Hindawi
Journal of Healthcare Engineering
Volume 2021, Article ID 9954089, 20 pages
https://doi.org/10.1155/2021/9954089

Research Article

Secure Patient Authentication Framework in the Healthcare System Using Wireless Medical Sensor Networks

Saeed Ullah Jan,[1] **Sikandar Ali**,[2,3] **Irshad Ahmed Abbasi**,[4] **Mogeeb A. A. Mosleh**,[5] **Ahmed Alsanad**,[6] **and Hizbullah Khattak**[7]

[1] *Department of Computer Science & IT, University of Malakand, Chakdara 18800, Pakistan*
[2] *Department of Computer Science and Technology, China University of Petroleum-Beijing, Beijing 102249, China*
[3] *Beijing Key Lab of Petroleum Data Mining, China University of Petroleum-Beijing, Beijing 102249, China*
[4] *Department of Computer Science, Faculty of Science and Arts at Belgarn, University of Bisha, Sabt Al-Alaya 61985, Saudi Arabia*
[5] *Faculty of Engineering and Information Technology, Taiz University, Taiz 6803, Yemen*
[6] *STC's Artificial Intelligence Chair, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia*
[7] *Department of Information Technology, Hazara University Mansehra, Mansehra 21130, Khyber Pakhtunkhwa, Pakistan*

Correspondence should be addressed to Sikandar Ali; sikandar@cup.edu.cn, Mogeeb A. A. Mosleh; mogeebmosleh@taiz.edu.ye, and Ahmed Alsanad; aasanad@ksu.edu.sa

Received 4 April 2021; Revised 4 July 2021; Accepted 10 July 2021; Published 23 July 2021

Academic Editor: Dilbag Singh

Biosensor is a means to transmit some physical phenomena, like body temperature, pulse, respiratory rate, electroencephalogram (EEG), electrocardiogram (ECG), and blood pressure. Such transmission is performed via Wireless Medical Sensor Network (WMSN) while diagnosing patients remotely through Internet-of-Medical-Things (IoMT). The sensitive data transmitted through WMSN from IoMT over an insecure channel is vulnerable to several threats and needs proper attention to be secured from adversaries. In contrast to addressing the security of all associated entities involving patient monitoring in the healthcare system or ensuring the integrity, authorization, and nonrepudiation of information over the communication line, no one can guarantee its security without a robust authentication protocol. Therefore, we have proposed a lightweight and robust authentication scheme for the network-enabled healthcare devices (IoMT) that mitigate all the identified weaknesses posed in the recent literature. The proposed protocol's security has been analyzed formally using BAN logic and ProVerif2.02 and informally using pragmatic illustration. Simultaneously, at the end of the paper, the performance analysis result shows a delicate balance of security with performance that is often missing in the current protocols.

1. Introduction

A healthy human body is a prerequisite to happiness, mental ease, and calm existence. Such a body ensures a sound and robust mind too. On the other hand, an unhealthy physique necessitates caring, treating, diagnosing, and preventing a human for injury or any other illness collectively termed as a healthcare system. While managing healthcare, sight negligence can upset the whole process and may turn counterproductive. This negligence and the flawed nursing system are an embarrassment for patient monitoring due to the attached modules to the human body and recurrent power supply. Each time replacement of power-source can also create serious risks for the patient's life. To ease the work of the whole team and stop human errors and aid the medical professional in examining a patient for a disease, technology and network-oriented devices (Internet-of-Medical-Things (IoMT)) are used that guarantee an authentic result [1]. IoMT facilitates healthcare personnel over the Internet and a decision control system without human-patient or patient-computer interaction. Such emerging technology needs novel services for grasping the attention of healthcare industries for the remote monitoring of their patients. This remote monitoring will not only minimize the cost of a disease for a layman, but also provide the facility for the maximum diagnosing of a patient in this crowded world [2].

Similarly, the healthcare industries are ever-growing, taking over 20.4bn technological interconnected and network-enabled devices. These devices have communication competencies that remotely collect patient information and send it to medical professionals for examination and treatment recommendations. However, the transmission of such sensitive data (body temperature, oxygen saturation, the glucose level in the blood, respiratory rate, heartbeat/pulse rate, etc.) is performed via an open network channel, vulnerable to several threats. It needs proper attention to make it secure. Security, communication, and computation cost or media consumption are also necessary, so that a doctor may easily recognize hand gestures, blood vessels contraction/relaxation, the flow of message in the neuron, and central nervous system (CNS) response of a patient, etc. Attention is also needed for a robust detection system, different color recognition, and stereo sequence of an image control via media [3].

The data acquisition and processing competencies of scalable and practicable devices/machines, interconnected devices, embedded sensors, and installed software applications that can push data flow for patient monitoring are at peak today. After sensing the patient, data is transmitted to the medical professional with wireless networks named Wireless Medical Sensor Network (WMSN) (WMSN is a type of self-organizing network with multiple or mini-embedded sensors inside the human body to sense physical conditions with wireless connectivity. The working procedure of WMSN is to transport data among different participating entities or in the coverage area. WMSN is the fundamental foundation of Internet-of-Medical-Things (IoMT) that can enhance patients' medical treatment) to practice for the diagnosis and medical care. The mutual authentication and cross-verification of each participating entity for such a sensitive transmission are impossible without a key-agreement protocol. It not only facilitates patients at home but is useful in diagnosing various types of diseases as well. Besides, health experts, too, are assisted in assessing and giving advice. While patients' data and physicians' diagnoses are linked/transferred via an open network channel, slight negligence may not only be detrimental and counterproductive, but will shatter people's trust as well. Therefore, it needs extra care and a renewed approach to tackle the issues [4].

Amin et al. [5] proposed the scheme for communicating patient-sensitive information to the doctor/medical professional for diagnosis, which is vulnerable to man-in-the-middle, privileged insider attacks, and lack of mutual authentication. We proposed an improved, lightweight authentication framework that mitigates these weaknesses. The proposed scheme's security has been analyzed using the BAN logic and Provierif2.02 toolkit with an informal discussion for justification. The evaluation results show that the scheme is lightweight in contrast to the state-of-the-art protocol in recent literature. As such, we recommend the proposed protocol for practical implementation in the healthcare online patient diagnoses environment. The main contributions of the research are as follows:

(1) In IoMT, the medical professionals having mobile-device can securely obtain the real-time patient's status for diagnosing

(2) The outdated data broadcasting flaw common in prior protocols designed for the healthcare system has been fully addressed in this research work

(3) A simple hash cryptographic function and public-private key pair are used for designing the security protocol that is lightweight and balances performance with security for the fast, reliable, consistent, and low-latency Wireless Medical Sensor Network (WMSN)

(4) The sensor revocation/reissue phase demonstrates that, upon stolen or misplaced sensor or mobile device at any time, no one can assess the internally stored credentials, which means that the prospective scheme is free of offline/online identity guessing and stolen-verifier attacks

(5) The protocol's security has been scrutinized both formally using BAN logic and informally using realistic illustration, showing the protocol's robustness

(6) The protocol's scalability, reachability, integrity, and authorization, as well as security features, have been achieved using ProVerif2.02 simulation

1.1. System Model. The wireless technology for the healthcare industry and installed applications in network-enabled devices can communicate seamlessly to the proper device via WMSN, which has limited battery capacity and low latency. It offers back-end services, quick and intelligent network features for IoMT in healthcare services delivery, while the embedded sensors in the human body can collect and communicate physical conditions to the gateway node using the said limited featured wireless network, for example, (i) visual sensor for sight checkup, (ii) pressure sensor on examining the breath duration of a patient or stress of central nervous system (CNS) or the lower part of the mouth, (iii) temperature sensor for finding the normal body heat, (iv) oxygen saturation sensor for oxygenated blood monitoring, (v) EEG/ECG/MRI sensor is for heart and other parts checkup, (vi) ventilator sensor to provide oxygen continuously to a patient, and (vii) imaging, treatment, diagnosing, and data analytics, etc.

Figure 1 represents the system model or architecture in this paper having four (04) main participants: online service provider for the healthcare system (Certificate Authority), the gateway node (GW), a set of sensors inside the patient body, and external user (medical professionals). The certificate authority (CA) is a specialized company that provides connectivity, data processing, and real-time problem-solving capabilities. The gateway node (GW) is an essential component of the system. All sensors and mobile devices used by patient/medical professionals must be fitted with a gateway node (GW) and connected with alternative network services such as 5G, 6G, and other wireless communication interfaces. The external user (medical professional) can access a designated sensor (patient monitoring) from some ward/location/area. When a patient is in a specialized region or location, the gateway node (GW) controls data broadcasting and verifies the patient's validity. The identification of illegitimate sensors or patient or mobile device or medical professional in the designated area or location or any place may also be easily recognized due to the capability of the intermediary agent (gateway-node (GW)).

It is noteworthy that the Certificate Authority (CA) is officially a fully trusted entity. Their confidence must be consistent, because the trust deficit may impair the system's reliability. The proposed scheme ensures that the registration center can be fully trusted by the patient/sensor/medical professional and the gateway node (GW). In contrast, any other entity alone may not be fully trusted.

1.2. Threat Model. The Dolev and Yao [6] model tells us about an adversary's authority between two communicating bodies through an open network channel. According to this model, all the possibilities with an attacker are as follows:

(i) An adversary might extract the stored data from the GW memory/sensor/mobile device of a medical professional and verify some credentials

(ii) An adversary might alter, delete, update, corrupt, or inject false information on participants' communication over a public network channel

(iii) Adversaries can also have the capabilities to replay, modify, or delete the beneficial information exchange among the participants over a private channel

(iv) An adversary can also obtain the internal sensitive credentials from a stolen sensor/mobile device of a medical professional or from the memory of misplaced sensor/mobile device of medical professional either by reverse engineering technique or by using some critical tags in offline mode, but cannot do both at the same time

With an adversary, our threat model additionally includes the following possibilities:

(1) Privacy Threat

Suppose that an adversary uses aircrack-ng software to extract sensor locations and other helpful information from stolen data packets. In that case, they are using airodump-ng software to detect signal strength, filtering it for additional attacks, and disrupting the synergy by utilizing airplay-ng software to deauthenticate it. The attacker also has the chance to disrupt the entire network by transferring disassociation packets frequently to disguise its normal operations.

(2) Stolen-Verifier Threat

Suppose that an attacker can physically steal the mobile device of a medical professional or sensor used by a patient and vice versa, or if it is misplaced, lost, or destroyed somewhere from a legitimate user, an adversary can attack it in order to obtain access to the information recorded in the sensor's/mobile device's memory. After that, they can reveal the encrypted data and begin authentication with another hospital's gateway node or sensor used by other medical professionals or patients.

(3) Traffic Analysis Threat

Suppose that an adversary can drill the data from IoMT and control the communication channel traffic of broadcasting information towards the sensors. The traffic also consists of sensitive patient's physical phenomenon packets transferred between a medical professional's sensor/mobile device and a gateway node; after the adversary's forensic, the packets in traffic can reveal sensitive information about the system. The adversary evaluated it to see if it might be used as a threat.

(4) Access Control Threat

The adversary also can understand the different policies and inject false information in the communication path, which connects the different participants for useful information exchange. They can also gain complete control of the channel by examining the overall system activities.

(5) Identity Spoofing Threat

An adversary can obtain the identity of a legitimate participant in the system and maliciously spoof/fool the system. If they become successful in getting legitimate participants' identities, they can easily control the communication line for altering, deleting, or injecting false information in it.

1.3. General Architecture of the Network Model. As explained earlier, the main participants in the proposed system are Certificate Authority (CA), Gateway Node (GW), Sensor Node (SN), and Medical Professional (Mobile-Device). The general working scenario of the system is as follows:

(i) Gateway node, sensor node, and a medical professional will first register with the certificate authority

(ii) Intelligent sensors embedded inside the patient's body can sense physical phenomenon and broadcast it towards the gateway node through resource constraint WMSN

(iii) From the gateway node, with the help of WMSN, the data is transmitted toward medical professionals for possible diagnosis

The diagrammatic representation of the proposed framework is shown in Figure 2.

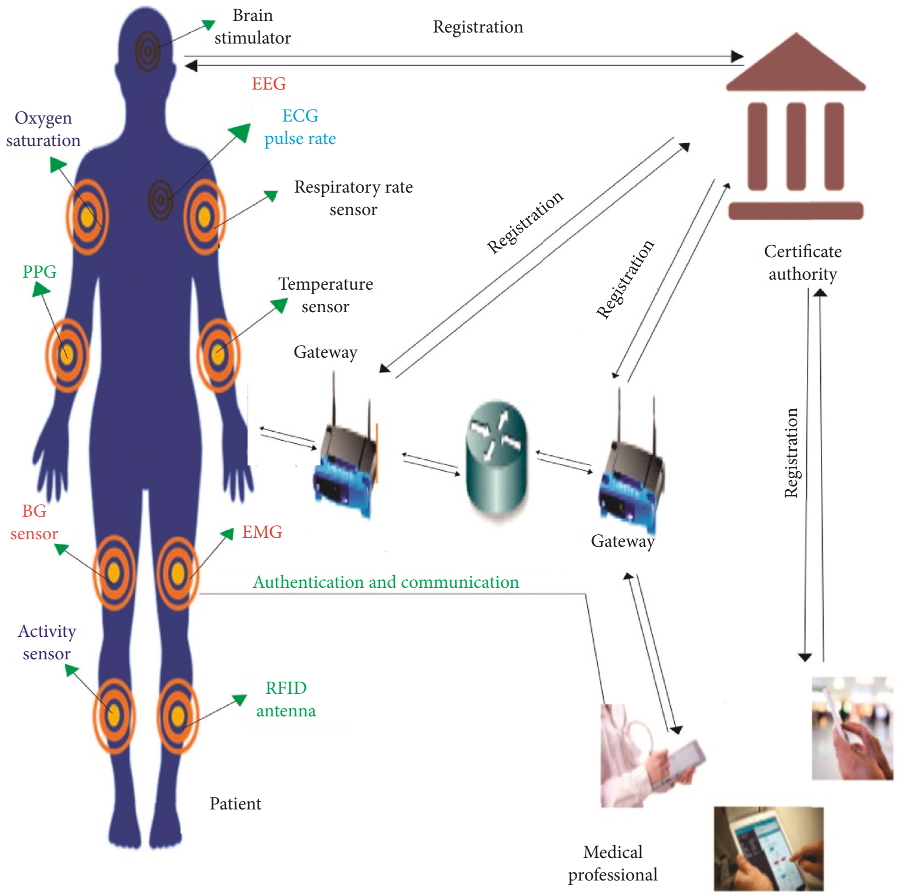


Figure 1: Network model.

2. Literature Review

Advances in technology for IoMT devices to transmit data of the healthcare domain and communicate with one another are increasing rapidly, and its security is a challenging task. Since their interconnectivity is vulnerable to several threats like other network-enabled devices, therefore, it needs to be appropriately authenticated with each other. Recently, Singh et al. [7] proposed a framework for orthopedics patients in the pandemic period of COVID-19. Such a patient is unable to attend the hospital for treatment due to chances of Corona. They demonstrated how the orthopedics' patient could use it for his/her healthcare at home while being remotely connected with the hospital. The connectivity of both patient and doctor with the hospital using cloud computing is mandatory. Cloud computing offers infrastructure in three specific models, i.e., Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). However, the stakeholders' cloud-saved database usage can create security and interoperability issues; therefore, [7] failed to design a dynamic authentication scheme for the participants. Alsubaei et al. [8] proposed an IoMT security assessment software framework for the developers/hospitals. But they failed to express the secure authentication of associated devices for examining a patient. Sanaz et al. [9] presented secure IoT-Based e-Healthcare architecture for patient monitoring. They installed an intelligent gateway among all the participants during patient monitoring. They proposed an authentication protocol that authenticates all the entities, including an embedded sensor inside the patient for sensing patients' data, time, temperature, and location intelligently, and transmits them to the health professional. A certificate-based methodology was adopted for the transport layer to work on Wireless Medical Sensor Networks (WMSNs), having a gateway node, a full-power computer system, and application software.

Subsequently, Lee et al. [10] suggested that a high-speed ICT tool can remotely be diagnosing a patient by monitoring and supervising his/her physical phenomenon, so that treatment costs can be minimized. They stated that the Graphical Processing Unit (GPU) is mandatory to reduce the load on the CPU during patient-sensitive data processing. However, they used simple encryption/decryption functions, which are not insufficient for security, privacy, and parallel computation. Rahimi et al. [11] enhanced the Datagram Transport Layer Security (DTLS) between the gateway nodes, patent, and medical professional. In addition, they stated that there is no need for a certificate for session initiation among the participants. Gope et al. [12, 13] suggested a useful structure for IoMT applications for data collection and interpretation based on privacy-preserving (P2DCA). Their architecture splits an

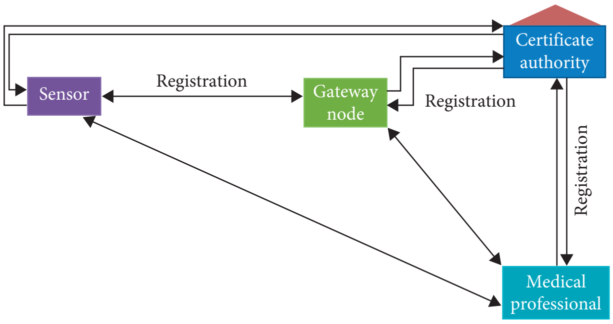


Figure 2: Working procedure of the proposed system.

interconnected network of integrated multimedia sensors into several clusters. A Cluster Head (CH) was defined as a bunch responsible for protecting the privacy of member MSNs and collecting data and location coordinates. Later, grouped multimedia data was analyzed on the cloud server using an artificial neural network for counterpropagation to extract meaningful information through segmentation. To integrate the infrastructure with mobile devices and overcome the shortage of medical services, Usman et al. [14] proposed an authentication protocol that mitigates medical resource misuse. A patient used its user's name and password on a mobile device to sign in to the public. It is without a password and identity table in the database. It satisfies specific standard protection criteria like protecting against offline password guessing attacks, replay attacks, impersonation attacks, man-in-middle attacks, and insider attacks. However, during decision-making at any crucial time, strong encrypted, authentic, and digitally signed information might be difficult to access even for a legitimate user and also vulnerable to known-key and forgery attacks.

Moghaddam et al. [15] implemented a client-based user authentication agent to validate client-side user identity; SaaS has been used to validate unregistered machines' authentication. The scalability, efficiency, security, man-in-the-middle attack, brute force attack, and timing attack have been evaluated according to the parameters. However, they used two separate servers for authentication and cryptography, which is the wastage of resources. Because the same can be managed from a single centralized server, this might decrease the overall cost and increase security. Satheesh et al. [16] proposed a framework for security and privacy in the healthcare system. Patient-centric confidential information and access control with an improved method of encryption was considered. A digital signature algorithm (DSA), patient pseudoidentity, and personal sensitive information protection were identified. The researchers addressed an enhanced security model for authentication and authorization to discover a new technique that can build security, privacy, and cross-verification of e-healthcare credentials. Allouzi and Javed [17] suggested a framework for authentication of health care devices called Soter. It offers a range of advanced features, such as trust of medical devices, promoting virtual federations, and a trust circle for customized and dynamic access control policy. It is worth noting that when an adversary can get a patient's login information by calling close to him, he/she can account for a hijacking attack on it. [18–20] proposed a cryptographic-based authentication framework, but such frameworks do not provide a fast and secure authentication mechanism, because the performance and security are unable to match each other. The researchers of [21, 22] designed a robust protocol for WMSN, in which multimedia type message was securely transmitted among peers. Still, the networks have not been fixed during multimedia message transmission and created hurdles for the end-user. Shrestha et al. [23] suggested a privacy-protection authentication scheme for healthcare information systems, in which they used digital signatures.

A blockchain is also a means of security for protecting healthcare system records. In this regard, Mikula and Jacobsen [29] proposed a blockchain-based authentication scheme for a centralized digital system. Their approach was implemented in the healthcare domain, in which fundamental patient data of size 3.8 MB has been executed in 2-3 seconds. Immutable data history has shown slow execution and wastage of resources data concerning patients. Further, Das et al. [30] proposed a dynamic identity-based authentication scheme that can resist forgery attacks, insider attacks, stolen verifier attacks, and guessing attacks. However, their strategy is suffering from a privileged insider attack, as the password and identity are transmitted from the user openly towards the server. Kumari et al. [31] provided high-level protection without reducing cloud/fog computing performance, mostly when IoMT is used, and they named it Fog-based Access Control Model (FACM). A cloud-based approach is applied in either mobile or nonmobile context, operating as an additional layer for fog servers, and can offer personalized access control environment. However, the execution time is related to several inputs. Upon increasing intakes, the model's performance will be degraded and vulnerable to impersonation and parallel session key attacks and lacks mutual authentication.

Finally, Rathore et al. [32] demonstrated a novel multilayer perception model for securely diagnosing diabetic patients. They said that the insulin pump inside a patient that controls blood glucose transmits patient sensitive information via the wireless channel and can easily be compromised. Neural-network-based multilayer security can provide security to the embedded medical device inside the patient. Their study revealed 91% accuracy upon an evaluation of the linear vector machine. However, still, no one can trust its reliability for such a sensitive treatment. Wu et al. [33] used Identity and password for designing a protocol via WMSN and healthcare applications. They said that, to overcome the noted disadvantages in their designed protocol, a novel approach is required. Their scheme attracts the modern healthcare industry, in which a paramedical professional can examine patent data remotely using a mobile device. However, because there are no encryption/decryption functions, their scheme is vulnerable to stolen-verifier attacks and privileged-insider attacks. Some related literature review is comprehensively described in Table 1.

Table 1: Comprehensive literature review.

Reference		Technique used	Main contribution	Limitation
[24]	Klonoff	Certificate-based datagram transport layer security (DTLS)	The proposed scheme consists of a secure and efficient end-user authentication and authorization architecture based on the certificate based DTLS handshake, secure end-to-end communication based on session resumption, and full mobility based on interconnected gateways	The authentication is performed in several steps, due to which multiple round trips can degrade the performance of the process. Also, the securities of the said architecture can easily be breached by an attacker
[25]	Borthakur et al.	Access-control determination (ACD) algorithm	This work proposes a fine-grained access control mechanism suitable for various implementation scenarios, including data storage, directories, and file management	The execution time length is associated with the number of the input task. Therefore the performance will be degraded by increasing the number of input tasks
[26]	Dastjerdi and Buyya	BLE bonding process	This paper addressed some of the fundamental problems. In designing, implementing, and deploying an end-to-end healthcare application that leverages the advantages of the fog computing approach	If the number of corresponding ECG devices increases, more storage will be required, and throughput will be reduced
[27]	Engineer et al.	Contextual-based access control (CBAC) technique and role-based access control (RBAC)	The paper suggested service-oriented security architecture in the IoT environment for remote medical services. The proposed framework accommodates dynamic security elements and requirements regarding different kinds of users	The proposed framework reduces sensitive information exposure by applying a security channel and encryption during the transmission of sensitive information between network parts
[9]	Sanaz et al.	Lightweight anonymous authentication protocol	A secure IoT-based healthcare system was proposed using BSN, called BSN-Care, which can efficiently accomplish various security requirements of the BSN-based healthcare	The proposed work can have stolen verifier attack, replay attack, and anonymity issue
[20]	Wang et al.	Machine learning/deep learning	This paper introduces a novel ECG-based biometric authentication approach that utilizes legendre polynomial extraction and MLP classifier for identification and authorization	Lack of standardization, not accommodate changes to the biometric overtime, sample collection phase is influenced by environmental and mental conditions
[28]	Akrivopoulos et al.	Physical unclonable functions (PUFs)	This paper presents a PUF based device authentication protocol capable of authenticating devices without demanding high CPU power from the end devices	No information about the end device is directly stored on the server, requiring an extra layer of security

3. Review Analysis of Amin et al. Protocol

Amin et al. [5] proposed a scheme for IoMT using WMSN in the healthcare domain. Their protocol consists of four phases, i.e., setup phase, registration phase, login and authentication phase, and password change phase. Each of these phases is described one by one under the following headings; notations used in their scheme and their description are shown in Table 2.

3.1. Setup Phase. The registration center (RC) first selects a secrete key K for the gateway node (GW) and calculates $\mathrm{SK}_{\mathrm{GW\text{-}SN}j} = h(\mathrm{ID}_{\mathrm{SN}j}||K)$. In contrast, n is the number of embedded sensors inside the patient's body, and its j^{th} value lies between 1 and n $(1 \leq j \leq n)$. The collision-free one way-hash cryptographic function is also defined here in this phase of the protocol as $h{:}\{0, 1\}^* \longrightarrow \{0, 1\}^1$.

3.2. Registration Phase. For user's registration, a legitimate user U_{ia} provides ID_{ia}, PW_{ia}, and computes $\mathrm{HPW} = h(\mathrm{ID}_{ia} \oplus \mathrm{PW}_{ia})$ and relays $\{\mathrm{ID}_{ia}, \mathrm{HPW}_{ia}\}$ towards gateway node (GW) via a secure channel. Upon receiving $\{\mathrm{ID}_{ia}, \mathrm{HPW}_{ia}\}$ message, the GW calculates $\mathrm{Reg}_{ia} = h(\mathrm{ID}_{ia}||R_{ia}||\mathrm{HPW}_{ia})$, $A_{ia} = \mathrm{HPW}_{ia}$, $B_{ia} = h(\mathrm{ID}_{ia}||R_{ia}||K)$, $C_{ia} = B_{ia} \oplus h(\mathrm{ID}_{ia} \oplus R_{ia} \oplus \mathrm{HPW}_{ia})$, and $D_{ia} = R_{ia} \oplus h(\mathrm{TID}^{ia}||K)$. It stores $\{\mathrm{TID}_{ia}, D_{ia}\}$ in its database and sends $\{\mathrm{TID}_{ia}, \mathrm{Reg}_{ia}, A_{ia}, C_{ia}, h(\cdot)\}$ towards user U_{ia} over a secure channel, where the user can also store all these parameters in its memory, while, for a patient's registration, he/she first provides his/her name to the registration center (RC). RC assigns the requisite sensor and sends it to the

Table 2: Notations and its descriptions.

Symbol	Description
U_{ia}	Medical professional
SN_{ja}	Sensor node
ID_{ia}	User's identity
K	Gateway secret key
R_1, R_2, R_3	Random numbers
$\|\|$	Concatenation function
GW	Gateway node
PW_{ia}	User's password
ID_{SNj}	Sensor nodes identity
TID_{ia}	Temporary-identity generated by GW for U_{ia}
$h(\cdot)$	Collision-free hash-operation
$\oplus$	Bitwise XOR operation

medical professional for future monitoring, prescription or diagnosis.

3.3. Login and Authentication Phase. The login and authentication phase of [5] has been completed in the following steps:

(i) In this phase of the protocol, the user U_{ia} provides identity ID_{ia} and password PW_{ia} using hand-held device (Smart Phone) and computes $\mathrm{HPW}^*{}_{\mathrm{ia}} = h(\mathrm{ID}_{ia} \oplus \mathrm{PW}_{ia})$, $R^*{}_{ia} = A_{ia} \oplus \mathrm{HPW}_{ia}$, $\mathrm{Reg}^*{}_{\mathrm{ia}} = h(\mathrm{ID}_{\mathrm{ia}} \| R^*{}_{ia} \| \mathrm{HPW}^*{}_{ia})$ and confirms $\mathrm{Reg}^*{}_{\mathrm{ia}} ?= \mathrm{Reg}_{ia}$; if a match occurs, further computation is performed; else, termination message is displayed. It generates an arbitrary number R_1 and computes $B^*{}_{ia} = C_{ia} \oplus h(\mathrm{ID}_{ia} \oplus R^*{}_{ia} || \mathrm{HPW}_{ia})$, $\mathrm{CID}_{ia} = \mathrm{ID}_{ia} \oplus h(\mathrm{TID}_{ia} || R^*{}_{ia} || T_1)$, $M_1 = h(\mathrm{ID}_{ia} || B^*{}_{ia} || R_1 || T_1)$, $M_2 = h(R_{ia} || T_1) \oplus R_1$ and relays $\{\mathrm{TID}_{ia}, \mathrm{ID}_{SNj}, \mathrm{CID}_{ia}, M_1, M_2, T_1\}$ towards gateway node (GW) via a public network channel.

(ii) The gateway node finds TID_{ia} in its storage table, extracts D_{ia}, and computes $R^*{}_{ia} = D_{ia} \oplus h(\mathrm{TID}_{ia} || K)$, $\mathrm{ID}^*{}_{\mathrm{ia}} = \mathrm{CID}_{ia} \oplus h(\mathrm{TID}_{ia} || R^*{}_{ia} || T_1)$, $B^*{}_{ia} = h(\mathrm{ID}^*{}_{\mathrm{ia}} || R^*{}_{ia} || K)$, $R^*{}_1 = M_2 \oplus h(R^*{}_{ia} || T_1)$, and $M^*{}_1 = h(\mathrm{ID}^*{}_{\mathrm{ia}} || B^*{}_{ia} || R^*{}_1 || T_1)$ and confirms $M^*{}_1 ?= M_1$; if not matched, authentication is denied; else, gateway node generates another arbitrary number R_2 and computes $\mathrm{SK}_{\mathrm{GW-SN}ja} = h(\mathrm{IDS}_{Nja} || K)$, $M_3 = h(h(h(\mathrm{ID}_{ia} || R^*{}_1 || R_2)) || \mathrm{S}_{K\mathrm{GW-SN}ja} || R_2)$, $M_4 = h(\mathrm{ID}_{ia} || R_1 || R_2) \oplus \mathrm{SK}_{\mathrm{GW-SN}ja}$, $M_5 = R_2 \oplus h(\mathrm{SK}_{\mathrm{GW-SN}ja})$ and relays $\{M_3, M_4, M_5\}$ message towards senor node (SN_j) via a public network channel.

(iii) The SN_j computes $R'_2 = M_5 \oplus h(\mathrm{SK}_{\mathrm{GW-SN}ja})$, $M'_6 = M_4 \oplus \mathrm{SK}_{\mathrm{GW-SN}ja}$, $M'_3 = h(h(M'_6 || 1) || \mathrm{SK}_{\mathrm{GW-SN}ja} || R'_2)$ and confirms $M'_3 ?= M_3$; if matched, sensor node produces a third arbitrary number R_3, calculates $\mathrm{SK} = h(M'_6 || R_2 || R_3)$, $M_7 = h(\mathrm{SK} || R_3 || \mathrm{SK}_{\mathrm{GW-SN}ja})$, $M_8 = h(R_2) \oplus R_3$, and sends $\{M_7, M_8\}$ message towards GW via the same public network channel.

(iv) The GW computes $R'_3 = M_8 \oplus h(R_2)$, $\mathrm{SK}' = h(h(\mathrm{ID}_{ia} || R_1 || R_2) || R_2 || R'_3)$, $M'_7 = h(\mathrm{SK}' || R'_3 || \mathrm{SK}_{\mathrm{GW-SN}ja})$ and confirms $M'_7 ?= M_7$; if matched, it produces a temporary identity TID'_{ia}, calculates $M_9 = R_2 \oplus h(\mathrm{ID}_{ia} || R_1)$, $M_{10} = h(\mathrm{ID}_{ia} || \mathrm{SK}' || R'_3)$, $M_{11} = \mathrm{TID}'_{ia} \oplus h(R_2 \oplus R_3)$, and transmits $\{M_8, M_9, M_{10}, M_{11}\}$ message towards user over the same insecure channel.

(v) The user calculates $R'_2 = M_9 \oplus h(\mathrm{ID}_{ia} || R_1)$, $R^*{}_3 = M_8 \oplus h(R^*{}_2)$, $\mathrm{TID}'_{ia} = M_{11} \oplus h(R^*{}_2 \oplus R^*{}_3)$, $\mathrm{SK}^* = h(h(\mathrm{ID}_{ia} || R_1\mathrm{s}$ $M'_{10} = h(\mathrm{ID}_{ia} || \mathrm{SK}^* || R^*{}_3)$ and confirms $M'_{10} ?= M_{10}$; if matched, it relays a confirmation acknowledgement message towards GW and modifies TID_{ia} to TID'_{ia}, while the gateway node calculates the fresh value $D'_{ia} = R_{ia} \oplus h(\mathrm{TID}'_{ia} || K)$ and interchanges $\{\mathrm{TID}_{ia}, \mathrm{D}_{ia}\}$ with the new calculates values $\{\mathrm{TID}'_{ia}, D'_{ia}\}$.

3.4. Password Change Phase. If a legitimate user wishes to change his/her password, the protocol provides password change facility in a secure way. The user provides his/her ID_{ia}, and PW_{ia} the computations performed are $\mathrm{HPW}_{ia} = h(\mathrm{ID}_{ia} \oplus \mathrm{PW}_{ia})$, $R^*{}_{ia} = \mathrm{A}_{ia} \oplus \mathrm{HPW}_{ia}$, $\mathrm{Reg}^*{}_{ia} = h(\mathrm{ID}_{ia} || R^*{}_{ia} || \mathrm{HPW}^*{}_{ia})$ and confirm $\mathrm{Reg}^*{}_{ia} ?= \mathrm{Reg}_{ia}$; if not matched, a denied message is displayed on the user's screen; else, the user is asked to enter a new password. Upon receiving the password change message, the user is now able to enter a fresh password $\mathrm{PW}^{\mathrm{new}}{}_{ia}$ of his/her own choice and computes $\mathrm{HPW}^{\mathrm{new}}{}_{ia} = h(\mathrm{ID}_{ia} \oplus \mathrm{PW}^{\mathrm{new}}{}_{ia})$, $\mathrm{Reg}^{\mathrm{new}}{}_{ia} = h(\mathrm{ID}_{ia} || R^*{}_{ia} || \mathrm{HPW}^{\mathrm{new}}{}_{ia})$, $A^{\mathrm{new}}{}_{ia} = R^*{}_{ia} \oplus \mathrm{HPW}^{\mathrm{new}}{}_{ia}$, $B_{ia} = h(\mathrm{ID}_{ia} || R_{ia} || \mathrm{K})$, $C^{\mathrm{new}}{}_{ia} = B_{ia} \oplus h(\mathrm{ID}_{ia} \oplus R^*{}_{ia} \oplus \mathrm{HPW}^{\mathrm{new}}{}_{ia})$ and replace $\{\mathrm{Reg}_{ia}, A_{ia}, C_{ia}\}$ with$\{\mathrm{Reg}^{\mathrm{new}}{}_{ia}, A^{\mathrm{new}}{}_{ia}, C^{\mathrm{new}}{}_{ia}\}$.

3.5. Cryptanalysis of Scheme [5]. By applying the Dolev and Yao [6] model, we find the following weaknesses in Amin et al. protocol:

(1) Masquerade Attack

An attacker can quickly identify the secret credentials from $\mathrm{CID}_{ia} = \mathrm{ID}_{ia} \oplus h(\mathrm{TID}_{ia} || R^*{}_{ia} || \mathrm{T}_1)$ and $M_2 = h(R_{ia} || T_1) R_1$. The adversary first recovers ID_{ia} from CID_{ia}, and then R_1 from M_2. These two are crucial parameters, and once an attacker gets access to these, he/she can masquerade the system.

(2) Privileged Insider Attack

Let a user U_{ia} transmit identity ID_{ia} and password PW_{ia} towards gateway-node (GW). The system operator, in which he/they can use the system, can quickly identify user credentials by either guessing password or computing $\mathrm{HPW}_{ia}{}^* = h(\mathrm{ID}_{ia} \oplus \mathrm{PW}_{ia})$ and run tuples to correct the password.

(3) Man-In-The-Middle Attack

In such a scheme, authors do not share the synchronized resource's detail. For example, after a successful login of the medical professional to monitor his/her patient, such scheme missed the secure log out procedure of him/her. According to the given scenario, the mutual authentication and cross-verification key are still stored in the synchronous storage. An attacker can easily copy and launch a man-in-the-middle attack, desynchronizing the shared resources, and can hang the system proper operations.

(4) Password Change Phase Issue

An attacker can easily initiate a new password request by using the power analysis technique. He/she first reaches TID_{ia}, Reg_{ia}, $h(\cdot)$, A_{ia} and C_{ia} and calculates $A_{ia} \oplus \mathrm{HPW}_{ia}$ and $h(\mathrm{ID}_{ia}||R^*{}_{ia}||\mathrm{HPW}^*{}_{ia})$ by confirming $\mathrm{Reg}^*{}_{ia}? = \mathrm{Reg}_{ia}$; if matched, he/she can get the message "Enter your new password," which is, in turn, harmful for the system.

(5) Anonymity Violation

According to such scheme of [5], the messages are transmitted over insecure channels like $\{\mathrm{TID}_{ia}, \mathrm{ID}_{\mathrm{SN}ja}, \mathrm{CID}_{ia}, M_1, M_2, T_1\}$, $\{M_3, M_4, M_5\}$, $\{M_7, M_8\}$, and $\{M_8, M_9, M_{10}, M_{11}\}$ and in such way, an attacker can easily detect the medical professional due to the match of extracted values/random number from M_2, M_5 and M_8, i.e., R_1, R_2, and R_3. These random numbers can be quickly figured out by an adversary, for whom he/she can easily trace the paramedical professional's location. Also, the attacker can disturb privacy and can quickly launch a traceability attack. Therefore, the scheme suffered from traceability attacks and could not withstand the privacy and legitimacy of a user, either patient or paramedical professional. Also, in the Identity, ID_{ia} and $\mathrm{ID}_{\mathrm{SN}j}$ are transmitted openly, in which an attacker can easily pick and launch an attack some other time.

(6) Traceability Attack

According to the scheme, the messages $\mathrm{CID}_{ia} = \mathrm{ID}_{ia} \oplus h(\mathrm{TID}_{ia}||R^*{}_{ia}||T_1)$, $M_2 = h(R_{ia}||T_1) \oplus R_1$, $M_4 = h(\mathrm{ID}_{ia}||R_1||R_2) \oplus \mathrm{SK}_{\mathrm{GW-SN}ja}$, $M_5 = R_2 \oplus h(\mathrm{SK}_{\mathrm{GW-SN}ja})$, and $M_8 = h(R_2) \oplus R_3$ are transmitted over a public network channel openly, in which an adversary can catch and figure out credentials by specifying location by repeatedly monitoring different sessions started by the same user. To prevent the adversary from figuring out any identity or tracing any credentials like the exact location of a legitimate user, it must be transmitted securely or linked with a vigorous session shared key (SK).

(7) Mutual Authentication Issue

The gateway node computes the session key as $\mathrm{SK}_{\mathrm{GW-SN}ja} = h(\mathrm{IDS}_{Nja}||K)$, and the sensor node $\mathrm{SK} = h(M'{}_6||R_2||R_3)$. In the second round, the gateway node computes the shared session as $\mathrm{SK}' = h(h(\mathrm{ID}_{ia}||R_1||R_2)||R^*{}_2||R'{}_3)$ and user $\mathrm{SK}^* = h(h(\mathrm{ID}_{ia}||R_1||R^*{}_2)||R_2||R^*{}_3)$, which means that the key between the user and gateway node is computed. Still, the sensor embedded in the patient does not know about the shared session key. Therefore, the scheme is failed to deliver mutual authentication and cross-verification with/of all the participants.

(8) Lack of Revocation/Reissue Phases

Besides the drawbacks mentioned above, [5] did not explain the expansion/recede of the network by the addition/revocation of a new patient/professional. The scheme has missed explaining sensor/patient revocation/reissue or professional revocation/reassignment phases.

4. Proposed Solution

We will use critical public infrastructure to generate dynamic numbers for each session for such a resource deficit environment. The scheme consists of the setup phase, registration phase, key-agreement phase, password change phase, and revocation/reissue phase; each of these is discussed one by one under the following headings:

4.1. Setup Phase. Extract a prime P, the CA first generates two random numbers x, y of size 160 bits, compute a secret key $s = \mathrm{xP}$, and $l = \mathrm{sP}$ called a public key, collision-free hash function $H(\cdot):\{0, 1\}^* \longrightarrow \{0, 1\}^1$. Keep $(\mathrm{ID}_{\mathrm{SN}j}||s)$ in sensor node, s, and l in gateway-node, which is the key role in the whole system.

4.2. Registration Phase. This phase consists of two subphases, including patients' and medical professionals' registration subphases, which are described as follows:

(1) Patient's Registration

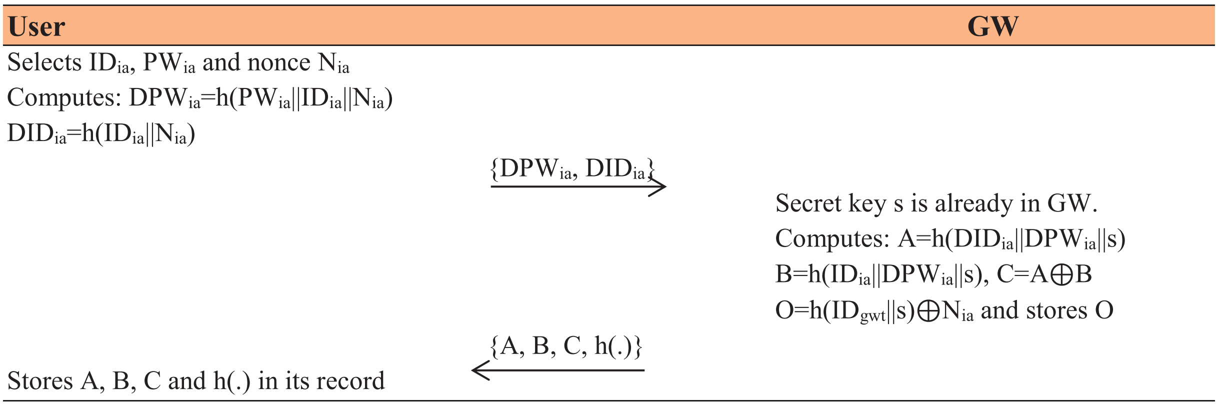
A patient first sends his/her name to the CA. CA allocates the requisite accurately and offers/entitles the services to medical professionals. CA also shares a patient's Identity and assigned sensor information to a medical professional.

(2) Professional Registration Phase

The user selects identity ID_{ia}, password PW_{ia}, nonce N_{ia} and computes $\mathrm{DPW}_{ia} = h(\mathrm{PW}_{ia}||N_{ia}||\mathrm{ID}_{ia})$, $\mathrm{DID}_{ia} = h(\mathrm{ID}_{ia}||N_{ia})$ and transmits $\{\mathrm{DPW}_{ia}, \mathrm{DID}_{ia}\}$ to gateway node over a secure channel. The gateway node has already a secret key s and computes $A = h(\mathrm{ID}_{ia}||\mathrm{DID}_{ia}||s)$, $B = h(\mathrm{ID}_{ia}||\mathrm{DPW}_{ia}||s)$, $C = A \oplus B$ and $O{=}C \oplus h(\mathrm{ID}_{gwt}||s)$. The gateway-node (GW) stores O and sends $\{A, B, C, h(\cdot)\}$ towards user over a secure channel and stores all these parameters in its own record too as shown in Figure 3.

4.3. Key Agreement Phase. This phase of the proposed protocol is accomplished in the following steps:

(i) A user provides his/her identity, and password computations performed are $\mathrm{HPW}^* = h(\mathrm{ID}_{ia} \oplus \mathrm{PW}_{ia})$, $A^* = h(\mathrm{ID}_{ia}||s||\mathrm{HPW})$, confirms $A^*? = A$; if not found valid, computation stops; else, it generates R_1, s^* and computes $B^* = C \oplus h(\mathrm{ID}_{ia} \oplus A^*||\mathrm{HPW}^*)$, $F = B^* \oplus h(s^*||A^*||T_1)$, $J_1 = h(\mathrm{ID}_{ia}||B^*||R_1||T_1)$, $J_2 = \mathrm{ID}_{ia} \oplus h(s||T_1)$ and $L_1 = E_l(J_2||R_1||s^*)$.



Selects ID_{ia}, PW_{ia} and nonce N_{ia}
Computes: $DPW_{ia}=h(PW_{ia}||ID_{ia}||N_{ia})$
$DID_{ia}=h(ID_{ia}||N_{ia})$

$\{DPW_{ia}, DID_{ia}\}$

Secret key s is already in GW.
Computes: $A=h(DID_{ia}||DPW_{ia}||s)$
$B=h(ID_{ia}||DPW_{ia}||s)$, $C=A\oplus B$
$O=h(ID_{gwt}||s)\oplus N_{ia}$ and stores O

$\{A, B, C, h(.)\}$

Stores A, B, C and h(.) in its record

Figure 3: Medical professional registration phase

Finally, it relays $\{ID_{SN}, F, L_1, T_1\}$ towards gateway node (GW) over public channel.

(ii) Verifies timestamp, T_1, decrypts L_1 using s to obtain ID_{ia}, R_1 and s^*. Next, it extracts O from the already stored record in gateway node (GW) and computes $O^* = k \oplus h(ID_{SN}||s)$ and confirms $O? = O^*$; if not matched, computation stops; else, it computes $ID^*_{ia} = F \oplus h(l||A^*||T_1)$, $B^* = h(ID^*_{ia}||A^*||l)$, $R^*_1 = J_2 \oplus h(A^*||T_1)$, $J_1^* = h(ID^*_{ia}||B^*||R^*_1||T_1)$ and again confirms $J_1^*? = J_1$; if not matched, the process terminated; else, it generates R_2 and computes $sk = h(ID_{SN}||l)$, $L_3 = h(h(h(ID_{ia}||R^*_1||R_2))||ID_{SN}||R_2)$, $L_4 = h(ID_{ia}||R_1||R_2) \oplus sk$, $L_5 = R_2 \oplus ID_{SNj}$ and $L_6 = E_l(ID_{SN}||R_1||R_2||L_5)$. In this step of the login and authentication phase, the gateway node forwards $\{L_3, L_4, L_5, L_6\}$ message towards sensor over a public network channel.

(iii) Upon receiving the $\{L_4, L_5, L_6\}$ message, the sensor node first decrypts L_6 using s to obtain ID_{SN}, R_1, R_2 and L_5 and computes $R^*_2 = L_5 \oplus sk$, $L_7 = L_4 \oplus sk$, $L_8 = h(h(L_7||ID_P)||sk||R^*_2)$, $L_3' = h(h(h(ID_{ia}||R^*_1||R^*_2))||ID_{SN}||R_2)$ and confirms $L_3'? = L_3$; if not matched, termination of the whole process takes place; else, it generates R_3 and computes $sk = h(h(ID_{ia}||R_1||R^*_2)||R_2||R_3)$, $L_9 = h(sk||R_3||R_1||R^*_2)$, and $L_{10} = ID_{ia}||R^*_2||R_2||R_3$ and sends $\{L_9, L_{10}\}$ to GW over public channel.

(iv) Further, GW computes and calculates $R'_3 = L_9||R_2$, $sk' = h(h(ID_{ia}||R_1||R^*_2)||R_2||R'_3)$, $L_9' = h(sk'||R'_3||R_1||R^*_2)$ and confirms $L_9'? = L_9$; if found not valid, the process becomes terminated; else, it produces 1^* and calculates $L_{11} = E_l(h(ID_{ia}||R_1) \oplus R_2)$, $L_{12} = h(ID_{ia}||sk'||R'_3)$, $L_{13} = E_k(ID_{SN}||1^*||L_{11})$ and transmits $\{L_{11}, L_{12}\}$ towards user over a public network channel.

(v) The user first decrypts L_{11} using s to obtain ID_{SNj}, R_3, L_{10} and calculates $R'_2 = L_{11} \oplus h(ID_{ia}||R_1)$, $R^*_3 = L_{10}||R^*_2$, $A' = L_{13}||h(R^*_2 \oplus R^*_3)$, $sk^* = h(h(ID_{ia}||R_1||R^*_2)||R_2||R^*_3)$, $L'_{11} = h(ID_{ia}||sk^*||R^*_3)$ and verifies $L'_{11}? = L_{11}$ and keeps sk, sk$'$and sk* session shared keys in each peer for secure message transmission among all the participants as shown in Figure 4, while general framework of the system is shown in Figure 5.

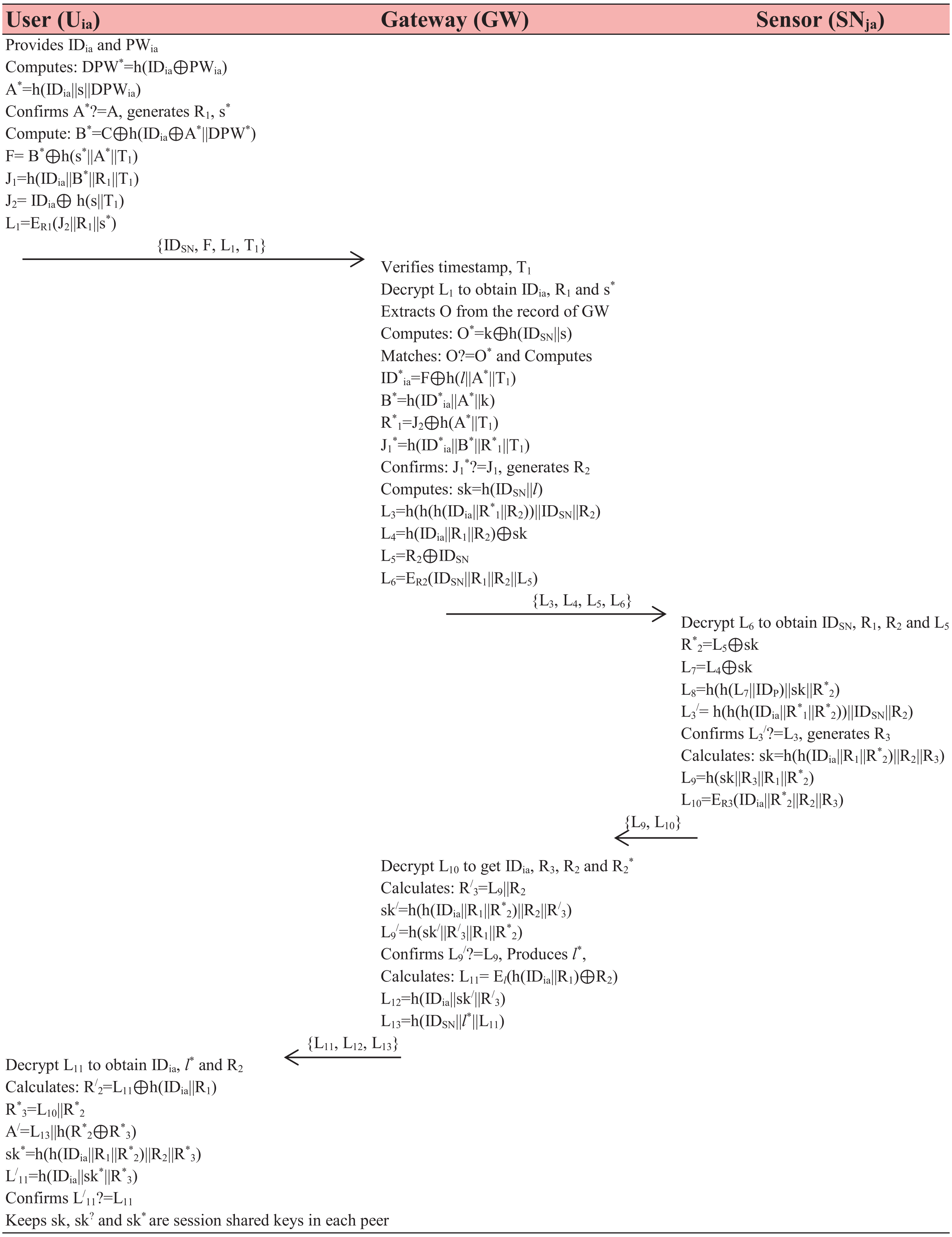
4.4. Revocation/Reissue Phase. This phase of the protocol is performed between the user's device and gateway node. The following steps are performed in this phase of the protocol.

(i) The user provides his/her previous identity ID_{ia}, password PW_{ia}, selects new identity ID_{ia}^{new} and computes $A_1 = h(ID_{ia}^{new}||R_1)$, $B_1 = O \oplus A_1$, $C_1 = ID_{ia} \oplus B_1$ and transmits $\{ID_{ia}, ID_{ia}^{new}, A_1, C_1\}$ towards the gateway node over a secure channel.

(ii) Upon receiving the $\{ID_{ia}, ID_{ia}^{new}, A_1, C_1\}$ message, the gateway node computes $B_1^* = h(s||l||A_1)$, $C_1^* = ID_{ia} \oplus B_1^*$, and confirms $C_1^*? = C_1$; if not hold, the process is terminated; else, it computes: $V_1 = h(ID_{ia}^{new}||A_1)$, $O_1 = B_1^* \oplus A_1$, $F_1 = E_l(A_1||s||l)$ and stores $\{V_1, O_1, F_1, h(\cdot)\}$ in its database and transmits it also to the medical device over a secure channel. In this regard, the sensor cancels/evokes/reissues that the process has been made successfully.

(iii) Further, if the medical professional desires to evoke/cancel/reenter, CA asks for entering the Identity ID_{ia}, and password PW_{ia} of the medical professional and computes: $W = h(ID_{ia} \oplus PW_{ia})$, $Y = h(ID_{ia}||s||W)$. CA confirms W and Y in its database; if not correct, the process is terminated; else, CA changes the status of a medical professional as inactive. CA also relays the revocation message to the patient to revoke the medical professional's credentials and transmits the changed status back to CA. Finally, CA also updates the gateway node to revoke the specified medical professional.

4.5. Password Change Phase. If a user desires to change his/her password, this protocol provides a password change facility to change the old one with a new one securely. The following steps are performed while changing the password:



User (U_{ia}) **Gateway (GW)** **Sensor (SN_{ja})**

Provides ID_{ia} and PW_{ia}
Computes: $DPW^{*}=h(ID_{ia}\oplus PW_{ia})$
$A^{*}=h(ID_{ia}\|s\|DPW_{ia})$
Confirms $A^{*}?=A$, generates R_1, s^{*}
Compute: $B^{*}=C\oplus h(ID_{ia}\oplus A^{*}\|DPW^{*})$
$F= B^{*}\oplus h(s^{*}\|A^{*}\|T_1)$
$J_1=h(ID_{ia}\|B^{*}\|R_1\|T_1)$
$J_2= ID_{ia}\oplus h(s\|T_1)$
$L_1=E_{R1}(J_2\|R_1\|s^{*})$

$\{ID_{SN}, F, L_1, T_1\}$ →

Verifies timestamp, T_1
Decrypt L_1 to obtain ID_{ia}, R_1 and s^{*}
Extracts O from the record of GW
Computes: $O^{*}=k\oplus h(ID_{SN}\|s)$
Matches: $O?=O^{*}$ and Computes
$ID^{*}_{ia}=F\oplus h(l\|A^{*}\|T_1)$
$B^{*}=h(ID^{*}_{ia}\|A^{*}\|k)$
$R^{*}_{1}=J_2\oplus h(A^{*}\|T_1)$
$J_1^{*}=h(ID^{*}_{ia}\|B^{*}\|R^{*}_{1}\|T_1)$
Confirms: $J_1^{*}?=J_1$, generates R_2
Computes: $sk=h(ID_{SN}\|l)$
$L_3=h(h(h(ID_{ia}\|R^{*}_{1}\|R_2))\|ID_{SN}\|R_2)$
$L_4=h(ID_{ia}\|R_1\|R_2)\oplus sk$
$L_5=R_2\oplus ID_{SN}$
$L_6=E_{R2}(ID_{SN}\|R_1\|R_2\|L_5)$

$\{L_3, L_4, L_5, L_6\}$ →

Decrypt L_6 to obtain ID_{SN}, R_1, R_2 and L_5
$R^{*}_{2}=L_5\oplus sk$
$L_7=L_4\oplus sk$
$L_8=h(h(L_7\|ID_P)\|sk\|R^{*}_{2})$
$L_3^{/}= h(h(h(ID_{ia}\|R^{*}_{1}\|R^{*}_{2}))\|ID_{SN}\|R_2)$
Confirms $L_3^{/}?=L_3$, generates R_3
Calculates: $sk=h(h(ID_{ia}\|R_1\|R^{*}_{2})\|R_2\|R_3)$
$L_9=h(sk\|R_3\|R_1\|R^{*}_{2})$
$L_{10}=E_{R3}(ID_{ia}\|R^{*}_{2}\|R_2\|R_3)$

← $\{L_9, L_{10}\}$

Decrypt L_{10} to get ID_{ia}, R_3, R_2 and R_2^{*}
Calculates: $R^{/}_{3}=L_9\|R_2$
$sk^{/}=h(h(ID_{ia}\|R_1\|R^{*}_{2})\|R_2\|R^{/}_{3})$
$L_9^{/}=h(sk^{/}\|R^{/}_{3}\|R_1\|R^{*}_{2})$
Confirms $L_9^{/}?=L_9$, Produces l^{*},
Calculates: $L_{11}= E_l(h(ID_{ia}\|R_1)\oplus R_2)$
$L_{12}=h(ID_{ia}\|sk^{/}\|R^{/}_{3})$
$L_{13}=h(ID_{SN}\|l^{*}\|L_{11})$

← $\{L_{11}, L_{12}, L_{13}\}$

Decrypt L_{11} to obtain ID_{ia}, l^{*} and R_2
Calculates: $R^{/}_{2}=L_{11}\oplus h(ID_{ia}\|R_1)$
$R^{*}_{3}=L_{10}\|R^{*}_{2}$
$A^{/}=L_{13}\|h(R^{*}_{2}\oplus R^{*}_{3})$
$sk^{*}=h(h(ID_{ia}\|R_1\|R^{*}_{2})\|R_2\|R^{*}_{3})$
$L^{/}_{11}=h(ID_{ia}\|sk^{*}\|R^{*}_{3})$
Confirms $L^{/}_{11}?=L_{11}$
Keeps sk, $sk^{?}$ and sk^{*} are session shared keys in each peer

FIGURE 4: Key agreement phase

(i) The user provides his/her Identity ID_{ia}, and old password PW_{ia} via its mobile device. The computations performed are $\text{DPW}_{ia}=h(\text{ID}_{ia}\oplus\text{PW}_{ia})$, $A=h(\text{DID}_{ia}\|s^{*}\|\text{DPW}_{ia}{}^{*})$, and confirm $A^{*}?=A$; if not matched, a denying message will display on the user's screen; else, it computes $h(\text{ID}_{gwt}\|s)\oplus N_{ia}$ and $O?=O^{*}$ and user is asked to enter the new password.

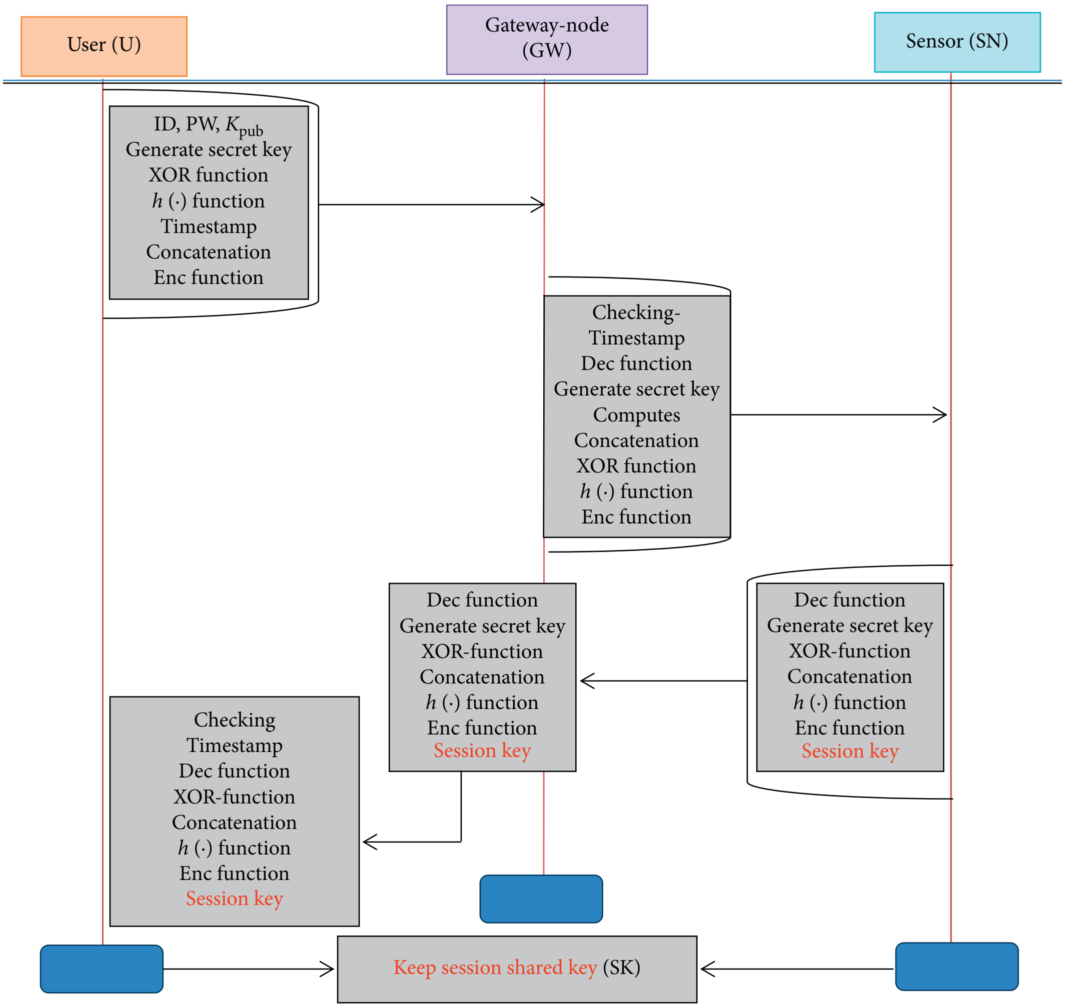


FIGURE 5: General framework.

(ii) Upon receiving the password change message, the medical professional is now able to enter a fresh password $PW^{new}{}_{ia}$ of his/her own choice, and computes: $DPW^{new} = h(ID_{ia} \oplus PW^{new}{}_{ia})$, $A^{new} = h(ID_{ia}||s^*||DPW^{new})$, $O^{new} = A^* \oplus DPW^{new}$, $B^{new} = h(ID_{ia}||s||l)$, $C^{new} = B^{new} \oplus h(ID_{ia} \oplus A^* \oplus DPW^{new})$ and replaces $\{A, O, C\}$ with$\{A^{new}, O^{new}, C^{new}\}$.Therefore, the medical professional can easily change his/her password without interacting with the gateway node and the senor, as shown in Figure 6.

5. Security Analysis

In this section, the security analysis of the proposed scheme can be performed both formally and informally. The formal security proof will be performed using a BAN logic and ProVerif2.02 and informal operating assumptions. These are discussed as follows:

5.1. BAN Logic Proof. The shared session key sk has been computed among the user, gateway node, and sensor node for future communication. This subsection is a result of This subsection is added in order to prove the scheme's robustness using BAN [27]. BAN is a logic of belief, and trust was first introduced by Mike Burrows, Martin Abadi, and Roger Needham called BAN. The BAN's reasoning covers the following major issues:

(a) Are participants familiar with one another?

(b) Do they know if the message is fresh?

(c) Is it possible to be confident that a third party did not simply insert incorrect information into the original message?

Different rules and their description for the proposed protocol are shown as follows:

(1) Message Meaning

According to this rule, embedded sensor (user) and gateway node communication are carried out on a secure secret session key. Suppose the user believes that the broadcasting between sensor and gateway-node is carried out on session private key SK. Both participants see the message M encrypted on key K. In that case, the user also believes in the freshness of

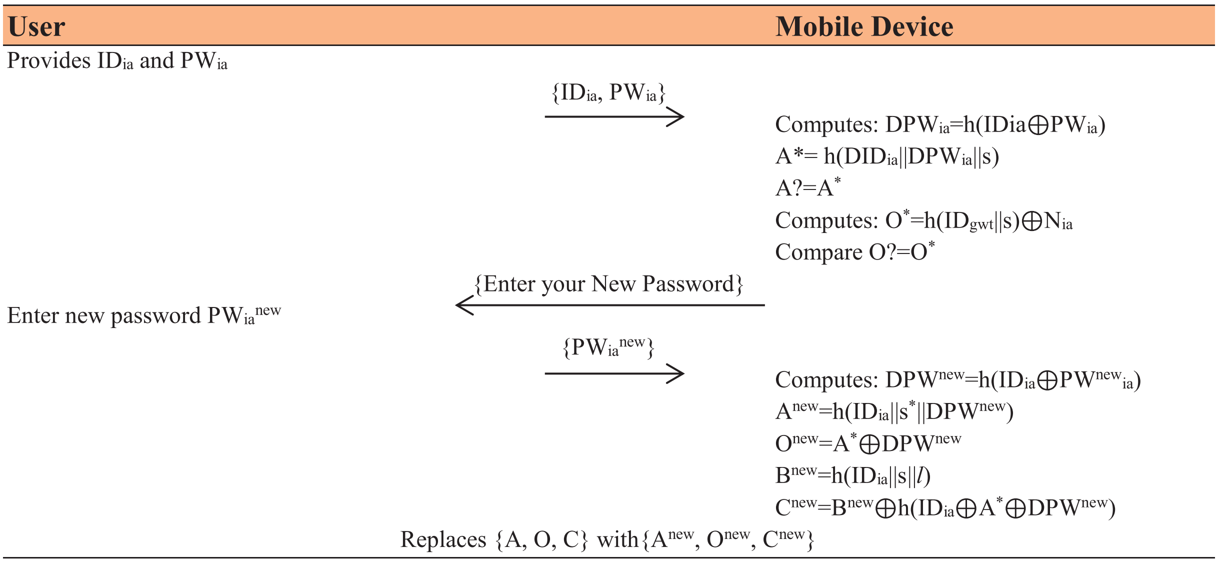

User
Mobile Device
Provides IDia and PWia
{IDia, PWia}
Computes: DPWia=h(IDia⊕PWia)
A*= h(DIDia||DPWia||s)
A?=A*
Computes: O*=h(IDgwt||s)⊕Nia
Compare O?=O*
{Enter your New Password}
Enter new password PWia new
{PWia new}
Computes: DPWnew=h(IDia⊕PWnew ia)
Anew=h(IDia||s*||DPWnew)
Onew=A*⊕DPWnew
Bnew=h(IDia||s||l)
Cnew=Bnew⊕h(IDia⊕A*⊕DPWnew)
Replaces {A, O, C} with{Anew, Onew, Cnew}

Figure 6: Password change phase

message M exchanged between user and gateway-node.

$$\frac{U_{ia}|\equiv U_{ia}\overset{SK}{\leftrightarrow}GW,\ \triangleleft\{M\}_K}{U_{ia}|\equiv GW|\sim M},$$
$$\frac{GW|\equiv\ GW\overset{SK}{\leftrightarrow}SN,\ \triangleleft\{M\}_K}{GW|\equiv\ SN|\sim\ M}. \tag{1}$$

Similar is the case in gateway node (GW); accordingly, if the gateway node believes that the information exchange among GW and SN is performed through a session shared secret key SK, and both participants see the encrypted message M via key K; then GW believes SN once said message M.

(2) Message Integrity

This rule means that if the user believes that the data transmission over session shared key SK towards gateway node (GW), the message M decrypted with key K, then the user also believes sensor node once said message M.

$$\frac{U_{ia}|\equiv\ \overline{\longrightarrow^{SK}}GW, \triangleleft\{M\}_{K^{-1}}}{U_{ia}|\equiv\ GW|\sim M}, \frac{U_{ia}|\equiv\ U_{ia}\overset{SK}{\Rightarrow}GW \triangleleft\{M\}_Y}{U_{ia}|\ \equiv GW|\sim M}. \tag{2}$$

Similarly, suppose a user believes the user that the data transmission over session shared key SK towards gateway node (GW) sees the encrypted message M via key K. In that case, the user also believes the gateway node (GW) once said message M.

(3) Seeing Message

If GW believes the data transmission towards SN over SK and sees message M via key K, then GW also believes SN once said message M.

$$\frac{GW|\equiv\ \overline{\longrightarrow^{SK}}SN, \triangleleft\{M\}_{K^{-1}}}{GW\equiv\ SN|\sim\ M}, \frac{GW|\equiv\ GW\overset{SK}{\Rightarrow}SN \triangleleft\{M\}_Y}{GW\equiv\ SN|\sim\ M}. \tag{3}$$

Similarly, suppose GW believes data transmission towards Sn through session shared key SK and sees message M encrypted over key K, then GW believes SN once said message M.

(4) Message Authorization

User believes data broadcasting towards Sn over SK and sees the decrypted message M through key Y, then user also believes GW once said message M.

$$\frac{U_{ia}|\equiv\ \overset{SK}{\Rightarrow}GW \triangleleft\{M\}_{Y^{-1}}}{U_{ia}|\equiv\ GW|\sim\ M},$$
$$\frac{GW|\equiv\ \overset{SK}{\Rightarrow}SN \triangleleft\{M\}_{Y^{-1}}}{GW|\equiv SN|\sim\ M}. \tag{4}$$

Similarly, if GW believes data broadcasting towards SN over Sk and sees the decrypted message M via key Y, then GW also believes SN once said message M.

(5) Message Freshness

Suppose the user believes that the message received is fresh and GW once said message M, then both user and GW believe that the received message M is also fresh.

$$\frac{U_{ia}|\equiv\ \neq(M), GW|\sim M}{U_{ia}|\equiv\ GW|\equiv\ \neq M},$$
$$\frac{GW|\equiv\ \neq(M),\ SN|\sim M}{GW|\equiv\ SN|\equiv\ \neq M}. \tag{5}$$

Similarly, GW believes that M's received message is fresh; SN once said message M then both GW and SN also believe that the received message M is fresh.

(6) Message Belief

Suppose both user and GW believe jurisdiction and encryption over key K, then GW believes encryption on message by key K.

$$\frac{U_{ia}|\equiv \mathrm{GW}|\Rightarrow(M), U_{ia}|\equiv \mathrm{GW}|\equiv\{M\}_K}{GW|\equiv\{M\}_K},\qquad \frac{U_{ia}|\equiv \mathrm{SN}|\Rightarrow(M), U_{ia}|\equiv \mathrm{SN}|\equiv\{M\}_K}{\mathrm{SN}|\equiv\{M\}_K}. \tag{6}$$

Similarly, if both user and SN believe message jurisdiction and message encryption on key K, then SN believes encrypted message M through key K.

(7) Message Hiding

Suppose user and GW jurisdiction over message M, and decrypted message M via key K, then GW believes the decrypted message M via key K.

$$\frac{U_{ia}|\equiv \mathrm{GW}|\Rightarrow(M), U_{ia}|\equiv \mathrm{GW}|\equiv\{M\}_{K^{-1}}}{\mathrm{GW}|\equiv\{M\}_{K^{-1}}},\qquad \frac{U_{ia}|\equiv \mathrm{SN}|\Rightarrow(M), U_{ia}|\equiv \mathrm{SN}|\equiv\{M\}_{K^{-1}}}{\mathrm{SN}|\equiv\{M\}_{K^{-1}}}. \tag{7}$$

Similarly, if a user and SN jurisdiction over message M, and decrypted message M via key K, then SN believes the decrypted message M via key K.

Remark: $|\equiv$ *Believes,*SK $\overset{\text{sk}}{\leftrightarrow}$ *Communication through session key,* $\lhd$ *sees,* $\Rightarrow$ *Jurisdiction,* ~ *once said, # freshness,* <*M*>$_K$ *encryption using K,* <*M*>$_{K-1}$ *Description via K and P/Q, if P then Q.*

Now, we are using these rules, equations, and definitions for realizing the secure communication between all the participants of the system. These steps are as follows.

Security goals defined for the proposed protocols are as follows:

Goal1: $U_{ia}|\equiv \mathrm{GW} \overset{\text{sk}}{\leftrightarrow} U_{ia}$

Goal2: $U_{ia}|\equiv \mathrm{GW}|\equiv \mathrm{SN} \overset{\text{sk}}{\leftrightarrow} U_{ia}$

Goal3: $\mathrm{GW}|\equiv \mathrm{SN} \overset{\text{sk}}{\leftrightarrow} U_{ia}$

Goal4: $\mathrm{SN}|\equiv U_{ia}|\equiv \mathrm{GW} \overset{\text{sk}}{\leftrightarrow} U_{ia}$

The idealization form of the communication message of the protocol is given as follows:

Msg_1: $U_{ia} \longrightarrow$ GW: $\{\mathrm{ID}_{\mathrm{SN}}, F, L_1, T_1\}_l$

Msg_2: GW $\longrightarrow$ SN: $\{L_3, L_4, L_6\}_l$

Msg_3: SN $\longrightarrow$ GW: $\{L_9, L_{10}\}_l$

Msg_4: GW $\longrightarrow U_{ia}$: $\{L_{11}, L_{12}, L_{13}\}_l$

Assumptions stated for the proposed authentication protocol is as follows:

Asmpt_1: $U_{ia}|\equiv \#\ (R_1)$

Asmpt_2: $\mathrm{GN}|\equiv \#\ (R_1, R_2)$

Asmpt_3: $\mathrm{SN}|\equiv \mathrm{GN} \overset{k}{\leftrightarrow} U_{ia}$

Asmpt_4: $\mathrm{GN}|\equiv \mathrm{SN} \overset{k}{\leftrightarrow} U_{ia}$

Asmpt_5: $U_{ia}|\equiv \mathrm{SN} \overset{\mathrm{sk}=h(L_7\|R_2\|R_3)}{\leftrightarrow} \mathrm{GN}$

Asmpt_6: $\mathrm{SN}|\equiv \mathrm{GW} \overset{\mathrm{SK}=h(h(ID_{ia}\|R_1\|R_2)\|R_2\|R_3)}{\leftrightarrow} U_{ia}$

Asmpt_7: $U_{ia}|\equiv \mathrm{GW} \Rightarrow (s\oplus R_1)$

Asmpt_8: $\mathrm{GW}|\equiv \mathrm{SN} \Rightarrow (R_2||l)$

Asmpt_9: $\mathrm{SN}|\equiv \mathrm{GW} \Rightarrow (R_2\oplus R_3)$

Asmpt_8: $\mathrm{GW}|\equiv U_{ia} \Rightarrow (R_3||l^*)$

Take Msg_1: $U_{ia} \longrightarrow$ GW: $\{\mathrm{ID}_{\mathrm{SN}}, F, L_1, T_1\}_l$ and Msg_2: GW $\longrightarrow$ SN: $\{L_3, L_4, L_6\}_l$

Sees rules for the proposed authentication protocol are defined as follows:

S_1: $\mathrm{GW}\lhd\ \{\mathrm{ID}_{\mathrm{SN}}, F, L_1, T_1\}_l$ and $\mathrm{SN}\lhd\{L_3, L_4, L_6\}_l$

As per Asmpt_1, and Asmpt_3 it is stated that:

S_2: $\mathrm{GW}|\equiv U_{ia}\sim\ \{\mathrm{ID}_{\mathrm{SN}}, F, L_1, T_1\}_l$

As per Asmpt_1, S_2, s, and L_1

S_3: $\mathrm{GW}|\equiv\mathrm{SN}|\equiv\ \{L_9, L_{10}\}_l$

As per Asmpt_7, S_3, and Jurisdictional rules

S_4: $\mathrm{GW}|\equiv\ \{L_9, L_{10}\}_l$

As per Asmpt_5, S_4, and *sk*

S_5: $U_{ia}\ |\equiv \mathrm{GW}|\equiv \mathrm{SN} \overset{\text{sk}}{\leftrightarrow} U_{ia}$ $\mathbf{G_1}$ Realized

According to Asmpt_7, S_5, and R_3

S_6: $U_{ia}\ |\equiv \mathrm{GW}|\equiv \mathrm{SN} \overset{\text{sk}}{\leftrightarrow} U_{ia}$ $\mathbf{G_2}$ Realized

Msg_3: SN $\longrightarrow$ GW: $\{L_9, L_{10}\}_l$, GW $\longrightarrow U_{ia}$: $\{L_{11}, L_{12}, L_{13}\}_l$ and take Msg_3 and Msg_4 as

Msg_3: SN $\longrightarrow$ GW: $\{L_9, L_{10}\}_l$ and Msg_4: GW $\longrightarrow U_{ia}$: $\{L_{11}, L_{12}, L_{13}\}_{l^*}$

Applying the seeing rules

S_7:$U_{ia}\lhd\mathrm{GW} \longrightarrow U_{ia}$: $\{L_9, L_{10}\}_{R_3}, L_{11}, L_{12}, L_{13}\}_l$, so as per S_7, Asmpt_4, and L_9

S_8: $U_{ia}|\equiv\mathrm{GW}\sim h(s||R_3||l)$, as per Asmpt_2, S_8, s, and L_{12}, gets

S_9: $\mathrm{SN}|\equiv U_{ia}|\equiv\ h(\mathrm{ID}_{ia}||\mathrm{sk}'||R'_3)$

As per Asmpt_6, S_9, and L_9, L_{10}

S_{10}: $U_{ia}|\equiv\{L_{11}, L_{12}, L_{13}\}$, as per Asmpt_4, S_{10}, and sk

S_{11}: $S|\equiv \mathrm{SN} \overset{\text{sk}}{\leftrightarrow} U_{ia}$ $\mathbf{G_3}$ Realized

As per Asmpt_8, S_{11}, and Jurisdictional rules

S_{12}: $\mathrm{SN}|\equiv\ U_{ia}|\equiv \mathrm{GW} \overset{\text{sk}}{\leftrightarrow} U_{ia}$ $\mathbf{G_4}$ Realized

It means that all the peers successfully authenticate each other and at any stage do not compromise on a session shared secret key (sk).

5.2. Proverif2.02 Simulation. In this subsection of the research paper, a widely used software verification toolkit is used to verify the scheme's confidentiality, authorization, authenticity, and reachability. The ProVerif2.02 simulation code is in appendix A of the paper.

5.3. Algorithmic Representation (a Formal Security Validation). It is to mention that the leading entities in the proposed authentication protocol are Certificate Authority (CA), Gateway Node (GW), Sensor Node (SN), and Medical Professional (User). Gateway node, sensor node, and a medical professional will first register with the certificate authority. The intelligent sensors embedded inside the patient's body can transmit data to the gateway node via a wireless medical sensor network. Finally, from the gateway node, with the help of WMSN, the data is transmitted toward medical professionals. The algorithmic overview/representation of the proposed authentication protocol is shown in Algorithm 1.

5.3.1. Privileged Insider Attack. A privileged user, either medical professional or any other administrator cannot extract any credentials for future usage, as each and everything are kept secret from all types of user.

5.3.2. Ensuring Anonymity. The session key is shared securely, and each computation round trip starts from a separate timestamp, in which the other peer verifies before starting of calculation. Similarly, after data transmission, all the credentials are successfully finished due to the log out facility, so no one traces a legitimate user. Therefore, the proposed protocol is ensuring anonymity and resists traceability drawbacks.

5.3.3. Denial-of-Service (DoS) Attack. As each session starts with a separate session key and time threshold, if an attacker, for example, desires to send false requests to any peer for a disturbance, he/she fails to do so, because Identity, password, and random keys are much secured, and peers respond only to authenticated credentials. Such requests are denied by peers and stopped for such unlawful activity. Therefore, the proposed protocol resists the DoS attack.

5.3.4. Sensor Attack. If two different sensors communicate simultaneously, it will not affect each other due to different identities. Also, the two sessions between the sensor and another user will not act.

5.3.5. Mutual Authentication. As each peer computes the session key sk and shares it for future communication, the proposed protocol has no mutual authentication.

5.3.6. Man-in-Middle Attack. The proposed protocol is modified by sensor revocation and patient revocation phases. These phases successfully log out the requisite user from the process; no credentials were left in either sensor or patient memory. This protocol never allows the evoking entity to start synchronization at any stage in the future. Therefore, the protocol resists the main-in-middle attack.

Finally, the researchers have the following recommendations:

(i) The proposed work can be tested for a deep learning approach for microarray cancer data classification [34]; graphology based handwritten character analysis for human behavior identification [35] and a deep neural network-based screening model for COVID-19-infected patients using chest X-ray images [36].

(ii) Also, the work done in this research can also be practiced/verified for the rapid COVID-19 diagnosis using ensemble deep transfer learning models from chest radiographic images [37], visibility improvement, and mass segmentation of mammogram images using quantile separated histogram equalization with local contrast enhancement [38–40].

6. Performance Evaluations

In this section of the paper, the proposed authentication scheme's performance analysis is performed by finding its storage overheads, computation, and communication. We analyze each of these features by considering the findings of previous experiment by [41, 42].

6.1. Attacks and Functionalities Comparison Analysis. Subsequently, it can be compared with some recent and prominent protocols like Kumari et al. [31], Rathore et al. [32], Wu et al. [33], and Amin et al. [5]. The result shows that our scheme is more robust than these schemes. It is worth mentioning that ✓ means that the mentioned attack is "Yes" for the said protocol; it cannot resist and cannot violate the mentioned features, whereas ✖ means that the mentioned security feature is "No" for the said protocol and cannot valid for the mentioned attack, security violation, loophole, etc., as shown in Table 3.

6.2. Storage-Overheads Analysis and Comparison. In the work done by [41, 42], identity occupies 64 bits of space, password 60 bits, timestamp 56 bits, secret key 60 bits, MD5 512 bits, encryption 192 bits, and decryption also 192 bits of memory space. Therefore, keeping in view these measures/calculations and computations, the storage overhead analysis of the proposed authentication protocol is shown in Table 4. Upon comparing it with Kumari et al. [31], Rathore et al. [32], Wu et al. [33], and Amin et al. [5], it proves different and fundamental security characteristics/objectives that are higher than those of the mentioned protocols. Graphically, the storage overhead analysis is shown in Figure 7.

Remark. Encryption = 192, decryption = 192 bits, identity = 64 bits, random numbers = 64 bits, MD5 = 512 bits, and public key = 64 bits, calculating for the proposed protocol $192 + 192 + 64(3) + 64(5) + 512 + 512 + 56(3) = 384 + 192 + 320 + 512 + 16\ 8 = 2088$

6.3. Computation Costs Analysis and Comparison. Comparing the proposed scheme in terms of computation time complexity due to the experiment performed by

```
Provide Identity, Password
Extract saved credentials from the server
if ($A^*$==$A$) then
Transmits Message$_1$
    if($T - T_1 \leq \Delta T$) then
    Extracts O from the record of GW
    $\mathrm{ID}^*_{\mathrm{ia}} = F \oplus h(R_1||A^*||\mathrm{T}_1)$, $B^* = h(\mathrm{ID}^*_{\mathrm{ia}}||A^*||R_1)$, $R^*_1 = J_2 \oplus h(A^*||T_1)$
    and $J_1{}^* = h(\mathrm{ID}^*_{\mathrm{ia}}||B^*||R^*_1||T_1)$
        if($J_1{}^*$==$J_1$) then
        key and computes
        $L_3 = h(h(h(\mathrm{ID}_{ia}||R^*_1||R_2))||\mathrm{ID}_{\mathrm{SN}}||R_2)$,
        $L_4 = h(\mathrm{ID}_{ia}||R_1||R_2) \oplus \mathrm{sk}$, $L_5 = R_2 \oplus \mathrm{ID}_{\mathrm{SN}}$ and $L_6 = E_l(\mathrm{ID}_{\mathrm{SN}}||R_1||R_2||L_5)$
        Transmits Message$_2$ and computes
        $R^*_2 = L_5 \oplus \mathrm{sk}$, $L_7 = L_4 \oplus \mathrm{sk}$, $L_8 = h(h(L_7||\mathrm{ID}_P)||\mathrm{sk}||R^*_2)$ and
        $L'_3 = h(h(h(\mathrm{ID}_{ia}||R^*_1||R^*_2))||\mathrm{ID}_{\mathrm{SN}}||R_2)$
            if($L'_3$==$L_3$) then
            key
            Computes
                if($L'_{13}$==$\mathrm{L}_{13}$)
                key
                Return(1) Pass
                else
                Return(0), fail
                end if
            Return(1) Pass
            else
            Return(0), fail
            end if
        else
        Return(1), Pass
        end if
    else
    Return(1) Pass
    end if
else
Return(1), Pass
end if
```

Algorithm 1: Algorithmic representation of the proposed protocol.

Table 3: Attacks and functionalities comparison.

Attack description	[31]	[32]	[33]	[5]	Our
Replay attack	✓	✓	✖	✖	✖
Masquerade attack	✓	✖	✓	✓	✖
Privileged insider attack	✖	✖	✖	✓	✖
Man-in-middle attack	✓	✖	✓	✖	✖
Malicious attack	✓	✓	✓	✖	✖
Anonymity violation	✖	✓	✓	✓	✖
Mutual authentication	✓	✖	✓	✓	✓
DoS attack	✖	✓	✖	✓	✖
Offline guessing attack	✓	✓	✖	✓	✖
Impersonation attack	✓	✖	✓	✖	✖
Spoofing attack	✖	✓	✖	✓	✖
Sensor capture attack	✖	✖	✖	✖	✖

[41, 42] of collision-free one-way hash(·) and XOR functions, it is demonstrated that the protocol presented in [31] consists of the registration phase of time complexity for the hash, and XOR functions are $4t_h + 1t_{\oplus}$; healthcare system upload phase $14t_h + 6t_{\oplus}$; patient upload phase $16t_h + 1t_{\oplus}$; treatment phase $15t_h + 6t_{\oplus}$ and checkup

Table 4: Storage overhead analysis and comparison.

Protocol	Storage overheads in bits
Kumari et al. [31]	2976
Rathore et al. [32]	3978
Wu et al. [33]	3968
Amin et al. [5]	2112
Our	2088

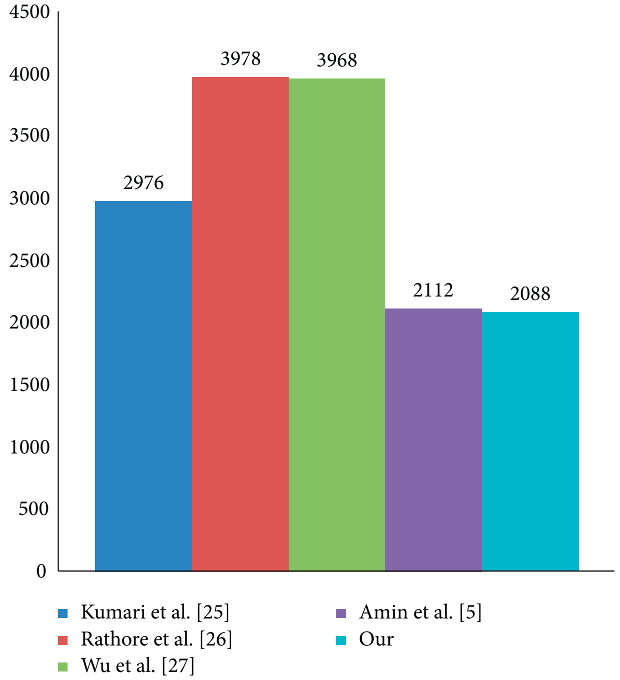


Figure 7: Storage overheads in bits.

Table 5: Computation cost analysis and comparison.

Protocol Phase↓	[31]	[33]	[5]	Our
Registration	$4t_h + 1t_{\oplus}$	$3t_h + 2t_{\oplus}$	$5t_h + 6t_{\oplus}$	$3t_h + 3t_{\oplus}$
Login and authentication	$10t_h + 1t_{\oplus}$	$19t_h + 11t_{\oplus}$	$35t_h + 22t_{\oplus}$	$34t_h + 22t_{\oplus}$

phase $6t_h + 1t_{\oplus}$. The computation time complexity of the proposed scheme is slightly higher compared to [5, 31, 33], as shown in Table 5.

The protocol presented by [31] is a minimum one-way hash time, but it has maximum exponential execution time, while the XOR time complexity is negligibly equal to zero. Rathore et al. [32] used Advanced Encryption Standard (AES) of key size 512, in which polynomial-time generated the random keys, so its hash value is minimal compared to the proposed and [5]. Similarly, [5] used an extra round trip during the login and authentication phase, which our scheme does not have. Therefore, our method consists of a simple hash cryptographic function based; here, it does not affect the computation cost, as shown in Figure 8.

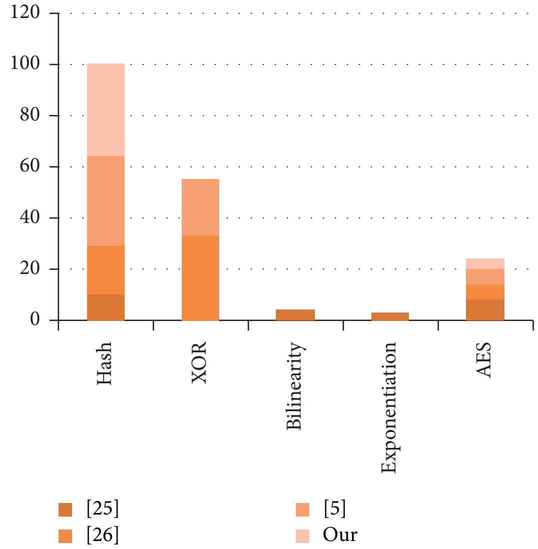


Figure 8: Computation cost comparison.

7. Conclusion and Future Work

In this modern era, the development of a robust certification environment for the healthcare system gains much attention from researchers, because the intelligent sensors, network-enabled devices (IoMT) and pervasive data acquisition, etc., pushed the healthcare industry to facilitate its patients for diagnoses and remote monitoring. Two things to be focused on for such environment, i.e., information authentication and identification authentication, are challenging, because, without solving these issues and challenges, no one can guarantee secure communication. To ensure data integrity, authorization, nonrepudiation, and user legitimacy and adequately tackle information identification, without a robust authentication protocol, it is not possible. Therefore, we have designed improved, lightweight, and robust authentication protocols for IoMT using WMSN. The proposed protocol mitigated all the known flaws noted for [5] and posed in the existing literature. The robustness of the protocol has been verified using a verification toolkit ProVerif2.00 and BAN logic of belief. In contrast, the performance evaluation result shows that the proposed scheme is fast and secure. The comparison analysis section shows that the proposed protocol is lightweight and balanced with security, often missing in several methods.

In the future, researchers plan to design protocols using the cloud, fog, and edge computing using 5G technology. This is ultra-low latency, which may be utilized for ultra-high reliability in examining a patient's physiological and psychosocial conditions. Also, we plan to discuss the COVID-19 patient X-ray image on a metaheuristic model-based deep learning/screening.

Appendix

(*---------*CHANNELS*----------*)

free ChSec:channel [private]. (*secure channel between Uia and GW)

```
free ChPub:channel. (*public channel between User, GW and SN)
(*-----------SESSION SHARED KEYS-----------*)
free sk:bitstring [private].
free skdash:bitstring [private].
free skstr:bitstring [private].
(*-----------CONSTANTS AND VARIABLES---------*)
free IDsn:bitstring.
free IDia:bitstring.
free IDiadash:bitstring.
free SN:bitstring [private].
free GW:bitstring.
Free Uia:bitstring.
free k:bitstring.
free kstr:bitstring.
free x:bitstring.
free xstr:bitstring.
free PWia:bitstring [private].
free R1: bitstring.
free R1str:bitstring.
free R2:bitstring.
free R2str:bitstring.
free R3:bitstring.
free R3str:bitstring.
free R1dash:bitstring.
free R2dash:bitstring.
free R3dash:bitstring.
free T1:bitstring.
(*-------QUERIES------*)
query attacker(sk).
query attacker(skdash),
query attacker(skstr).
query attacker(x).
query attacker(xstr).
query attacker(R1).
query attacker(R2).
query attacker(R3).
query id:bitstring; inj-event(end_SN(IDsn))==>inj-event(start_SN(IDsn)).
Query id:bitstring; inj-event(end_IDia(IDia))==>inj-event(start_IDia(IDia)).
(*----------EVENTS----------*)
event start_Uia(bitstring).
event end_Uia(bitstring).
event start_GW(bitstring).
event end_GW(bitstring).
event start_SN(bitstring).
event end_SN(bitstring).
(*----------REDUCTIONS and FUNCTIONS----------*)
fun h(bitstring):bitstring.
fun mult(bitstring, bitstring):bitstring.
fun con(bitstring, bitstring):bitstring.
fun xor(bitstring, bitstring):bitstring.
fun Encsk(bitstring):bitstring.
fun Encsksn(bitstring):bitstring.
fun Decsksn(bitstring):bitstring.
fun Decsksn(bitstring):bitstring.
fun PBKDF(bitstring):bitstring.
(*----------EQUATIONS----------*)
equation forall u: bitstring, v: bitstring; xor(xor(u, v), u) = v.
(*-------------USER'S PROCESSES--------------*)
let Uia =
event start_Uia(IDia); let HPWstr = h(xor(IDia, PWia) in
let Astr = h(concat(IDia, x, HPW)) in
if Astr = A then
let Bstr = xor(h(xor(concat(C, IDia, Astr, HPWstr))) in
let F = xor(h(IDia, (concat(xstr, Astr, T1))) in
let J1 = h(concat(IDia, Bstr, R1, T1)) in
let J2 = xor(h(concat(xstr, T1))) in
let L1 = Enc(xor(concat(J2, R1, xstr)) in
out(ChPub, (IDsn, F, L1, T1)); in(ChPub, (L11: bitstring, L12: bitstring, L13: bitstring)); let Dec(concat(IDsn, k, L11)) in
let R2dash = xor(L11, h(concat(IDia, R1))) in
let R3str = concat(L10, Rstr2)) in
let Adash = xor(L13, h(xor(R2str, R3str))) in
let skstr = h(h(concat(IDia, R1, R2str), R2, R3str)) in
let L11dash = h(concat(IDia, skstr, R3str)) in
if L11dash = L11 then
event end_Uia(IDia)
else
0.
(*-------------SENSOR NODE PROCESSES--------------*)
let UiaReg =
in(ChSec, (IDia:bitstring, HPWia:bitstring)); let HPWia = concat(PWia, Nia) in
let A = h(concat(IDia, IDg, x)) in
let B = h(concat(IDia, HPWia, x)) in
let C = xor(C, B) in
let O = xor(Nia, h(concat(IDsn, x))) in
```

out(CheSec, (A, B, C)); let GW =

event start_GW(IDGW); in(ChPub, (IDsn:bitstring, F: bitstring, T_1: bitstring)); Dec(concat(J_2, R_1, xstr)) in

let Ostr = xor(R_1, h(concat(IDsn, xstr))) in

if Ostr = O then

let IDiastr = xor(F, h(concat(R_1, Astr, T_1))) in

let Bstr = h(concat(IDia, A, R_1)) in

let R1str = xor(J_2, h(concat(Astr, T_1))) in

let J1str = h(concat(IDiastr, Bstr, R1str, T_1)) in

if J1str = J_1 then

let sk = h(concat(IDsn, R_1)) in

let L_3 = h(h(h(concat(IDia, R1str, R_2, h(concat(IDsn, R_2))))) in

let L$_4$ = xor(h(concat(IDia, R_1, R_2), sk)) in

let L_5 = sor(R_2, IDsn) in

let L_6 = Enc(concat(IDsn, R_1, R_2, L_5)) in

out(ChPub, (L_3, L_4, L_5, L_6)); in(ChPub, (L_9: bitstring, L_{10}: bitstring)); let Dec(concat(IDsn, R_1, R_2), sk)) in

let R3dash = concat(L_9, R_2)) in

let skdash = h(h(concat(IDia, R_1, R2str), h(R_2, R3dash)) in

let L9dash = h(concat(skdash, R3dash, R2str)) in

if L9dash = L_9 then

Let L_{11} = xor(h(concat(IDia, R_1), R_2)) in

Let L_{12} = h(concat(IDia, skdash, R3dash)) in

let L_{13} = Enc(IDsn, kstr, L_{11})) in

out(ChPub, (L_{11}, L_{12}, L_{13}));

event end_GW(IDGW)

else

0.

process ((!GW) | (!Uia))

Running the code, the listed results are displayed, which shows that the attacker could not trace the session share key SK for reconstruction and secure from cracking, as shown below.

```
(*......................RESULT......................*)
Completing equations...
-- Query not attacker(sk[]),
Completing...
Starting query not attacker(sk[])
RESULT not attacker(sk[]) is true.
-- Query inj-event(end_Ui(id))==> inj-event(start_Ui(id)),
Completing...
Starting query inj-event(end_Ui(id))==> inj-event(start_Ui(id))
RESULT inj-event(end_Ui(id))==> inj-event(start_Ui(id)) is true.
-- Query inj-event(end_S(id_57))==> inj-event(start_S(id_57)).
Completing...
Starting query inj-event(end_S(id_57))==> inj-event(start_S(id_57))
RESULT inj-event(end_S(id_57))==> inj-event(start_S(id_57)) is true.
```

Data Availability

The data collected during the data collection phase will be provided upon request to the corresponding authors.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The authors are grateful to the Deanship of Scientific Research, King Saud University, for funding through Vice Deanship of Scientific Research Chairs.

References

[1] S. Vishnu, S. J. Ramson, and R. Jegan, "Internet of medical things (IoMT)-an overview," in *Proceedings of the 5th International Conference on Devices, Circuits and Systems (ICDCS)*, pp. 101–104, Coimbatore, India, March 2020.

[2] D. Rizk, R. Rizk, and S. Hsu, "Applied layered-security model to IoMT," in *Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, p. 227, July 2019.

[3] V. Yanambaka, S. Mohanty, E. Kougianos, D. Puthal, and L. Rachakonda, "PMsec: PUF-based energy-efficient authentication of devices on the internet of medical things (IoMT)," in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)*, pp. 320-321, IEEE, Rourkela, India, December 2019.

[4] A. Yang, S. M. Chun, and J. G. Kim, "Detection and recognition of hand gesture for wearable applications in IoMT," in *Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT)*, pp. 1046–1053, IEEE, hunched-si Gangwon-do, Chuncheon, Korea, February 2018.

[5] R. Amin, S. H. Islam, G. P. 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.

[6] 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.

[7] R. P. Singh, M. Javaid, A. Haleem, R. Vaishya, and S. Al, "Internet of medical things (IoMT) for orthopedic in COVID-19 pandemic: roles, challenges, and applications," *Journal of Clinical Orthopaedics and Trauma*, vol. 11, pp. 1–5, 2020.

[8] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "IoMT-SAF: internet of medical things security assessment framework," *Internet of Things*, vol. 8, Article ID 100123, 2019.

[9] M. R. Sanaz, E. Nigussie, M. Levorato, S. Virtanen, and J. Isoaho, "Performance analysis of end-to-end security

schemes in healthcare IoT," *Procedia computer science*, vol. 130, pp. 432–439, 2018.

[10] J. D. Lee, T. S. Yoon, S. H. Chung, and H. S. Cha, "Service-oriented security framework for remote medical services in the Internet of Things environment," *Healthcare informatics research*, vol. 21, no. 4, pp. 271–282, 2015.

[11] M. S. Rahimi, T. N. Gia, and E. Nigussie, "session resumption-based end-to-end security for healthcare internet-of-things," in *Proceedings of the IEEE International Conference*, pp. 581–588, Liverpool, UK, October 2015.

[12] P. Gope, Y. Gheraibia, S. Kabir, and B. Sikdar, "A secure IoT-based modern healthcare system with the fault-tolerant decision-making process," *IEEE Journal of Biomedical and Health Informatics*, vol. 1, p. 1, 2020.

[13] P. Gope and T. Hwang, "BSN-Care: a secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, pp. 1368–1376, 2015.

[14] M. Usman, M. A. Jan, X. He, and J. Chen, "P2DCA: a privacy-preserving-based data collection and analysis framework for IoMT applications," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1222–1230, 2019.

[15] F. F. Moghaddam, S. G. Moghaddam, S. Rouzbeh, S. K. Araghi, and N. M. Alibeigi, "A scalable and efficient user authentication scheme for cloud computing environments," in *Proceedings of the IEEE Region 10 Symposium*, pp. 508–513, Kuala Lumpur, Malaysia, April 2014.

[16] S. R. Satheesh, D. Sangeetha, and V. Vaidehi, "EPSSHIC-enabling privacy and security of smart health care system in the cloud," in *Proceedings of the 2013 International Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 79–83, Chennai, India, July 2013.

[17] M. A. Allouzi and I. K. Javed, "Soter: trust discovery framework for internet of medical things (IoMT)," in *Proceedings of the 2019 IEEE 20th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–9, Washington, DC, USA, June 2019.

[18] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan et al., "Based medical systems for patient's authentication: towards a new verification secure framework using CIA standard," *Journal of Medical Systems*, vol. 43, no. 7, p. 192, 2019.

[19] L. C. Chen, T. Tsai, F. Y. L. Yang, and Y. L. Huang, "Designing a healthcare authorization model based on cloud authentication," *Intelligent Automation & Soft Computing*, vol. 20, pp. 65–379, 2014.

[20] X. Wang, L. Wang, Y. Li, and K. Gai, "Privacy-Aware efficient fine-grained data access control in internet of medical things based fog computing," *IEEE Access*, vol. 6, pp. 47657–47665, 2018.

[21] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, "Optimized blockchain model for internet of things based healthcare applications," in *Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, pp. 135–139, IEEE, Budapest, Hungary, July 2019.

[22] M. Selim and K. Elgazzar, "BIoMT: blockchain for the internet of medical things," in *Proceedings of the 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 1–4, IEEE, Sochi, Russia, June 2019.

[23] M. N. Shrestha, A. Alsadoon, P. W. C. Prasad, L. Hourani, and A. Elchouemi, "Enhanced e-health framework for security and privacy in the healthcare system," in *Proceedings of the 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)*, pp. 75–79, IEEE, Beirut, Lebanon, April 2016.

[24] D. C. Klonoff, "Fog computing and edge computing architectures for processing data from diabetes devices connected to the medical internet," *Journal of Diabetes Science and Technology*, vol. 11, 2017.

[25] D. Borthakur, H. Dubey, N. Constant, L. Mahler, and K. Mankodiya, "Smart fog: fog computing framework for unsupervised clustering analytics in wearable internet of things," in *Proceedings of the 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 472–476, IEEE, Montreal, Canada, 2017, November.

[26] A. V. Dastjerdi and R. Buyya, "Fog computing: helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, 2016.

[27] M. Engineer, R. Tusha, A. Shah, and K. Adhvaryu, "Insight into the importance of fog computing on the internet of medical things (IoMT)," in *Proceedings of the 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC)*, pp. 1–7, IEEE, Nagercoil, India, 2019 March.

[28] O. Akrivopoulos, I. Chatzigiannakis, C. Tselios, and A. Antoniou, "On the deployment of healthcare applications over fog computing infrastructure," in *Proceedings of the 2017 IEEE 41st annual computer software and applications conference (COMPSAC)*, pp. 288–293, IEEE, Turin, Italy, 2017 July.

[29] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *Proceedings of the 2018 21st Euromicro conference on digital system design (DSD)*, pp. 699–706, IEEE, Prague, Czech Republic, August 2018.

[30] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[31] A. Kumari, V. Kumar, M. Y. Abbasi et al., "CSEF: cloud-based secure and efficient framework for smart medical system using ECC," *IEEE Access*, vol. 8, pp. 107838–107852, 2020.

[32] H. Rathore, L. Wenzel, A. K. Al-Ali, A. Mohamed, X. Du, and M. Guizani, "Multi-layer perceptron model on chip for secure diabetic treatment," *IEEE Access*, vol. 6, pp. 44718–44730, 2018.

[33] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two-factor authentication protocol for healthcare applications with wireless medical sensor networks," *Multimedia Systems*, vol. 23, no. 2, pp. 195–205, 2017.

[34] R. Mishra and S. P. Tripathi, "Deep learning based search engine for biomedical images using convolutional neural networks," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 15057–15065, 2021.

[35] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, "Graphology based handwritten character analysis for human behaviour identification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 55–65, 2020.

[36] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.

[37] N. Kumar, M. Gupta, D. Gupta et al., "Novel deep transfer learning model for COVID-19 patient detection using X-ray chest images," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, 2021.

[38] B. Gupta, M. Tiwari, and S. Singh Lamba, "Visibility improvement and mass segmentation of mammogram images

using quantile separated histogram equalisation with local contrast enhancement," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 73–79, 2019.

[39] H. S. Basavegowda and G. Dagnew, "Deep learning approach for microarray cancer data classification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 22–33, 2020.

[40] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, pp. 1–19, 2020.

[41] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1005–1023, 2013.

[42] P. Bart, "Cryptographic hash functions," *European Transactions on Telecommunications*, vol. 5, no. 4, pp. 431–448, 1994.