A Privacy-Preserving Authentication Scheme for Real-time Medical Monitoring Systems

Seyed Ahmad Soleymani, Shidrokh Goudarzi, Mohammad Hossein Anisi, Anish Jindal, Nazri Kama, Saiful Adli Ismail

***Abstract*—In real-time medical monitoring systems, given the significance of medical data and disease symptoms, a secure and always-on connection with the medical centre over the public channels is essential. To this end, an edge-enabled Internet of Medical Things (IoMT) scheme is designed to improve flexibility and scalability of the network and provide seamless connectivity with minimum latency. The entities involved in such network are vulnerable to various attacks and can potentially be compromised. To address this issue, an authentication scheme comprised of digital signature and Authenticated Key Exchange (AKE) protocol is proposed which guarantees only authorized entities get access to the services available in the medical system. Moreover, to fulfill the privacy-preserving, each entity is mapped to a different pseudo-identity. The non-mathematical and performance analysis show that the proposed scheme is robust against various attacks such as impersonation and replay attacks.**

***Index Terms*—Authentication, Privacy, Medical Monitoring System, Edge Computing, WBAN.**

I. Introduction

The real-time medical monitoring system is one of the main components of the e-healthcare system. This system facilitates gathering the data essential for improving the healthcare service delivery quality [1]. In the Covid-19 pandemic, the significance of remote monitoring systems is highlighted and the real-time monitoring systems employing the IoMT framework can be effective and helpful to quickly identify potential coronavirus cases and in a result minimize the spread of the coronavirus [2].

In a real-time medical monitoring system, the medical data and symptoms can be periodically measured and collected through a Wireless Body Area Network (WBAN) and transmitted to the medical cent over an open wireless channel [3]. Subsequently, healthcare professionals in the medical centers are allowed to analyze the data and symptoms for a more accurate diagnosis and transmit the proper command to the user/patient.

S. A. Soleymani is with 5GIC & 6GIC, Institute for Communication Systems (ICS), University of Surrey, Guildford GU2 7XH, UK. (E-mail: s.soleymani@surrey.ac.uk).

S. Goudarzi is with the Centre for Vision Speech and Signal Processing, University of Surrey, Guildford GU2 7XH, U.K.(e-mail: s.goudarzi@surrey.ac.uk).

M. H. Anisi is with School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, UK; (E-mail: m.anisi@essex.ac.uk).

A. Jindal is with Department of Computer Science, Durham University, UK; (E-mail: anish.jindal@durham.ac.uk).

N. Kama and S. A. Ismail are with Fakulti Teknologi & Informatik Razak, Fakulti Teknologi Dan Informatik Razak, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia.; (E-mail: mdnazri@utm.my; saifuladli@utm.my).

In such a system, given the importance and sensitivity of medical data/command, security and privacy are considered as main concerns. This is mainly because of the open nature of wireless communication technology used in such a system. In an insecure network, an attacker can acquire the medical data of the user/patient by eavesdropping on the channel. The attacker can impersonate the trusted entities and or a man-in-the-middle attack is able to intercept communications between legitimate entities or alter them. These systems are also facing other concerns such as latency, scalability, and flexibility.

In the past decade, a few studies have been conducted to guarantee the authentication and privacy of the patient's health information in medical monitoring systems such as [4]. Authors in [5] proposed a cloud-based privacy authentication procedure was further to protect the personal information and access the medical resources of patients for the medical setting. However, this protocol cannot present the features of patient anonymity, real telemedicine, and message authentication. To address these problems, a cloud-based privacy authentication scheme for sharing medical information is designed in [6]. However, this protocol is unable to support the anonymity of the patients and ensure the protection against the mobile device stolen attacks.

In [7], a two-factor user authentication protocol is presented for an integrated patient information system. In [8], three-factor user authentication along with key consistency outline with anonymity preservation for monitoring systems is presented. A secure RSA-based user authentication protocol is proposed in [9] with user anonymity for telecare medical information system to ensure the system security via the verification tool and rigorous security analysis. However, latency is a critical issue in these protocols. To address network latency issue, a two-layer encryption scheme in a fog-based data aggregation architecture preserving privacy is proposed in [10]. However, data integrity is a problem in this system. In medical monitoring systems, the system contributors need to access and privilege exclusively the specific information, and the medical data kept in the system can be categorized into various types of information in terms of the user desires and system levels. To this end, a secure biometrics-based access control scheme with authentication is proposed in [11] for the remote monitoring systems. In this scheme, the patient unlinkability is maintained by concealing the medical association between the doctor and the patient through communications. In [12] an anonymous user authentication scheme is developed for monitoring the patient health through wireless medical sensor networks. However, scalability remains an issue in this work. In [13], NTRU lattice-based digital signature scheme to deal

with a quantum attack is proposed. The authors designed a cloud-based telemedicine framework. This scheme is scalable and meets ever-increasing demand as it is based on cloud computing, however, latency is an issue. In [14], given the memory and energy limitation in IoT healthcare devices, in order to cope with node tampering and replacement attacks, a two-stage authentication scheme, between the patient and the sink node and between the sink node and the server, based on Physical Unclonable Functions (PUFs) is developed. However, in the proposed scheme, scalability and delay remain issues. In [15], an encryption scheme based on Boneh Franklin's identity is used to keep personal health records secure. In this work, a decryption scheme based on distributed identity to preserve privacy and share encrypted data between single/multiple parties. In [16], [17] privacy is the main challenge in healthcare systems. In the former, blockchain is used as a technique to preserve privacy, and the latter utilized the block design technique to keep data private. Since the focus is on user privacy, data integrity remains an issue in these works.

In most existing related works, security and privacy of data-in-transit are taken into account as main concerns while, as mentioned earlier, latency, scalability, and flexibility are also other concerns in such a system. To deal with these concerns and in order to handle the big data generated in the network as well as to fulfill the ever-increasing demands, integrating cloud and edge computing into IoMT can be an appealing strategy [18]. However, the edge nodes involved in such a network are also vulnerable to different attacks and may be compromised. In some related works, edge nodes are considered as fully trusted entities, which is not always practical. Motivated by the complexity of practical network architecture in the medical monitoring system, in order to have a secure, flexible, scalable with the lowest communication, we developed an authentication scheme with privacy-preserving for edge-cloud IoMT in which symmetric encryption method is employed for sharing the encrypted data among involved entities. In this study, the major contributions are summarized as follows:

1- We integrate edge-cloud into IoMT to provide a flexible and scalable architecture in the real-time remote medical monitoring system.
2- We develop an authentication scheme with privacy-preserving using the authenticated key agreement and digital signature to support data confidentiality, data integrity, and user privacy.
3- We use non-mathematical analysis to prove that the proposed scheme resists different attacks such as impersonation attacks and man-in-the-middle attacks.
4- We use iFogSim to simulate the proposed scheme. The network delay and accuracy are two indexes that used to evaluate the proposed scheme.

The structure of this paper is presented in the following. Section II presents the relevant preliminaries. In Section III, our scheme is presented. In Section IV, the security analysis and discussion of security features are presented. In Section V, the performance analysis and evaluation are presented. The paper is concluded in Section VI.

II. Preliminaries

A. System Model

In this work, we developed a network architecture framework comprised of five entities in different layers namely Trusted Authority (TA) and Cloud Server (CS) in the top layer, Edge Nodes (EN) in the middle layer, Medical Center (MC), and users in the lower layer as shown in Figure 1.

In this framework, TA and CSs are considered as fully trusted entities whereas ENs are semi-trusted entities. It is supposed that all communication between these entities is by utilizing wired communication technologies such as Ethernet via a secure and safe way. In contrast, an open wireless technology such as 4G/LTE/5G is used for the communication between the user, EN, and MC.

TA acts as the registry center of the cloud servers, edge nodes, medical centers, and users. It is responsible for distributing key materials to all entities. It is able to trace the real identity of the user if necessary. In this network, the responsibility of CS is to distribute generated tasks among nearby edge nodes. Due to the high number of tasks created in the network, it is necessary to distribute the tasks appropriately and fairly among nearby edge nodes. CS also sends some required materials to users, edge nodes, and medical centers. EN is responsible to connect users to the proper medical centers. EN generates a session key based on the required information received from the user and medical center and then shares it between the authorized user and the medical center. In the designed network, MC collects the medical data from the user and sends back the proper commands to the user. In this network, we assumed that each WBAN has three types of nodes are distributed in different positions with the star structure. These nodes including: (i) master node; (ii) actuator node; (iii) sensor node. A master node with a high computational capability, storage, and energy collects the reported data such as temperature, heartbeat rate, and blood pressure from implanted or wearable sensor nodes. It encrypts the data packet using the agreed session key and sends it to the medical center through the wireless communication. Master node also receives the encrypted commands from the medical center. It firstly decrypts the data and then broadcast commands to the actuator nodes to perform required actions.

In this system, each user in order to connect with the suitable and available medical center firstly needs to connect with the proper edge node. The selection of edge node is depending on the quality of link between user and edge node which can be assessed using characteristics like bandwidth, Signal-to-Noise Ratio (SNR), and Bit Error Rate (BER) [19]; however, more discussion on this issue is out of the scope of the paper. Then, the proper edge node, after checking the legitimacy of the user, chooses the best medical center using a query on its table. Since the intended medical monitoring system is time-sensitive, low delay is the most important feature to select a suitable medical center. It is worth noting that, the corresponding tables of edge nodes will be upgraded by the cloud server, continuously. After choosing the appropriate medical center, by exchanging the required information, a

session/secret key finally will be generated and shared between the user and the medical center for future communication.

B. Security Requirements

In this work, the proposed privacy-preserving authentication scheme should be able to ensure the validity and integrity of medical data or commands and also keeps the information private. To achieve this aim, the following essential requirements need to be addressed:

- **Resistance to Impersonation Attack:** This attack attempts to impersonate the legitimate user/medical center of the system. Defense against this attack is a requirement.
- **Session Key Agreement:** It is essential to create a shared session key between the medical center and user to guarantee integrity, confidentiality, and non-repudiation of medical data collected in WBANs.
- **Known-Key Security and Perfect Forward Secrecy:** In the remote medical monitoring system, an attacker may achieve the shared session key using the obtained secret keys of the user/medical center. In result, the attacker is able to encrypt/decrypt the medical data/commands transmitted over the network. It is required that the authentication scheme guarantees strong forward secrecy. It should ensure that the attacker is unable to achieve the session key even with the long-term private keys and or in the worst-case attacker gets only a small amount of sensitive data.
- **Resistance to Replay Attack:** The attacker eavesdrops on secure communication and captures the valid data transmitted over the network. Then, the attacker replays or re-sends these data. Resistance to a replay attack is necessary.
- **User's Anonymity:** It ensures that the attacker is unable to achieve the real identity of the legal user during authentication process. To satisfy privacy only TA can extract the real identity of the user from the message.

C. Threat Model

The Dolev-Yao (DY) threat model [20] is employed to verify the properties of the work. Based on this threat model, an adversary $\mathbf{\Lambda}$ threatens data confidentiality by intercepting a message and reading the user data in plain text. $\mathbf{\Lambda}$ also threatens integrity by manipulating the content of a message, creating and sending its own messages, and duplicating a message.

III. Proposed Scheme

In this study, to set up the real-time medical monitoring system in order to identify quickly potential coronavirus cases, we utilized five entities, namely, TA, CS, EN, MC, and user (patient). In this system, it is assumed that the communication between users and EN (U2EN), MC and EN (MC2EN), and user and MC (U2MC) is over wireless communication technologies. The medical data transmitted over an open channel are vulnerable to different security attacks. Due to the particular importance of medical data/symptoms, data encryption in order to protect data as well as keep user's preference privacy is essential [16]. We developed a privacy-preserving authentication scheme based on ECC to ensures the legitimacy of user/MC and data integrity as well as keeps user's information private. Table I represents the notations used throughout the paper.

Table I: Notations used in the paper

Model	Method
$\oplus$	XOR operation
$\|\|$	Concatenation operation
TA	Trusted authority
CS	Cloud server
EN	Edge node
MC	Medical center
U	User/Patient
h	Secure hash function
s	System private key
P_{pub}	System public key
ψ	Master secret key
$SysPara$	System public parameters
$ID_U, ID_{EN}, ID_{MC}, ID_{CS}$	Real identity of U, EN, MC, and CS
s_{en}, s_{mc}, s_{cs}	Private key of EN, MC, and CS
Q_{EN}, Q_{MC}, Q_{CS}	Public key of EN, MC, and CS
$DID_U, EID_{EN}, MID_{MC}$	Pseudo-identity of U, EN, and MC
$\mathbf{\Lambda}$	The attacker
$SK_{U \leftrightharpoons MC}$	Symmetric key

A. Privacy-Preserving Authentication Scheme

The proposed scheme could be devided into he following four phases: The initialization, registration, pseudo-identity generation, and authentication are four phases of the proposed scheme.

1) Phase I- Initialization Phase: In the initialization phase, first TA has to generate the system parameters and then release it to all legal entities in the network. To that end, it randomly picks the system private key $s \in Z_q^*$ and computes the system public key $P_{pub} = s.P$ where q is a large prime number and P is the generator element of the group G. In addition, TA picks a master secret key $\psi \in Z_q^*$. A secure one-way hash function $h : \{0,1\}^* \rightarrow Z_q^*$ is also selected by TA and it sets $SysPara = \{q, E_q(a,b), P, P_{pub}, h\}$ as system parameters to be published for the users, edge nodes, cloud servers, and medical centers wherein $E_p\,(a,b) : y^2 = x^3 + ax + b \ \ mod \ \ p$ is a non-singular elliptic curve with $\left(4a^3 + 27b^2\right) mod \ \ q \neq 0$.

2) Phase II- Registration Phase: This phase contains user registration, edge node registration, cloud server registration, and medical center registration as follows:

- **Cloud Server:** Consider $\mathcal{G}_{CS} = \{CS_1, CS_2, \cdots, CS_k\}$ as a set of cloud servers in which each $CS_i \in \mathcal{G}_{CS}$ with real identity ID_{CS_i} has a private key $s_{cs_i} \in Z_q^*$ and a public key $Q_{CS_i} = s_{cs_i}.P$.
- **Edge Node:** Let $\mathcal{G}_{EN} = \{EN_1, EN_2, \cdots, EN_m\}$ be a set of legal edge nodes that have been joined the network. For each edge node in this list $EN_i \in \mathcal{G}_{EN}$ there exist a unique real identity ID_{EN_i}, a private key $s_{en_i} \in Z_q^*$, a public key $Q_{EN} = s_{en_i}.P$, and pseudo-identity $EID_{EN_i} = h\left(ID_{EN_i} \parallel s_{en_i} \parallel \psi\right)$. Besides, this information will be shared with the relevant cloud server via TA.

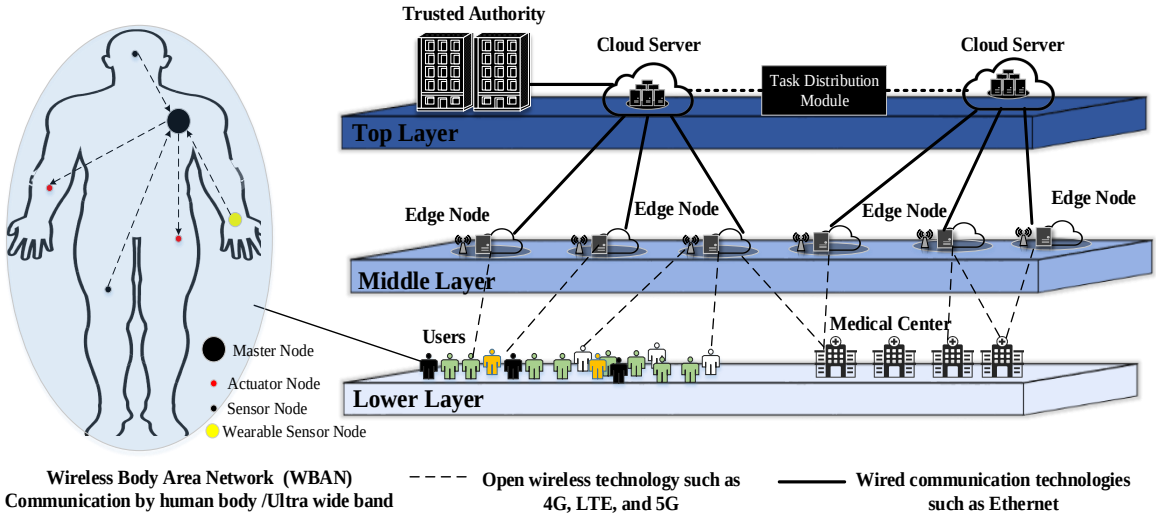


Figure 1: System architecture.

- **Medical Center:** Let $\mathcal{G}_{MC} = \{MC_1, MC_2, \cdots, MC_l\}$ as authorized medical centers in the network. TA assigns $\{ID_{MC_i}, MID_{MC_i}, s_{mc_i}, Q_{MC_i}\}$ to each medical center MC_i where ID_{MC_i} is real identity, $s_{mc_i} \in Z_q^*$ and $Q_{MC_i} = s_{mc_i}.P$ are private and public key, and $MID_{MC_i} = h\left(ID_{MC_i} \parallel s_{mc_i} \parallel \psi\right)$ is pseudo-identity. TA sends these data to the relevant cloud server i.e. CS_i and in addition to the relevant edge node i.e. EN_i.
- **User:** Let $\mathcal{G}_U = \{U_1, U_2, \cdots, U_n\}$ be a list of authorized users that have been registered in the network. A database with personal users'details in the $\mathcal{G}_U$ is used by TA. For each user, TA assigns a real identity ID_{U_i} and PWD_{U_i}.

3) Phase III- User Pseudo-Identity Generation: To meet privacy, each user needs to generate a pseudo-identity UID_U to establish communication with other entities in the network. The generated pseudo-identity is valid for a period of time (VT_{PID}) and after this time, it has to regenerate a new pseudo-identity. Nevertheless, to generate the pseudo-identity, the user U randomly picks a number $r \in Z_q^*$ and computes $UID_U = ID_U \oplus h\left(r.P_{pub}\right)$. Then, it securely sends $\{ID_U, PWD_U, UID_U\}$ to TA. Once receiving this message, TA calculates $SID_U = h\left(UID_U \parallel \psi\right)$ and sends SID_U to user via a secure manner. TA also sends $\{UID_U, SID_U\}$ to the relevant cloud server CS.

4) Phase IV- Authentication Phase: Whenever a user U wants to connect to the proper medical center MC using an edge node EN and via an open channel, the authentication process should be performed among U, MC, and EN for preventing impersonation attacks. In the following, the process of entity authentication and session initiating among U, MC, and EN are described.

Step 1 - U2EN Communication: The user U_i creates a login request in order to submit to the suitable edge node. To this end, it selects a random number $r_u \in Z_q^*$ and computes $R_u = r_u.P$, $B_1 = R_u \oplus h\left(SID_{U_i} \parallel UID_{U_i}\right)$, $B_2 = h(R_u) \oplus UID_{U_i}$, $B_3 = h\left(SID_{U_i} \parallel R_u \parallel UID_{U_i}\right)$. Then, U_i submits the login request $L_1 = \{B_1, B_2, B_3, T_1\}$ to the proper EN_l. In this message T_1 is current timestamp.

Step 2 – EN2MC Communication: When EN_l receives a login request from U_i with pseudo-identity UID_{U_i}, it firstly needs to check whether T_1 is fresh. If $\triangle T < T_{EN_l} - T_1$, it rejects the request where T_{EN_l} is the latest timestamp of the EN_l. Otherwise, if $\triangle T \geq T_{EN_l} - T_1$, it computes $SID_{U_i}^* = h(UID_{U_i} \parallel \psi)$, $R_u^* = B_1 \oplus h\left(SID_{U_i}^* \parallel UID_{U_i}\right)$, and $B_3^* = h\left(SID_{U_i} \parallel R_u^* \parallel UID_{U_i}\right)$. Next, it checks whether $B_3 \stackrel{?}{=} B_3^*$. If does not hold, EN_l rejects the login request. But, if it holds, EN_l checks its database to find a suitable medical center. Then, it generates a request and broadcast to the best medical center i.e. MC_j. If it is the first communication between EN_l and MC_j, so, EN_l sends a query to the CS_w to regarding to ask MID_{MC_j}. Then, it selects a random number $r_{en} \in Z_q^*$ and computes $R_{en} = r_{en}.P$, $B_4 = R_{en} \oplus h(MID_{MC_j})$, $B_5 = R_u^* \oplus h\left(MID_{MC_j} \parallel EID_{EN_l}\right)$ and $B_6 = h\left(MID_{MC_j} \parallel R_{en} \parallel EID_{EN_l}\right)$. Finally, it sends the request message $L_2 = \{B_2, B_4, B_5, B_6, T_2\}$ to MC_j where T_2 is current timestamp.

Step 3 – MC2EN Communication: When MC_j receives a request from the EN_l, it first checks T_2. When T_2 is not fresh, it rejects the request. Otherwise, it extracts EID_{EN_l} from the list of nearby authorized edge nodes $\{EN_1 : EID_{EN_1}, \cdots, EN_n : EID_{EN_n}\}$. This list has been sent from the relevant cloud server via a secure way and stored by medical center with care to prevent information leakage to attackers. Nevertheless, it computes $R_{en}^* = B_4 \oplus h\left(MID_{MC_j}\right)$, $R_u^{**} = B_5 \oplus h\left(MID_{MC_j} \parallel EID_{EN_l}\right)$, $UID_{U_i}^* = B_2 \oplus h\left(R_u^{**}\right)$, and $B_6^* = h\left(MID_{MC_j} \parallel R_{en}^* \parallel EID_{EN_l}\right)$. If $B_6 \neq B_6^*$, the request is terminated. Otherwise, if $B_6 = B_6^*$, EN_l is authenticated by MC_j. Next, MC_j selects a random number $r_{mc} \in Z_q^*$ and computes $R_{mc} = r_{mc}.P$, $B_7 = R_{mc} \oplus h\left(EID_{EN_l}\right)$, and

$B_8 = h\left(EID_{EN_l} \parallel R_{mc} \parallel MID_{MC_j}\right)$. Next, it submits $L_3 = \{B_7, B_8, T_3\}$ to EN_l where T_3 is the current timestamp.

Step 4 – EN2U Communication: When EN_l receives the message L_3 from the MC_j, it first checks T_3. When T_3 is not fresh, it rejects the request. Otherwise, it computes $R^*_{mc} = B_7 \oplus h\left(h\left(ID_{EN_l} \parallel s_{en_l} \parallel \psi\right)\right)$. Then, it calculates $B^*_8 = h\left(EID_{EN_l} \parallel R^*_{mc} \parallel MID_{MC_j}\right)$. If $B_8 \neq B^*_8$, this request is terminated by EN_l. Otherwise, MC_j is authenticated by EN_l and hence it computes $B_9 = R_{en} \oplus h(R_u \parallel SID^*_{U_i})$, $B_{10} = R^*_{mc} \oplus h(SID^*_{U_i})$, and $B_{11} = h\left(SID^*_{U_i} \parallel R_{en} \parallel R_{mc}\right)$. Then, it sends the $L_4 = \{B_9, B_{10}, B_{11}, T_4\}$ to U_i where T_4 is current timestamp.

Step 5: Once U_i received the message L_4 from the EN_l, it first checks T_4. When T_4 is not fresh, it rejects the request. Otherwise, it computes $R^{**}_{en} = B_9 \oplus h\left(R_u \parallel SID_{U_i}\right)$, $R^{**}_{mc} = B_{10} \oplus h\left(SID_{U_i}\right)$, and $B^*_{11} = h\left(SID_{U_i} \parallel R^{**}_{en} \parallel R^{**}_{mc}\right)$. Then, U_i checks whether $B_{11} \stackrel{?}{=} B^*_{11}$. If does not hold, the session is terminated. Otherwise, EN_l and in result MC_j are authenticated by U_i. Hence, U_i and MC_j can establish a secure communication session via a symmetric encryption. It is important to note that, if any step of the above validation process is unsuccessful, then entities involved in this scheme will abort the execution of the scheme.

Step 6: To have a fast and secure communication session between U_i and MC_j, we use symmetric encryption algorithm. To this purpose, it needs to be generated a shared session key, first. This key will be used to encrypt and decrypt medical data/commands. In the proposed scheme, the session key $SK_{U_i \leftrightharpoons MC_j}$ is a combination of R_{en}, R_u, R_{mc} and a random number $r_{sk} \in Z^*_q$ selected by EN_l. This number will be sent to both known parties, U_i and MC_j, securely. Then, U_i and MC_j are able to create the session key $SK_{U_i \leftrightharpoons MC_j} = h\left(r_{sk}.R_u \parallel R_{en} \parallel r_{sk}.R_{mc}\right)$.

Since r_{sk} has an important role to generate the session key, we employed the message signature in order to ensure the message's integrity (r_{sk}) and the legitimacy of sender (EN_l). To this end, it computes the signature $\sigma_{ij} = s_{en_l}.h\left(R_u \parallel R_{mc}\right) + r_{en}.h\left(B_{12} \parallel T_5\right)$ where s_{en_l} is EN_l's private key, and $B_{12} = R_u \oplus R_{mc} \oplus r_{sk}$. Then, EN_l signs B_{12} and simultaneously sends $\{\sigma_{ij}, B_{12}, T_5\}$ to both U_i and MC_j via open channel where T_5 is timestamp.

Step 7: When U_i and MC_j received a signed message from the EN_l, they check T_5 is fresh or not. If it is not fresh, this message will be rejected; otherwise, they have to verify the signature to guarantee that the relevant edge node is not impersonating another valid edge node or disseminating bogus session keys. To that, they verify whether

$$\sigma_{ij}.P \stackrel{?}{=} Q_{EN_l}.h\left(R_u \parallel R_{mc}\right) + R_{en}.h\left(B_{12} \parallel T_5\right) \quad (1)$$

is established. If does not hold, the request is terminated. Otherwise, U_i and MC_j are able to initiate a session for secure communication by the session key. To this end, both U_i and MC_j computes $r_{sk} = R_u \oplus R_{mc} \oplus B_{12}$ and then generate the session key $SK_{U_i \leftrightharpoons MC_j}$. Figure 2 shows the whole process of authentication, and session key generation. The Equation 1 can be verified as follows:

$$\begin{aligned}\sigma_{ij}.P \stackrel{?}{=} &\left(s_{en_l}.h\left(R_u \parallel R_{mc}\right) + e_{en}.h\left(B_{12} \parallel T_5\right)\right).P = \\ &s_{en_l}.P.h\left(R_u \parallel R_{mc}\right) + e_{en}.P.h\left(B_{12} \parallel T_5\right) = \\ &Q_{EN_l}.h\left(R_u \parallel R_{mc}\right) + R_{en}.h\left(B_{12} \parallel T_5\right)\end{aligned}$$

IV. Security Analysis and Discussion

Here, we discuss the security and functionality features of the proposed scheme through the non-mathematical security investigation.

1) Mutual Authentication: The proposed scheme provides authentication among U, EN, and MC. The authentication between U and EN is relied on R_u and EID_{EN}, which is held by U and is recoverable by EN from $L_1 = \{B_1, B_2, B_3, T_1\}$ by using private key s_{en}, master secret key ψ and edge-node identity ID_{EN}. As shown earlier, EN and U can authenticate each other by checking $B_3 \stackrel{?}{=} B^*_3$ and $B_{11} \stackrel{?}{=} B^*_{11}$, respectively. Similarly, the authentication between EN and MC is relied on $B_6 \stackrel{?}{=} B^*_6$ and $B_8 \stackrel{?}{=} B^*_8$. So, U is trustable to MC if and only if U is authenticated by EN. Moreover, the session key $SK_{U \leftrightharpoons MC}$ generated using random numbers r_u, r_{en}, and r_{mc}, will be signed by EN and then share among U and MC. In order to use $SK_{U \leftrightharpoons MC}$, it needs to verify the signature σ by U and MC. Therefore, our scheme provides mutual authentication.

2) Resistance to Impersonation Attacks: In our scheme, whenever an adversary $\mathbf{\Lambda}$ impersonates U as a user by forging L_1, it has to know both SID_U and UID_U. To this end, $\mathbf{\Lambda}$ needs to have $\{ID_U, PWD_U\}$ corresponding to U. This information is generated by TA and stores safe in the master node. Hence, $\mathbf{\Lambda}$ is unable to imitate as the U without knowing $\{ID_U, PWD_U, SID_U, UID_U\}$. Also, the edge node impersonation attacks can be avoided by our scheme. This is mainly because $\mathbf{\Lambda}$ needs to know the edge node real identity ID_{EN}, private key s_{en} and system master secret key ψ that are held by fully trusted TA. Additionally, our scheme can resist medical center impersonation attack, because $\mathbf{\Lambda}$ needs to know $MID_{MC} = h\left(ID_{MC} \parallel s_{mc} \parallel \psi\right)$ to impersonate a MC and it is impossible.

3) Session Key Agreement: In the execution of our scheme, EN picks the random number r_{en} and shares it with U and MC to generate the session key $SK_{U \leftrightharpoons MC} = h\left(r_{sk}.R_u \parallel R_{en} \parallel r_{sk}.R_{mc}\right)$ where $R_u = r_u.P$, $R_{en} = r_{en}.P$, and $R_{mc} = r_{mc}.P$. The required parameters have been shared among the participants during authenticated key exchange. Therefore, our scheme could provide a session key agreement.

4) Forward Secrecy and Known-Key Security: In the proposed scheme, U and MC use the session key $SK_{U \leftrightharpoons MC} = h\left(r_{en}.R_u \parallel R_{en} \parallel r_{en}.R_{mc}\right)$. It is achieved once all entities participated in current communication be authorized. $SK_{U \leftrightharpoons MC}$ can be used to keep subsequent communication between two parties U and MC, secure and safe. The session key is based on the $r_u.P$, $r_{en}.P$ and $r_{mc}.P$, and they are

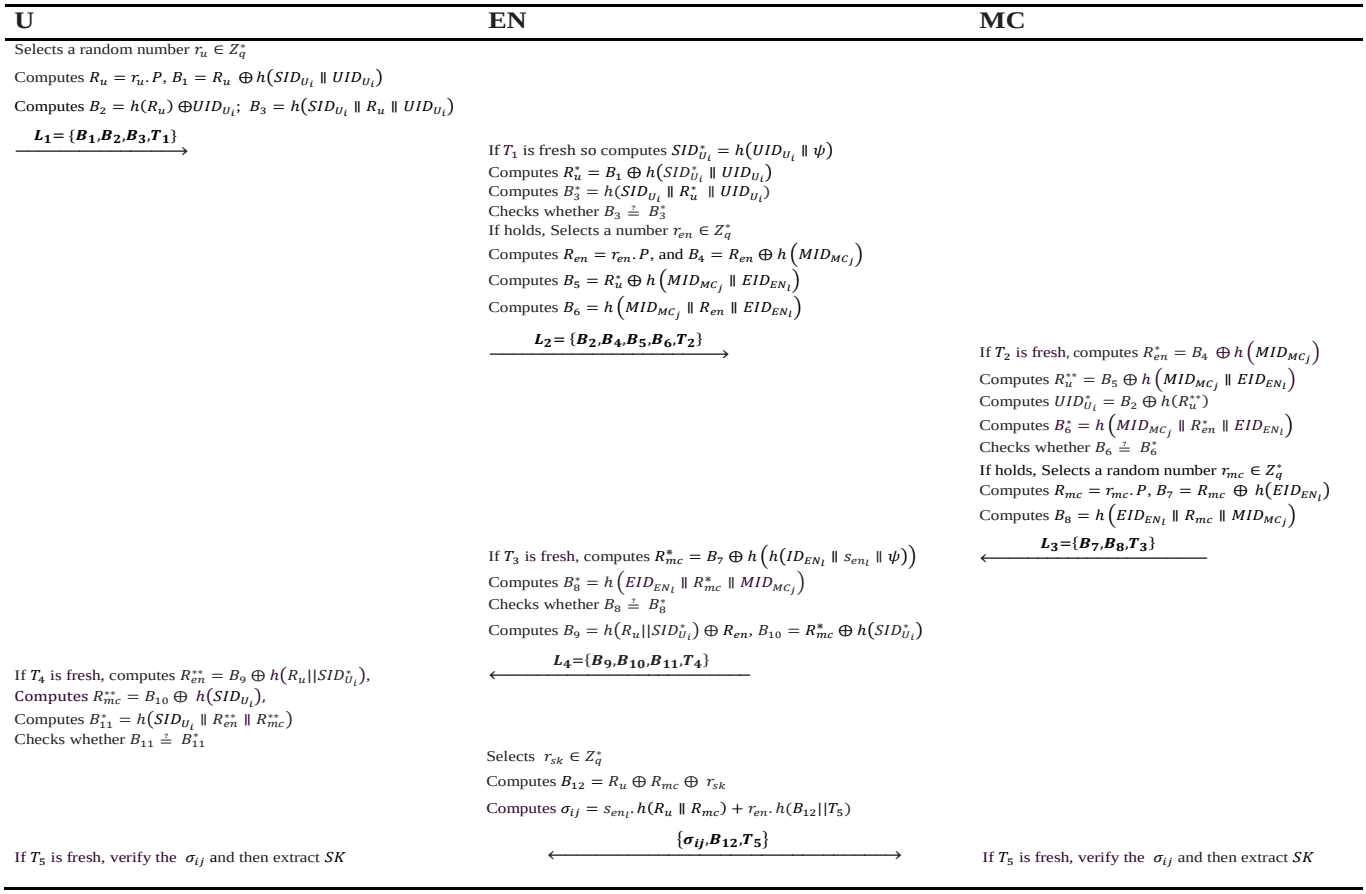


Figure 2: Session key generation and authentication process.

different in each session. This is mainly because r_u, r_{en} and r_{mc} will be changed for each session. In this scheme, a session is not dependent on other sessions and the generated session key is valid for a period of time VP_{SK}. To extend the period length, it needs both U and MC send a same request to the relevant EN. Due to the fact that negotiating a session key in the current session cannot be used to compromise past or future sessions, our system is known-key secure.

5) Resistance to Replay Attack: Our scheme uses the random number generator to ensure that communication messages are as fresh as possible. In this scheme, the numbers r_u, r_{en}, and r_{mc} are randomly selected by U, EN, and MC for each session, which guarantees the messages are fresh. Moreover, the timestamp employed for each communication among U, EN, and MC is another reason to guarantee the freshness of communication. Consider an adversary $\mathbf{\Lambda}$ intercepts a login request message $L_1 = \{B_1, B_2, B_3, T_1\}$ including the timestamp T_1 and it presents a replay attack at the time $T_1^{'}$. Due to the $\triangle T < T_{EN} - T_1^{'}$, the receiver will reject the message in which $\triangle T$ is a conjointly agreed to transmission delay, and T_{EN} is the latest timestamp of the EN as receiver of the message. Hence, our scheme is not vulnerable to replay attacks.

6) User's Anonymity: U_i sent a login request to the relevant edge node and it authenticates the U_i by pairing operations without knowing the U_i real identity. Also, $\mathbf{\Lambda}$ cannot forge the pseudonyms and the corresponding private keys, since r_i selected by U_i is secure. Based on Definition 2, it is hard to compute the r_i of the user through UID_{U_i} and P. As a result, our scheme meets privacy-preserving as it is impossible for the adversary to extract ID_{U_i}. Furthermore, for each communication, a user frequently changes pseudonyms, and only TA can reveal the relationship among these pseudonyms.

Definition 2: Discrete Logarithm Problem (DLP). Considering an additive elliptic curve group G of order q. Given $P, Q \in G$ on E and $x \in Z_q^*$ such that $Q = x.P$, it is hard to compute x from Q.

The comparison between our scheme and other related schemes [12], [21], [22], and [23] shows that our scheme conforms to all of the security requirements, whereas the comparable schemes fulfil only partial security requirements.

V. Performance Analysis

Here, we present a quantitative performance study of our scheme by making a comparison with other related schemes [12], [21], [22], and [23].

A. Computation and Communication Cost

In order to easily analysis, we respectively define some cryptography operations T_{sm}, T_{mph} ,T_{pa}, and T_h as the cost

of the scalar-point multiplication, map-to-point hash function, point addition, and a hash function.

Here, we estimate the computation cost of our scheme, [12], [21], [22], and [23]. Due to the different framework and architecture of our scheme and other related works, we separately calculate the computation cost for each layer. In our scheme, the total computation cost consists of the $U/EN/MC$ authentication cost, signature generation and verification cost for sharing session key, and data encryption/decryption cost by session key. In user layer, it is including one scalar-point multiplication and six hash function $T_{sm} + 6T_h$. The computation cost of edge node compromise of one scalar-point multiplication and twelve hash functions $T_{sm} + 12T_h$; whereas in the medical center layer, the computation cost consists of one scalar-point multiplication and two hash function $T_{sm}+6T_h$. Therefore, one scalar-point multiplication and four hash function. Therefore, the overall computation cost for our scheme is $3T_{sm} + 22T_h$.

In [12], the computation cost at user layer, gateway layer and medical center layer is $6T_h$, $19T_h$, and $12T_h$, respectively. The total cost of computation is $37T_h$. In [21], the computation cost in the user layer is including five scalar multiplication operations, three map-to-point hash function operations, two point-addition operations, and two general hash function operations. At the user layer, the computational cost is $5T_{sm} + 3T_{mph} + 2T_{pa} + 2T_h$. In similar fashion, the total computation cost for this scheme is $13T_{sm} + 5T_{mph} + 10T_{pa} + 3T_h$. The user's computation cost of the suggested scheme in [22] is including four scalar multiplication operations, three general hash function operations, and two point-addition operations. At the user layer, the computational cost is $4T_{sm}+2T_{pa}+3T_h$. As the same way, the total computation cost in this scheme is $8T_{sm} + 3T_{pa} + 6T_h$. In [23], the computation cost in the user layer is including two scalar multiplication operations, one point-addition operations, and three general hash function operations. The computational cost at the user layer is $2T_{sm} + T_{pa} + 3T_h$. In similar fashion, the overall computation cost for this scheme is $3T_{sm} + 2T_{pa} + 5T_h$.

Besides, we compute the communication cost of our scheme and other comparable schemes. We assume the length of medical center identity ID_{MC}, edge node identity ID_{EN}, $h(.)$ as the output of hash function, random number $x \in Z_q^*$ is 160 bits while timestamps, size of each element $P \in G$ and the length of user identity ID_U are considered to be 32 bits, 320 bits, and 80 bits, respectively [24]. If the Advanced Encryption Standard (AES) applied as the symmetric encryption algorithm, the block size of cryptography is equal to 128 bits [25]. In our scheme, the login request $L_1 = \{B_1, B_2, B_3, T_1\}$ in the user layer needs $160 + 160 + 160 + 32 = 512$ bits. In the edge layer, messages $L_2 = \{B_2, B_4, B_5, B_6, T_2\}$, $L_4 = \{B_9, B_{10}, B_{11}, T_4\}$, and $\{\sigma_{ij}, B_{12}, T_5\}$ respectively need $160+160+160+160+32 = 672$ bits, $160+160+160+32 = 512$ bits, and $160 + 160 + 32 = 352$ bits. For the $L_3 = \{B_7, B_8, T_3\}$ in the medical center layer, $160+160+32 = 352$ bits are needed. Therefore, the total communication cost of our scheme is $512 + 672 + 512 + 352 + 352 = 2400$ bits (300 Bytes). The performance comparisons of our scheme and other related schemes [12], [21], [22], and [23] is presented in Table II. Regarding communication efficiency, the cost of our scheme is less than other comparable schemes. Our scheme is the most secure with adequate computing efficiency, as it incorporates security, efficiency, and scalability factors.

B. Symmetric Encryption Discussion and Analysis

Symmetric encryption algorithms use a secret key to encrypt/decrypt data. Generally, these algorithms are more faster than asymmetric algorithms. As discussed in [26], symmetric algorithms are also quite efficient to secure communication. Nevertheless, distribution of the secret key is considered as one of the major challenges in symmetric algorithms. One of the best solutions to deal with this concern is choosing the asymmetric algorithms to encrypt the secret key. In this work, we proposed a message signature based on ECC in order to share the random number (r_{sk}). This number has an important role to generate the session key by the user and the medical center.

The life-time of key as well as the length of key (Len_{SK}) are other concerns related to the session key in symmetric encryption algorithms. These parameters have an impact on the security strength and computation cost of the symmetric algorithm. In the following, we discuss more on these two concerns.

In the proposed scheme, the session key used for secure communication between U and MC is valid for a period of time. Once the session key is expired, a new session key needs to be generated. Since the expiration time of the key has an impact on security strength, it is important to choose a suitable period of time for the life-time of the session key. The long life-time of the session key reduces the security strength, in contrast, the short expiration time increases the strength of security. Besides, the expiration time affects computation cost. Hence, it is important to consider the tradeoff between security strength and computation costs. As explained in [27], it is difficult to set a specific time for the session key life-time as it depends on the requirement of the real system, nevertheless, they recommended 24 hours for the life-time of the session key. In our scheme, in order to decrease the computation cost related to new key generation, the life-time of the session key can be extended simply by sending a common request from both U and MC to the relevant EN. Once the EN received this request it only needs to select a new random number r_{sk} and send back to two parties U and MC.

The length of the key (Len_{SK}) is another parameter that affects security strength. When Len_{SK} is long, the security strength will be increased, in contrast, the security strength will be reduced when Len_{SK} is short. It also has an impact on encryption and decryption time. It means if the Len_{SK} be long, the time of encryption and decryption will be increased and the short length of the key reduces these times. Since both security and latency are requirements in a real-time monitoring system, it is important to consider a tradeoff between security level and encryption/decryption time.

Here, we analyse our scheme in terms of security strength with different length of the session key. To this end, we compute the False Positive Rate (FPR) under different percentages

Table II: Performance Comparisons.

Ref.	User Layer	EN/AP/CS Layer	MC Layer	Total Computation Cost	Commun. Cost
[12]	$6T_h$	$19T_h$	$12T_h$	$37T_h$	284 Bytes
[21]	$6T_{sm}+3T_{mph}+6T_{pa}+2T_h$	$7T_{sm}+2T_{mph}+4T_{pa}+T_h$	-	$13T_{sm}+5T_{mph}+10T_{pa}+3T_h$	520 Bytes
[22]	$4T_{sm}+2T_{pa}+3T_h$	$4T_{sm}+T_{pa}+3T_h$	-	$8T_{sm}+3T_{pa}+6T_h$	482 Bytes
[23]	$2T_{sm}+T_{pa}+3T_h$	$T_{sm}+T_{pa}+2T_h$	-	$3T_{sm}+2T_{pa}+5T_h$	402 Bytes
Our Scheme	$T_{sm}+6T_h$	$T_{sm}+12T_h$	$T_{sm}+6T_h$	$3T_{sm}+22T_h$	300 Bytes

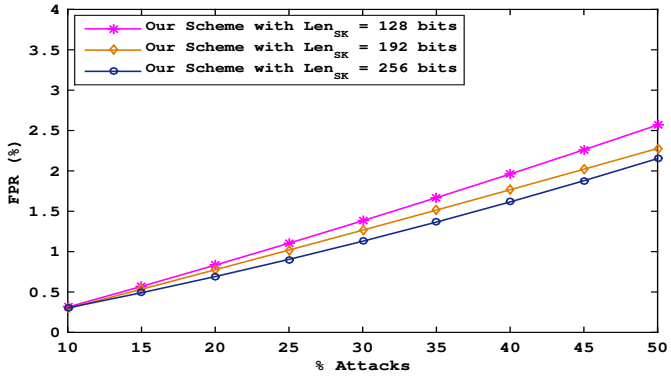


Figure 3: FPR for our scheme with different length of session key under different percentages of attacks.

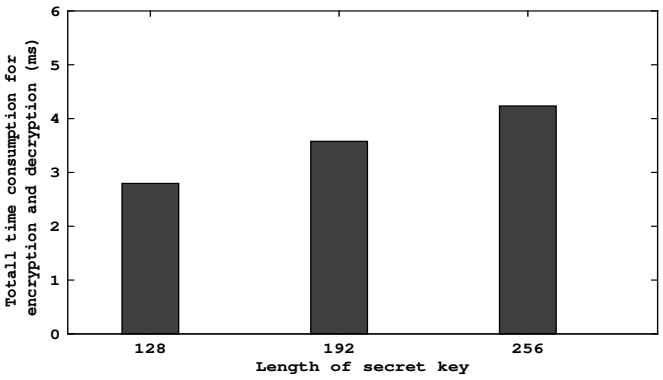


Figure 4: Time consumption for encryption and decryption 1GB data under different length of session key.

of attacks as well as with Len_{SK}= 128 bits, 192 bits, and 256 bits. As mentioned in [28], FPR is measured as follow:

$$FPR = \frac{FP}{FP + TN} \tag{2}$$

where FP is the number of users incorrectly found as attacker and TN is the number of users correctly detected as non-attacker.

Figure 3 shows security strength of our scheme with different length of secret key Len_{SK} = 128, 192 and 256 bits. As we can see in this figure, the proposed scheme with Len_{SK} = 256 bits is more secure than our scheme with Len_{SK} = 192, and 128 bits, but it is negligible.

Besides, we analyse the computation cost of our scheme for symmetric encryption under different length of secret key. To this end, we simulate the symmetric algorithm used in our scheme to encrypt and decrypt 1GB of data. The running time of the cryptographic operations on U and MC is derived by repeated simulation experiment. As we can see in Figure 4, the

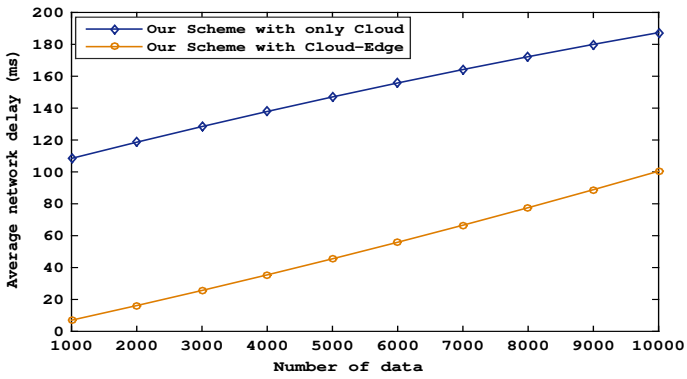


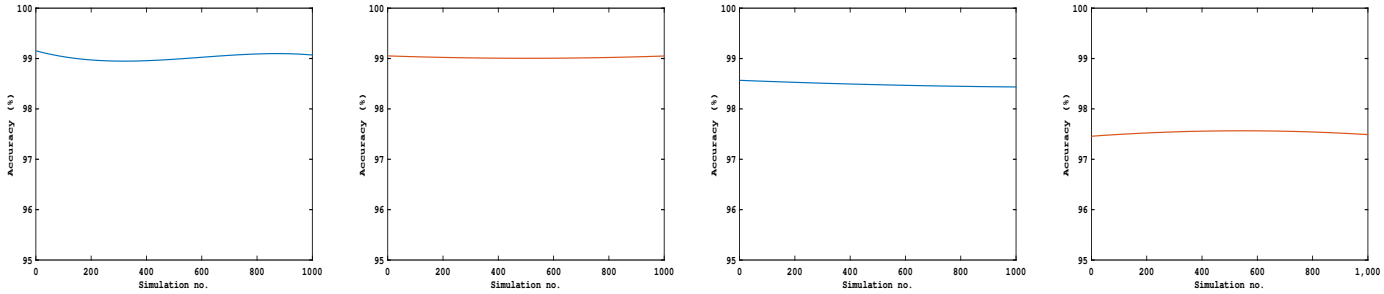
Figure 5: Network delay in two scenarios.

time consumption for encryption and decryption of data is 2.76 (ms) when Len_{SK} = 128, and it is 4.23 (ms) when Len_{SK} = 256 bits. Since latency is a primary concern for pervasive real-time applications, we recommend Len_{SK} = 128 bits for the session key.

C. Numerical Results

In a real-time medical monitoring system, because of the importance of data-in-transit, it is important that such a system be accurate with the lowest delay. In this study, in order to analysis our scheme we take into account two parameters network delay and overall accuracy. In order to demonstrate the feasibility of proposed cloud-edge medical monitoring system, we simulate both environment and integrated architecture using iFogSim [29]. We simulate 60 minutes real-life scenario on a Linux host using Intel Core i7-980X, 3.33GHz with a maximum of 150 devices in our simulation, and around 50K tasks are generated.

We also built a dataset including the raw medical data related to 275 patients positive for Covid-19, 156 patients suspected of having coronavirus, and 160 samples from healthy people (Covid-19 negative cases) [30]. These data were extracted from a dataset created by nationally recognized sources in Iran. The raw data contains body temperature, peripheral capillary oxygen saturation (SpO_2), and respiratory rate along with the age and weight of the user/patient. And, for the sake of simplicity, we considered only three medical advice issued by the medical center: (i) isolate at home, (ii) need more testing, (ii) become hospitalized. All medical data and advice will be encrypted by the proposed scheme and exchange securely between the user and the medical center. In a real-time medical monitoring system, because of the importance of data-in-transit, data must be handled with the highest possible accuracy and lowest delay. Hence, similar to



(a) 20% Attackers (b) 30% Attackers (c) 40% Attackers (d) 50% Attackers

Figure 6: The overall accuracy of the proposed scheme when all positive, suspected and negative Covid-19 cases are participated in the system along with different percentages of attackers.

[31], in this study, we use network delay and overall accuracy as two parameter indexes for performance analysis.

Network delay: Here, we illustrate the influence of edge nodes in the developed architecture for a remote medical monitoring system, in further detail. To that end, synthetic workload is utilized as the real-world workload to simulate such environment in large scale that is not currently available [32]. Since latency is a concern in the real-time systems, when there are no bandwidth limitations, we analyze and compare our scheme in terms of network latency in two distinct scenarios: (i) with only cloud; (ii) with cloud-edge. Figure 5 shows the average network delay recognized by the proposed monitoring system is high when we use only cloud. In contrast, in second scenario, average network delay for availability of data in this system is low.

Overall Accuracy: Here, we use the Monte-Carlo simulation to evaluate the accuracy of our scheme. The evaluation is under man-in-the-middle and impersonate attack. Monte-Carlo simulation checks the validity of a model by repeating the experiment many times [28]. In this work, we conducted 1000 Monte-Carlo simulations to assess the overall accuracy of our scheme when all data related to all Covid-19 cases (positive, suspected, and negative) plus medical advice are exchanged in the network. Equation 3 is utilized to compute the overall accuracy. As we can see in Figure 6, the obtained results show the average overall accuracy for our scheme in each case is approximately 97%. It proves that our scheme is valid and accurate.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

where TP and FP refer to the number of forged and correct messages detected properly and TN and FN are the number of forged and correct messages detected incorrectly.

VI. Conclusion

In the corona virus pandemic, the remote monitoring system in e-health has been more highlighted. In this study, we have discussed the issues related to security and privacy in real-time medical monitoring systems. To address the security concerns, we have proposed an efficient authentication scheme with privacy-preserving for the cloud-edge based monitoring system. The non-mathematical analysis have proved that the proposed scheme is secure against various attacks. Furthermore, we have compared our scheme with some previous works in terms of computation and communication cost. The obtained results illustrated that our scheme is robust and efficient for the real-time medical monitoring system. The numerical and simulation results have also proved that our scheme is valid and accurate.

Acknowledgment

This work is partially-supported by Universiti Teknologi Malaysia under the UTM Fundamental Research Grant (UTMFR) with vote no Q.K130000.2556.21H12.

References

[1] A. Jindal, A. Dua, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "An efficient fuzzy rule-based big data analytics scheme for providing healthcare-as-a-service," in *2017 IEEE international conference on communications (ICC)*. IEEE, 2017, pp. 1–6.

[2] M. Otoom, N. Otoum, M. A. Alzubaidi, Y. Etoom, and R. Banihani, "An iot-based framework for early identification and monitoring of covid-19 cases," *Biomedical Signal Processing and Control*, vol. 62, p. 102149, 2020.

[3] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body area networks: A survey," *Mobile networks and applications*, vol. 16, no. 2, pp. 171–193, 2011.

[4] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned iot-based healthcare monitoring," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 491–499, 2020.

[5] C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, "A privacy authentication scheme based on cloud for medical environment," *Journal of medical systems*, vol. 38, no. 11, p. 143, 2014.

[6] S.-Y. Chiou, Z. Ying, and J. Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment," *Journal of medical systems*, vol. 40, no. 4, p. 101, 2016.

[7] S. H. Islam, M. K. Khan, and X. Li, "Security analysis and improvement of a more secure anonymous user authentication scheme for the integrated epr information system'," *PloS one*, vol. 10, no. 8, p. e0131368, 2015.

[8] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for tmis," *Security and Communication Networks*, vol. 9, no. 13, pp. 1983–2001, 2016.

[9] A. K. Sutrala, A. K. Das, V. Odelu, M. Wazid, and S. Kumari, "Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems," *Computer methods and programs in biomedicine*, vol. 135, pp. 167–185, 2016.

[10] L. Lyu, K. Nandakumar, B. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, "Ppfa: Privacy preserving fog-enabled aggregation in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3733–3744, 2018.

[11] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, A. G. Reddy, K. Park, and Y. Park, "On the design of fine grained access control with user authentication scheme for telecare medicine information systems," *IEEE Access*, vol. 5, pp. 7012–7030, 2017.

[12] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483–495, 2018.

[13] Z. Xu, D. He, P. Vijayakumar, K.-K. R. Choo, and L. Li, "Efficient ntru lattice-based certificateless signature scheme for medical cyber-physical systems," *Journal of medical systems*, vol. 44, no. 5, pp. 1–8, 2020.

[14] T. Alladi, V. Chamola *et al.*, "Harci: A two-way authentication protocol for three entity healthcare iot networks," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 361–369, 2020.

[15] Y. Zhang, D. He, M. S. Obaidat, P. Vijayakumar, and K.-F. Hsiao, "Efficient identity-based distributed decryption scheme for electronic personal health record sharing system," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 384–395, 2020.

[16] A. Tahiliani, V. Hassija, V. Chamola, S. S. Kanhere, M. Guizani *et al.*, "Privacy-preserving and incentivized contact tracing for covid-19 using blockchain," *IEEE Internet of Things Magazine*, vol. 4, no. 3, pp. 72–79, 2021.

[17] T. Zhou, J. Shen, D. He, P. Vijayakumar, and N. Kumar, "Human-in-the-loop-aided privacy-preserving scheme for smart healthcare," *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2020.

[18] S. Garg, A. Singh, K. Kaur, G. S. Aujla, S. Batra, N. Kumar, and M. S. Obaidat, "Edge computing-based security framework for big data analytics in vanets," *IEEE Network*, vol. 33, no. 2, pp. 72–81, 2019.

[19] S. Goudarzi, M. H. Anisi, A. H. Abdullah, J. Lloret, S. A. Soleymani, and W. H. Hassan, "A hybrid intelligent model for network selection in the industrial internet of things," *Applied Soft Computing*, vol. 74, pp. 529–546, 2019.

[20] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[21] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2327–2339, 2014.

[22] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[23] C. Guo, P. Tian, and K.-K. R. Choo, "Enabling privacy-assured fog-based data aggregation in e-healthcare systems," *IEEE Transactions on Industrial Informatics*, 2020.

[24] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.-K. R. Choo, "A robust and energy efficient authentication protocol for industrial internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606–1615, 2017.

[25] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE journal of biomedical and health informatics*, vol. 22, no. 4, pp. 1299–1309, 2017.

[26] S. Li, "Iot node authentication," in *Securing the Internet of Things*. Syngress Boston, 2017, pp. 69–95.

[27] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 2, pp. 94–107, 2016.

[28] S. A. Soleymani, S. Goudarzi, M. H. Anisi, N. Kama, S. Adli Ismail, A. Azmi, M. Zareei, and A. Hanan Abdullah, "A trust model using edge nodes and a cuckoo filter for securing vanet under the nlos condition," *Symmetry*, vol. 12, no. 4, p. 609, 2020.

[29] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments," *Software: Practice and Experience*, vol. 47, no. 9, pp. 1275–1296, 2017.

[30] *Iran Ministry of Health and Medical Education. Report of COVID-19 pandemic in Iran*, 2020. [Online]. Available: http://dme.behdasht.gov.ir/

[31] S. Tuli, N. Basumatary, S. S. Gill, M. Kahani, R. C. Arya, G. S. Wander, and R. Buyya, "Healthfog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated iot and fog computing environments," *Future Generation Computer Systems*, vol. 104, pp. 187–200, 2020.

[32] D. L. Kiskis and K. G. Shin, "A synthetic workload for a distributed real-time system," *Real-Time Systems*, vol. 11, no. 1, pp. 5–18, 1996.