IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 30, 2020, accepted July 19, 2020, date of publication July 23, 2020, date of current version August 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3011503

A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System

JUNXIA LI[1], JINJIN CAI[2], FAZLULLAH KHAN[3,4], (Member, IEEE), ATEEQ UR REHMAN[5], (Member, IEEE), VENKI BALASUBRAMANIAM[6], (Member, IEEE), JIANGFENG SUN[1], (Member, IEEE), AND P. VENU[7]

[1]School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454000, China
[2]College of Mechanical and Electric Engineering, Hebei Agricultural University, Baoding 071001, China
[3]Informetrics Research Group, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam
[4]Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam
[5]Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, Pakistan
[6]School of Science, Engineering and Information Technology, Federation University, Mount Helen, VIC 3350, Australia
[7]Department of Mechanical Engineering, SCMS School of Engineering and Technology, Ernakulam 683576, India

Corresponding author: Fazlullah Khan (fazlullah@tdtu.edu.vn)

ABSTRACT The Internet of Things (IoT) consists of resource-constrained smart devices capable to sense and process data. It connects a huge number of smart sensing devices, i.e., things, and heterogeneous networks. The IoT is incorporated into different applications, such as smart health, smart home, smart grid, etc. The concept of smart healthcare has emerged in different countries, where pilot projects of healthcare facilities are analyzed. In IoT-enabled healthcare systems, the security of IoT devices and associated data is very important, whereas Edge computing is a promising architecture that solves their computational and processing problems. Edge computing is economical and has the potential to provide low latency data services by improving the communication and computation speed of IoT devices in a healthcare system. In Edge-based IoT-enabled healthcare systems, load balancing, network optimization, and efficient resource utilization are accurately performed using artificial intelligence (AI), i.e., intelligent software-defined network (SDN) controller. SDN-based Edge computing is helpful in the efficient utilization of limited resources of IoT devices. However, these low powered devices and associated data (private sensitive data of patients) are prone to various security threats. Therefore, in this paper, we design a secure framework for SDN-based Edge computing in IoT-enabled healthcare system. In the proposed framework, the IoT devices are authenticated by the Edge servers using a lightweight authentication scheme. After authentication, these devices collect data from the patients and send them to the Edge servers for storage, processing, and analyses. The Edge servers are connected with an SDN controller, which performs load balancing, network optimization, and efficient resource utilization in the healthcare system. The proposed framework is evaluated using computer-based simulations. The results demonstrate that the proposed framework provides better solutions for IoT-enabled healthcare systems.

INDEX TERMS Healthcare systems, security, software-defined network, edge computing, Internet of Things.

I. INTRODUCTION

The development and proliferation in hardware technologies have enabled the integration of Artificial Intelligence (AI), Internet of Things (IoT), Edge Computing, and real-time decision making. The integration of AI and IoT has coined a new term, the Artificial Intelligence of Things (AIoT), where the IoT devices metaphor the digital nervous system and AI as the brain of a system. In AIoT, the IoT devices have some limitations such as accuracy and speed of data transmission, whereas AI does not have human-like intelligence but to learn from a pattern and improve itself [1]. The AIoT is entering daily operations of various industrial applications such as smart health, smart city, smart retail,

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

industrial automation, logistics, and transportation, etc [2]. In these applications, the AIoT devices transmit data to the Cloud servers via Edge computing for decision making. For example, a smart city application improves the Quality of Life (QoL) by providing healthcare facilities securely and efficiently. The AIoT-enabled health applications gained popularity after integrating AI-enabled Edge computing and heterogeneous IoT-enabled networks for transmitting medical data in an efficient and timely manner. This integration of heterogeneous IoT-enabled networks, wearable devices, AI, IoT, and Edge computing has increased the interest of academia and industry. For example, the 2018 survey of SADA systems [3] listed AI, Edge computing, and IoT as the most popular technologies currently used and companies investing the most are AIoT as shown in Fig. 1. Currently, AI-enabled Edge computing in healthcare systems is very critical for the research community to solve major issues at a global level.

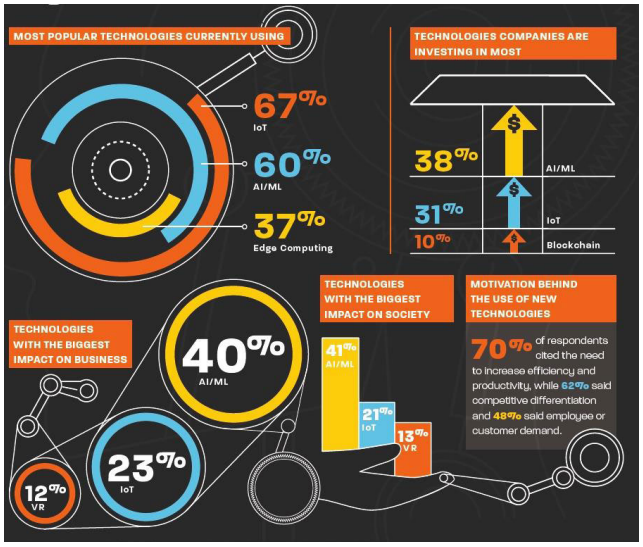

FIGURE 1. Popular Technologies by percentage, IoT 67%, AI 60%, Edge computing 37% [3].

The fundamental issues with most of the IoT-based applications are the resource-constrained nature of IoT devices and their security. As a result, AIoT applications are getting popularity by securely and efficiently utilizing the limited resources of IoT devices, particularly in healthcare [4], [5]. Because in healthcare systems IoT devices continuously monitor patients and transmit the required data constantly [6], that need to be protected from malicious activities. AIoT enhances the operational efficiency of healthcare by reducing administrative work of clinical staff. In this way, healthcare practitioners have more time to spend with patients as desired in a patient-centric approach. Furthermore, it also provides facilities like tracking of patients, healthcare practitioners, drug inventory, drug management, remote health control, real-time monitoring, and analysis [7]. Real-time monitoring and analysis of healthcare data have two fundamental problems, secured and continuous data transmission. The best way to secure a low-powered IoT-enabled network is through lightweight authentication schemes. For example, [8] has used a fast authentication scheme in large-scale IoT by using a support vector machine for quantizing the features of a probed channel. The quantized features have been used for generating a pseudo-random binary sequence (PRBS). On the other hand, the continuous transmission is not possible on low-powered AIoT devices while collecting multiple data from the body of a patient. To overcome these limitations, it is desired to use a lightweight authentication scheme and process data at the network edge, close to the wearables, using Edge computing. In AIoT, AI is embedded into IoT devices and augments Edge computing to bring intelligence to the IoT devices [9]. It is better to use AI techniques at the network Edge in IoT-enabled networks. Because the data generated by IoT devices can fuel AI techniques to increase intelligence in the IoT devices and Edge servers. A common way in the design of such a system is to embed a software-defined network (SDN) controller in the Edge server or an intelligent SDN controller assists the Edge server, which is helpful in achieving load balancing and efficient resource utilization.

In IoT-enabled healthcare systems, IoT devices need to be authenticated before data transmission. After authentication, the sensed data need to be offloaded to powerful Edge computing for quick processing. The offloading to Edge should be done intelligently with the help of the SDN controller, which has the ability to develop full network programmability. The intelligence of SDN fulfills the demands of Edge computing in terms of resource allocation and load balancing, whereas security is provided by a lightweight authentication scheme. The SDN controller is responsible for data management, time-sensitivity, Edge orchestration, and to provide quick and highly reliable data transmission. These characteristics are the main requirements of a healthcare system, which are not covered in the literature. In literature, most of the researchers have studied different aspects and applications of IoT, Edge computing in IoT, AI-based IoT systems, security in IoT, and SDN. There is no single study that covers all these technologies, especially in a critical system like healthcare. Therefore, in this paper, we fill this gap and combine these technologies in a secured framework for SDN-based Edge computing in an IoT-enabled healthcare system. In the proposed framework, a lightweight authentication approach is used to authenticate low-powered IoT-enabled health networks. Furthermore, an SDN-based Edge computing is used for load balancing via collaboration between Edge servers that aim to overcome the limited capabilities of a single Edge server. The main contributions of this article are as follows:

- To the best of our knowledge, the proposed framework is the first one to integrate Edge computing and SDN with security in the IoT-enabled healthcare systems in a multi-faced data perspective. The existing studies discuss Edge computing, SDN, and security in IoT-enabled healthcare systems independently and do not consider multi-dimensional data.

- To secure the IoT-enabled healthcare system, we propose a lightweight authentication approach. Using this approach the Edge server authenticates wearable and IoT devices. After authentication, these devices exchange data with the Edge servers.
- To overcome the limited capabilities of a single Edge server, the proposed framework allows collaboration between Edge servers to solve the real-time and high-bandwidth problems in terms of load balancing and efficient network utilization with the help of SDN controller.
- To efficiently utilize network resources the SDN controller is configured in such a way to deliver the critical data on time. The proposed framework allows the migration of activities between the Edge server for load balancing and network optimization.
- Finally, we evaluate the performance of the proposed framework by conducting extensive simulations. The simulation results illustrate that the proposed framework performs better in terms of average response time, packet delivery ratio, average delay, throughout, and control overhead, thereby, providing a better solution for SDN-based Edge computing in IoT-enabled healthcare system.

The remaining paper is organized as follows. The related work is summarized in Section II, followed by the System model in Section III. In Section IV, the proposed secured framework in the IoT-enabled healthcare system is explained in detail. The simulation results and discussions are given in Section V. Finally, Section VI concluded the paper and future research directions are given.

II. RELATED WORK

In this section, we briefly discuss the fundamental concepts of IoT, security in IoT, SDN, and Edge computing.

A. INTERNET OF THINGS

Several billion devices are connected to the Internet. These are growing continuously as reported by Gartner [10], which states that approximately 8.4 billion devices were connected to the Internet. This number increased by 2.5 times in the next two years, due to the Internet of Things (IoT) concept that seems to be the backbone of the future connected world. Gartner reports that by the end of 2020 there will be 20.4 billion IoT devices connected to the Internet [10]. The IoT is a new paradigm in communication, which is the interconnection of existing devices with additional intelligence. These devices process the sensed data and communicate with other devices through the internet [11], [12]. Initially, the IoT devices were operated in the unlicensed band using Bluetooth and ZigBee technologies. Currently, the 4G mobile infrastructures are used for IoT deployment. However, they do not fulfill the IoT requirements, and new technologies are needed to improve the existing capabilities. Apart from the limitation of short-range transmission of these devices, the IoT devices have overcrowded the unlicensed spectrum. As a result, it has opened various research issues and opportunities for the research community. For example, IoT devices can use the licensed spectrum opportunistically using the concepts of cognitive radio (CR). A CR is capable of using the licensed spectrum when it is free, and this will make IoT devices suitable for long-range applications. Similarly, the notion of Licensed Spectrum Access (LSA) in 5G, which is an implementation of the CR concept, is another open research area. In this way, the applications of IoT are expanding into various fields, which causes different challenges, like security and privacy of IoT devices and networks.

B. SECURITY IN THE INTERNET OF THINGS

The resource-constrained IoT devices are vulnerable to various threats that severely affects their performance. To secure IoT-enabled networks, conventional cryptographic algorithms do not perform well, resulting in complex security issues [13], [14]. The IoT has three layers, i.e., perception layer, network layer, and application layer, where each layer is vulnerable to security threats. These threats can be active or passive and can be launched from inside or outside the network. There are numerous security attacks on IoT that can degrade network communication such as replay, sniffing, and eavesdropping, etc. However, the Sybil and denial of service (DoS) attacks are more dangerous as they deplete network bandwidth and device resources [15]. In [16], authors have discussed Cloud-Fog based IoT architecture using different features of Cloud and Fog. They have proposed a cost-effective and energy-efficient data offloading algorithm for efficient resource utilization.

C. SOFTWARE DEFINED NETWORKS

The main theme of the software-defined network (SDN) is to isolate the network control from forwarding functions, i.e., control and data plane, respectively [17]. In SDN, each networking device forwards data packets according to the rules configured on that device. The control plane is responsible for configuring the rules on network devices and controlling the network behavior. The SDN helps to simplify the control and management of next-generation networks, most importantly the IoT, Cloud Computing, and Cyber-Physical Systems [18]. These technologies have caused exponential growth in the connectivity of heterogeneous devices to the internet [19], [20]. However, security provisioning of the SDN, particularly with the advent of IoT that connects heterogeneous devices with their diverse access protocols is a real challenge leading to security risks. Furthermore, the logical centralized controlled intelligence of the SDN architecture represents a plethora of challenges due to its single point of failure [21], [22]. It remains the prime obstacle that may throw the entire network into chaos and thus expose it to various known and unknown security threats and attacks. In SDN, security still in infancy and thus presents the most striking challenge for both the industry and academia.

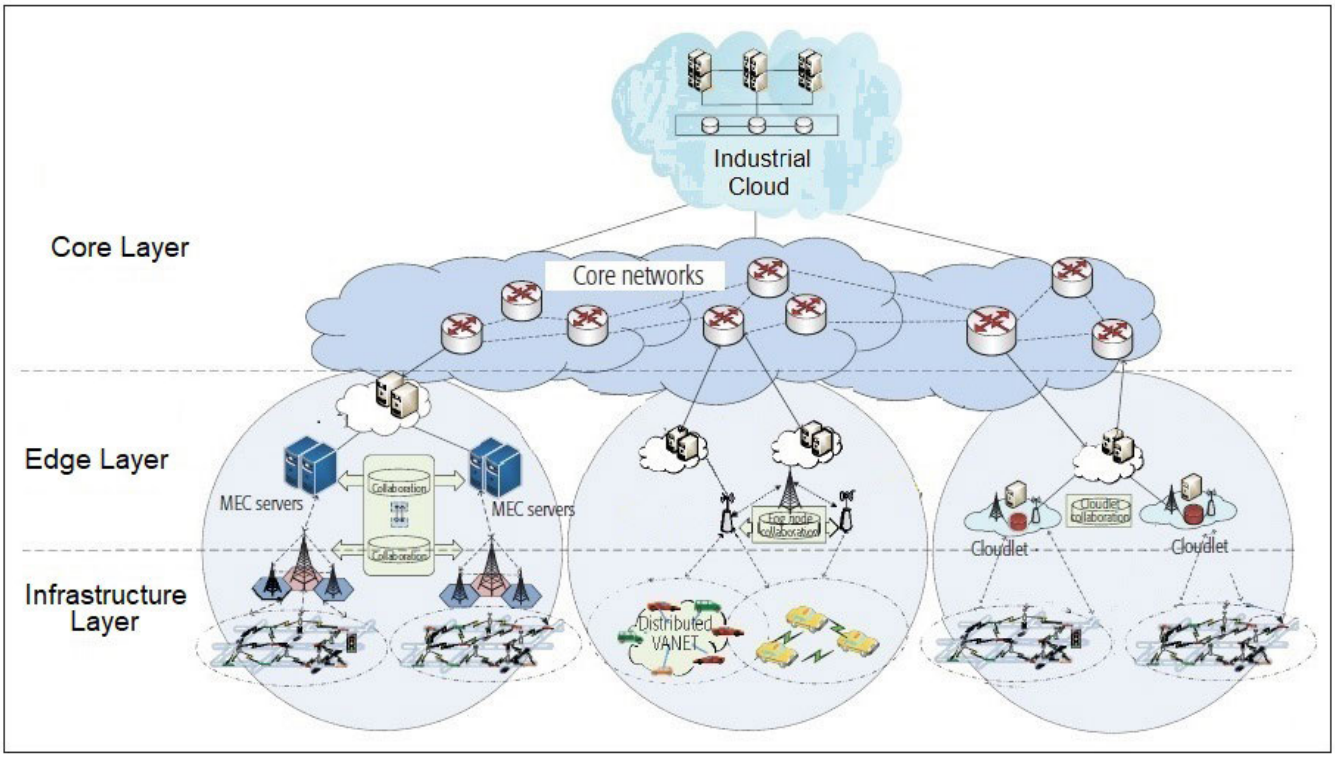

FIGURE 2. Proposed system model.

D. EDGE COMPUTING

Edge computing is an economical and efficient paradigm that extends Cloud computing. It provides low latency data services by bringing computing resources close to the edge of an IoT-enabled network. The purpose is to alleviate the processing and traffic load from low-powered IoT devices to powerful servers at the edge. In this way, load-balancing is achieved which results in lower delay and mobility support [1], [9]. Edge computing is supportive technology for IoT applications, that has numerous advantages. For example, energy-efficient communication among IoT nodes, IoT applications in vehicular networks [23], sensor and actuator networks [12], [24]. Furthermore, it is best used in applications like healthcare [15], [25], which requires context-aware processing to delay-sensitive data. In [26], authors have used the concept of clustering for decentralized Edge computing for increasing the processing capabilities of the overall system. They have used multi-channel to minimize delays and increase system stability in real-time applications. In [27], the authors have used Edge computing in secured brain-to-brain communication. They have used a wireless electroencephalogram headset using which the receiver receives the thoughts of the sender. For example, if the sender thinks a word or number, the receives it.

III. SYSTEM MODEL

In this section, we discuss the system model of the proposed framework. The proposed framework has three layers as shown in Fig. 2. These layers are the infrastructure layer, Edge computing layer, and core computing layer. The details of these layers are given below.

A. INFRASTRUCTURE LAYER

The infrastructure layer, also called the IoT-enabled healthcare architecture layer, is composed of low-powered embedded sensors and IoT devices. These devices are either attached to the patient's body or installed in the hospital. They have limited resources and use different operating systems, CPU, memory, and transmission powers. In certain cases, these devices are remote and impossible to human interventions. Therefore, it is essential to efficiently utilize these devices by authentic data and connectivity to other entities in the network.

B. EDGE COMPUTING LAYER

The Edge computing layer consists of different kinds of Edge servers. The IoT and wearable devices are huge in number having multi-functions highlighting the importance of multi-service Edge server in the network. This layer performs different functions such as data exchange, storage, processing, and job migration between different Edge servers. Furthermore, this layer deals with different kinds of data, variable packet size, associated protocols, and built-in security. However, data coming from the IoT layer may suffer from man-in-the-middle, replay, confidentiality, data

integrity, and spoofing attacks. Furthermore, it can also cause a higher delay and control overhead in the network.

C. THE CORE COMPUTING LAYER

The core layer has two parts, the core networks, and the cloud services. The core networks are responsible for hosting various applications that provide different services and manage the end-to-end architecture of IoT. This layer has a good security mechanism for data protection but is still prone to denial-of-service (DoS) attacks. For example, the wireless medium is always vulnerable to a DoS attack. The security threats in these layers can be resolved by using authentication, authorization, and cryptographic schemes.

IV. SDN-BASED EDGE IN IoT-ENALBED HEALTHCARE

In this section, we discuss our proposed secured framework for software-defined network-based Edge computing in IoT-enabled healthcare systems. The main theme of the proposed framework is divided into three phases, i.e., a lightweight authentication approach, SDN-based collaborative edge computing, and job migration on Edge servers. as discussed below.

A. LIGHTWEIGHT AUTHENTICATION APPROACH

The IoT-enabled healthcare layer has no built-in security mechanisms, and its security is mandatory for the success of the proposed framework. For this purpose, we have proposed a lightweight authentication approach. Unlike [8], the proposed authentication approach uses p-KNN for required feature extraction from the probed channel and two hash functions ($H_1(.)$ and $H_2(.)$) for encrypting the selected features and quantization results. Note that, we assumed that the hash functions are shared in the pre-deployment phase. To extract characteristics from the probed channel we have used probabilistic k-nearest neighbor (p-KNN) because it is simple to implement and robust to noisy training data. p-KNN performs classification using a simple majority vote and is sensitive to outliers and removes them to get better results. Moreover, channel probing is obtained using a lightweight probing scheme given in [28]. Using this scheme, the IoT devices are identified based on the operating frequency bands, i.e., access frequencies or time slots. The accessing frequencies of legitimate devices always need to be identical to their unique pseudo-random binary number (PBN). The PBN of a device-Edge pair is generated by using the unique characteristics and attributes of the physical layer [28], [29], extracted through p-KNN [30] as shown in Fig. 3. As evident from this figure, the device request for connection to the Edge server, and exchange channel probing signals. The Edge server uses p-KNN to obtaining the required features, applies a hash function ($H_1(.)$), and sends encrypted results to the IoT device. The device-Edge pair perform quantization, get the seed for generating PBN, and applies the hash function ($H_2(.)$) to it. The hashed values are exchanged, and PBN is generated after encrypting the hashed values. The device sends generated PBN to the Edge server for authentication, where the Edge server decides on the results obtained by matching both PBNs. In this way, authentication is performed. The pseudo-code of the lightweight authentication approach for IoT devices is presented in Algorithm 1, and flow chart in Fig. 3.

B. SDN-BASED COLLABORATIVE EDGE COMPUTING

The Edge computing layer consists of different SDN-based Edge servers, responsible for intelligent data processing, storage, and collaboration with other servers. The purpose of SDN-based Edge computing is to obtain the different quality of services, such as low latency, low response-time, higher efficiency, higher throughput, and proximity services. The SDN controller is configured in such that it performs efficient resource utilization by load balancing and optimal network configuration. The SDN controller has all the details about the storage, processing, and communicating capabilities of each Edge server along with the outgoing and incoming traffic from IoT devices. The SDN controller decides the collaboration between Edge servers based on the load on these servers and some predefined rules. In this way, efficient utilization of computational and storage resources are obtained by collaboration between Edge servers. The SDN controller uses Algorithm 2 for collaboration decisions with predefined rules.

C. JOB MIGRATION ON EDGE SERVERS

The servers in Edge computing are deployed on the network edge. They offer services to low-power and IoT devices to offload jobs to the servers with minimum delay. Indeed the backbone of a successful IoT-enabled healthcare system is Edge computing, however, the main problem with this setup is how to minimize the response time, especially when job arrival is arbitrary. The response time is the sum of job uploading time, processing, job offloading time, and job downloading time. One of the best solutions is to migrate certain jobs to another server that be easily done by configuring the SDN controller as shown in Algorithm 3.

The flow chart of Edge collaboration and job migration is depicted in Fig. 4. In this figure, when an Edge server receives jobs from wearable devices of patients, it checks the number of jobs against its capacity. If the server capacity is higher, it processes them locally and sends a Beacon to the neighboring servers. The Beacon signals contain information that how many jobs the sender can execute. When the neighboring server has jobs and receives Beacon, it sends a request for job execution and waits for ACK. If ACK is received on time, the job is sent to the collaborator Edge server, otherwise forwarded to the Cloud server.

V. RESULTS AND DISCUSSION

In this section, we use computer-based simulations to evaluate the performance of our proposed framework for secured healthcare systems. We begin by providing experimental

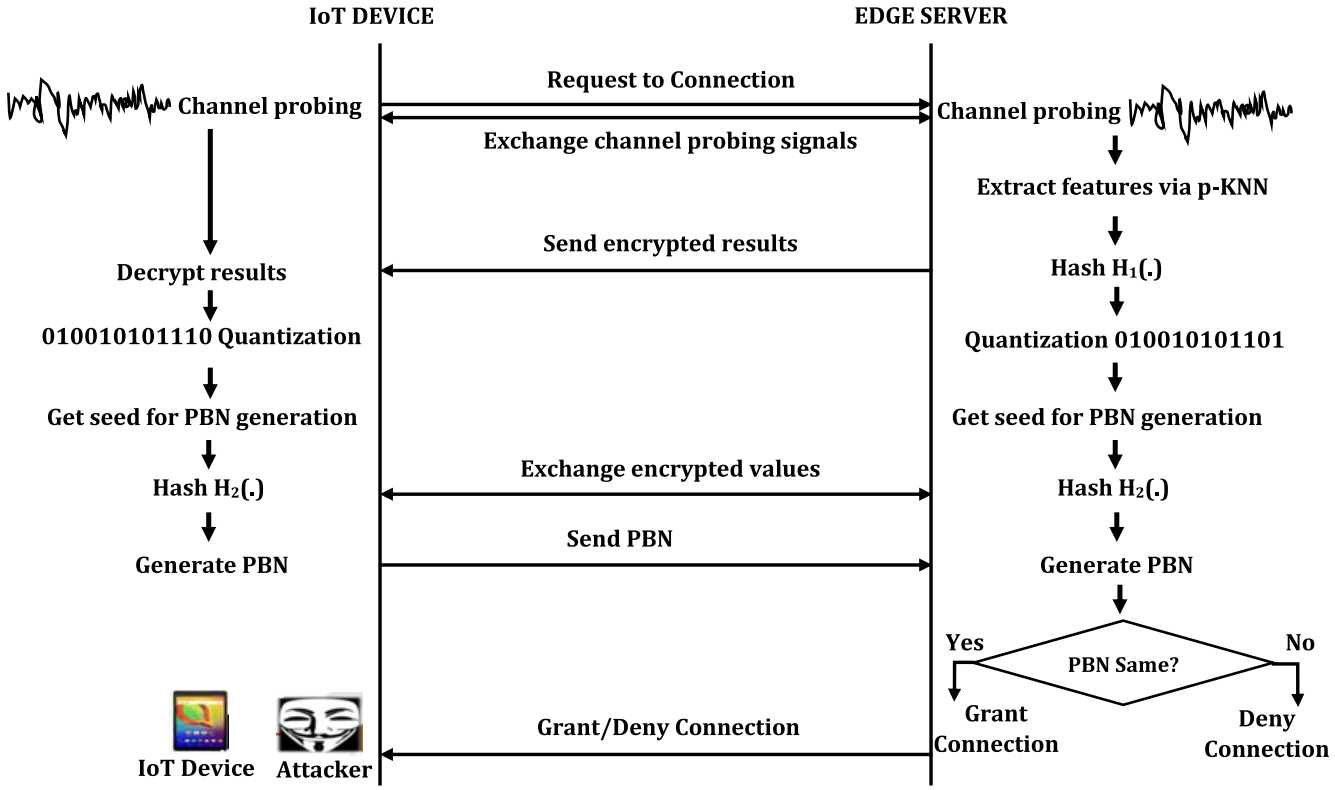

FIGURE 3. Flow chart of lightweight authentication scheme.

Algorithm 1 A Lightweight Authentication Appraoch

Initialization: sum = 0.
input: communication channels

procedure
  for each Edge_{server} **do**
    Perform channel probing using [28]
    Extract features using p-KNN, and remove outliers
    Encrypt features with hash $H_1(.)$
    Send encrypted data to Device_i
    Perform quantization using [31] ▷ Device_i also performs quantization
    Exchange encrypted (using $H_2(.)$) quantization results
    Edge_{server} and Device_i acquires the seed for generating the PBN ▷ Both parties generate PBN
    Device_i sends PBN to the Edge_{server} for authentication
    Edge_{server} check if PBN are identical
    if true **do**
      Grant access to this legitimate Device_i
    else
      Abort connection and save ID as intruder
    end if
  end for
end procedure

setup & simulation scenarios, performance evaluation metrics, and analyze simulation results using different parameters.

A. EXPERIMENTAL SETUP

In our simulation MATLAB has been used to analyze the strength of the proposed system under different conditions.

Algorithm 2 Colloborator Edge Server

Initialization: sum = 0.
input: j ▷ A job j, submitted by a node in IoT-enabled network.

```
procedure
    for each E_i do                                   ▷ E_i is Edge server
      sum the size of all submitted jobs j
  sum_i = sum_i + size_j
      if sum_i < E_c do                               ▷ E_c is Edge server capacity
        Process the job locally
        E_i also sends a BEACON to its neighbors E_{i-1} and/or E_{i+1} as a potential candidate   ▷ BEACON shows available space and time for sharing processing
      else
        E_i submits j to Neighboring server
      end if
    end for
end procedure
```

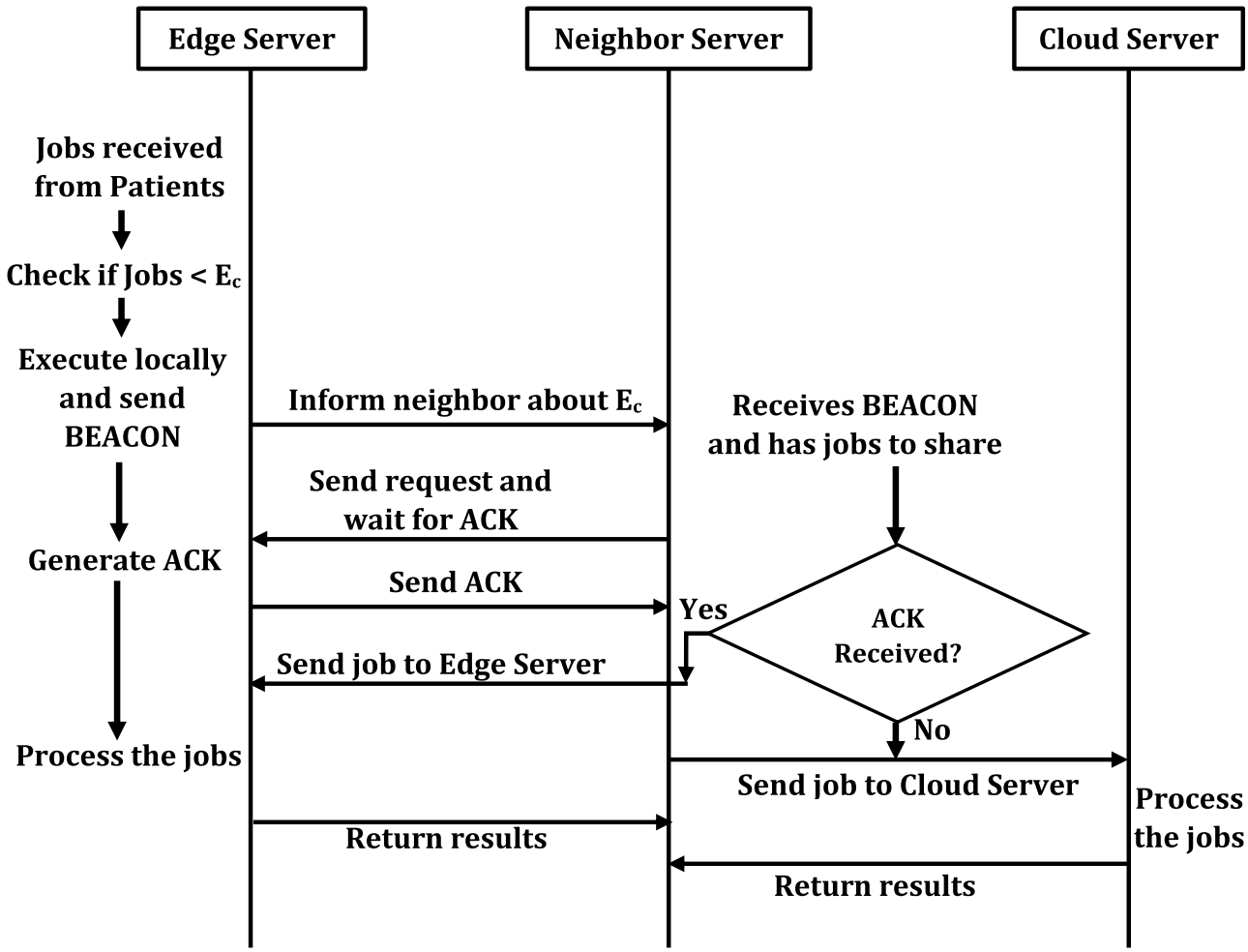

FIGURE 4. Flow chart of edge server collaboration and job migration.

The different thread has been used for simulating SDN controller, Edge Server, and authentication protocol. The authentication protocol thread is used to secure the overall system, whereas the Edge server thread is used to achieve load balancing and efficient resource utilization. The SDN controller thread is used to analyze network parameters at

Algorithm 3 Jobs Migration Between Edge Servers

input: List of Potential Candidates from Algorithm 2.

```
procedure
    while BEACON received AND has a job to share? do
      Neighbor node sends j to E_i and waits for ACK
      if ACK received on-time do
        E_i submits j to E_i
      else
        j is submitted to Cloud server
      end if
    end while
end procedure
```

constant intervals. These parameters are used for optimal Edge-to-gateway configuration, Edge collaboration, and job migration. The number of Edge servers, number of patients, and the data generated by patients (jobs) are used for test case development. The results given in the paper are reported on average. The simulation conditions are given in Table 1.

TABLE 1. The simulation conditions.

Parameters	Values
Number of Patients	1000
Number of Edge Servers	[5 -50]
Channel data rate	1 [Mbps]
Antenna type	Omni direction
Radio Propagation	Two-ray ground
Transmission range	250 [m]
Simulation time	1000 [s]

B. PERFORMANCE EVALUATION METRICS

The performance evaluation metrics are used to analyze the proposed scheme. We have used the following metrics.

1) **Average Response Time:** Average response time refers to the time by the Edge Server to return the processed data to the patients. The factors degrade the response time are the data rate, processing and communication speed, number of jobs, and the types of job submitted.
2) **Packet Delivery Ratio:** The packet delivery ratio (PDR) is based on the number of packets sent and the number of packet successfully received. It is defined as the ratio of sent packets to the received packet as computed in Eq. 1.

$$pdr = \frac{\sum_{i=1}^{n} S_i}{\sum_{i=1}^{n} R_i} \times 100 \tag{1}$$

where S_i is the number of packets sent and R_i is the number of packets received.
3) **Average Delay:** The delay (δ) is the total time required for a packet to be successfully received at the destination, while average delay is the sum of all delay sample divided by number of delay samples as computed in Eq. (2).

$$\delta = \tau - \mu \tag{2}$$

where, τ is the time a packet is transmitted and μ is the time a packet successfully arrived at destination. The average delay E(δ) is given in Eq. (3),

$$E(\delta) = \frac{\sum_{i=1}^{n} \delta_i}{n} \tag{3}$$

4) **Throughput** (η)**:** The network throughput is normally measured in bits per second (bps) or packets per second (pps). The network throughput is the sum of the data rates that are delivered to all nodes in a network. It is calculated as in Eq. (4).

$$\eta = \frac{\sum_{i=1}^{n} R_i}{\sum_{i=1}^{n} S_i} \tag{4}$$

5) **Control Overhead** (υ)**:** Control overhead is the ratio of the total number of control messages generated by each node in the network to the number of successfully received packets, It is calculated as in Eq. (5).

$$\upsilon = \frac{\sum_{i=1}^{n} C_i}{\sum_{i=1}^{n} R_i} \tag{5}$$

where C_i is the number of control messages.

C. EVALUATION RESULTS

In this section, we evaluate the proposed framework in terms of metrics discussed in Section V-B.

1) AVERAGE RESPONSE TIME (ART)

The Average response time of the healthcare system against the number of jobs is shown in Fig. 5. In this figure, the upload/download time and waiting time of Edge and Cloud server is depicted for the amount of data (job) generated by patients. The waiting time is the amount of time required by a job before its processing, and the upload/download time is the time taken by uploading. downloading jobs to/from the Server. The upload/download time for a Cloud server is double than the Edge server. Similarly, the waiting time for a job to execute at the Edge server is much less than the Cloud server. It is because the Edge servers are installed on network Edge and they forward job to the Cloud server. When the number of jobs increases the ART increases.

In Fig. 6 the ART for different system loads against the number of servers is demonstrated. In this figure, the ART for collaborative servers is lesser than the non-collaborative servers, when the number of server increase the ART decreases for different loads on systems. For example, for 1000 jobs on a system the ART for collaborative servers is lesser and it goes down when the number of servers increases. Whereas, for 5000 jobs the ART is higher when the number of servers is less and decreases by increasing the number of servers. It is also evident from Fig. 6 that ART for Cloud server is higher than the Edge server for different systems loads.

In Fig. 7, the ART for upload/download (U/D) time against number of servers is shown. In this figure,

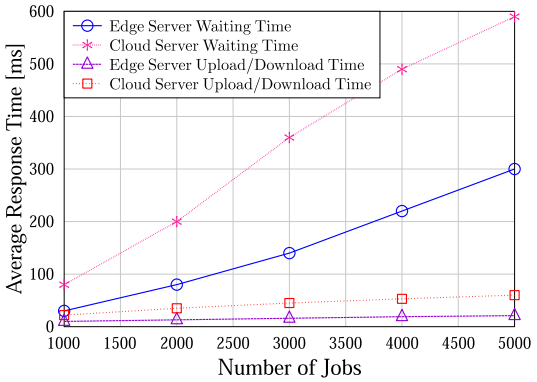

FIGURE 5. Waiting and upload/download time of edge and cloud server.

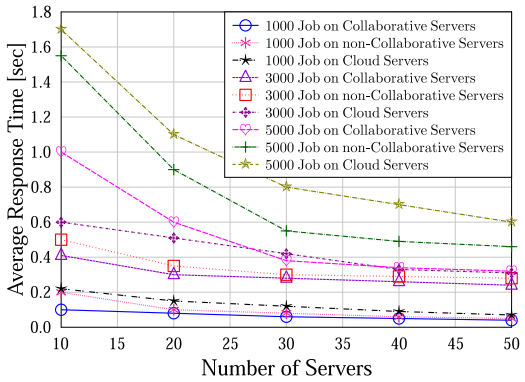

FIGURE 6. System loads for various number of servers.

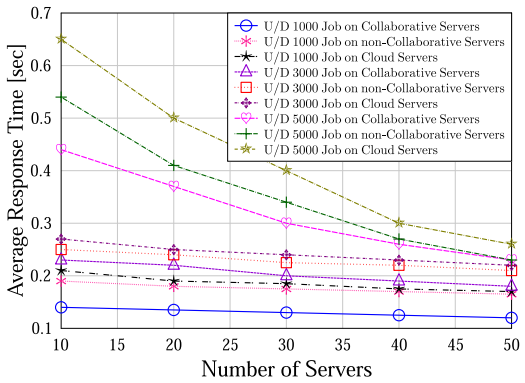

FIGURE 7. Packet loss against number of nodes.

the upload/download time is higher for Cloud server than the non-collaborative Edge servers and it decreases by increasing the number of servers, whereas the collaborative Edge servers produce the best results. In Fig. 6 and 7 the quick decrease of ART by the increasing server is because the number of job is processed by multiple servers.

2) PACKET DELIVERY RATIO (PDR)

The packet delivery ratio in healthcare system is shown in Fig. 8. In this figure, the PDR against the number of patients for three different scenarios is demonstrated. The first scenario depicts the PDR of a traditional network in a

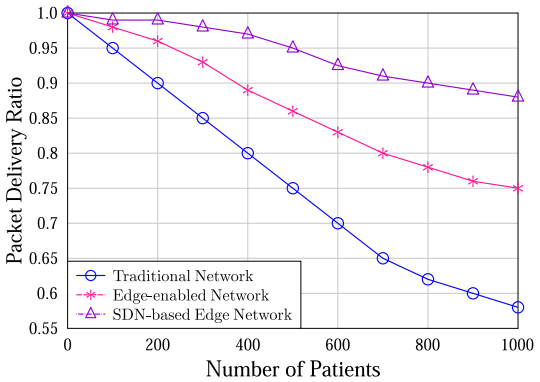

FIGURE 8. Packet deliver ratio against the number of patients.

healthcare system, whereas the second and third scenarios demonstrate the effect of Edge computing and SDN-based Edge computing. The PDR decreases when the number of patients transmitting data increases. The PDR in the first scenario is going down quickly because the low powered IoT device cannot process and transmit a large amount of patient data. In the second scenario, the PDR improves because the processing and data analysis is performed at the Edge server, whereas the third scenario produces the best results. After all, the Edge server takes intelligent decisions with the help of the SDN controller. The PDR decreases as the number of users increases, especially when a high amount of data is generated in peak hours. The IoT devices cannot perform well due to congestion and high amount of data, while in other scenario Edge collaboration, load balancing, and network optimization gives better results.

3) AVERAGE DELAY

The average delay of patients in healthcare system is illustrated in Fig. 9 and 10. In these figures, the delay of the system against the number of patients is depicted. It is worth mentioning, that this delay includes, processing, communication, upload/download delay of patient data. In Fig. 9, the delay of three of different scenarios is illustrated, the traditional network, the Edge-enabled network, and the SDN-based Edge-enable network. In the first scenario, the delay is higher due to the low-processing of IoT devices, whereas better delays in scenario two and three are due to the processing at Edge and SDN-based Edge servers. In the second scenario, the Edge servers collaborate while in the third scenario the SDN controller provides intelligence to the Edge server for network optimization, load balancing, and efficient resource utilization. Likewise, the delay of critical and highly sensitive data is depicted in Fig. 10. In this figure, delay for the same three scenarios is shown, however, this delay is of critical patients, whose data has given higher priority. The delay of critical data is less than the delay illustrated in Fig. 9 because of their highest priority.

4) THROUGHPUT

The throughput of the proposed framework is shown in Fig. 11, which is analyzed under three different

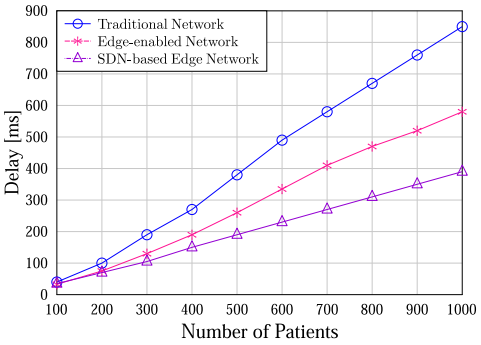

FIGURE 9. Average delay against number of patients.

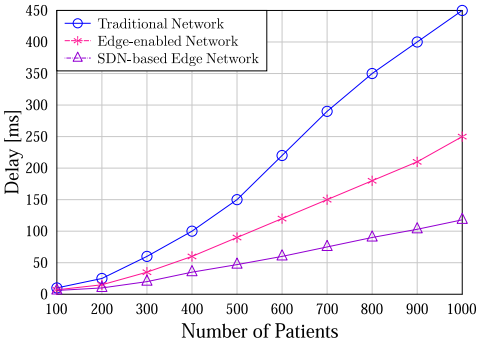

FIGURE 10. Average delay of critical data against number of patients.

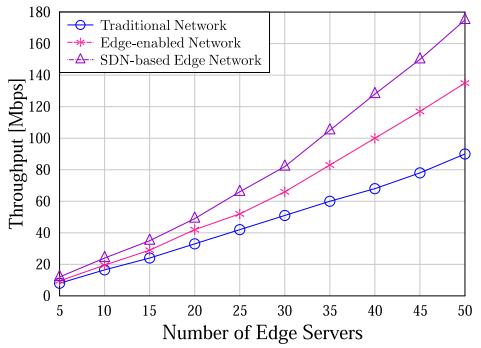

FIGURE 11. Throughput against number of edge servers.

approaches. In the first approach, a traditional network is analyzed, whereas in the second and third approach an Edge-enabled network and SDN-based Edge-enabled network is considered, respectively. The throughput of the SDN-based Edge computing is higher due to intelligent decision about load balancing, Edge collaboration, and efficient utilization of network resources. The Edge-based network produces higher throughput than traditional networks because in traditional network IoT devices cannot process large volumes of data efficiently.

5) CONTROL OVERHEAD

The control overhead of the proposed system is shown in Fig. 12. In this figure, the control overhead of three different network scenarios is demonstrated, i.e., traditional

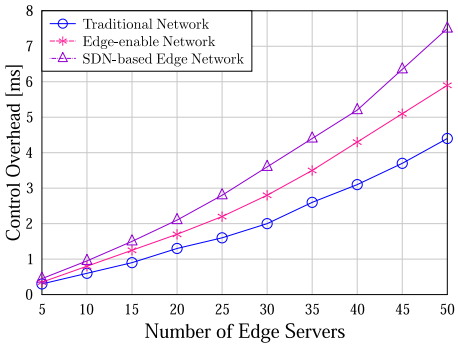

FIGURE 12. Control overhead against number of edge servers.

network, Edge-based network, and SDN-based Edge-enabled IoT network. In the traditional network scenario, the control overhead is lesser due to few control message exchanges, whereas in the Edge-based networks the extra control messages are exchanged for Edge collaboration and upload/download data, which causes higher control overhead. The SDN-based Edge-enabled network exchanges a higher number of control messages that cause relatively higher overhead than Edge-based networks due to extra control messages for network optimization and load balancing.

VI. CONCLUSION

In this paper, a secured framework for software-defined network-based Edge computing in IoT-enabled healthcare systems is proposed. The IoT devices are authenticated using a lightweight authentication scheme. After authentication, data from patients are sent to the Edge server for processing. The Edge servers collaborate for load balancing and have a configured SDN controller for intelligent decisions. The SDN-based Edge computing has better Edge collaboration and efficient resource utilization via optimal network configuration. It results in better network performance such as average response time, packet delivery ratio, low latency, higher throughput, and network control overhead. The simulation results for three different network scenarios have verified the efficiency of the proposed scheme. In the future, we aim to enhance the proposed framework by protecting the privacy of patients and their data. Furthermore, we want to save the data patterns in a dataset and use a machine-learning algorithm to predict malicious activities in the network.

REFERENCES

[1] W. Yao, F. Khan, M. A. Jan, N. Shah, I. ur Rahman, A. Yahya, and A. ur Rehman, "Artificial intelligence-based load optimization in cognitive Internet of Things," *Neural Comput. Appl.*, pp. 1–11, Mar. 2020. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s00521-020-04814-w.pdf

[2] H. Liao, Z. Zhou, X. Zhao, L. Zhang, S. Mumtaz, A. Jolfaei, S. H. Ahmed, and A. K. Bashir, "Learning-based context-aware resource allocation for edge-computing-empowered industrial IoT," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4260–4277, May 2020.

[3] N. Galstian. *SADA Systems 2018 Tech Trends Survey: AI/ML Top List of Priorities for It Pros*. Accessed: Jun. 20, 2020. [Online]. Available: https://sada.com/blog/news/sada-systems-2018-tech-trends-survey-aiml-top-list-priorities-pros/

[4] Z. Chang, W. Guo, X. Guo, Z. Zhou, and T. Ristaniemi, "Incentive mechanism for edge computing-based blockchain," *IEEE Trans. Ind. Informat.*, early access, Feb. 11, 2020, doi: 10.1109/TII.2020.2973248.

[5] M. Babar, F. Khan, W. Iqbal, A. Yahya, F. Arif, Z. Tan, and J. M. Chuma, "A secured data management scheme for smart societies in industrial Internet of Things environment," *IEEE Access*, vol. 6, pp. 43088–43099, 2018.

[6] F. Khan, M. A. Jan, and M. Alam, *Applications of Intelligent Technologies in Healthcare*. Cham, Switzerland: Springer, 2019. [Online]. Available: https://link.springer.com/book/10.1007%2F978-3-319-96139-2

[7] A. A. Mutlag, M. K. Abd Ghani, N. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Gener. Comput. Syst.*, vol. 90, pp. 62–78, Jan. 2019.

[8] H. Fang, A. Qi, and X. Wang, "Fast authentication and progressive authorization in large-scale IoT: How to leverage AI for security enhancement," *IEEE Netw.*, vol. 34, no. 3, pp. 24–29, May 2020.

[9] M. A. Jan, W. Zhang, M. Usman, Z. Tan, F. Khan, and E. Luo, "SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application," *J. Netw. Comput. Appl.*, vol. 137, pp. 1–10, Jul. 2019.

[10] Gartner. *8.4 Billion Connected 'Things' Will Be Use in 2017, Up 31 Percent From 2016*. Accessed: Apr. 7, 2019. [Online]. Available: https://www.gartner.com/newsroom/id/3598917

[11] G. Yang, M. A. Jan, V. G. Menon, P. G. Shynu, M. M. Aimal, and M. D. Alshehri, "A centralized cluster-based hierarchical approach for green communication in a smart healthcare system," *IEEE Access*, vol. 8, pp. 101464–101475, 2020.

[12] F. Khan, A. U. Rehman, A. Yahya, M. A. Jan, J. Chuma, Z. Tan, and K. Hussain, "A quality of service-aware secured communication scheme for Internet of Things-based networks," *Sensors*, vol. 19, no. 19, p. 4321, Oct. 2019.

[13] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet Things*, Jun. 2019, Art. no. 100075. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660519301799

[14] X. Li, J. Li, Y. Liu, Z. Ding, and A. Nallanathan, "Residual transceiver hardware impairments on cooperative NOMA networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 680–695, Jan. 2020.

[15] F. Khan, A. U. Rehman, and M. A. Jan, "A secured and reliable communication scheme in cognitive hybrid ARQ-aided smart city," *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106502.

[16] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration," *ACM Comput. Surveys*, vol. 51, no. 6, pp. 1–29, Feb. 2019.

[17] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2637–2670, 3rd Quart., 2019.

[18] H. Li, K. Ota, and M. Dong, "LS-SDV: Virtual network management in large-scale software-defined IoT," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 8, pp. 1783–1793, Aug. 2019.

[19] Z. Zhou, H. Liao, B. Gu, S. Mumtaz, and J. Rodriguez, "Resource sharing and task offloading in IoT fog computing: A contract-learning approach," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 4, no. 3, pp. 227–240, Jun. 2020.

[20] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," 2020, *arXiv:2004.14563*. [Online]. Available: http://arxiv.org/abs/2004.14563

[21] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K.-R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Comput. Secur.*, vol. 85, pp. 288–299, Aug. 2019.

[22] X. Li, Q. Wang, Y. Liu, T. A. Tsiftsis, Z. Ding, and A. Nallanathan, "UAV-aided multi-way NOMA networks with residual hardware impairments," *IEEE Wireless Commun. Lett.*, early access, May 22, 2020, doi: 10.1109/LWC.2020.2996782.

[23] W. Yao, A. Yahya, F. Khan, Z. Tan, A. U. Rehman, J. M. Chuma, M. A. Jan, and M. Babar, "A secured and efficient communication scheme for decentralized cognitive radio-based Internet of vehicles," *IEEE Access*, vol. 7, pp. 160889–160900, 2019.

[24] F. Khan, A. ur Rehman, M. Usman, Z. Tan, and D. Puthal, "Performance of cognitive radio sensor networks using hybrid automatic repeat ReQuest: Stop-and-Wait," *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 479–488, Jun. 2018.

[25] V. G. Menon, S. Jacob, S. Joseph, and A. O. Almagrabi, "SDN-powered humanoid with edge computing for assisting paralyzed patients," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 5874–5881, Jul. 2020.

[26] A. J. Ferrer, J. M. Marquès, and J. Jorba, "Towards the decentralised cloud: Survey on approaches and challenges for mobile, ad hoc, and edge computing," *ACM Comput. Surveys*, vol. 51, no. 6, pp. 1–36, Feb. 2019.

[27] S. Rajesh, V. Paul, V. G. Menon, S. Jacob, and P. Vinod, "Secure brain-to-brain communication with edge computing for assisting post-stroke paralyzed patients," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2531–2538, Apr. 2020.

[28] W. Gong, H. Liu, J. Liu, X. Fan, K. Liu, Q. Ma, and X. Ji, "Channel-aware rate adaptation for backscatter networks," *IEEE/ACM Trans. Netw.*, vol. 26, no. 2, pp. 751–764, Apr. 2018.

[29] P. Zhang, T. Taleb, X. Jiang, and B. Wu, "Physical layer authentication for massive MIMO systems with hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1563–1576, Mar. 2020.

[30] L. Yang, H. Chen, Q. Cui, X. Fu, and Y. Zhang, "Probabilistic-KNN: A novel algorithm for passive indoor-localization scenario," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, May 2015, pp. 1–5.

[31] J.-P. Heo, Z. Lin, and S.-E. Yoon, "Distance encoded product quantization for approximate K-nearest neighbor search in high-dimensional space," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 9, pp. 2084–2097, Sep. 2019.

JUNXIA LI received the M.S. degree in communication and information system from Henan Polytechnic University, in 2013, and will get the Ph.D. degree from Xinjiang University. She is currently a Lecturer with the School of Physics and Electronic Information Engineering, Henan Polytechnic University. She has several articles published in journals and conferences. Her current research interests include physical-layer security, cooperative communications, and the performance analysis of fading channel.

JINJIN CAI received the Ph.D. degree in engineering from Hebei Agricultural University, China. She is currently a Lecturer with the College of Mechanical and Electrical Engineering, Hebei Agricultural University. Her research interests include automation and control systems, image and video processing, the Internet of Things, artificial intelligence, and intelligent information processing.

FAZLULLAH KHAN (Member, IEEE) is currently a Researcher at Ton Duc Thang University, Ho Chi Minh City, Vietnam. He is also an Assistant Professor of computer science at Abdul Wali Khan University Mardan, Pakistan. His research interests include security and privacy, the Internet of Things, machine learning, and artificial intelligence. Recently, he has been involved in the latest developments in the field of Internet of Vehicles security and privacy issues, software-defined networks, fog computing, and big data analytics. His research has been published in the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGIES, IEEE ACCESS, *Computer Networks* (Elsevier), *Future Generations Computer Systems* (Elsevier), the *Journal of Network and Computer Applications* (Elsevier), *Computers and Electrical Engineering* (Elsevier), and *Mobile Networks and Applications* (Springer). He has served over ten conferences in leadership capacities, including the General Chair, the General Co-Chair, the Program Co-Chair, the Track Chair, the Session Chair, and a Technical Program Committee member, including IEEE TrustCom 2017, 2018, EuroCom, GCCE 2019, ITNG 2018, Future5V 2017, CCODE-2017, and IoT-BC2 2016. He has served as the Guest Editor for IEEE ACCESS journal, *Multimedia Technology and Applications* (Springer), *Mobile Networks and Applications* (Springer), *Inderscience Big data Analytics*, and *Ad Hoc & Sensor Wireless Networks*.

ATEEQ UR REHMAN (Member, IEEE) received the B.Eng. degree in computer science and information technology from the Islamic University of Technology (OIC) Dhaka, Bangladesh, in 2009, and the Ph.D. degree in wireless communications from the University of Southampton, in January 2017. He is currently an Assistant Professor of computer science with Abdul Wali Khan University Mardan, Pakistan. He has published 20 quality scholarly articles. His major research interests include next-generation wireless communications and cognitive radio networks, cooperative communication, and resource allocation, particularly cross-layer approach and hybrid ARQ. Currently, he is working on the security and privacy of the Internet of Things using machine learning algorithms. His most recent research achievements have been published in several highly cited IEEE Transactions and Elsevier journals, including the IEEE Internet of Things Journal, *Future Generation Computer Systems* (FGCS), and *Computer Networks* (CN). His research contribution on network security is internationally recognized. Moreover, he has earned various research awards, including the Best Paper Award and the Kaspersky Lab's Annual Student Cyber Security Conference Finalist Award, over the past years. He has also actively participated in public engagement. He has been invited to serve as a Technical Program Committee Member for 13 international conferences so far. He has also been an Active Reviewer for 12 high-cited international journals, including IEEE Access, the IEEE Transactions on Parallel and Distributed Systems, the IEEE Transactions on Information Forensics and Security, the IEEE Transactions on Dependable and Secure Computing, and the *Journal of Network and Computer Applications* (JNCA).

VENKI BALASUBRAMANIAM (Member, IEEE) received the Ph.D. degree in body area wireless sensor network (BAWSN) for remote healthcare monitoring applications. He is the Pioneer in building (pilot) remote healthcare monitoring application (rHMA) for pregnant women at the New South Wales Healthcare Department. His research establishes a dependability measure to evaluate rHMA that uses BAWSN. His research opens up a new research area in measuring time-critical applications. He contributed immensely to eResearch software research and development that uses cloud-based infrastructure and a Core Member for the project sponsored by Nectar Australian research cloud provider. He contributed heavily in the field of healthcare informatics, sensor networks, and cloud computing. He also founded Anidra Tech Ventures Pty Ltd., a smart remote patient monitoring company.

JIANGFENG SUN (Member, IEEE) received the M.S. degree in communication and information system from Zhengzhou University, in 2009, and will get the Ph.D. degree from the Beijing University of Posts and Telecommunications. He is currently a Lecturer with the School of Physics and Electronic Information Engineering, Henan Polytechnic University. He has several articles published in journals and conferences. His current research interests include physical-layer security, cooperative communications, and the performance analysis of fading channels.

P. VENU is currently a Professor and the Head of the Department of Mechanical Engineering, SCMS School of Engineering and Technology, SCMS Group of Educational Institutions, India. He is also the Dean of Student Affairs and Innovation. His research interests include cloud and fog networks, quality function deployment, prototyping technologies, and multiplatform machine communication.