Peer-to-Peer Networking and Applications
https://doi.org/10.1007/s12083-021-01162-x

A robust and lightweight secure access scheme for cloud based E-healthcare services

Mehedi Masud[1] · Gurjot Singh Gaba[2] · Karanjeet Choudhary[2] · Roobaea Alroobaea[1] · M. Shamim Hossain[3]

Received: 31 August 2020 / Accepted: 8 April 2021

Abstract

Traditional healthcare services have transitioned into modern healthcare services where doctors remotely diagnose the patients. Cloud computing plays a significant role in this change by providing easy access to patients' medical records to all stakeholders, such as doctors, nurses, patients, life insurance agents, etc. Cloud services are scalable, cost-effective, and offer a broad range of mobile access to patients' electronic health record (EHR). Despite the cloud's enormous benefits like real-time data access, patients' EHR security and privacy are major concerns. Since the information about patients' health is highly sensitive and crucial, sharing it over the unsecured wireless medium brings many security challenges such as eavesdropping, modifications, etc. Considering the security needs of remote healthcare, this paper proposes a robust and lightweight, secure access scheme for cloud-based E-healthcare services. The proposed scheme addresses the potential threats to E-healthcare by providing a secure interface to stakeholders and prohibiting unauthorized users from accessing information stored in the cloud. The scheme makes use of multiple keys formed through the key derivation function (KDF) to ensure end-to-end ciphering of information for preventing misuse. The rights to access the cloud services are provided based on the identity and the association between stakeholders, thus ensuring privacy. Due to its simplicity and robustness, the proposed scheme is the best fit for protecting data security and privacy in cloud-based E-healthcare services.

Keywords Secure access · E-healthcare · Cloud · Privacy · Internet of things

1 Introduction

Storing the health records manually and retaining them for future references becomes challenging to manage with large data volumes. The most peculiar example is the number of patients surpassing the capacity of the hospitals due to the coronavirus pandemic. In countries like the USA, Brazil, and India, the healthcare system has been reeling under pressure as its capacities were falling short of taking in more patients. The load on the healthcare infrastructure is unimaginable due to the current global crises of this current pandemic.

The problem with the traditional method of storing all data manually or on paper is that it's tough to find a patient's data from the record room where a large number of health records are being kept. It takes a lot of time and energy to find the specific medical record of a patient. It is also possible that data can get lost and eradicated in any natural or human-made disaster. Data can be stolen easily because it is in the form of plain text so anyone can read and write the data in records or modify it as it is easily accessible [1]. Keeping the health records in digital format is enabled by the technology powered by the Internet of Things (IoT) [2, 3]. Security in E-healthcare is even more important because it concerns the sensitive health data of the patient. The attackers can exploit the vulnerabilities of the open wireless channels to conduct attacks [4–10]. These attacks can cause various types of damage to the E-healthcare framework.

Let us consider a scenario where a patient has received treatment from a hospital in a different city from his

This article belongs to the Topical Collection: *Special Issue on Security of Mobile, Peer-to-peer and Pervasive Services in the Cloud*
Guest Editors: B. B. Gupta, Dharma P. Agrawal, Nadia Nedjah, Gregorio Martinez Perez, and Deepak Gupta

✉ M. Shamim Hossain
mshossain@ksu.edu.sa

Extended author information available on the last page of the article.

Published online: 03 May 2021

hometown, after which he/she gets discharged and goes home. Later, he suddenly falls ill and is admitted to a nearby hospital, but he does not have the full details or the file of his treatment from the previous hospital. Lack of information can cause a delay in his treatment, which can be fatal. But if the patient already has/her his data on devices accessible via the cloud, retrieval of patient's data would be done in seconds, thus enabling the new hospital staff to begin the treatment as soon as possible [11–15]. The health care department can store data on the cloud in encrypted form with high secure algorithms used in cryptography that allow only the legitimate user to access any remote location provided it has internet connectivity, wired or wireless. The "cloud" has servers on which many software and databases are run, and they are accessed over the Internet. Cloud servers are located in every part of the world. With the help of cloud computing, stakeholders, insurance companies, and healthcare departments don't have to manage physical servers by themselves or run any software applications on their machines [16]. Cloud computing offers advantages like sharing enormous amounts of data, and patients' medical records in a timely and safe manner [17–23]. Digital solutions in hospitals recommend healthcare providers manage their infrastructure well and provide them ample opportunity to familiarize themselves with IT, service providers [24, 25]. Other benefits of Cloud and mobile computing include scalability, cost-effectiveness, agility enhancement, and collaborative sharing of resources [26–28].

E-healthcare can be made flexible in hospitals not having the full provisions for implementing cloud-based services. Some of the hospital's data can be stored using the traditional medium of paper to store the general data, and the cloud can be used to store more important data. The access to the legitimate users is provided irrespective of the location, and the exchange of data is secure [29–31]. Only specific stakeholders can read the data, delete the data, and modify the data according to the need or future use [29, 32, 33]. The health data of patients must be protected end to end, and it's also a big challenge to ensure patients' privacy while also retaining data quality [1]. 90 percent of healthcare institutions in Australia and many other countries have already adopted E-healthcare to facilitate effective health care services. Digitally, the medical records are stored in the form of Electronic medical record (EMR), Electronic Health Data (EHD), and Personal Health Record (PHR) [34]. EHR and EMR health records are maintained by health care professionals, whereas PHR is handled by the patients themselves or by their relatives. The communication exchange between doctors and patients or between cloud and systems usually occurs through a wireless medium, which is highly prone to attacks like denial of service (DoS), man in the middle attack (MITM), and eavesdropping, and so forth. Although the health care department asserts that it is the staff's responsibility to maintain the patient's data confidentiality, the technology used in e-healthcare should also protect the data.

The stakeholders in the dynamic and complex IoT environment of the healthcare system are the patient, nurse, doctor, pharmacist, lab technicians, etc. To successfully run the healthcare system, a specific set of regulations are necessary. There are several organizations in the world like Health Information Technology for Economic and Clinical Health (HITECH) and Health Insurance Portability and Accountability Act (HIPAA) that provide the regulations related to healthcare [35–37].

In 1996, HIPAA [37] was established to regulate the US healthcare industry. The HIPAA's primary focus is to ensure the patients' security and privacy and protect the full information of the hospital and its different services. HIPAA ensures that only authorized users can access the hospital data from any part of the world.

This paper proposes a scheme in which only legitimate staff can access the patient's data. The doctor has access to reading and writing the data, and others can only read the data but cannot modify it. The proposed scheme explains how an admin generates the subkeys from the master key to ensure end-to-end security of critical information. We have also addressed the requirements of key security for a secure healthcare system such as integrity, confidentiality, and protection from known key attacks, etc. [5, 38–43].

1.1 Motivation

Internet of Things offers a variety of features that support the real-time applications of the e-healthcare. The IoT and WSN networks are prone to diverse attacks because they share the information through insecure public channels. Moreover, cloud access, if not protected, could disclose potential confidential information to adversaries. It becomes more dangerous for medical applications as it can endanger the lives of the patients. The adversary can misuse the information to exploit the reputation of the hospital as well. The frequency of cyberattack incidents reported in the HIPAA journal points out the adversaries' interest in the information stored in the cloud. As per the report, 32,205 users information were breached through 8 separate incidents of unauthorized access reported in August 2020 [44]. The few healthcare institutions whose users are victimized are the University of Florida Health, Northwestern Memorial Healthcare, Hamilton Health Center, Inc. A possible solution to protect against these cyber attacks in the future is the use of robust access control protocols. However, designing such protocols is challenging due to the resource-constrained user devices and vulnerable wireless channels. Therefore, lightweight security protocols with extreme robustness to protect sensitive networks should be developed.

1.2 Our contribution

1. We propose a robust and lightweight, secure access scheme for cloud-based e-healthcare services.
2. The proposed security protocol verifies the user's identity (doctor, patient, nurse, etc.) and permits only legitimate users to access cloud services.
3. The proposed protocol attains data confidentiality, message freshness, etc., as security measures while preventing the networks from various threats like man in the middle (MITM) attack, message modification attack, replay attack, etc.

The remaining paper is structured as follows: Section 2 discusses the literature review whereas Section 3 presents the system model. Section 4 describes the proposed scheme. Section 5 provides the security and comparative analysis followed by conclusions in Section 6.

2 Literature review

Olutayo Boyinbode et al. [45] suggests a new web-based technology that enables nurse, doctor, and pharmacist to access the patients' medical records. It uses the local cloud to store the information of the patient. The data is accessible remotely, and it can also be updated. It is ideal for healthcare units where patients' data records need to be shared with other doctors for collaborative treatments. But the drawback of this scheme is that it does not allow the patient to access the health records.

Another group of researchers at the Eindhoven University of Technology have proposed a secure E-healthcare scheme, "My PHR Machine" [46]. It is a mixture of cloud and PHR systems. The hospital crew and himself can access, share, and analyze the PHR data through HR software. Another advantage of this scheme is that the data of different users can be accessed with more flexibility at the same time and with proper security measures. The information accessed through My PHR machine is also accessible via the cloud. This scheme does not enable faster access to health records.

The authors in [47] have suggested a cloud-based healthcare framework for successful communication between caregivers and healthcare providers that can completely replace the manual record system in hospitals. The healthcare providers, as well as the patient, can access the records using the above system without any restriction of time or place. The framework incorporates a collaborative service so that only the legitimate healthcare provider or the patient himself can access the data through the Authentication Management service. Patients are not allowed to modify the data, whereas the healthcare staff can write, read, or modify. The patient's health record is divided into two parts, one of which is stored in the concerned health care department's system in local databases, and the other is stored in a cloud server database. This system's main problem is that if a hospital or a healthcare unit does not have its local EHR system, the whole data is stored on the cloud server.

Masud and Hossain [48] introduces a new methodology of storing medical records electronically in the cloud storage system. The suggested method takes care of data privacy using Shamir's Secret Sharing Mechanism. The EHR is categorized into multiple segments by the healthcare center. The segments are distributed equally to the cloud servers. Whenever any legitimate user wants to access the EHR, the healthcare center captures all segments from partial cloud servers to reconstruct the EHR. This method increases the efficiency of the EHR by outsourcing every patient's data, which can be reconstructed using cloud computing. The authors claim that they have introduced the novel concept of separation and reconstruction of EHR. The method's experiential and theoretical analysis suggests that it is a highly efficient and secure method of handling medical records electronically. The framework is not suitable to protect from intruders and unauthorized access of resources.

Shekha chenthara, [34] and a few other experts have surveyed, investigated, and reviewed various articles and identified multiple concerns in protecting E-healthcare. Some of them are EHR privacy, EHR security, and EHR cloud architecture. Authors also indicate that there is still a broad scope of research in EHR security.

Another approach in [49] discusses a data sharing and profile matching scheme for Mobile Healthcare Social Networks (MHSN) in cloud computing for EHR. The scheme allows the encryption of health records using an identity based encryption scheme. Not only this, attribute-based conditional data re-encryption can also be performed under this scheme. The scheme is claimed to be preventive against eavesdropping on sensitive data. A profile matching mechanism in MHSN based on identity-based encryption and an equality test helps achieve a very flexible and robust authorization. A trust negotiation based framework is proposed to provide authentication, sensitivity, and other access control services in healthcare systems [50–52]. Mutual disclosure of attributes to perform sensitive transactions is done using digital credentials. However, the technique is not able to protect E-healthcare system from all the prominent threats.

The authors in [53] emphasized the security aspects of the E-Healthcare systems especially access control mechanisms. The authors have declared that their scheme outperforms the traditional access control systems. The proposed access control model is based on the trust degree of the communicating parties. The degree of trust is evaluated based on user behavior. The user request is only granted when the degree of trust from both parties (from the user and service) is greater than or equal to the mutual trust threshold value. The author explains that the model ensures that only legitimate and trustful users can access medical records.

Table 1 provides a comprehensive comparison of various E-Healthcare security protocols. Table 1 elaborates the various vulnerabilities that could easily be exploited by attackers to conduct cyber-attacks on different medical devices. Additionally, the level of difficulty required to conduct a successful cyber-attack, the impact of cyber-attacks on medical devices, and the cyber awareness of stakeholders are also included in Table 1. Conclusively, it can be stated that most of the techniques discussed in the literature review section do not offer complete security in terms of identity anonymity, authenticity, confidentiality, and integrity of communications. Absentia of these security properties makes the traditional schemes inappropriate for the sensitive applications of e-healthcare. The inadequacies in the framework of existing schemes allow the adversaries to intrude and access unauthorized resources. Besides, the conventional schemes incur high computation and communication costs that result in precious resource deprivation of tiny smart nodes. Therefore, E-Healthcare applications need a robust authenticated key agreement scheme to protect the network from unauthorized abuses.

3 System model and adversary model

3.1 System model

The system model describes the relationship between admin, gateway (G_W), doctor, patient, and nurse. Figure 1 illustrates the process of accessing the medical records from the cloud by stakeholders via Gateway.

3.1.1 Admin

Admin is an IT in charge of the hospital who successfully registers the hospital with the cloud. The admin communicates securely with the cloud through the gateway by using a public key of the cloud. The cloud computes the master key of the hospital upon registration and returns this master key to the admin. Afterward, the admin creates various subkeys from the master key through KDF. Admin also performs the offline registration of the patient, doctor, and nurse's devices and issues the subkeys to them.

3.1.2 Doctor

A doctor is a person who takes care of the patients assigned to him for treatment. Ideally, only the associated doctor should access the information of the patient. This is achieved by matching the patient id (stored in the cloud) with the patient id requested by the doctor, and if the association exists, the request is permitted else denied. According to his treatment, the doctor has the right to both read and write/modify the patient's medical record. The doctor enters all the patient information and stores it in the cloud using encryption, hash, and subkey. Only the legitimate staff can access the information for reading. The doctor provides his two unique identity

Table 1 Comparison related work

Scheme	E-Healthcare	Security Concern	Difficulty	Awareness	Impact
[54]	A	I	S	L	S
[55]	B	II	M	L	L
[56]	C	III	S	L	S
[57]	D	IV	M	L	S
[58]	D	I	S	L	M
[59]	E	V	S	S	L
[60]	A	VI	S	M	M
[61]	A	VII	S	M	L
[62]	A	II	M	L	S

Acronyms: A: Radio Frequency Identification (RFID), B: Pacemaker, C: Internet Protocol (IP), D: Implantable Medical Devices (IMDs), E: Implantable Cardiac Defibrillators (ICDs), I: Authentication issues (AU), II: Radio attack (RA), III: Hijacking attack (HA), IV: Device cloning issue (DC), V: Electromagnetic interference (EI), VI: Unauthorized remote monitoring (URM), S: Substantial, M: Moderate L: Low

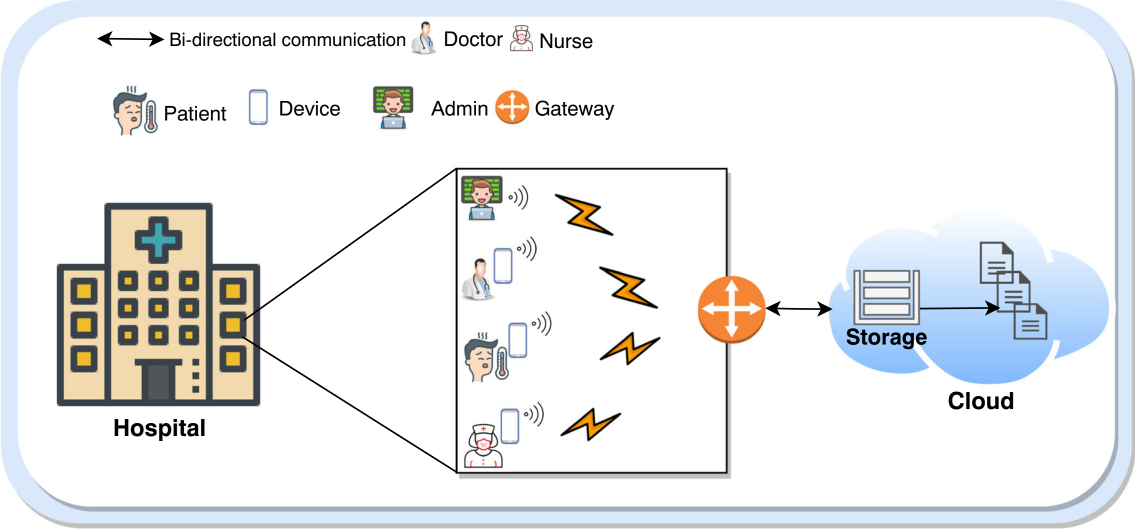


Fig. 1 Secure cloud based E-Healthcare system

numbers to the admin, UID_G and UID_H to the admin. The admin stores them in the cloud. Cloud returns a unique D_{ID} number. A doctor uses the secret subkey provided by the admin to communicate securely with the gateway.

3.1.3 Patient

The patient is the person who is admitted to the hospital for his diagnosis or checkup. According to his diagnosis, a particular doctor and nurse are assigned to take care of him in the hospital. The patient also provides the two unique identity numbers issued by the govt. (UID_G) and the hospital (UID_G), respectively to the admin. Admin receives both the ids and stores the same on the cloud. The cloud returns the unique patient id (P_{ID}) to the admin. A patient uses the secret subkey provided by the admin to communicate with the gateway securely. It is assumed that devices used by the stakeholders are resource constrained.

3.1.4 Nurse

A nurse is the caretaker of the patient after the doctor leaves. She uses her subkey S_K to securely get the information from the cloud via a gateway. In offline registration, the nurse provides her unique identity number issued by govt. (UID_G) and the hospital (UID_H). In return, the nurse gets the secret subkey S_K, issued by admin and N_{ID} issued by cloud. A nurse can only access the data of patients assigned to her by the healthcare department. A nurse can only read the data and can not change the data because she does not have access to modify or write the information in the patient's EHR. The nurse also uses her secret subkey provided by the admin to communicate with the gateway securely, and it is assumed that the user's devices are resource constrained.

3.1.5 Gateway

Gateway provides the interface to the doctor, patient, nurse, and admin to get connected to the cloud. The present system model is constructed considering the hospital's applications, where the Gateway is not resource-constrained. The Gateway receives full security credentials of doctor, patient, and nurse from the admin and provides a secure interface to access the records from the cloud. During the offline registration, the Gateway receives the master key M_K, subkeys S_K, and H_{ID} from the admin. Gateway secures the communication with different users like a doctor, nurse, and patient using various subkeys, whereas it uses the master key (M_K) for ciphering the communication between Gateway and cloud.

3.2 Adversary model

The adversarial nodes are deployed to hinder the routine operations of the network and its services. The authors have considered the Dolev-Yao (DY) adversary model to evaluate the proposed protocol's strength against malicious activities. As per the DY model, the adversary can eavesdrop on the messages exchanged between the user, gateway, and cloud. The attacker can capture the authentication messages while in transit from the user to the cloud and replay those messages to get unauthorized access to cloud services. The captured messages can also lead to the disclosure of secret credentials that the adversary may use later by the adversary to perform impersonation, known key, and man-in-the-middle attacks. Besides, the adversary can flood the cloud with redundant requests to launch a DoS attack. Therefore, it can be summarized that adversary has the power to disrupt the functioning of the network either temporarily or permanently.

4 Proposed secure access scheme

In the hospital environment, the staff's work life is very complicated as they have to do multi-tasking when it comes to handling and storing the patient's records, and it is a big challenge for every hospital. To solve their problem, we have proposed the scheme in which the medical records are stored in the cloud, which helps the hospital staff get relief from doing everything manually. Note that to run the proposed protocol, we have considered the following assumptions:

- The user device is a resource-constrained entity having limited storage and computation capabilities, whereas gateway and cloud are trusted entities with extensive computation and storage resources.
- All the entities (user device, gateway, and cloud) can execute the identical cryptography functions.
- The user can access the data only after the authentication at a cloud.

The cryptography function used to derive one or more secret keys from the master key is the Key Derivation Function (KDF). KDF can be used for stretching keys into longer key or to obtain the keys of the required format. KDF is an example of a pseudo-random function used for key derivation. KDF is used as DK = KDF (key, salt, iteration), DK is the derived key, KDF is the key derivation function, key is the original key, salt is the random number that acts as cryptographic salt, and iteration is the number of iterations of sub-function.

The proposed protocol has been implemented in four steps: a) Hospital registration phase, b) Offline registration phase, c) Information retrieval phase, and d) Information storage phase.

4.1 Hospital registration

Table 2 lists out the notations used throughout the paper. Figure 2 illustrates the hospital registration process with the cloud by the admin through the gateway. Admin generates the nonce (N_1) and concatenates the values R_{RN} || P_{RN} || H_{ID} || N_1 to form α. The message α is encrypted using PU_C to form β and the generated message (M_1) is sent to the gateway. Gateway receives the message β and generates the nonce N_2 which is encrypted using PU_C to generate γ. The encrypted message is concatenated with β to form δ and the generated message M_2 is sent to the cloud.

Table 2 Notations and descriptions

Notations	Description
K_{TG}, K_{TA}	Temporary key of gateway and Admin
R_{RN}, P_{RN}	Reference and Payment receipt number
PU_C, PR_C	Public and Private key of cloud
M_K, S_K	Master key and subkey
D_{ID}, P_{ID}, H_{ID}	doctor id, patient id, and Hospital id
K_{DF}, R_D	Key derivation function and Requested data
UID_G, UID_H	Unique id issued by govt. and hospital
D, E, N_n	Decryption, Encryption and Nonce
H, S_N, D_A	Hash, serial number and Data to be stored
$\|\|$, $\{M_n$, Sn, $K_n\}$	Concatenation operation, message number

The received message is decrypted with PR_C to compute ϵ followed by generation of nonce N_2. The cloud verifies the freshness of the nonce N_2. If N_2 is fresh, then the operation is continued else aborted. The cloud decrypts the message β with PR_C to compute F. Cloud also verifies the freshness of nonce N_1, if fresh then operation is carried on else canceled. The cloud verifies R_{RN} || P_{RN} || H_{ID}, if not found true then the process is aborted. The cloud now generates the master key M_K and nonces N_3, N_4. All values are concatenated H_{ID} || M_K || N_3 to compute G. Cloud also computes K_{TA} at this point by concatenating and hashing, H(R_{RN} || P_{RN} || H_{ID} || N_1).

The computed value G is encrypted with a key, K_{TA}. Using the hash function, K_{TG} is obtained (= H(N_2). The obtained key, K_{TG}, is used to encrypt the nonce N_4 to form L. The message L is concatenated with K and stored in M.

The message M is sent to the gateway. The gateway computes the K_{TG} by taking the hash of N_2. The message L is decrypted using K_{TG} to form R. The freshness of N_4 is checked if found true then the process recommences else it is stopped. Gateway sends the value K as the message M_4 to the admin. Admin computes the hash value of {R_{RN} || P_{RN} || H_{ID} || N_1} to generate K_{TA}. The received message K is decrypted with K_{TA} to generate Y. The freshness of nonce N_3 is checked at this stage, if found fresh, then the operation is returned to where it was left off. Finally, the admin is able to retrieve the master key (M_K) successfully. This master key is a secret key to securing the communications between the gateway and the cloud.

4.2 Offline registration

Figure 3 illustrates the offline registration process of devices. The admin records stakeholders' unique identity details, i.e., UID_G, UID_H. Gateway provides MAC address and the serial number S_N to admin as identity

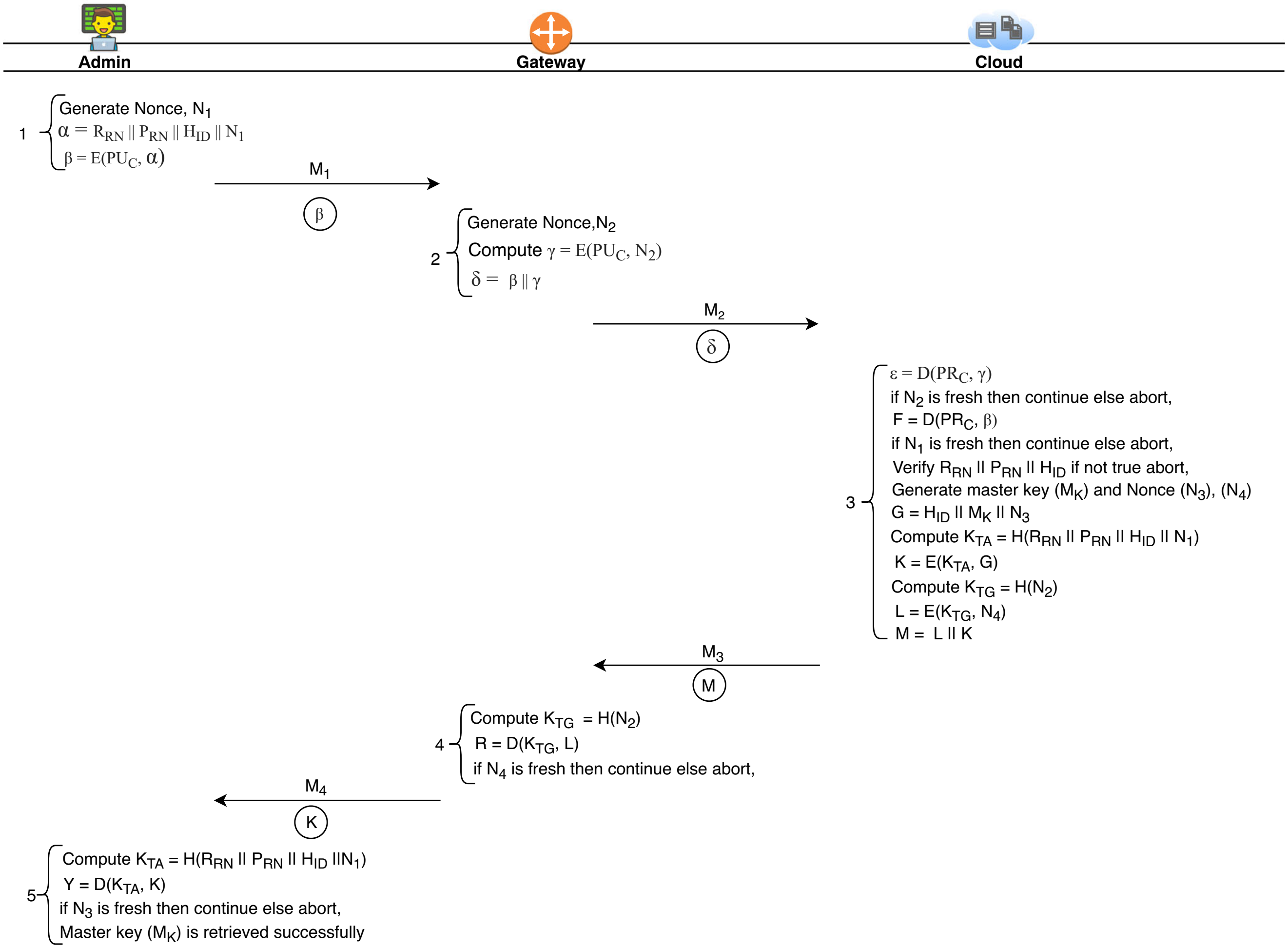

Admin
Gateway
Cloud
1
Generate Nonce, N_1
$\alpha = R_{RN} \| P_{RN} \| H_{ID} \| N_1$
$\beta = E(PU_C, \alpha)$
M_1
β
2
Generate Nonce,N_2
Compute $\gamma = E(PU_C, N_2)$
$\delta = \beta \| \gamma$
M_2
δ
3
$\varepsilon = D(PR_C, \gamma)$
if N_2 is fresh then continue else abort,
$F = D(PR_C, \beta)$
if N_1 is fresh then continue else abort,
Verify $R_{RN} \| P_{RN} \| H_{ID}$ if not true abort,
Generate master key (M_K) and Nonce (N_3), (N_4)
$G = H_{ID} \| M_K \| N_3$
Compute $K_{TA} = H(R_{RN} \| P_{RN} \| H_{ID} \| N_1)$
$K = E(K_{TA}, G)$
Compute $K_{TG} = H(N_2)$
$L = E(K_{TG}, N_4)$
$M = L \| K$
M_3
M
4
Compute $K_{TG} = H(N_2)$
$R = D(K_{TG}, L)$
if N_4 is fresh then continue else abort,
M_4
K
5
Compute $K_{TA} = H(R_{RN} \| P_{RN} \| H_{ID} \| N_1)$
$Y = D(K_{TA}, K)$
if N_3 is fresh then continue else abort,
Master key (M_K) is retrieved successfully

Fig. 2 Hospital registration at cloud

information. After recording the information, the admin stores the information in the cloud, and the cloud, in turn, generates the M_K and unique ids' for the doctor (D_{ID}), patient (P_{ID}) and nurse (N_{ID}) and provides it to admin. The admin makes use of KDF to derive multiple sub-keys (S_K) from securing communication between the gateway and other entities. The admin provides the identity details and unique secret sub-keys to users (doctor, patient, etc) whereas the gateway receives the M_K, S_K, D_{ID}, P_{ID}, N_{ID}, and H_{ID}. In the offline registration phase, the unique identifiers help the admin ensure that the patient's records' privacy is maintained. The admin gives the patient access to only those doctors and nurses who are treating that particular patient.

The proposed scheme enables the admin to choose stakeholders' access rights to the information stored in the cloud. Table 3 provides the default settings used by the administrator, where doctors treating the patient has been given rights to access and store the information. In contrast,

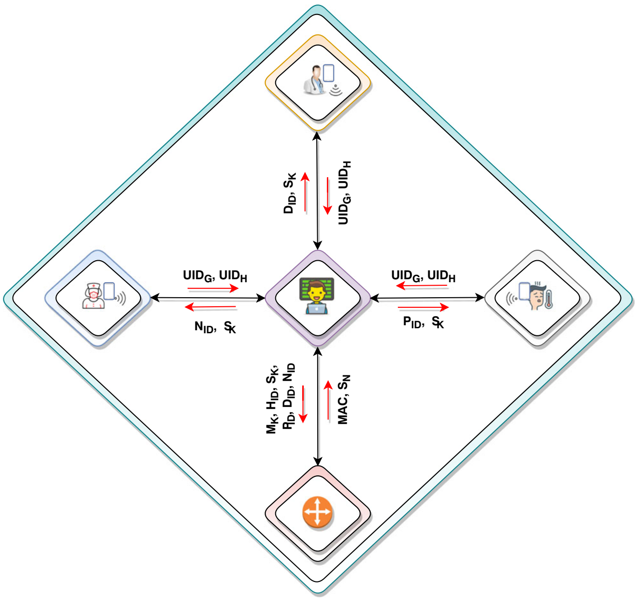


Fig. 3 Offline Registration of devices

Table 3 Distribution of access rights

Device	Read	Write
Doctor	✓	✓
Patient	✓	×
Nurse	✓	×

other stakeholders have been given the right to access the information only.

4.3 Information retrieval phase

In Fig. 4, the user (doctor) approaches the gateway to show interest in communication with the cloud. The device of the user (doctor) generates the nonce N_1 which is concatenated with D_{ID} and P_{ID} to compute ζ. The resulting message ζ is encrypted (S_K, ζ) to compute η. Using the hash function, H(D_{ID}) is computed and stored in O. η is concatenated with the message O to generate A. The user sends the value A as message S_1 to the gateway. D_{ID} is extracted from the database by the gateway, and its hash value is calculated and stored in B. The gateway compares B with O (B == O) to choose the appropriate subkey for decryption. Using the subkey S_K, η is decrypted to form θ. The gateway checks the freshness of nonce N_1, if it is fresh then operation is resumed else aborted. Gateway generates the nonce N_2 and concatenates it with all other values H_{ID} || D_{ID} || P_{ID} || N_2 and form μ. Then μ is encrypted with M_K to form λ. Now gateway sends message S_2 to cloud. After receiving the message cloud decrypts λ using M_K to give κ. If N_2 is fresh, then the operation is continued else aborted. The values H_{ID}, P_{ID}, D_{ID} are verified, if found not true then process is aborted. It is verified if P_{ID} belongs to D_{ID} or not, if it does then the operation is proceeded with further. Upon successful verification, nonce (N_3) and requested data (R_D) is generated which is concatenated with other values H_{ID} || P_{ID} || D_{ID} || R_D || N_3 to form ξ. The computed ξ is encrypted with M_K to generate π. Cloud sends message S_3 to the gateway. Gateway upon receiving the message, decrypts it D(M_K, π) to form ρ. Nonce N_3 is checked, if found fresh then operation is kept on else halted. Now gateway verifies H_{ID} and generates the nonce N_4. Next, σ is computed by concatenating all values D_{ID} || P_{ID} || R_D || N_4 and then σ is encrypted with S_K to form τ. Thereafter, gateway sends the message S_4 to user (doctor). After receiving the message, the user decrypts τ using S_K and computes υ. If nonce N_4 is fresh, only then operation is pursued further. Upon verification of the freshness, the user (doctor) is able to successfully retrieve the requested data, R_D.

4.4 Information storage phase

In Fig. 5, the user device (doctor) generates the Nonce N_1 and concatenates the all other values D_{ID} || P_{ID} || D_A || N_1 to generate ϕ. The value ϕ is encrypted with S_K to give χ. Using the hash function, H(D_{ID}) is computed and stored in Q. Now user concatenates the values χ || Q to form W. Next, the user sends the message K_1 to the gateway. D_{ID} is extracted from the database by the gateway and its hash value is calculated to form Z. Gateway compares, Z == Q for choosing the appropriate subkey for decryption. Next, gateway compute Ψ by decrypting the χ with S_K. Now gateway checks the freshness of the nonce N_1, if fresh then operation stays on else it is abandoned. Gateway generates the nonce N_2 which is concatenated with other values as H_{ID} || P_{ID} || D_{ID} || D_A || N_2 to generate ω. Next, ω gets encrypted using M_K and result is stored in $\sum$. Now gateway sends the message K_2 to cloud. Cloud decrypts the message $\sum$ using M_K to prepare Ω. Cloud evalutes the freshness of nonce N_2, if found fresh then operation is kept going else stopped right there. Cloud verifies the values H_{ID}, P_{ID}, D_{ID}, if not found true, then operation is aborted. Cloud checks if P_{ID} belongs to D_{ID} ($P_{ID} \in D_{ID}$), if result is false then operation is aborted. Cloud generates nonce N_3 and acknowledgment A, then concatenates with other values H_{ID} || D_{ID} || P_{ID} || A || N_3 to form $\forall$. Further cloud encrypts the $\forall$ with M_K to compute $\exists$. Now cloud sends the message K_3 to the gateway and gateway decrypts the message to form $\not\subset$ = D(M_K, $\exists$). Gateway checks the freshness of nonce N_3, if found fresh then operation is taken up again else process is aborted. Gateway verifies the value H_{ID} and generates the nonce N_4. Next, Gateway concatenates the values D_{ID}, P_{ID}, A, N_3 in order to form $\propto$. After this, the gateway encrypts the message $\propto$ with S_K and form $\notin$. Then gateway sends the message K_4 to user device (doctor). After receiving the message, the user decrypts the message $\emptyset = $ D(S_K, $\notin$). Further, the user device examines the freshness of nonce N_4, if found fresh, then the operation is carried forward else terminated. In the end, the user can retrieve the acknowledgment (A) successfully.

Similarly, the nurse and the patient can also use the proposed access model to securely access the cloud's information. We have shown only one instance, that of the doctor in the paper, since the process is identical for other stakeholders as well.

Table 4 demonstrates the computational cost of different entities (device, gateway, and cloud) in all phases: hospital registration, information retrieval, and information storage phase. It can be seen from the Table 4 that resource constrained nodes, i.e., user's device is only computing few crypto operations in each phase; thus the proposed scheme is suitable for all resource constrained devices and applications.

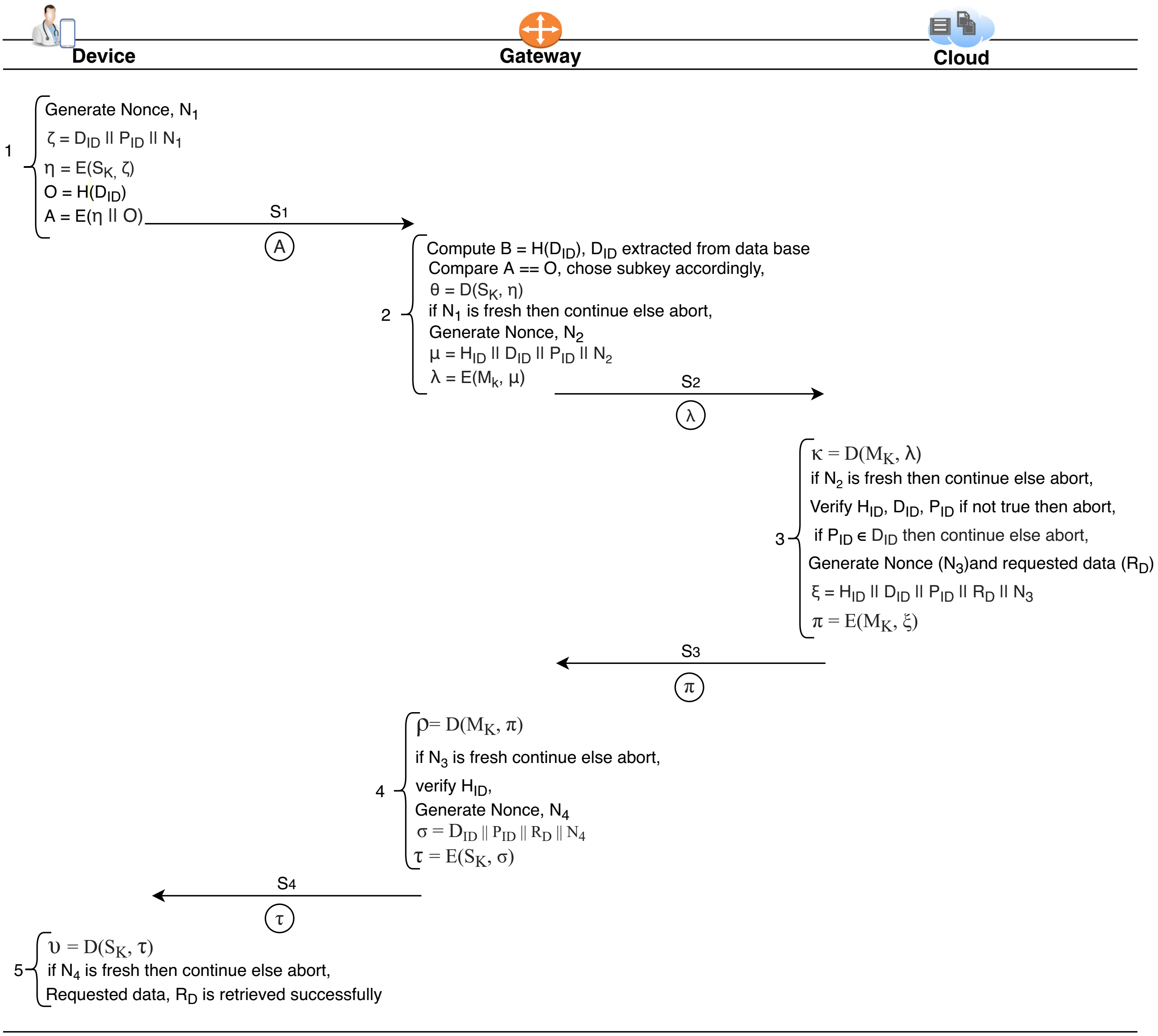

Device
Gateway
Cloud
1
Generate Nonce, N_1
$\zeta = D_{ID} \| P_{ID} \| N_1$
$\eta = E(S_{K,} \zeta)$
$O = H(D_{ID})$
$A = E(\eta \| O)$
S1
A
2
Compute $B = H(D_{ID})$, D_{ID} extracted from data base
Compare A == O, chose subkey accordingly,
$\theta = D(S_K, \eta)$
if N_1 is fresh then continue else abort,
Generate Nonce, N_2
$\mu = H_{ID} \| D_{ID} \| P_{ID} \| N_2$
$\lambda = E(M_k, \mu)$
S2
λ
3
$\kappa = D(M_K, \lambda)$
if N_2 is fresh then continue else abort,
Verify H_{ID}, D_{ID}, P_{ID} if not true then abort,
if $P_{ID} \in D_{ID}$ then continue else abort,
Generate Nonce (N_3)and requested data (R_D)
$\xi = H_{ID} \| D_{ID} \| P_{ID} \| R_D \| N_3$
$\pi = E(M_K, \xi)$
S3
π
4
$\rho = D(M_K, \pi)$
if N_3 is fresh continue else abort,
verify H_{ID},
Generate Nonce, N_4
$\sigma = D_{ID} \| P_{ID} \| R_D \| N_4$
$\tau = E(S_K, \sigma)$
S4
τ
5
$\upsilon = D(S_K, \tau)$
if N_4 is fresh then continue else abort,
Requested data, R_D is retrieved successfully

Fig. 4 Information retrieval phase

5 Security and comparative analysis

5.1 Formal analysis

We have used the 'Automated Validation of Internet Security Protocols and Applications (AVISPA)' tool to evaluate the proposed protocol's strength operating in a vulnerable environment. AVISPA uses four backends, namely, 'on-the-fly mode-checker (OFMC)', 'constraint-logic based attack searcher (CL-AtSe)', 'SAT (Boolean satisfiability problem) based model checker (SATMC),' and 'tree automata-based on automatic approximations for the analysis of security protocols (TA4SP) [8]. However, only OFMC and CL-AtSe are considered for the present evaluation; SATMC and TA4SP are excluded because they do not support few cryptography operations used in the algorithm [9]. The simulation requires the conversion of protocol code to the 'High-Level Protocol Specification Language (HLPSL)'. Afterward, the HLPSL script is transformed into 'Intermediate Format' (IF) for understanding by OFMC and CL-AtSe backends [63]. The script consists of agent descriptions, session information, intruder capabilities, security goals, and environment details. The interested readers can refer to [64] for detailed knowledge on AVISPA. The backends of AVISPA produces any of these outcomes: 'safe', 'unsafe',

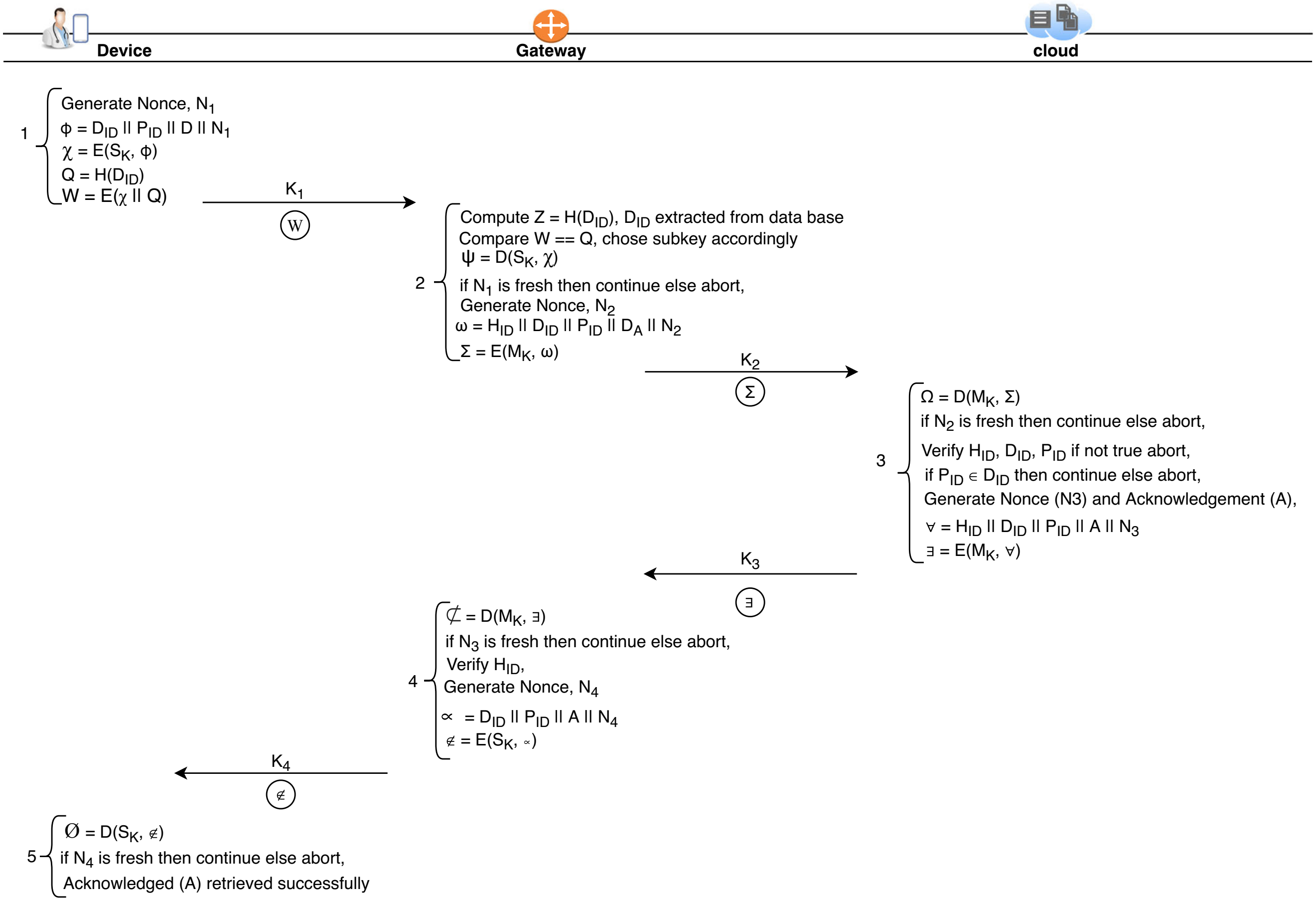

Device
Gateway
cloud
1
Generate Nonce, N1
ϕ = DID II PID II D II N1
χ = E(SK, ϕ)
Q = H(DID)
W = E(χ II Q)
K1
W
2
Compute Z = H(DID), DID extracted from data base
Compare W == Q, chose subkey accordingly
ψ = D(SK, χ)
if N1 is fresh then continue else abort,
Generate Nonce, N2
ω = HID II DID II PID II DA II N2
Σ = E(MK, ω)
K2
Σ
3
Ω = D(MK, Σ)
if N2 is fresh then continue else abort,
Verify HID, DID, PID if not true abort,
if PID ∈ DID then continue else abort,
Generate Nonce (N3) and Acknowledgement (A),
∀ = HID II DID II PID II A II N3
∃ = E(MK, ∀)
K3
∃
4
⊄ = D(MK, ∃)
if N3 is fresh then continue else abort,
Verify HID,
Generate Nonce, N4
∝ = DID II PID II A II N4
∉ = E(SK, ∝)
K4
∉
5
Ø = D(SK, ∉)
if N4 is fresh then continue else abort,
Acknowledged (A) retrieved successfully

Fig. 5 Information storage phase

and 'inconclusive'. Figure 6 demonstrates the robustness of the proposed protocol against various vulnerabilities. After many reiterations, it is concluded by AVISPA that the proposed protocol is safe to use for e-healthcare applications.

5.2 Informal analysis

The informal security analysis of our proposed scheme has been discussed in this sub-section.

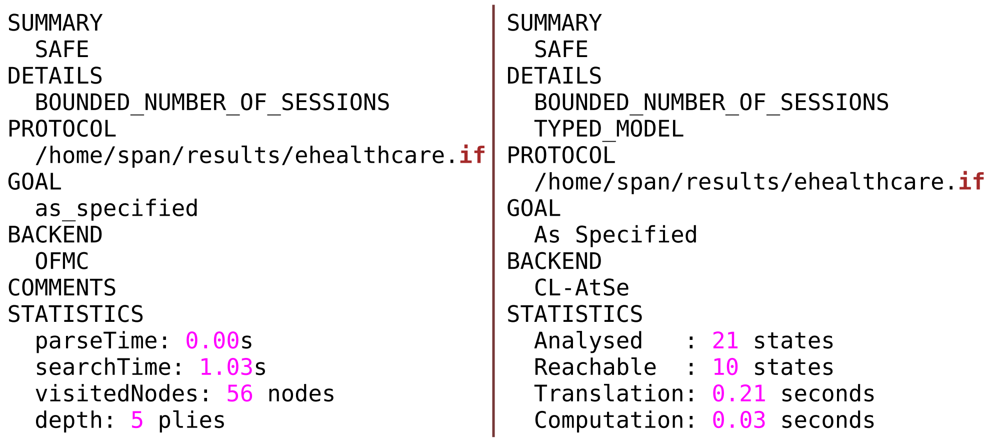
Theorem 1 *Resistant to replay attacks.*

Proof of Theorem 1 Freshness in each session is guaranteed as the messages (M_N, S_N, K_N) are composed of nonce N_1, N_2, N_3, N_4. Every entity verifies the freshness of the message by examining the nonce present in the message. For example, when gateway sends the encrypted message δ = E(β || γ) to cloud, it decrypts the message γ with PR_C to form ϵ. Further cloud verifies the freshness of nonce N_2, if found true, then operation goes on else it is closed. Assume that an attacker eavesdropped the message, δ = E(β || γ) and

Table 4 Computational cost of proposed protocol

	Phase 1	Phase 2	Phase 3
Device	$C_E + C_D + C_H$	$C_E + C_D + C_H$	$C_E + C_D + C_H$
Gateway	$C_E + C_D + C_H$	$2C_E + 2C_D + C_H$	$2C_E + 2C_D + C_H$
Cloud	$2C_E + 2C_D + C_H$	$C_E + C_D$	$C_E + C_D$
Total cost	$4C_E + 4C_D + 3C_H$	$4C_E + 4C_D + 2C_H$	$4C_E + 4C_D + 2C_H$

Acronyms: C: Computation, E: Encryption, D: Decryption, H: Hash, Phase 1: Hospital Registration, Phase 2: Information Retrieval, Phase 3: Information Storage



```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/results/ehealthcare.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.03s
  visitedNodes: 56 nodes
  depth: 5 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/results/ehealthcare.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed    : 21 states
  Reachable   : 10 states
  Translation: 0.21 seconds
  Computation: 0.03 seconds
```

Fig. 6 Robustness evaluation of proposed protocol using OFMC and CL-AtSe backend of AVISPA

it replays the same later to the cloud for getting unauthorized access. Since it contains the old nonce (N_2), the cloud discards the request and terminate the session. Furthermore, adversary cannot read and alter the nonce's (N_1, N_2, N_3, N_4) as messages M_1 and M_2 are ciphered with the public key of cloud whereas M_3 is encrypted with temporary key of gateway K_{TG}. Hence any alteration requires either the private key of the cloud or the secret temporary key of gateway unknown to the attacker. Similarly, other messages are protected. Thus, the proposed scheme is secured against replay attacks. □

Theorem 2 *Resistant to man in the middle (MITM) attack.*

Proof of Theorem 2 In a MITM attack, the adversary modifies the captured messages in such a way that the destination cannot differentiate the modified message from the original message. Assume an attacker performs MITM between the gateway and the cloud by capturing and modifying the message δ = E(β || γ). These computations are hard for the attacker due to the non-availability of the master key (M_K) required for deciphering the captured message. Therefore, the attacker fails to attempt a MITM attack between the gateway and the cloud. Similarly, other messages M_N, K_N, S_N, are also encrypted and hence cannot be modified. Therefore, the proposed scheme is protected from MITM attacks. □

Theorem 3 *Secure against modification attack.*

Proof of Theorem 3 Integrity is preserved due to the use of one way hash function (i.e., SHA). For example, the element O = hash (D_{ID}) guarantees prevention against modification attacks. Any form of alterations in O can be easily identified during reconstruction and hash comparison at other entities. Apart from one way hash functions, the

Table 5 Comparison of protocols based on security properties

Scheme	P_1	P_2	P_3	P_4	P_5
[14]	×	M	×	×	×
[17]	×	M	✓	✓	✓
[38]	×	M	✓	✓	✓
[42]	×	O_W	×	✓	✓
[65]	×	O_W	✓	✓	✓
[66]	×	O_W	✓	✓	✓
[67]	×	O_W	✓	✓	✓
[68]	×	O_W	×	×	✓
[69]	×	M	✓	✓	✓
[70]	×	O_W	✓	×	✓
[71]	×	O_W	✓	×	✓
P_S	✓	M	✓	✓	✓

Acronyms: M: Mutual, O_W: One Way, ✓: compliance to the security properties, ×: non compliance to the security properties, P_1: Anonymity, P_2: Authentication, P_3: Authorization, P_4: Confidentiality, P_5: Integrity, P_S: Proposed Scheme messages exchanged are encrypted to ensure the integrity of the communication. Let us assume that the attacker captures the message δ = E(β || γ), and tries to modify δ = E(β || γ)*. However, it is computationally difficult for the attacker to make any changes as the information is encrypted with the secret key. Neither the key nor the security credentials are ever shared in plain text over the unsecured medium. Therefore, the attacker does not find a way to modify the content. Similarly, other messages M_N, S_N, K_N are ciphered to prevent modifications. Thus, the proposed scheme is secure against modification attacks.

□

Theorem 4 *Proposed scheme exhibits data confidentiality.*

Proof of Theorem 4 Revealing information to unreliable entities can pose serious threats to the existence of any network. Let us assume that an attacker eavesdrops a message, γ = E(PU_C, N_2). Despite successful eavesdropping, the attacker would not be able to interpret the information due to the non-availability of the private key of Cloud, D($PR_C^?$, N_2). The Cloud has never shared its private key (PR_C) with anyone; therefore, the attacker remains unsuccessful in obtaining the information from the captured message. Similarly, the messages M_N, S_N, K_N are also encrypted. Therefore, the confidentiality of the information is ensured at all levels of communication. The attacker does not have these keys, PU_C, S_K, M_K. Thus the proposed scheme exhibits the security property of data confidentiality.

□

Theorem 5 *Proposed scheme exhibits Authorization of legitimate stakeholders.*

Proof of Theorem 5 The proposed cloud based e-healthcare system assigns a unique identity (D_{ID}, P_{ID}, etc.) to each stakeholder to classify the access level and the privileges assigned to each authorized entity. The proposed scheme allows only the authorized entities to communicate with the cloud. The admin during offline registration collects the identity details (UID_G, UID_H) of the legitimate users and stores it in the cloud. Cloud generates a unique identifier for every user (D_{ID}, P_{ID}, etc.) and shares it with the admin. Admin provides the unique identifier to each user during offline registration and the secret subkey (S_K). During the communication, a user has to append its hashed identity (e.g., H(D_{ID}) along with the message. The hashed identity is verified at the gateway (G_W) to prevent the flow of unauthorized abuses. Moreover, the communication is encrypted using the admin's secret subkey and shared securely during offline registration. Therefore, permitting the authorized entities to communicate with the gateway. The scheme offers two-step authenticity verification, i.e., gateway and cloud. Cloud upon reception of messages also verifies the details (H_{ID}, D_{ID}, P_{ID}, etc.). If the details do not match with the database, the request is aborted. Therefore, the proposed scheme only allows the authorized entities to read and write data in the cloud. □

5.3 Comparative analysis

The Table 5 depicts a clear comparison of old and the proposed protocols' security properties. It can be observed from the last row in the Table 5 that the proposed scheme attains all the significant security properties (e.g., confidentiality, integrity, authorization, authentication and anonymity). In contrast, none of the traditional approaches is able to attain all of them, as is evident from all the rows of the table except the last one. Non-achievement of all essential security properties by not even a single traditional scheme points out the possible vulnerabilities and increased possibility of attacks. Therefore, based on the investigation, the proposed scheme is found more superior in contrast to the conventional schemes.

6 Conclusions

Cloud based e-healthcare services are becoming increasingly popular due to the easy availability and mobility of the patient's medical records. Practices like telemedicine have become a reality due to the cost-effective solutions provided by cloud service vendors. Despite the benefits, the framework of storing and accessing the information through the cloud is highly vulnerable due to the use of open wireless channels. The proposed scheme provides a secure interface of access that only permits the legitimate entities (doctors, nurses, etc.) to store and access the patient's information. The scheme provides end-to-end encryption using multiple keys derived through KDF to preserve patient's sensitive information privacy. The hospital's burden of patient record keeping is eased, and the health records' access and storage are enhanced. Investigation reveals that the proposed scheme is lightweight and exhibits the must have security properties like confidentiality, integrity, authentication, freshness, etc. Security analysis revealed the scheme's robustness against various prominent attacks like message modification, MITMA, and replay, etc. The potential of the scheme for cloud based solutions is evident. However, the proposed scheme is not cost-effective for Low Power Wide Area Networks (LPWAN) using a local database. This is the future scope to enhance the scheme a cost-effective solution for LPWAN.

Acknowledgements The authors are grateful to the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, for funding this work through the Vice Deanship of Scientific Research Chairs: Research Chair of Pervasive and Mobile Computing.

References

1. Kruse CS, Mileski M, Vijaykumar AG, Viswanathan SV, Suskandla U, Chidambaram Y (2017) Impact of electronic health records on long-term care facilities: systematic review. JMIR Med Informa 5(3):e35
2. Hossain MS, Muhammad G (2018) Emotion-aware connected healthcare big data towards 5g. IEEE Internet of Things Journal 5(4):2399–2406
3. Zhang Y et al (2019) Edge intelligence in the cognitive internet of things: Improving sensitivity and interactivity. IEEE Netw 33(3):58–64
4. Azfar A, Choo K-KR, Liu L (2016) An android social app forensics adversary model. In: 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, pp 5597–5606
5. Ghoneim A, Muhammad G, Amin SU, Gupta B (2018) Medical image forgery detection for smart healthcare. IEEE Commun Mag 56(4):33–37
6. Gaba GS, Kumar G, Kim T-H, Monga H, Kumar P (2021) Secure device-to-device communications for 5g enabled internet of things applications. Comput Commun 169:114–128
7. Chen M et al (2018) Urban Healthcare Big Data System Based on Crowdsourced and Cloud-Based Air Quality Indicators. IEEE Commun Mag 56(11):14–20
8. Gaba GS, Kumar G, Monga H, Kim T-H, Liyanage M, Kumar P (2020) Robust and lightweight key exchange (lke) protocol for industry 4.0. IEEE Access 8:132808–132824
9. Choudhary K, Gaba GS, Butun I, Kumar P (2020) Make-it—a lightweight mutual authentication and key exchange protocol for industrial internet of things. Sensors 20(18):5166
10. Min W et al (2015) Cross-platform multi-modal topic modeling for personalized inter-platform recommendation. IEEE Trans Multimed 17(10):1787–1801
11. Stergiou CL, Psannis KE, Gupta B (2020) Iot-based big data secure management in the fog over a 6g wireless network. IEEE Internet of Things Journal
12. Zheng Q, Wang X, Khan MK, Zhang W, Gupta BB, Guo W (2017) A lightweight authenticated encryption scheme based on chaotic scml for railway cloud service. IEEE Access 6:711–722
13. Han K, Mun H, Shon T, Yeun CY, Park JJJH (2012) Secure and efficient public key management in next generation mobile networks. Pers Ubiquit Comput 16(6):677–685
14. Hiremath S, Yang G, Mankodiya K (2014) Wearable internet of things Concept, architectural components and promises for person-centered healthcare. In: 2014 4th international conference on wireless mobile communication and healthcare-transforming healthcare through innovations in mobile and wireless technologies (MOBIHEALTH). IEEE, pp 304–307
15. Alelaiwi A et al (2015) Enhanced engineering education using smart class environment. Comput Human Behav 51:852–856
16. Masud M et al (2012) Data interoperability and multimedia content management in e-health systems. IEEE Trans Inf Technol Biomed 16(6):1015–1023
17. Abbas A, Khan SU (2014) A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE J Biomed Health Inform 18(4):1431–1441
18. Hossain MS (2017) Cloud-supported cyber–physical localization framework for patients monitoring. IEEE Syst J 11(1):118–127
19. Masud M, Gaba GS, Alqahtani S, Muhammad G, Gupta BB, Kumar P, Ghoneim A (2020) A lightweight and robust secure key establishment protocol for internet of medical things in covid-19 patients care. IEEE Internet of Things Journal
20. Alhussein M et al (2018) Cognitive iot-cloud integration for smart healthcare: Case study for epileptic seizure detection and monitoring. Mobile Netw Appl 23:1624–1635
21. Hossain M. S., Muhammad G. (2016) Audio-visual emotion recognition using multi-directional regression and Ridgelet transform. J Multimodal User Interfaces 10:325–333
22. Amin SU et al (2019) Multilevel weighted feature fusion using convolutional neural networks for eeg motor imagery classification. IEEE Access 7:18940–18950
23. Al Osman H, Dong H, El Saddik A (2016) Ubiquitous biofeedback serious game for stress management. IEEE Access 4:1274–1286
24. AlOtaibi M, Tawalbeh Lo'ai A, Jararweh Y (2016) Integrated sensors system based on iot and mobile cloud computing. In: 2016 IEEE/ACS 13th international conference of computer systems and applications (AICCSA). IEEE, pp 1–5
25. Alhamid MF et al (2015) Towards context-sensitive collaborative media recommender system. Multimed Tools Appl 74(24):11399–11428
26. Atziori L, Iera A, Morabito G (2010) The internet of things: A survey computer networks
27. Lin K et al (2017) Green video transmission in the mobile cloud networks. IEEE Trans Circuits Sys Vid Technol 27(1):159–169
28. Kumar P, Gaba GS (2020) Biometric-based robust access control model for industrial internet of things applications. IoT Security: Advances in Authentication: 133–142
29. Alkeem EA, Shehada D, Yeun CY, Jamal Zemerly M, Hu J (2017) New secure healthcare system using cloud of things. Clust Comput 20(3):2211–2229
30. Alshehri S, Radziszowski SP, Raj RK (2012) Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In: 2012 IEEE 28th international conference on data engineering workshops. IEEE, pp 143–146
31. Azeez NA, Van der Vyver C (2019) Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal 20(2):97–108
32. Akter M, Gani A, Md OR, Hassan MM, Almogren A, Ahmad S (2018) Performance analysis of personal cloud storage services for mobile multimedia health record management. IEEE Access 6:52625–52638
33. Siddhartha V, Gaba GS, Kansal L (2020) A lightweight authentication protocol using implicit certificates for securing iot systems. Procedia Computer Science 167:85–96
34. Chenthara S, Ahmed K, Wang H, Whittaker F (2019) Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access 7:74361–74382
35. Prevention Centers for D. C. et al (2003) Hipaa privacy rule and public health. guidance from cdc and the us department of health and human services. MMWR: Morbidity and mortality weekly report 52(Suppl 1):1–17
36. Ghoneim A, Muhammad G, Amin SU, Gupta B (2018) Medical image forgery detection for smart healthcare. IEEE Commun Mag 56(4):33–37
37. McGraw D (2013) Building public trust in uses of health insurance portability and accountability act de-identified data. J Am Med Inform Assoc 20(1):29–34
38. Azfar A, Choo K-KR, Liu L (2015) Forensic taxonomy of popular android mhealth apps. arXiv:1505.02905
39. He D, Kumar N, Wang H, Wang L, Choo K-KR, Vinel A (2016) A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network. IEEE Trans Dependable Secure Comput 15(4):633–645

40. Muhammad G et al (2021) Eeg-based pathology detection for home health monitoring. IEEE J Sel Areas Commun 39(2):603–610
41. El-Latif AAA et al (2018) Secure quantum steganography protocol for fog cloud internet of things. IEEE Access 6:10332–10340
42. Huang Lu-Chou, Chu Huei-Chung, Lien Chung-Yueh, Hsiao Chia-Hung, Kao T (2009) Privacy preservation and information security protection for patients' portable electronic health records. Comput Biol Med 39(9):743–750
43. Al Hamid HA et al (2017) A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access 5:22313–22328
44. Alder S (2020) August 2020 healthcare data breach report
45. Boyinbode O, Cloudemr GT (2015) A cloud based electronic medical record system. Int J Hybrid Inf Technol 8(4): 201–212
46. Gorp PV, Comuzzi M (2013) Lifelong personal health data and application software via virtual machines in the cloud. IEEE J Biomed Health Inform 18(1):36–45
47. Hossain MS, Muhammad G (2014) Cloud-based collaborative media service framework for healthcare. Int J Distributed Sensor Netw 10(3):858712
48. Masud M, Hossain MS (2018) Secure data-exchange protocol in a cloud-based collaborative health care environment. Multimed Tools Appl 77(9):11121–11135
49. Huang Q, Yue W, He Y, Yang Y (2018) Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing. IEEE Access 6:36584–36594
50. Hossain MS, Muhammad G, Guizani N (2020) Explainable ai and mass surveillance system-based healthcare framework to combat covid-i9 like pandemics. IEEE Netw 34(4):126–132
51. Vawdrey DK, Sundelin TL, Seamons KE, Knutson CD (2003) Trust negotiation for authentication and authorization in healthcare information systems. In: Proceedings of the 25th annual international conference of the IEEE engineering in medicine and biology society (IEEE Cat. No. 03CH37439), vol 2. IEEE, pp 1406–1409
52. Hu L et al (2015) Software defined healthcare networks. IEEE Wirel Commun 22(6):67–75
53. Singh A, Chatterjee K (2017) A mutual trust based access control framework for securing electronic healthcare system. In: 2017 14th IEEE India council international conference (INDICON). IEEE, pp 1–6
54. Hatzivasilis G, Soultatos O, Ioannidis S, Verikoukis C, Demetriou G, Tsatsoulis C (2019) Review of security and privacy for the internet of medical things (iomt). In: 2019 15th international conference on distributed computing in sensor systems (DCOSS). IEEE, pp 457–464
55. Halperin D, Heydt-Benjamin TS, Fu K, Kohno T, Maisel WH (2008) Security and privacy for implantable medical devices. IEEE Pervasive Computing 7(1):30–39
56. Li C, Raghunathan A, Jha NK (2011) Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: 2011 IEEE 13th international conference on e-health networking, applications and services. IEEE, pp 150–156
57. Daniluk K, Niewiadomska-Szynkiewicz E (2012) Energy-efficient security in implantable medical devices. In: 2012 federated conference on computer science and information systems (FedCSIS). IEEE, pp 773–778
58. Camara C, Peris-Lopez P, Tapiador JE (2015) Security and privacy issues in implantable medical devices: A comprehensive survey. J Biomed Inform 55:272–289
59. Stachel JR, Sejdić E., Ogirala A, Mickle MH (2013) The impact of the internet of things on implanted medical devices including pacemakers, and icds. In: 2013 IEEE international instrumentation and measurement technology conference (I2MTC). IEEE, pp 839–844
60. Rajagopalan H, Rahmat-Samii Y (2010) On-body rfid tag design for human monitoring applications. In: 2010 IEEE antennas and propagation society international symposium. IEEE, pp 1–4
61. Kumar V et al (2015) Ontology based public healthcare system in internet of things (iot). Procedia Computer Science 50:99–102
62. Katagi M, Moriai S et al (2008) Lightweight cryptography for the internet of things. Sony Corporation 2008:7–10
63. Gaba GS, Kumar G, Monga H, Kim T-H, Kumar P (2020) Robust and lightweight mutual authentication scheme in distributed smart environments. IEEE Access 8:69722–69733
64. Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuéllar J, Drielsma PH, Héam P-C, Kouchnarenko O, Mantovani J, et al. (2005) The avispa tool for the automated validation of internet security protocols and applications. In: International conference on computer aided verification. Springer, pp 281–285
65. Al Ameen MA, Liu J, Kwak K (2012) Security and privacy issues in wireless sensor networks for healthcare applications. J Med Sys 36(1):93–101
66. Do Q, Martini B, Choo K-KR (2015) Exfiltrating data from android devices. Computers & Security 48:74–91
67. D'Orazio CJ, Lu R, Choo K-KR, Vasilakos AV (2017) A markov adversary model to detect vulnerable ios devices and vulnerabilities in ios apps. Appl Math Comput 293:523–544
68. Appari A, Johnson ME (2010) Information security and privacy in healthcare: current state of research. International Journal Of Internet and Enterprise Management 6(4):279–314
69. Toninelli A, Montanari R, Corradi A (2009) Enabling secure service discovery in mobile healthcare enterprise networks. IEEE Wireless Commun 16(3):24–32
70. Castillejo P, Martínez J-F, López L, Rubio G (2013) An internet of things approach for managing smart services provided by wearable devices. Int J Distrib Sensor Netw 9(2):190813
71. Bui N, Zorzi M (2011) Health care applications: a solution based on the internet of things. In: Proceedings of the 4th international symposium on applied sciences in biomedical and communication technologies, pp 1–5

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Affiliations

Mehedi Masud[1] · Gurjot Singh Gaba[2] · Karanjeet Choudhary[2] · Roobaea Alroobaea[1] · M. Shamim Hossain[3]

Mehedi Masud
mmasud@tu.edu.sa

Gurjot Singh Gaba
gurjot.17023@lpu.co.in

Karanjeet Choudhar
karanchoudhary8399@gmail.com

Roobaea Alroobaea
r.robai@tu.edu.sa

[1] Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia

[2] School of Electronics and Electrical Engineering, Lovely Professional University, Punjab 144411, India

[3] Research Chair of Pervasive and Mobile Computing, and Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia