Interface (API) such as Web3 protocol. Here, programming functions are called to execute policies and rules in smart contract operations.

D. User Plane

Several 5G-enabled IoT devices are clustered with an edge node in its coverage via 5G communication.

IV. Experimental Evaluation

This section presents a case study to validate the feasibility of the proposed framework in the practical application. The case study involves object detection tasks at the three different planes, specifically how the proposed services can play a significant role in overcoming existing challenges in 5G-enabled IoT. Each plane employs the basic components and technologies described in the previous section.

A. Experimental configuration

The experimental evaluation of the proposed framework was carried out by implementing a prototype model with four major components: cloud server, fog nodes, edge nodes, and 5G-enabled IoT devices. Here, Amazon EC2 cloud data center is employed as a cloud server supporting high-performance computing, processing, and caching capabilities, configuring SVDFeature [30] as an estimation algorithm to estimate strategic contents. An OpenStack deployment functions as the fog computing nodes, wherein high-performance Dell PowerEdge R630 and Dell PowerEdge C730x rack servers and Cisco 3850 switch are deployed. The typical configuration of each rack server includes 18 independent CPU cores, 256 GB RAM, and a CentOS 7. Python-based software-defined networking, known as the POX controller [31], is employed as a development platform to facilitate the SDN-based fog node. Workstations with Intel processor are deployed to function as the edge nodes and 5G-enabled IoT devices. A total of 40 workstations are configured wherein each workstation is associated with several Raspberry Pi 3 Model B single-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3077069, IEEE Access

board computers. The configuration of each Raspberry Pi includes the Raspbian Operating System, 1 GB RAM, and 32GB storage and consists of additional accessories including cameras and Google bonnet. A MacAir laptop with 4 GB RAM is set up to monitor and analyze the entire network's operation. A 5G network is configured with a high-performance Cisco WiFi. The blockchain configuration at each fog and edge node includes Go-*ethereum [32] for private blockchain setup*, solidity language for writing smart contracts, and Truffle development suite for blockchain deployment. The DL application is set up by each node by employing Tensorflow version 2.0.

The object detection problem is widely discussed by many researchers, such as indoor guarding, crowd control, and city surveillance, requiring highly accurate result at low latency. For object detection, a well-known MS COCO dataset containing 82,783 training instances and 40,504 validation instances of 80 different object classes [33] was used.

B. Experimental Results

For object detection, video frames (objects) were captured with a camera module integrated with Raspberry Pi in 60Hz frequency and 1080p resolution and processed by employing the proposed framework. We carried out the object detection task at the different plane (i.e., cloud, fog, and edge) that illustrates distinct performance outcomes and feasibility for the task. To measure performance outcomes, standard evaluation metrics, including Mathew Correlation Coefficient (MCC), *Mean precision accuracy*, F-measure, Detection Rate, Latency, and area under the Receiver Operating Characteristic (AUC) curve were used. We measured these standard metrics with a varying amount of data traffic. As shown in Fig. 2, the detection task at the edge plane always outperformed that at the fog and cloud planes. However, the fog plane distributes the task to several fog nodes (i.e., employing SDN controllers) instead of processing the data at the central cloud server, which supports efficient processing and data availability to increase performance compared to the cloud plane. On the other hand, the edge plane decentralizes the processing task among several edge nodes (i.e., employing blockchain) and shares only significant data (i.e., DL model parameters) to the fog node rather than the whole data. It lowers the reluctance of an edge node to participate in the detection task that supports higher cooperation, thereby leading to better task performance than the fog plane.

In order to evaluate the QoE of the proposed framework, we considered measurements of the satisfaction ratio and the backhaul load with variation in traffic intensity. Here, the satisfaction ratio signifies the fraction of the detection requests satisfied, and the backhaul load describes the ratio of average traffic carrying by the backhaul links to the total amount of traffic generated at the different planes. Traffic intensity indicates the average count of requests arriving within a given time slot.

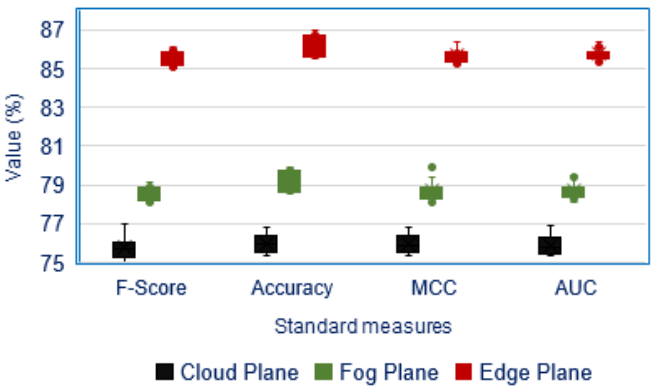


Fig. 2. Performance measurement of the proposed security framework

Fig. 3(a) shows that the edge plane has higher satisfaction ratio than the fog and cloud planes. Obviously, the edge plane satisfies more detection requests than the fog plane due to decentralization, and the fog plane further satisfies more detection requests than the cloud plane due to distribution. Fig. 3(b) shows that the cloud plane contributes to higher backhaul load due to the highest amount of traffic carrying by the backhaul links to perform the task, whereas going to the lower plane from fog to edge decreases the load of backhaul links.

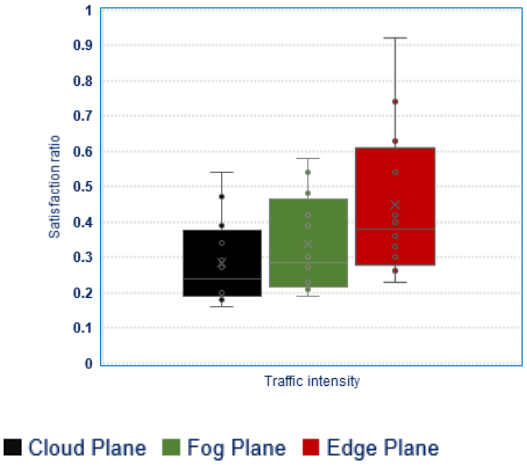
We also evaluated the QoS of the proposed framework by measuring factors, including accuracy and latency, with the varying data traffic rate. Fig. 4(a) shows the increment in latency with the increasing amount of data traffic for all three planes. Since edge nodes prepare the detection models at their end, which has higher proximity to the end devices than the detection model at the fog node, such further leads to lower latency at the edge plane. In general, proceed from the cloud toward the edge plane with higher proximity to end devices that lower the latency. Similarly, Fig. 4(b) illustrates the significant improvement in accuracy with the varying amount of data traffic. However, the use of the SDN controller and distribution of data processing at the fog plane support a higher quantity of data for detection tasks, leading to a more accurate detection model than that of the cloud plane. Furthermore, the edge plane employs blockchain technology that enables cooperation among several edge nodes (i.e., sharing local model updates to an associated fog node) to prepare an accurate global model update for an excellent detection task.

V. Conclusion

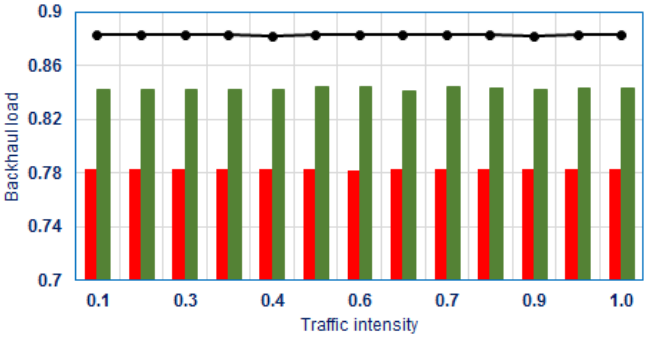
This study investigated the design and development requirement for emerging networks and services in 5G-enabled IoT. A DL and blockchain-powered security framework for intelligent 5G-enabled IoT that delivers intelligent data and security operations across the 5G-enabled IoT network was presented. The proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3077069, IEEE Access

framework contributes to employing DL and blockchain strength along with the four layers of a hierarchical

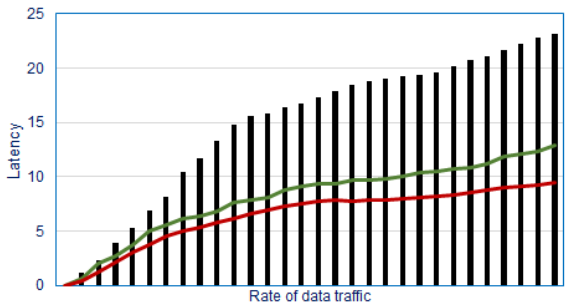


(a)

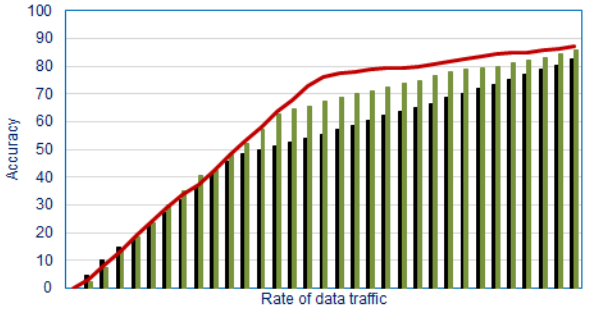


(b)

Fig. 3. Performance of the proposed security framework in terms of a) Satisfaction ratio and b) Backhaul load with variation in traffic intensity



(a)



(b)

Fig. 4. Performance of the proposed security framework in terms of a) Latency and b) Backhaul load with variation in traffic intensity

architecture: cloud, fog, edge, and user. The proposed framework's simulation was done on a widely used object detection task to validate its feasibility in practical applications. The simulation results demonstrate that the proposed framework satisfies the fundamental aspects of design and development in a 5G-enabled IoT environment, including scalability, reliability and performance, QoS, computational complexity, security and privacy, and QoE.

ACKNOWLEDGMENTS

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-2018-0-01799) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation)

REFERENCES

[1] Khan, R., Kumar, P., Jayakody, D. & Liyanage, M. (2019). "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," IEEE Communications Surveys & Tutorials, 22(1), pp. 196-248

[2] Agiwal, M., Saxena, N., & Roy, A. (2019). "Towards connected living: 5G enabled internet of things (IoT)," IETE Technical Review, 36(2), pp. 190-202

[3] Chettri, L., & Bera, R. (2019). A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet of Things Journal*, *7*(1), 16-32.

[4] 5G IoT Market. Accessed: May. 2020 [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/5g-iot-market-164027845.html

[5] Ericsson Mobility Report. Accessed: May. 2020 [Online]. Available: https://www.ericsson.com/en/mobility-report/reports/november-2019

[6] The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. Accessed: May. 2020 [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[7] Al-Aqrabi, H., Johnson, A. P., Hill, R., Lane, P., & Liu, L. (2019). "A multi-layer security model for 5G-enabled industrial Internet of Things," In International Conference on Smart City and Informatization, Singapore, 2019, Springer, pp. 279-292

[8] 5G Security Market by Technology, Solution, Category, Software, Services, and Industry Vertical Support 2020–2025. Accessed: May. 2020 [Online]. Available: https://www.researchandmarkets.com/reports/4846259/5g-security-market-by-technology-solution

[9] Sara, J. J., Hossain, M. S., Khan, W. Z., & Aalsalem, M. Y. (2019, October). Survey on Internet of Things and 4G. In *2019 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)* (pp. 1-6). IEEE.

[10] https://m2mconnectivity.com.au/4glte-for-the-internet-of-things-iot/

[11] Hassebo, A., Obaidat, M., & Ali, M. A. (2018). Commercial 4G LTE cellular networks for supporting emerging IoT applications. In *2018 Advances in Science and Engineering Technology International Conferences (ASET)* (pp. 1-6). IEEE.

[12] Nejkovic, V., Visa, A., Tosic, M., Petrovic, N., Valkama, M., Koivisto, M., ... & Kuonen, P. (2019). Big data in 5G distributed applications. In *High-performance modelling and simulation for big data applications* (pp. 138-162). Springer, Cham.

[13] Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). 5G in the Internet of Things era: an overview on security and privacy challenges. *Computer Networks*, 107345.

[14] Lai, C., Lu, R., Zheng, D., & Shen, X. S. (2020). Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Network*, *34*(2), 37-45.

[15] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). "Deep learning for IoT big data and streaming analytics: A survey," IEEE Communications Surveys & Tutorials, 20(4), pp. 2923-2960

[16] LeCun, Y., Bengio, Y., & Hinton, G. (2015). "Deep learning," Nature, 521, pp. 1-436

[17] Wang, D., Chen, D., Song, B., Guizani, N., Yu, X., & Du, X. (2018). From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies. *IEEE Communications Magazine*, *56*(10), 114-120.

[18] Mohammed, T., Albeshri, A., Katib, I., & Mehmood, R. (2020). UbiPriSEQ—Deep Reinforcement Learning to Manage Privacy, Security, Energy, and QoS in 5G IoT HetNets. *Applied Sciences*, *10*(20), 7120.

[19] Singh, S. K., Rathore, S., & Park, J. H. (2020). Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems*, *110*, 721-743.

[20] Rathore, S., Kwon, B. W., & Park, J. H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *Journal of Network and Computer Applications*, *143*, 167-177.

[21] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*, 102693.

[22] Roman, R., Lopez, J., & Mambo, M. (2018). "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, 78(2), pp. 680-698

[23] Park, J. H., Salim, M. M., Jo, J. H., Sicato, J. C. S., Rathore, S., & Park, J. H. (2019). "CIoT-Net: a scalable cognitive IoT based smart city network architecture," Human-centric Computing and Information Sciences, 9(1), pp. 1-29

[24] Khan, M. A. (2019, October). Fog Computing in 5G Enabled Smart Cities: Conceptual Framework, Overview and Challenges. In *2019 IEEE International Smart Cities Conference (ISC2)* (pp. 438-443). IEEE.

[25] S. Rathore, V. Loia, and J. H. Park, "SpamSpotter:An efficient spammer detection framework basedon intelligent decision support system onfacebook," Appl. Soft Comput., vol. 67,pp. 920–932, 2017.

[26] Rathore, S., Ryu, J. H., Sharma, P. K., & Park, J. H. (2019). DeepCachNet: A proactive caching framework based on deep learning in cellular networks. *IEEE Network*, *33*(3), 130-138.

[27] J. Lee et al., "A Comparative Study of Collaborative Filtering Algorithms," arXiv: 1205.3193, 2012.

[28] J. F.Huang et al., "Heterogeneous Flow Table Distribution in Software-Defined Networks," IEEE Trans. Emerging Topics in Computing, vol. 4, no. 2, 2016, pp. 252–61.

[29] M. Moshref et al., "Scalable Rule Management for Data Centers," Proc. NSDI, vol. 13, Apr. 2013, pp. 157–70.

[30] T. Chen et al., "SVDFeature: A Toolkit for Feature-Based Collaborative Filtering," J. Machine Learning Research, no. 13, Dec. 2012, pp. 3619–22.

[31] Noxrepo, 23-Nov-2017. noxrepo/pox," GitHub [Online]. Available: https://github.co m/noxrepo/pox. (Accessed 30 November 2018).

[32] bitfly.at, "Etherchain," Charts - etherchain.org - the ethereum blockchain Explorer. [Online]. Available: https://www.etherchain.org/[Accessed: 30-Nov-2018].

[33] COCO dataset. [Online]. Available: http://cocodataset.org/#download.

BIOGRAGHY

Dr. Shailendra Rathore received Ph.D. degrees in the Graduate School of Computer Science and Engineering at Seoul National University of Science and Technology, Seoul, South Korea (June 2020). Dr. Rathore is now an assistant professor in the School of Engineering, Computing & Mathematics, University of Plymouth, England, United Kingdom. Prior to beginning the Ph.D. program, he worked as a researcher at Crompton Greaves Global R&D Center, Mumbai, India. He received his master's degree in Computer Science from the Thapar University, India in 2014. His current research interests are focused on the areas of Artificial intelligence, Blockchain, Information security, and IoT. He is the author of various top journal and magazine articles in the field of computer science. He is reviewer of IEEE Transaction of Industrial Informatica, IEEE wireless communication magazine, IEEE Transactions on Network and Service Management, and FGCS.

Dr. James J. (Jong Hyuk) Park received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December, 2002 to July, 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September, 2007 to August, 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor

at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has been serving as chair, program committee, or organizing committee chair for many international conferences and workshops. He is a steering chair of international conferences – MUE, FutureTech, CSA, CUTE, UCAWSN, World IT Congress-Jeju. He is editor-in-chief of Human-centric Computing and Information Sciences (HCIS) by Springer, The Journal of Information Processing Systems (JIPS) by KIPS, and Journal of Convergence (JoC) by KIPS CSWRG. He is 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 Univ. press, Emerald, Inderscience, MDPI. He got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, PDCAT-11, IEEE AINA-15. Furthermore, he got the outstanding research awards from the SeoulTech, 2014. His research interests include IoT, Human-centric Ubiquitous Computing, Information Security, Digital Forensics, Vehicular Cloud Computing, Multimedia Computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.

Dr. Hangbae Chang is a Professor at Chung-Ang University. He received his Ph.D. in Information System Management from the Graduate School of Information at Yonsei University, Korea. He has published many research papers in international journals and conferences. He has served as chairs, in program committee or organizing committee for many international conferences and workshops viz., FutureTech, WCC, ITCS, CSA and so on. His works have been published in journals such as Journal of Super Computing, Electronic Commerce Research, Computers and Mathematics with Applications, Mathematical and Computer Modeling, Mobile Information Systems, Personal and Ubiquitous Computing, and Journal of Internet Technology. His research interests include issues related to Security Management and System in Internet of Things Environment.