Cloud based mutual authentication scheme in multi gateway healthcare environment

S. D. Suganthi[1], R. Anitha[2], V.Suresh Kumar[1]
{sds.amcs@psgtech.ac.in[1]}

[1,2,3]Dept of AMCS, PSG College of Technolgy, Coimbatore, Tamilnadu 641004

Abstract: Wireless Body Sensor Network (WBSN) has gained attention due to its potential in improving the quality of healthcare services especially during the recent pandemic across the globe. Using WBSNs, vital signs of the patient can be gathered from the different sensor nodes equipped on the patient's body and can be accessed by the healthcare professional using a mobile device ensuring confidentiality and anonymity. The physiological data collected by sensor devices may be stored in a cloud based environment and can be accessed by a doctor for a suitable treatment. In a modern healthcare environment, the globally connected IoT, sensors, gateways and cloud based infrastructure brings new opportunities for assisting medical professional to provide on demand and real time patient monitoring services with higher accuracy and better efficiency. The doctor can access the data after proper authentication at the cloud server. At the same time, the patient with the wearable sensors should be supported with mobility as the patient cannot be expected to be in the same location. In a multi gateway environment, the patient thus may be connected either to the home gateway node or to a foreign gateway node while on the move. Hence, mutual authentication between the entities is indispensable to ensure that only authorized entities are communicating through trusted gateway nodes. In the proposed cloud based healthcare authentication system, we use lightweight crypto primitives to construct a secure end to end authentication between body sensors, the gateway and the cloud server with mobility management. The proposed authentication scheme is augmented with a secure roaming protocol that will allow the patients' body sensors to use the roaming services delivering the health data to the cloud server through the foreign gateway. The security of the designed protocol is analysed against various attacks using BAN logic and AVISPA tool.

Keywords: Medical sensor network, Mutual Authentication, Gateway, Foreign gateway,| cloud server

1 Introduction

The healthcare industry in India is growing at a tremendous pace owing to ICT based technologies like Electronic Health Records, Electronic transfer of prescription and Telemedicine. Besides, with increasing urbanization, problems related to modern day living has increased which demands for specialized care. To meet these demands, mobile patient monitoring systems are the most viable option, which makes use of Internet of Things (IoT), wearable body sensor network and Cloud based storage.

The body sensor networks (BSNs) employ various lightweight, portable and autonomous sensing devices on, or around the body for pervasive health monitoring. BSNs can help in determining real-time physiological parameters like body temperature, heart rate etc., which can reduce human-interactions. Besides, healthcare applications utilizing body sensor networks generate a vast amount of data that require reliable, scalable, secure storage and computing

ICCAP 2021, December 07-08, Chennai, India

DOI 10.4108/eai.7-12-2021.2314589

infrastructure. The real time data collected from the BSNs are forwarded to the Gateway(GW) nodes which are then stored at the Cloud server. These gateway nodes are interconnected by a backbone network. The authorized medical professional access the medical records from the cloud server for further analysis and treatment. The integration of all the entities in a multi gateway network poses many security challenges. The security issues should be addressed carefully to provide patients with secure and reliable healthcare experience. Hence, proper authentication of sensor nodes of the BSN and the healthcare professional must be ensured before allowing the medical professional to access the data in addition to automatic data collection/sensing.

The system architecture is designed with two phases viz, data collection from the BSN by the gateway nodes and data reporting to the cloud server as shown in the Figure 1.

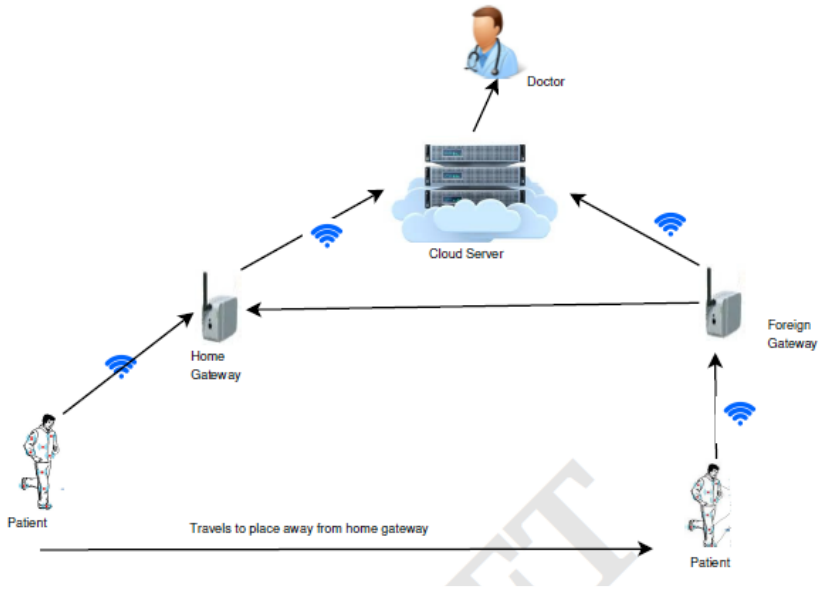


Figure 1: Proposed architecture

In the propsed work, the BSN comprises of wearable sensors like pulse oximeter, glucometer, motion sensors,EEG, ECG, blood pressure and motion sensors that are customized according to the patient disease monitoring needs. In addition, the BSN consists of a master sensor that collects the physiological data from the patient and sends it to the gateway node during the data collection phase. In the data reporting phase, the gateway node would further forward the health data to the cloud server securely. At the cloud server, the medical information of every patient is stored in the form of digital record. The authorized medical professional can access the patient health data and make appropriate decision for continuous patient monitoring. The region where the patient with his body sensor network has registered with a home gateway is termed as a home region and rest are foreign networks for that patient. In a real time scenario, the patient may be registered with one of the gateways, but may not be tied up in the same region, rather moving out of the home region(i.e, home gateway) for various reasons. For example, a patient is registered with an authorized centre of a corporate hospital, and a doctor has been assigned by that centre to receive the patient's physiological parameters and the vital signs for continuous monitoring. When the patient with the wearable

sensors moves out of coverage of the home region still the healthdata from the body sensors needs to be reported tothe home gateway node through the foreign gateway where he is currently associated with. Hence,appropriate mobility management is inevitable tomaintain connection between the patient and thehospital network.

Generally, the query for the patient data is issued by the gateway where the doctor, after due authentication will be able to access the patient data. But in real time monitoring of the patient, it is appropriate to stream the sensor data from the patients' body to the cloud server through the gateway from where the designated medical professional can have access to the patient's data.The system provides a noticeable feature that adds mobility to the patient,i.e, even when the patient moves into a foreign region away from the home region, the WBSN should be able to connect to the Cloud sever through appropriate gateway nodes. Thus, in a multi gateway environment, the authentication of the patient is essential wherever he is roaming. This feature will enable the patient to have seamless connectivity to the cloud server through the gateway and thus the medical professional on the other side will be able track the patient health data without interruption.

To meet these objectives, we have proposed a mutual authentication scheme that covers sensor nodes and the home gateway with Cloud server in a multi gateway environment. Considering the obvious need to add mobility to the patient with BSN, the scheme includes a secure roaming authentication protocol that aims to authenticate a patient securely when he has migrated to a foreign region.

2 Related work

With the large number of devices of IoT, scalability is one of the major issues in the existing authentication schemes. To secure the patient's health data, it needs to be encrypted and stored in the cloud server.Entity authentication is the most basic and commonly used method to resolve the security and privacy issues of WBSN. There have been a large number of authentication and key establishment schemes for WBSNs in a multi gateway environment in the literature [1],[8] ,[15],[16] without using the cloud server. A secure lightweight two factor authentication scheme for multi-gateway based wireless sensor networks was presented by Amin et al., [1]. Wu et.alpresented an improved authentication scheme [16] where they point out that the scheme in [1] is vulnerable to sensor capture, the off-line guessing and desynchronization attacks. The scheme by Das et.al in [8], does not involve all the three participants for final session key computation and is not resistance to user tracking attack. Also, the smart card must store some parameters such as identity of Foreign gateway node and login parameters for Foreign gateway (FG), which is seen as an overhead.

In Srinivas et.al's [15] work, the medical professional extracts the sensor ID of the patient from the public directory of the Home Gateway node. If not available, the home gateway node through a broadcast message finds the location of the patient's body sensors. It is obvious that the traffic on the network is increased by the broadcast message and all the gateway nodes have to spend energy in checking for the sensor ID in their registered list of sensor IDs. All these schemes [1],[8] ,[15] ,[16] are based on the login request initiated by the user/doctor or the medical professional. But in a real time scenario, for the continuous monitoring it will be more appropriate if the login and authentication phase is initiated by the patient for streaming the sensor data from the BSN to the cloud server through the gateway node at regular intervals. After the entities are mutually authenticated, a session key is generated. The shared keys of the registered BSNs are stored in home gateway, leading to scalability problem in the schemes [1],[8],[15], [16]

Cloud computing infrastructure integrated with BSN-based platforms addresses these issues and provides the facility to access the medical records in a ubiquitous way. These cloud based solutions offer scalability in terms of data storage, processing power for diverse on-line and off-line data analysis. The authentication scheme by Siddique et.al [14] makes use of IMEI, IMSI number and Fingerprints scanners of the mobile phone to authenticate the user. The framework transforms a smart phone to act as a unique and only identity required to access the TMIS system remotely, eliminating smart card, which can be seen as a limitation for a critically ill patient/patient in emergency condition. In Chen et.al[4]'s scheme, the registered entities sign and upload the medical record/ health inspection report to the cloud server. Their scheme not only has a high degree of computational complexity but also fails to provide patient anonymity and message authentication. Also, the scheme is limited to face to face medical service i.e, unable to achieve real tele medicine.

Chiou et.al [5] proposed a mutual authentication scheme based on pairing based cryptography with anonymity, unlinkability, message authentication. Later Cheng et.al [6], demonstrated that Chiou et.al's scheme is defenseless against key compromise impersonation (KCI) attack and also fails to provide forward security. But their scheme does not support patient anonymity and lacks security against mobile device stolen attack. In the scheme proposed by Mohit et.al, the patient has to visit the healthcare centre, where the patient data is uploaded to the cloud server[12].

In 2019, Xie and Hwang [18] in their work developed a secured roaming authentication protocol using ECC algorithm involving smart cards. The session key between the Home agent and the foreign agent lack security against ephemeral DH, where the exponent $\boldsymbol{x}$ is exposed to the adversary. Also it cannot withstand the replay attack and MITM attacks. Subsequently Lopes et al. [10] in their proposed a mutual authentication scheme for D2D communication in cloud based E health system. This scheme is based on cellular communication and does not support multiple gateways. Masud et al. [11] in their work also proposed a mutual authentication scheme having a single gateway node. The authentication is carried out between the group sensor node and the doctor and not between the individual sensor node and the group node.The proposed protocol aims focuses on minimizing energy consumption like reducing CPU overhead of the node by the use of few hash functions. Zhang et al. [20] in their multi factor authentication protocol withstands various attacks , but their scheme smart card and add Bio metrics as authentication factors which are considered as overhead from the patient side.

Besides, there are few Roaming authentication protocols proposed for the wireless environment, that are discussed below: Shin et.al [13] have proposed an efficient authentication scheme providing mutual authentication and secure session key agreement ensuring user anonymity.Then, Farash et.al [9] simultaneously presented the vulnerabilities of Shin et al.'s scheme in [13], proving that the scheme does not guarantee untraceability, secrecy of the sensitive parameter of home agent, secrecy against impersonation attack.

Chung et al. [7] proposed an enhanced lightweight anonymous authentication scheme to resolve the weaknesses of Farash et al.'s scheme namely lack of anonymity against a malicious mobile node, with less computation cost. The Roaming Authentication protocol of Xie et.al [17] encrypts the identity authentication material using the private key of the home cluster head , which is decrypted by the foreign cluster head by the corresponding public key, which is also possible for any attacker to extract the same authentication material as well. Moreover, the mobile sensor node after authenticating with the foreign cluster head becomes a member of the same, while disassociating with the home cluster head. This feature may seems to be viable, but on revisiting the home region especially in healthcare environments, the

mobile node will be seen as visitor and roaming authentication protocol needs to be executed. Obviously, this feature can be seen as a overhead on the cluster head /gateway nodes.

In our proposed scheme, the patient with the BSN may be roaming in a foreign zone will have the facility of associating with the home region at any time.Thus, the patient‘s credentials are with the home gateway node. More importantly, there is no broadcast message in search of the required sensor ID, thus making the scheme secure. The authentication procedure makes use of light weight cryptoprimitives for communication between the entities. In addition, the scheme is scalable as all the patient data and including the patient ID is stored at the cloud server.

3 Proposed scheme

This proposed work is to ensure continuous monitoring of patients with use of wearable body sensor network system that provides health data of the patient in station or roaming. With the objective of continuous monitoring of the patient, it would be more appropriate for the sensors on the wearable BSN of the patient to stream the health data observed through the sensors to the cloud data centre. The doctor or the healthcare professional on the other side can access the data and assess the health status of the patient. This approach would quickly report the condition of the patient to the doctor without waiting for the doctor to check the patient’s health data, thus enhancing the quality of health care. This work consists of distinct phases namely: Registration phase,login and authentication phase for data collection and data reporting.

3.1 Assumptions

The following assumptions are regarded as true in this protocol .

1. Registration of all the entities are carried out in a secure environment.
2. Each gateway node has a unique master secret x_{GW}
3. Each gateway node has a shared key K_{HG-MS_i} with the sensor nodes registered with it.
4. All the gateway nodes are interconnected through a backbone network and share a pairwise symmetric key between them.

Table 1: Notations used in the proposed scheme

Symbol	Description
ID_M, PID_M	Real and Pseudo identity of an entity M
x	Master key x of the server
r_i	128 bit Random Number , n=128
K_{HG-MS_i}	Symmetric key between MS and HG
K_{HG-FG}	Symmetric key between HG and FG
SK_{GW-MS_i}	Shared key between the MS and the GW
SK_{GW-S}	Shared key between the GW and CS
T	Time stamp

3.2 Registration phase

In the registration phase,the doctor/medical professional registers with the cloud server initially, whose service can be accessed by the patient. At the same time, the gateway nodes which updates the patient data from the BSN, registers with the cloud server. Finally, the patient's master sensor node registration at the home gateway node is discussed.

3.2.1 Doctor/Medical Professional Registration

In this registration phase, The doctor/medical professional registers with the cloud server to access the patient's health records that are stored in the server database. The doctor/medical professional will use their hand held device to connect with the cloud server, executing the following steps:

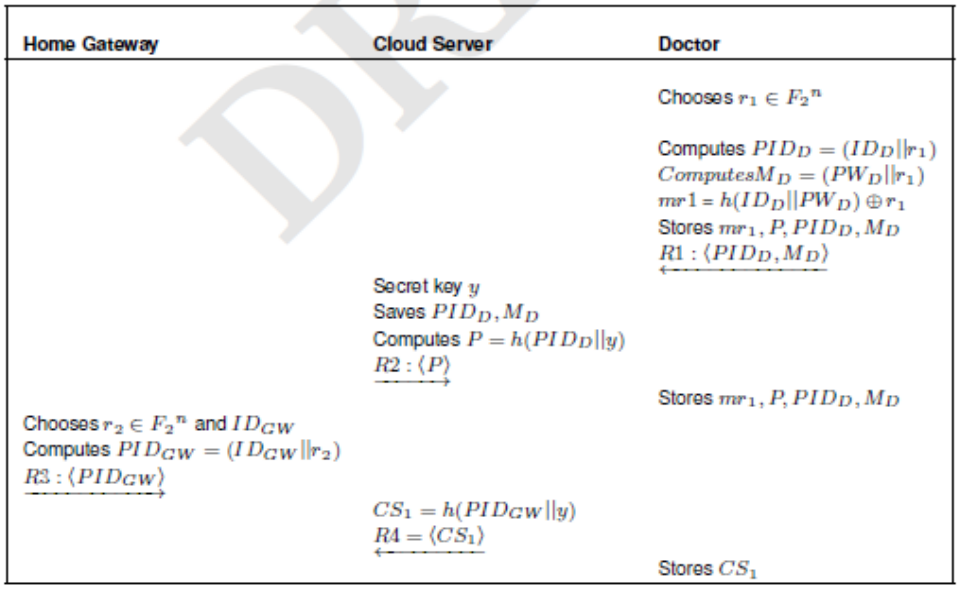


Figure 2: Doctor and Gateway Registration

Step 1: At the time of registration,the medical professional selects his identity ID_D and PW_D ,along with a 128 bit random number $r_1 \in {F_2}^n$.

Step 2: The handheld device computes $PID_D = (ID_D||r_1)$ and $M_D = h(PW_D||r_1)$. The mask value mr_1 is computed as $mr_1 = h(ID_D||PW_D) \oplus r_1$ and stored in the doctor's personal device discarding r_1. In step $R1$, the doctor will send PID_D and M_D to the cloud server through a secure channel.

Step 3: At the server side, $P = h(PID_D||y)$ is computed , where y is the master secret key of the cloud server and returns P to the Doctor's device in step $R2$. At the end of step $R2$, the doctor's device will have PID_D ,M_D, mr_1 and P.

3.2.2 Gateway Registration

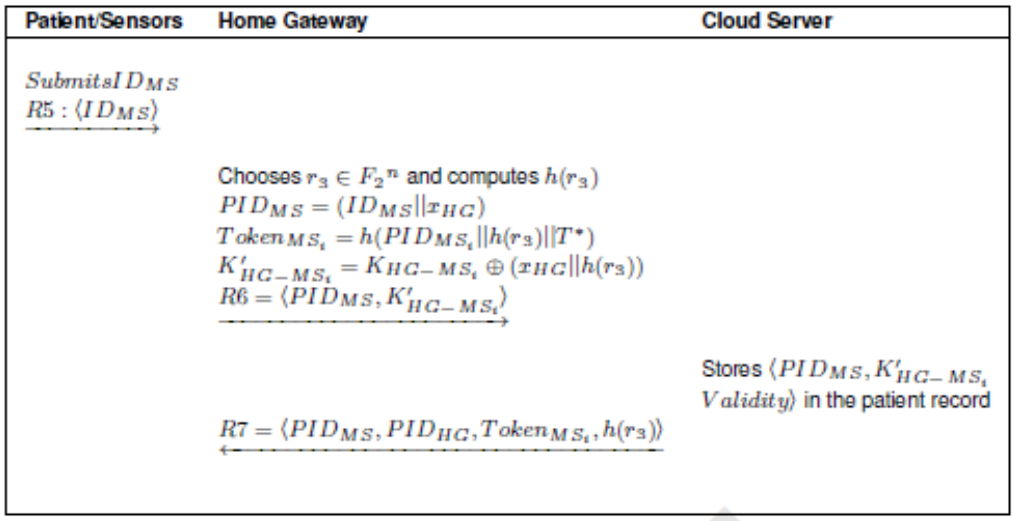
In this phase, each gateway node registers with the cloud server, for authentically collecting patient data from his BSN and forwarding them to the cloud server.

Each gateway node with an ID ID_{GW} chooses random number $r_2 \in {F_2}^n$ and computes $PID_{GW} = h(ID_{GW}||r_2)$, which is submitted to the cloud server for registration through a secure channel,in step $R3$. The cloud server with its master secret key y , computes $CS1 = h(PID_{GW}||y)$ and is sent to the gateway in step $R4$.

3.2.3 Patient Registration

Step 1: The various wearable sensors on the patient's body will have ID's as$(ID_{SN1}, ID_{SN2},,, ID_{SNm})$. These wearable sensors would report the sensed data to a master sensor node having an ID ID_{MS}, which will be communicating with the gateway node. The ID of master sensor node ID_{MS} is computed as $ID_{MS} = ID_{SN1} \oplus ID_{SN2}..\oplus ID_{SNm}$.

Step 2: Once the patient registers his master sensor ID (ID_{MS_i}) to the gateway node in step $R5$, the home gateway computes the pseudo identity of the patient $PID_{MS_i} = h(ID_{MS_i}||x_{HG})$, where x_{HG} is the master secret of the home gateway. The masked value of shared key between the home gateway and the master sensor node is computed as $K'_{HG-MS_i} = K_{HG-MS_i} \oplus (h(r_3)||x_{HG})$, and is stored in thecorresponding record of the patient at the cloud server database along with the PID_{MS_i},as shown step $R6$ of Figure 3.



Step 3:During this time, on the request of Home gateway the cloud server will assign a doctor with identity PID_D. Here, either the patient may choose the Doctor or the home gateway will assist the patient in choosing the doctor.

Step 4: The home gateway(HG) proceeds to create a token $Token_{MS_i}$ for the patientID_{MS_i}.The HG chooses a 128 bit random number $r_3 \in {F_2}^n$, computes $Token_{MS_i} =$

$h(PID_{MS_i}||h(r_3)||T^*)$, where T^* is the time at which the token is created and $h(r_3)$ is the long term secret shared between the home gateway and the patient. Then the home gateway sends the following parameters to the patient in the message $R7$ in a secure channel. $R7: \langle (PID_{MS_i}, h(r_3), Token_i, PID_{HG}) \rangle$.

4 Login and Authentication Phase

The login and authentication phase comprises of two sections namely, Data collection phase for the data stream to be collected by the Gateway node and Data update phase where the gateway uploads the sensor data to the cloud server.

In all the authentication steps, whenever a message is transmitted from an entity at time t_i , it will reach the other end at time t_{i+1} where $t_{i+1} \geqslant t_i$ by Δt, This time difference Δt takes into consideration the maximum transmission time of any message. Whenever the relation holds true, it implies that the message transmission is successful. Else, it is a case of replay attack where the receiving entity will suspend the session immediately.

4.1 Data collection phase

The master sensor node MS_i of the patient collects the health data from the patient's BSN. The master sensor node MS_i then tries to login to the nearby gateway at time t_1 and sends the message Z_1 to the that gateway. $Z_1: \langle PID^*_{MS}, Token^*_i, PID^*_{HG}, t_1 \rangle$. The gateway records the time t_2 at which the message has arrived and then checks for the time difference t_2 - $t_1 \leqslant \Delta t$ for possible replay attack. This time difference Δt takes into consideration the maximum transmission time of any message from the BSN to reach the nearest gateway.

Further, the gateway node checks whether its own ID PID_{GW} matches with that of the ID submitted by the MS node. i.e, $PID_{GW} \stackrel{?}{=} PID^*_{HG}$. If true, it implies that the patient is in the home region. Thus the gateway attempts to execute *Home Authentication protocol(HAP).* On the other hand if the condition is not valid, it implies that the patient has migrated to a foreign region. The gateway then, proceeds to execute the *Roaming Authentication Protocol (RAP).*

4.1.1 Home Authentication Protocol(HAP)

The home gateway on confirming the identityPID^*_{HG} sends a request to the cloud server for the credentials of the patient in $Z_2: \langle PID_{MS_i}, PID_{HG},$ Req for key $\rangle$.The server retrieves the key K'_{HG-MS_i} using PID_{MS_i} as index and returns the value in Z_3. The home gateway will generate a 128 bit random number $r_4 \in {F_2}^n$ to compute $H1 = (h(r_3)||r_4) \oplus K_{HG-MS_i}$ and sends it to the master sensor in the message $Z_4: \langle H1, t_3 \rangle$ which is received at t_4.

The MS node of the patient performs the following steps as depicted in the Figure 4:

Step 1: Checks $t_4 - t_3 \leqslant \Delta t$ for any replay attack. If validated, retrieves $h(r_3)^*$ and r_4 from $H1$ as $H1 \oplus K_{HG-MS_i}$

Step 2: Compares $h(r_3)^* \stackrel{?}{=} h(r_3)$. If matches, then the Home gateway is authenticated and stores the random number r_4, else the session is aborted.

Step 3: Computes $Z_5^* = h(h(r3)||r4)$ and sends Z_5: (Z_5^*, t_5) to the home gateway at time t_5.The Home gateway receives the message Z_5 at time t_6 and checks $t_6 - t_5 \leqslant \Delta\, t$ for a replay attack. It validates $Z_5^* \stackrel{?}{=} h(h(r_3)||r_4)$. If equal, then the MS node is authenticated by the home gateway, else the session is aborted. At the end, both the gateway and MS node generate the session key SK_{HG-MS_i} between them as $SK_{HG-MS_i} = h((h(r_3) \oplus h(r_4))||PID_{MS_i})$.

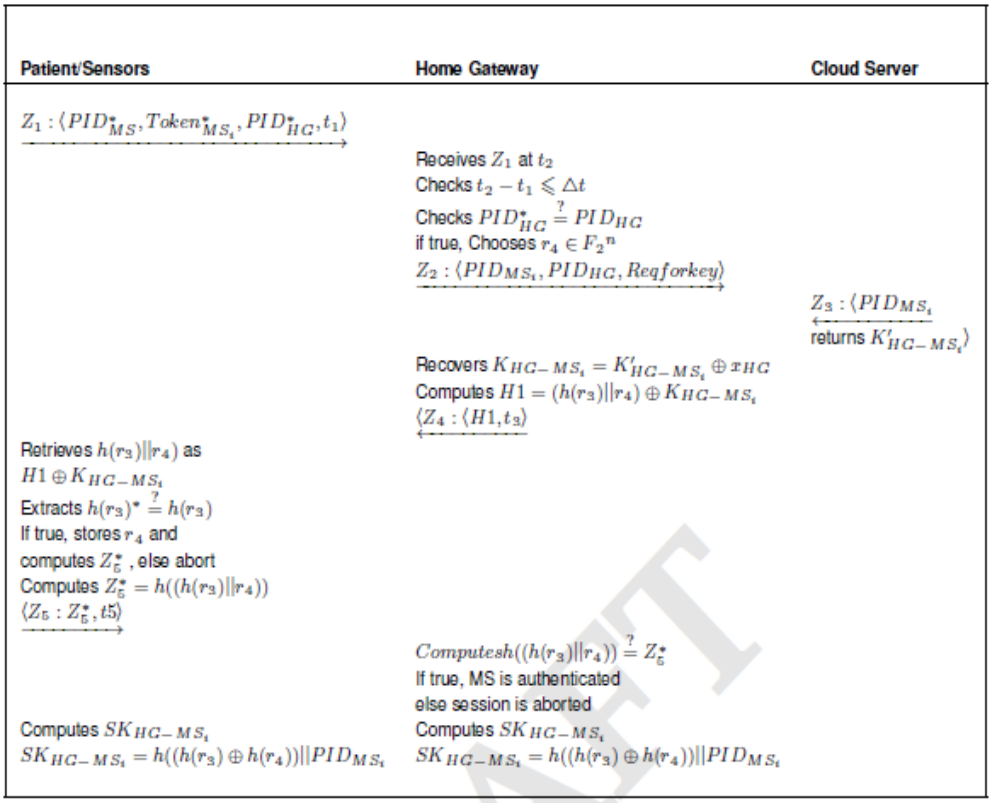


Figure 4 : Home Authentication Phase

4.1.2 Roaming Authentication Protocol(RAP)

This phase would be executed when the patient has migrated to a foreign network. The patient submits the credentials to the foreign gateway (FG) in the login request, which then forwards the login request to the corresponding HG for authenticating the patient.The patient submits his pseudo identity PID_{MS_i}, PID_{HG} and the token $Token_{MS_i}$ to the gateway, at time t_1 in RZ_1. The gateway on receiving the credentials at time t_2 will check for $t_2 - t_1 \leqslant \Delta\, t$. The ID of the home gateway is validated as $PID_{HG} \stackrel{?}{=} PID_{GW}$. If not true, it implies that the MS node is in the foreign region and the following actions are carried out . This gateway not being

the home gateway,will then prepare hand off token $HT1$ to forward the patient's credentials to the home gateway for authentication.

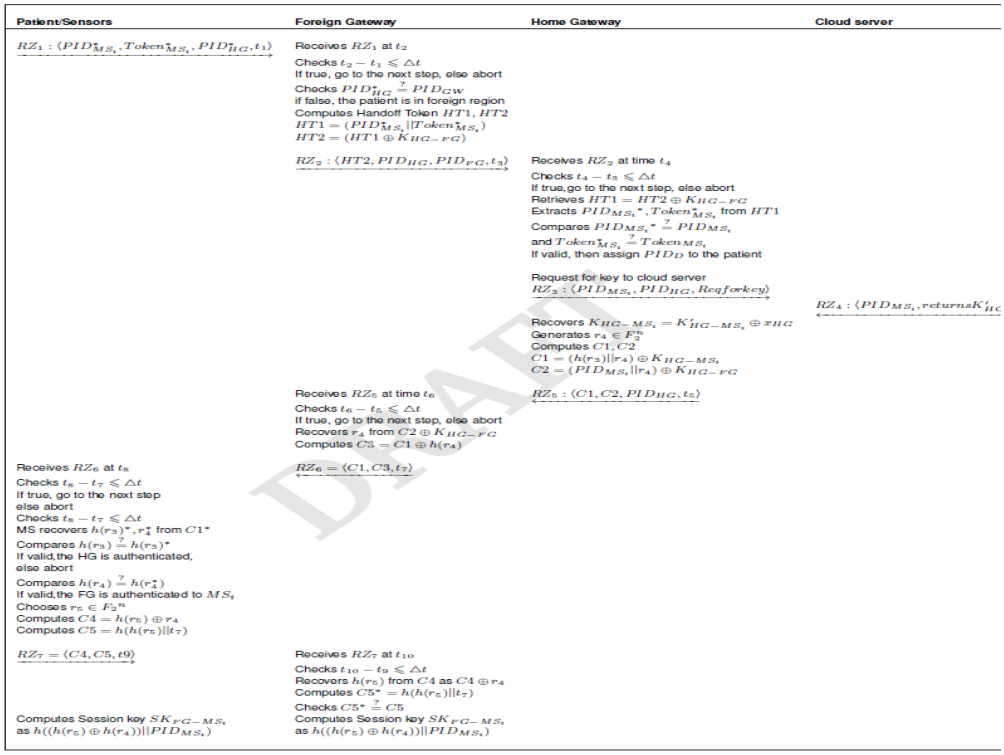


Figure 5: Roaming Authentication Phase

It computes Handoff Tokens $HT1 = (PID_{MS_i}||Token_{MS_i})$ and $HT2 = HT1 \oplus K_{HG-FG}$ and sends $RZ_2 = \langle HT2, PID_{HG}, PID_{FG}, t_3 \rangle$. The message would reach the HG at time t_4. The time is validated for any replay attack by comparing $t_4 - t_3 \leqslant \Delta\, t$. If successful, the HG carries out the following sequence of steps as shown in Figure 5:

Step 1: It retrieves $HT1 = HT2 \oplus K_{HG-FG}$ and extracts $PID^*_{MS_i}, Token^*_{MS_i}$ from $HT1$.

Step2:verifies whether $PID_{MS_i{}^*}$ is available in its database and if found , checks for $Token^*_{MS_i} \stackrel{?}{=} Token_{MS_i}$ of the PID_{MS_i}. If not true, the session is aborted.

Step 3: The HG requests the cloud server for the corresponding MS_i in the message $RZ_3 = \langle PID_{MS_i}, PID_{HG} \rangle$ .The cloud server returns K'_{HG-MS_i} in $RZ_4 = \langle PID_{MS_i}, K'_{HG-MS_i} \rangle$, from which the HG recovers K_{HG-MS_i} as $K'_{HG-MS_i} \oplus x_{HG}$.

Step 4: Further,the HG generates a random number $r_4 \in F_2^n$, where n is 128 bits and computes $C1$ and $C2$ as follows: $C1 = (h(r_3)||r_4) \oplus K_{HG-MS_i}$ and $C2 = (PID_{MS_i}||r4) \oplus K_{FG-HG})$ and sends $RZ_5 = (C1, C2, PID_{HG}, t_5)$

The FGW on receiving Z_5 at time t_6 carries out the following sequence:

Step 1: Verifies for replay attack with $t_6 and t_5$, and if not a replay performs the following steps. Else,the session aborted.

Step 2: Recovers r_4 from $C2 \oplus K_{HG-FG}$ and computes $C3 = C1 \oplus h1(r_4)$,where h1(.) is a 256 bit random function and sends the message $RZ_6 = (C1, C3, t_7)$ to the MS node of the patient.

The MS node on receiving this message at time t_8 would perform the following:

Step 1:Validates the time as $t_8 - t_7 \leqslant \Delta\ t$ and if true ,the MS node recovers $h(r_3)^*$ and r_4^* from $C1^*$,in addition to extracting $h1(r_4^*)$ from C3 .Otherwise,the session is aborted.

Step 2: Verifies $h(r_3)^* \stackrel{?}{=} h(r_3)$, and if true then the HG is authenticated. Also,it compares $h1(r_4) \stackrel{?}{=} h1(r_4^*)$. If this is also validated, then the FG is authenticated and the MS node and proceeds to the next step,otherwise the session is aborted.

Step 3: Chooses a 128 bit random number $r_5 \in F_2^n$ and computes $C4 = h(r_5) \oplus r_4$ and $C5 = h(h(r_5)||t_7)$ and sends the message RZ_7 comprising of $C_4, C5$ at t_9 to the FG for authentication.

Step 4: The FG node on getting the message RZ_7at time t_{10} will check for replay attack by comparing $t_{10} - t_9 \leqslant \Delta\ t$. Iftrue FG recovers $h(r_5)$ as $C4 \oplus r_4$ else the session is aborted.

Step 5: It computes $C_5^* = h(h(r_5)||t_7)$and compares $C_5^* \stackrel{?}{=} C_5$. If true,the FG will authenticate MS node and both the entities will create a session key $SK_{FG-MS_i} = h(h(r_5) \oplus h(r_4))||PID_{MS_i})$.

4.2 Data update phase

4.2.1 Gateway and Cloud server authentication

On obtaining the health data from the patient's BSN, the GW node (either Home gateway or Foreign gateway), updates at the Cloud server after due authentication. Hence, few authentication steps are required between the gateway and the cloud server.

The Gateway node computes the parameters $G1, G2$ and $G3$ and sends them to the cloud server as follows.

It chooses a 128 bit random number $r_6 \in F_2^n$ and computes $G1 = CS1 \oplus r_6$; $G2 = h(PID_{GW}||CS1||r_6)$; $G3 = h(CS1||G2||r_6)$

The gateway then proceeds to send $G1$ and $G3$ at time tt_1 to the cloud server in the message K_1: $\langle G1, G3, tt_1 \rangle$ .On receiving the the message K_1 at tt_2, the Cloud sever checks for the replay attack by comparing $tt_2 - tt_1 \leqslant \Delta\ t$. If true, then the following actions take place at the cloud server. Otherwise, the session is aborted. On getting these parameters from the gateway, it recovers r_6^* from $G1$ as $r_6^* = CS1 \oplus G1$ and computes $G2^*$ as $h(PID_{GW}||CS1||r_6^*)$ and $G3^*$ as $h(CS1||G2^*||r_6^*)$.

If $G3^* \stackrel{?}{=} G3$, then the gateway is authenticated, else the session is terminated.If authentication is successful, the Cloud Server computes $CS2 = G2^* \oplus CS1$ and sends $CS2$ at time tt_3, to the Gateway. The gateway node on the receipt of $K2$ at $tt4$ checks for the replay attack as $tt_4 - tt_3 \leqslant \Delta\ t$. After validation, the GW node recovers $G2^*$ from $CS2 \oplus CS1$. If $G2^* \stackrel{?}{=} G2$, the cloud server is authenticated. Then the session key between the GW node and the cloud server is created as $SK_{CS-GW} = h(G1||G2||G3)$

4.2.2Doctor/Medical professional authentication

To access the patient's health records, a registered medical professional transmits a login request message to the cloud server with his credentials, ID_D, PW_D, through a handheld device.

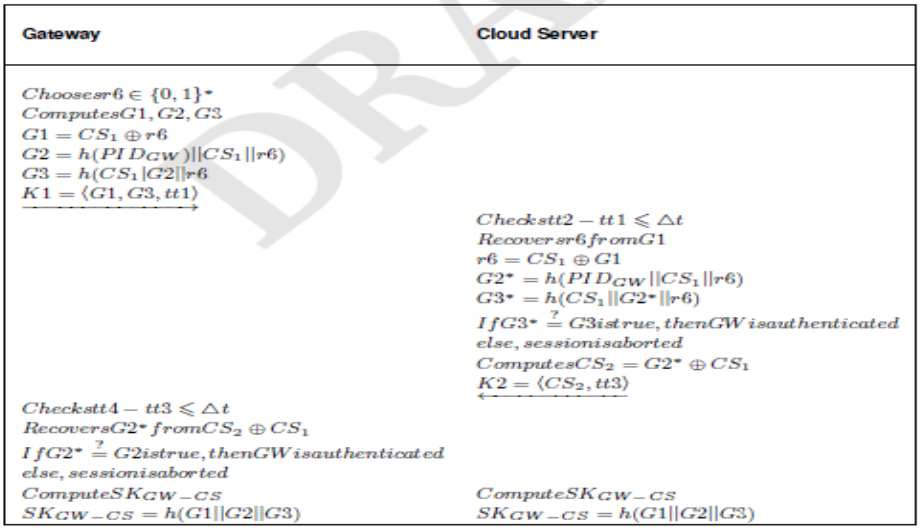


Figure 6 : Data Update Phase

Step 1: The PDA /handheld device retrieves r_1^* from the stored value of mr_1 as $r_1^* = mr_1 \oplus h(ID_D||PW_D)$, and computes $PID_D^* = h(ID_D||r_1^*)$ and $M_D^* = h(PW_D||r_1^*)$. The medical professional submits the parameters $(PID_D{}^*, M_D{}^*, tt_5)$ to the cloud server.

Step 2: The Cloud server on receiving the values at time tt_6, checks for the time validity by performing $tt_6 - tt_5 \leqslant \Delta\, t$. If successful, the server chooses a 128 bit random number $r_7 \in F_2^n$ and computes $CS3 = P \oplus r_7$ and server passes $\langle CS3\ ,\ tt_7 \rangle$ to the doctor/medical professional ,which may reach at time tt_8

Step 3: The PDA checks for the time validity as $tt_8 - tt_7 \leqslant \Delta\, t$ and if valid, retrieves r_7 from $CS3$ as $r_7 = CS3 \oplus P$

Step 4:If the previous condition is validated, then the CS and the medical professional are mutually authenticated.They proceed to generate the session key as $SK_{CS-D} = h(P||r_7)$.

5 Security Analysis

In this section, we analyse the security of the proposed scheme and show that our scheme satisfies the essential security requirements of healthcare system using Cloud based Body sensor network in a multi gateway environment. The informal security analysis shows that our proposed scheme is resilient against various security attacks.In addition, the formal security analysis was carried out using the BAN Logic to strengthen our claim. Also, we have simulated the proposed authentication protocol using AVISPA tools to prove that the security goals are achieved.

5.1 Informal security analysis

Patient Anonymity and unlinkability of sensor nodes: The original identities are aggregated to form a master sensor ID ID_{MS_i} and the patient does not submit his original ID_{MS_i} anywhere on the channel.The adversary $\mathcal{A}$ can only observe the pseudo identity $PID_{MS_i} = h(ID_{MS_i}||x_{HG})$, where x_{HG} is the master secret of the home gateway. The identity protection is through the hash function's one-way property.Thus,the sensor ID's are not traceable from any one of these values in the eavesdropped messages. Furthermore, ID_{MS_i} is not guessable from PID_{MS_i} since it requires the master secret key of the home gateway node.

Sensor Node Impersonation:An adversary trying to impersonate may not know PID_{MS_i} with the knowledge of the identities of the individual identities. Each PID_{MS_i} is associated with a $Token_{MS_i}$. Any attempt to forge can be prevented since this token, $h(PID_{MS-i}||h(r_3)||T^*)$, cannot be reproduced by an adversary$\mathcal{A}$, without knowing $h(r_3)$ and T^* ,the time at which the token was created. Hence, our protocol can resist sensor node impersonation attack.

GW Impersonation:The gateway node at the time of registration computes the pseudo ID PID_{GW} and only the pseudo ID PID_{GW} is used by the gateway in further communication and the original ID is not revealed.Thus in the step Z_1 of Home authentication protocol or in the RZ_1 and RZ_2 of Roaming authentication protocol , the adversary $\mathcal{A}$ cannot compute the original ID. Also, since the gateway node with its master secret value $x_H G$, creates PID_{MS_i}. if it is forged, the PID_{MS_i} values may not match any of the sensor node identities , thus failing in authentication.By the long term key value $h(r_3)$ shared between the master sensor and the gateway nodes, the adversary $\mathcal{A}$, cannot compute $H1$.

Replay attack: In our proposed scheme, replay attack is not possible at any stage of communication since all the messages are attached with a timestamp. The master sensor node, gateway nodes and cloud server check for the freshness of the received message as whether $t_{i+1} - t_i \leqslant \Delta t$ before processing it.This time difference Δt considers the maximum time delay for data transfer between any two communicating entities. If the condition fails, it is a replayed message and hence session is aborted.Therefore, the proposed protocol can resist replay attacks.

Protection of Long term key: The long term keys K_{HG-MS_i} are not stored in the gateway. These keys are masked and stored at the cloud server. For every login, the key K'_{HG-MS_i} is fetched from which the the actual K'_{HG-MS_i} is derived. Thus even if the gateway is compromised, it is not possible for an adversary $\mathcal{A}$ to guess these keys without knowing the master secret key of the gateway x_{HG} .

Session key leakage prevention: The session key is generated for every session uniquely after the entities are mutually authenticated.It is computed at both the ends separately using the secret values r_4 and r_5, the gateway and the master sensor node respectively. The session key is computed as a one way hash function $SK = h((h(r_5) \oplus h(r_4))||PID_{MS_i})$, using the random numbers generated by the master sensor node and the home gateway . Since it is not transmitted between the nodes and not reused, the leakage of the session key is efficiently prevented.

Mutual authentication: The communicating entities authenticate each other before the actual data transmission.In this proposed scheme, the long term secret key $h(r3)$ and $r4$ are used for authentication of the master sensor node and the home gateway in the message $Z5^* = h(h(r3)||r4)$ of HAP and similarly in RAP the authentication happens after the confirmation

of $C4, C5$ and the session key SK_{FG-MS_i} as $h((h(r_5) \oplus h(r_4))||PID_{MS_i})$ is generated only after mutual authentication is successful. Hence, for an adversary $\mathcal{A}$, it is infeasible to authenticate with the entities without knowing the long term secret values $h(r_3)$,$h(r_4)$ and $h(r_5)$. Also, the gateway node authenticates to the cloud server before uploading the data to the server, in addition to the doctor or the medical professional getting authenticated before accessing the health records from the cloud server.

Forward Secrecy:In our proposed scheme, the session key is computed as $SK = h((h(r_5) \oplus h(r_4))||PID_{MS_i})$, using the random numbers generated by the master sensor node and the home gateway respectively. Since it is not transmitted between the nodes and not reused , the session key will be renewed for every session with the values of r_4 and r_5.Since the session key is generated at the ends of communication from their shared secrets, it is not feasible for an adversary to guess the session key.

Ensures patient mobility: The patient sends the health data to the cloud medical server via a gateway node. The master sensor node with the help of the $Token_{MS_i}$ it posses, will be able to get authenticated whether it is in home region or roaming in the foreign region. the patient is not constrained by the geographical location or home region where he has registered with. The roaming authentication phase takes care of the patient getting authenticated by the home gateway node through the Foreign gateway code.

Doctor impersonation: The user(doctor)is authenticated on valid entry of his credentials, that is, ID_D and PW_D, which then computes the PID_D and M_D , by hash function. The computed PID_D and $M_D$are sent to the medical server for authentication. The correctness of the PID_D and PW_D are checked with the retrieved value of r_1^*, and computes $PID_D^* = h(ID_D||r_1^*)$ and $M_D^* = h(PW_D||r_1^*)$. These conditions will not authenticate for incorrect values of PID_D and PW_D and makes the possibility of user impersonation very low.

5.2 Security proof using BAN logic

In this section security of the proposed protocol is analyzed using well-popular formal method Burrows-Abadi-Needham (BAN) logic [3]. The formal security analysis using the BAN logic proves the secure mutual authentication between sensor nodes and HG/FG. The authentication proof is based on the BAN logic for Home Authentication Protocol (HAP) as well as Roaming Authentication Protocol (RAP) and key agreement phase.

Protocol idealization: The protocol needs to be idealized so that the analysis in BAN logic can be carried out. The communication steps for idealization are as follows:

$$ILZ4 = HG \longrightarrow MS < \langle (h(r_3), r_4), t_3 \rangle >_{K_{HG-MS}}$$
$$ILZ5 = MS \longrightarrow HG < Z_5^*, t5 > r_4 >$$
$$ILRZ1 = FG \longrightarrow HG < HT1, HT2, PID_{HG}, PID_{FG}, t_3 >_{K_{HG-FG}}$$
$$ILRZ5 = FG \longrightarrow MS < \langle C1^* = C1 =< (h(r_3)||r_4) >_{K_{HG-MS_i}}, C3^*, t_7 \rangle >_{h(r_4)}$$
$$ILRZ6 = D \longrightarrow MS < \langle C4, C5 = h(h(r_5)||t7), t9 \rangle >_{r_4}$$

Since the other messages $Z1, Z2$ and $Z3$ are plain notification messages, they are omitted in the analysis. In the following section, we prove the above test goals in order to show the secure authentication using the BAN logic rules and the assumptions.

Security goals: According to the analytic procedures of the BAN logic, the proposed protocol should satisfy the following goals and the assumptions made during the verification process are listed below:

$G1: MS| \equiv h(r_3)$ $\quad$ $A1: MS| \equiv MS \ \underline{K_{HG-MS}} \ HG$

$G2: HG| \equiv Z_5^*$ $\quad$ $A2: MS| \equiv$ ⍰t_3

$G3: HG| \equiv MS| \equiv SK_{HG-MS} A3: HG| \equiv ?t_5$
$G4: MS| \equiv HG| \equiv SK_{HG-MS}$ $A4: HG| \equiv ?r_4$
$G5: HG| \equiv HT1$ $A5: HG| \equiv FG$ $\underline{K_{HG-FG}}$ HG
$G6: MS| \equiv r_4 A6: HG| \equiv ?t_3$
$G7: FG| \equiv h(r_5)$ $A7: FG| \equiv FG$ $\underline{h(r_4)}$ HG

Scheme analysis: By seeing rule and $ILZ4$, we get $D1 = MS \triangleleft (\langle (h(r_3), r_4), t_3 \rangle_{K_{HG-MS}})$. Using message meaning rule in $D1$ with $A1$, we get $D2 = MS| \equiv HG| \sim ((h(r_3), r_4), t_3)$. Using $A2$, $D2$ and nonce verification rule, we get $D3 = MS| \equiv HG| \equiv h(r_3)$. Using $D3$ and jurisdiction rule, we get our $G1 = MS| \equiv h(r_3)$ GW which is our goal $G1$.

By seeing rule and$ILZ5$, we get$D4 = HG \triangleleft\!< Z_5^*, t5 >_{r_4}$. Using message meaning rule in $D4$ with$A3$, we get $D5 = HG| \equiv MS| \sim (Z_5^*, t5 >_{r_4})$. Using $A4$, $D5$ and nonce verification rule, we get $D6 = HG| \equiv MS| \equiv Z_5^*$. Using $D6$ and jurisdiction rule, we realize the goal $G2 = MS| \equiv Z_5^*$ GW .Since $h(r_4)$ and $h(r_3)$ are necessary parameters in the construction of the session key SK_{HG-MS}, using $G1$ and $G2$ with session key rule we get $G3 = HG| \equiv MS| \equiv SK_{HG-MS}$ and $G4 = MS| \equiv HG| \equiv SK_{HG-MS}$.

By seeing rule and $ILRZ1$, we get $D7 = HG \triangleleft \langle HT1, HT2, PID_{HG}, PID_{FG}, t_3 \rangle >_{K_{HG-FG}}$. Using message meaning rule in $D7$ with $A5$, we get $D8 = HG| \equiv FG| \sim (HT1, HT2, PID_{HG}, PID_{FG}, t_3)$. Using $A6, D8$ and nonce verification rule, we get $D9 = HG| \equiv FG| \equiv HT1$. Using $D9$ and jurisdiction rule, we get our goal $G5 = MS| \equiv HT1$ GW.

By seeing rule and $ILRZ5$, we get $D10 = MS \triangleleft \langle C1^* = C1 =\!< (h(r_3)||r_4) >_{K_{HG-MS_i}}, C3^*, t_7 \rangle >_{h(r_4)}$. Using message meaning rule in $D10$ with $A7$, we get $D11 = FG| \equiv HG| \sim ((h(r_3)||r_4) >_{K_{HG-MS_i}}, C3^*, t_7)$. Using $A7$, $D11$ and nonce verification rule, we get $D12 = HG| \equiv FG| \equiv h(r_3)$. Using $D12$ and jurisdiction rule, we get our $G6 = MS| \equiv h(r_3)$ which is our goal$G6$.

5.3 Automated Security Analysis using AVISPA

In this section, the simulation results of our proposed protocol are shown. To strengthen the security proof we have simulated and analyzed the the security attributes of the protocol design using AVISPA tool. Four validation tools are supported in AVISPA tool namely OFMC, ATSE, SATMC and TA4SP. The security of the protocol is simulated by applying HLSPL.

The security protocols to be analyzed under the AVISPA are first specified in the HLPSL (High Level Protocols Specification Language).Note that each role represented in HLPSL is independent from the others, which gets some initial information by parameters, and then communicates with the other roles by channels [2]. The role system also defines a number of sessions, and a number of principals and some basic roles.

SUMMARY: This section represents that whether the tested protocol is safe, unsafe, or whether the analysis is inconclusive.

DETAILS: This is a section, which either explains under what condition the tested protocol is declared safe, or what conditions have been used for finding an attack, or finally why the analysis was inconclusive.

PROTOCOL, GOAL and BACKEND: These are the sections that denote the name of the protocol, the goal of the analysis and the name of the back-end used, respectively.

The OFMC back-end checker and the CL-AtSe back-end checker are executed and shown in Figures 7 and 8. Both the reports for the OFMC back-end checker and the CL-AtSe back-end checker show that the scheme is SAFE under this checker model and satisfies all the specified security goals.

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED NUMBER OF
SESSIONS
PROTOCOL
/home/span/span/testsuite/results/c
ase1.if
GOAL
as specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.07s
visitedNodes: 64 nodes
```

Figure 7: OFMC Summary report

```
%OFMC
%Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED NUMBER OF SESSIONS
TYPED MODEL
PROTOCOL
/home/span/span/testsuite/results/case1.if
GOAL
As Specified
BACKEND
CL-AtSe
STATISTICS
Analysed : 0 states
Reachable : 0 states
Translation: 0.03 seconds
Computation: 0.00 seconds
```

Figure 8: CL-AtSe summary report

6 Performance and Security Requirements Comparisons

In this section, the performance of our proposed mutual authentication scheme is compared with the recently proposed related authentication schemes applied for multi gateway WSNs as shown in the following Table 2. The no of hash operations are 8 which is lesser as compared to all the other schemes and there is no encryption /decryption as used by Das et al. In addition, the performance is also compared with that of existing roaming authentication protocols, which is shown in Table 3.

Table 3, and 4 show the summary of performance of the proposed scheme with other roaming authentication protocols for mobility networks.and the security features of the proposed scheme with that of other schemes respectively

Table 2 : Performance Comparison of multi gateway based schemes

Scheme		Computational Cost			
		User in Home Reg	User in Foreign Reg		Total
Amin et al. (1)	Sensor	$5T_h$	$5T_h$	$10T_h$	$26T_h$
	HG	$8T_h$	$1T_h$	$9T_h$	
	FG	0	$7T_h$	$7T_h$	
Wu et al.(4)	Sensor	$4T_h$	$4T_h$	$8T_h$	$33T_h$
	HG	$11T_h$	$7T_h$	$18T_h$	
	FG	0	$7T_h$	$7T_h$	
Das et al.(15)	Sensor	$1T_e + 4T_h$	$1T_e + 3T_h$	$2T_e + 7T_h$	$6T_e + 17T_h$
	HG	$2T_e + 5T_h$	0	$2T_e + 5T_h$	
	FG	0	$2T_e + 5T_h$	$2T_e + 5T_h$	
Srinivas et al.(3))	Sensor	$6T_h$	$5T_h$	$11T_h$	$40T_h$
	HG	$13T_h$	0	$13T_h$	
	FG	0	$16T_h$	$16T_h$	
Xie et al.(17)	Sensor	NA	$1T_e + 5T_h$	$1T_e + 5T_h$	$4T_e + 10T_h$
	HG	NA	$2T_e + 3T_h$	$2T_e + 3T_h$	
	FG	NA	$1T_e + 2T_h$		
Zhang et al. (13)	Sensor	$5T_h$	$7T_h$	$7T_h$	$44T_h$
	HG	$12T_h$	$6T_h$	$18T_h$	
	FG	NA	$14T_h$	$14T_h$	
Proposed Scheme	Sensor	$4T_h$	$1T_h$	T_h	$5T_x + 8T_h$
	HG	$2T_h$	$3T_x + 1T_h$	$3T_x + 3T_h$	
	FG	0	$2T_x$	$2T_x$	

Table 3: Performance Comparison of Roaming authentication protocols

Scheme	Sensor node	FG/FA	HG/HA
Shin et.al[2013](14)	$8T_h$	$1T_h + +8T_x$	$3T_h + 3T_{E/D}$
Farash et.al [2015](15)	$6T_h$	$1T_h + 2T_S$	$5T_h + 2T_S$
Chung et.al[2016] (16)	$6T_h$	$4T_h$	$7T_h$
Proposed Scheme	$10T_h + 5T_x + 2T_S$	$2T_h + +2T_S$	$3T_h + 2T_x + 3T_S$

Table 4: Security comparisons with Multi GW authentication

Attacks	cheng (8)	chiou (7)	Sidq (5)	Yeh (20)	Amin (1)	Wu (4)	Das (2)	Srini (3)	Xie (17)	Lopes (11)	Proposed
Patient Anonymity	✔	✔	✗	✔	✔	✗	✗	✗	✗	✔	✔
SN Impersonation	✗	✔	✗	✗	✔	✗	✔	✗	✗	✔	✔
GW Impersonation	✗	✗	✔	✗	✔	✗	✔	✔	✗	✗	✔
Longterm Key Protection	✗	✗	✗	✔	✔	✗	✗	✗	✗	✔	✔
Replay Attack	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
SN Capture	✗	✗	✗	✗	✗	✔	✔	✔	✗	✗	✔
SK Leakage Prevention	✔	✗	✗	✗	✗	✔	✔	✗	✗	✔	✔
Mutual Authentication	✗	✗	✔	✔	✔	✔	✔	✔	✔	✔	✔
FwdSecrecy	✔	✔	✔	✗	✔	✔	✗	✗	✔	✔	✔

7 Conclusions

Mutual authentication has been proved as the best technique for securing unauthorized access of medical data. In this paper, we proposed a lightweight mutual authentication scheme in a multi gateway environment for remote monitoring and it provides anonymity for the patient and the doctor while achieving the mutual authentication between the different entities. The authentication scheme is secure as well achieves energy efficiency and scalability. The proposed scheme achieves mutual authentication with the use of hash operations and XOR operations, and it is more efficient than previously related schemes in terms of energy efficiency of the sensor nodes. From the perception of storage costs, the scheme performs better as the shared keys are stored in the cloud servers releasing the storage space at the gateway nodes, at the same time making the key storage secure and scalable. The security of the proposed scheme is formally proved by using BAN logic and simulated using AVISPA tool to prove the scheme is safe. Although there are certain authentication schemes for WBSN, either of these schemes are not designed for complete mutual authentication in a multi gateway environment or for a roaming authentication supported by cloud storage. Besides, the collected data of WBSN contains sensitive information of patients, privacy protection would be another important issue in WBSN security. In future, this work may be extended to enhance the security problems of WBSN in communication ad storage.

8 References

[1] Ruhul Amin and G.P. Biswas. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Netw.*, 36(P1):58–80, January 2016.

[2] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron. *The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications*, pages 281–285. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[3] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. *ACM Trans. Comput. Syst.*, 8(1):18–36, February 1990.

[4] Chin-Ling Chen, Tsai-Tung Yang, Mao-Lun Chiang, and Tzay-Farn Shih. A privacy authentication scheme based on cloud for medical environment. *Journal of Medical Systems*, 38(11):143, Oct 2014

[5] Shin-Yan Chiou, Zhaoqin Ying, and Junqiang Liu, Improvement of a privacy authentication scheme based on cloud for medical environment. *Journal of Medical Systems*, 40(4):101, Feb 2016.

[6] Qingfeng Cheng, Xinglong Zhang, and Jianfeng Ma. ICASME: an improved cloud-based authentication scheme for medical environment. *J. Medical Systems*, 41(3):44:1–44:14, 2017.

[7] Youngseok Chung, Seokjin Choi, Youngsook Lee, Namje Park, and Dongho Won. An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in wireless sensor networks. *Sensors*, 16(10), 2016.

[8] Ashok Kumar Das, Anil Kumar Sutrala, Saru Kumari, Vanga Odelu, Mohammad Wazid, and Xiong Li. An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks. *Security and Communication Networks*, 9(13):2070–2092, 2016.

[9] Mohammad Sabzinejad Farash, Mahmoud Ahmadian Attari, and Saru Kumari. Cryptanalysis and improvement of a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps. *International Journal of Communication Systems*, 30(1):e2912–n/a, 2017.

[10] Ana Paula G. Lopes and Paulo R. L. Gondim. Mutual authentication protocol for d2d communications in a cloud-based e-health system. *Sensors*, 20(7), 2020
[11] Mehedi Masud, Gurjot Singh Gaba, Karanjeet Choudhary, M. Shamim Hossain, Mohammed F. Alhamid, and Ghulam Muhammad. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. *IEEE Internet of Things Journal*, , 2021.
[12] Prerna Mohit, Ruhul Amin, Arijit Karati, G. P. Biswas, and Muhammad Khurram Khan. A standard mutual authentication protocol for cloud computing based health care system. *Journal of Medical Systems*, 41(4):50, Feb 2017.
[13] Hongjin Shin, Soobok andYeh and Kangseok Kim. An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks. *Peer-to-Peer Networking and Applications*, 8(4):674–683, Jul 2015.
[14] Zeeshan Siddiqui, Abdul Hanan Abdullah, Muhammad Khurram Khan, and Abdullah S. Alghamdi. Smart environment as a service: Three factor cloud based user authentication for telecare medical information system. *Journal of Medical Systems*, 38(1):9997, Dec 2013.
[15] Jangirala Srinivas, Sourav Mukhopadhyay, and Dheerendra Mishra. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. *Ad Hoc Networks*, 54:147 – 169, 2017.
[16] Fan Wu, Lili Xu, Saru Kumari, Xiong Li, Jian Shen, Kim-Kwang Raymond Choo, Mohammad Wazid, and Ashok Kumar Das. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment. *Journal of Network and Computer Applications*, 89:72 – 85, 2017. Emerging Services for Internet of Things (IoT).
[17] Qing-Qing Xie, Shunrong Jiang, Liangmin Wang, and Chin-Chen Chang. Composable secure roaming authentication protocol for cloud-assisted body sensor networks. *I. J. Network Security*, 18(5):816–831, 2016.
[18] Qi Xie and Lingfeng Hwang. Security enhancement of an anonymous roaming authentication scheme with two-factor security in smart city. *Neurocomputing*, 347:131–138, 2019.
[19] Kuo-Hui Yeh. Bsncare+: A robust iot-oriented healthcare system with non-repudiation transactions. *Applied Sciences*, 6(12), 2016.
[20] Shuailiang Zhang, Xiujuan Du, Xin Liu, and James Ying. An efficient and provable multifactor mutual authentication protocol for multigateway wireless sensor networks. *Sec. and Commun. Netw.*, 2021, January 2021.