Lightweight Authentication Protocol For Smart Healthcare

Saja A. Hussein[1], Issa Ahmed Abed[2] , Zaid Alaa Hussien[3]
{saja.abhadli5@gmail.com[1], issaahmedabed@stu.edu.iq[2], zaid.alaa@stu.edu.iq[3]}

Basrah Engineering Technical College, Southern Technical University, Iraq[1,2],
Management Technical College Basrah, Southern Technical University, Iraq[3]

Abstract. The application of modern technology to human health, is a hot research subject, especially in medical technology. In developing countries, the Telecare Medicine Information System (TMIS) is widely used in smart healthcare systems, allowing a physician to obtain patient-related information from a distance. The privacy of such data has been identified as a prominent obstacle to the widespread development of IoT. Because of the importance of this data, it must be transmitted between the patient and the cloud server. So, we proposed a lightweight and fast protocol to ensure data access and also, to prevent attackers from generating fake data, and we have proven that this protocol is more secure.

Keywords: Authentication, Lightweight, Smart Healthcare, IoT, Cloud.

1 Introduction

The availability and exchange of knowledge around the spectrum of medical care is a major problem for healthcare organizations. since healthcare data is usually distributed through multiple health systems in a bunch of locations. Many of these systems do not joint with one another, allowing data to remain separate inside silos. This anti-pattern results in clinical care knowledge shortages, data access inefficiencies, and increased costs for healthcare organizations. Data isolation is a major problem for healthcare organizations, as it prevents them from taking advantage of the latest IT technologies, such as cloud computing's data processing and analytics capabilities, which can help optimize treatment while lowering costs. Modern IT systems areto an increasing extent taking over cloud computing and transferring their workloads to the cloud to gain economic advantages, of scale, energy consumption, scalability, and elasticity[1]. The Popularity of long-term in-home smart healthcare Monitoring Systems has resulted from the aging population and the prevalence of chronic diseases[2]. In addition to the Coronavirus at present. Intelligent health monitoring IoT devices, such as ECG, blood pressure bands, pulse oximeters, and other devices, can capture health data and provide direct input to patients and hospitals, either as an alert of imminent medical emergencies or as a monitoring aid during workouts, thanks to the rapid advancement of sensing technology[3]. Patients use a variety of medical IoT devices to keep track of their health. The details received (personal health records) would be sent back to hospitals for diagnosis and prompt responses. However, since the tracked health data contains

IMDC-IST 2021, September 07-09, Sakarya, Turkey

DOI 10.4108/eai.7-9-2021.2314798

personal information, there are significant protection and privacy breaches in terms of data privacy and identity authentication. As a result, the data must be well secured against unauthorized access[4]. A protected user authentication strategy is built around two or three main security components:(1) any information that is only identified by the user (e.g. passwords and PIN codes),(2) a physical entity, token, that is only held by the user (e.g. smart card and smart device), and(3) a physical attribute that reflects the user's specific biometrics (e.g. fingerprint)[5]. Several security protocols, such as authentication and access control protocols, that use public-key cryptographic systems have recently been proposed to improve privacy and security in the healthcare setting. As an example, Shehzad et al.[6] in 2017 proposed a protocol that is powerful enough to defend against all types of attacks, especially stolen smart devices and patient anonymity violations. Azad et al.[7] In 2020 proposed a scheme for a SIP-based next-generation network that relies on a low-entropy mutual password rather than a Public-Key Infrastructure PKI or a trusted third-party mechanism. Zahid et al.[8] 2019 proposed biometrics-based authentication and key agreement protocols for E-Health Services that are reliable and efficient. Tan et al.[9] 2017 proposed a scheme By combining biometrics, hash function operations, and an effective smart card-based password authentication. As healthcare systems can not afford high communication and computation overheads, authentication schemes should be as cost and transmission-efficient as possible while also maintaining high security. and this weakness was observed in previous protocols. As a result, we proposed in this paper a scheme that is more lightweight and secure against attacks by using a one-way-hash that cannot be decrypted, and we demonstrated the proposed scheme is lightweight, resulting in low communication and computation overheads.

2 System Model

The components of the proposed system are depicted in Fig 1. The main components can be classified into two categories, as seen in the figure: patients, and cloud server, and that will physicians/doctors connected with. The patients are supposed to be equipped with different sensors and monitors that record the physiological parameter values in real-time, like as heart rate and temperature, and so on. The data is then transmitted to the doctor through the open channel through a cloud server. This aids in the distance check of symptoms, the provision of online and without-complications care to patients. even so, the physiological data of patients is extremely important and can easily be compromised when transmitted through the internet. As a result, this paper introduces a practical mutual authentication scheme for establishing safe and trustworthy two-way communication between patients and medical servers. A patient's personality is defined by coded values. Nevertheless, these parameters can not be derived from transmitted messages because they are sent in a secret structure over the channel, All of this at a low cost of communication and computation overhead.

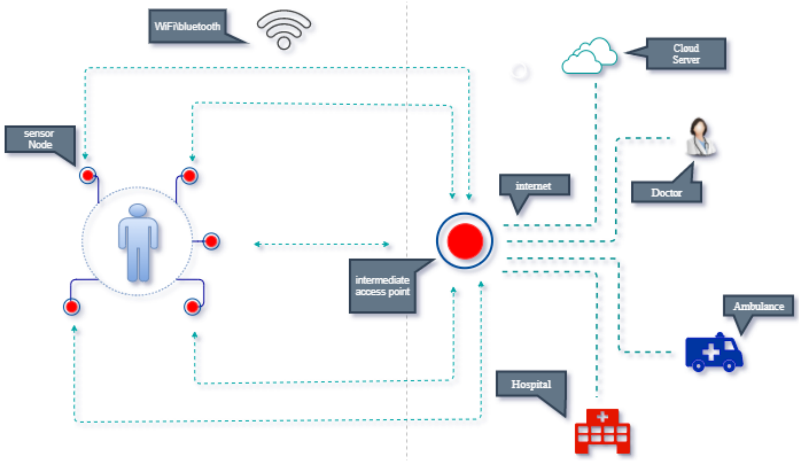
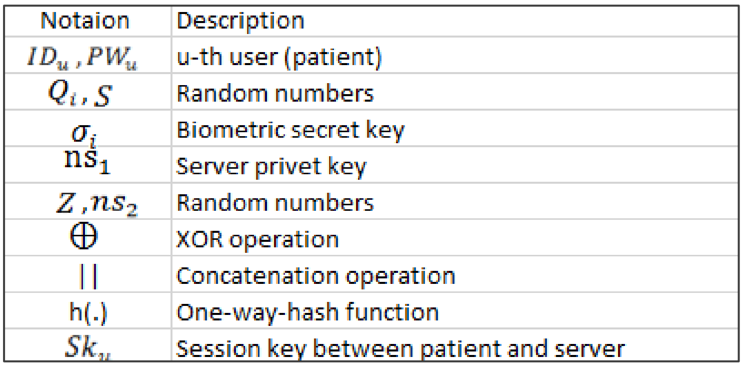


Fig 1. The components of the smart healthcare system.

3 Proposed Protocol

The authentication of the proposed protocol is divided into three different sections: A) Registration, B) login and C) Authentication. This section contains extensive details about these phases, which are as follows, **Table1.** represents the notations of the proposed protocol.

Table 1. Notations and their Description.



Notaion	Description
ID_u , PW_u	u-th user (patient)
Q_i , S	Random numbers
σ_i	Biometric secret key
ns_1	Server privet key
Z , ns_2	Random numbers
$\oplus$	XOR operation
||	Concatenation operation
h(.)	One-way-hash function
Sk_u	Session key between patient and server

3.1 Registration Phase

Throughout these steps, the patient uses the safe channel to register with the cloud server. Step 1. The Patient select an identity ID_u, password PW_u and scan (his or her) biometrics B_u (for example, fingerprint, and so on) on a smart device, and this SD will generate a random number Q_i. Then it will compute pseudo-identity and password respectively.

$$PID_i = h(ID_u \parallel Q_i) \tag{1}$$

$$HPW_i = h(PW_u \parallel Q_i) \tag{2}$$

After selected Biometric secret key σ_i then compute

$$X_i = h(B_u \parallel \sigma_i) \tag{3}$$

And this step will be finished with sending the message include the pseudo-identity and password < PID_i, HPW_i> through a protected channel to the cloud server.

Step 2. When the cloud server is received the data include the registration request, then it's start compute

$$R_i = h(PID_i \parallel ns_1) \tag{4}$$

After the server secret key ns_1 is generated, and compute

$$g_i = R_i \oplus HPW_i \tag{5}$$

$$D_i = h(HPW_i \| PID_i \| R_i) \tag{6}$$

The server generates a random number S to compute

$$m_i = h(S \| ns_1) \oplus PID_i \tag{7}$$

Then store $< m_i, g_i, D_i, h(.) >$ in its database and send these values to the patient through a secure channel.

Step 3. On the patient side after it's received the values from the server, then start to compute

$$W_i = Q_i \oplus h(ID_u \parallel PW_u) \tag{8}$$

$$E_i = \sigma_i \oplus h(HPW_i \parallel PID_i) \tag{9}$$

and then store these values in the smart device, finally, the content of it will be $< W_i, m_i, g_i, X_i, D_i, E_i, h(.) >$. The sequence of steps performed by the cloud server and the patient is depicted in Fig 2.

3.2 Login Phase

Step 1. In this phase, the patient will insert (his or her) own parameters ID_u, PW_u, into the smart device and then imprints the biometric B_u in the same smart device. After that compute

$$Q_i^* = W_i \oplus h(ID_u \| PW_u) \tag{10}$$

$$HPW_i = h(PW_u \| Q_i^*) \tag{11}$$

$$PID_i = h(ID_u \parallel Q_i^*) \tag{12}$$

$$\sigma_i' = E_i \oplus h(HPW_i \parallel PID_i) \tag{13}$$

then compute

$$X_i' = h(B_u^* \parallel \sigma_i) \tag{14}$$

and check if

$$X_i' = X_i \tag{15}$$

Then the verification is passed and proceeds to the next steps. Else, try again to enter the parameters for two more attempts only, and after three failed attempts, the login will stop. When the condition is true then compute

$$R_i = g_i \oplus HPW_i \tag{16}$$

$$D_i' = h(HPW_i \parallel PID_i \parallel R_i) \tag{17}$$

and check if

$$D_i' = D_i \tag{18}$$

that's mean the pseudo-identity and password are each correct otherwise server terminates the session.

Step 2. The smart device will generate Z as a random number and calculates

$$L{=}m_i \oplus PID_i = h(S \| ns_1) \tag{19}$$

$$M_1 = h(R_i \| L \| PID_i) \tag{20}$$

$$M_2 = h(M_1 \| D_i \| t_1) \oplus Z \tag{21}$$

at the end of this step login request will send to the server content these values $< PID_i, M_1, M_2, t_1 >$.

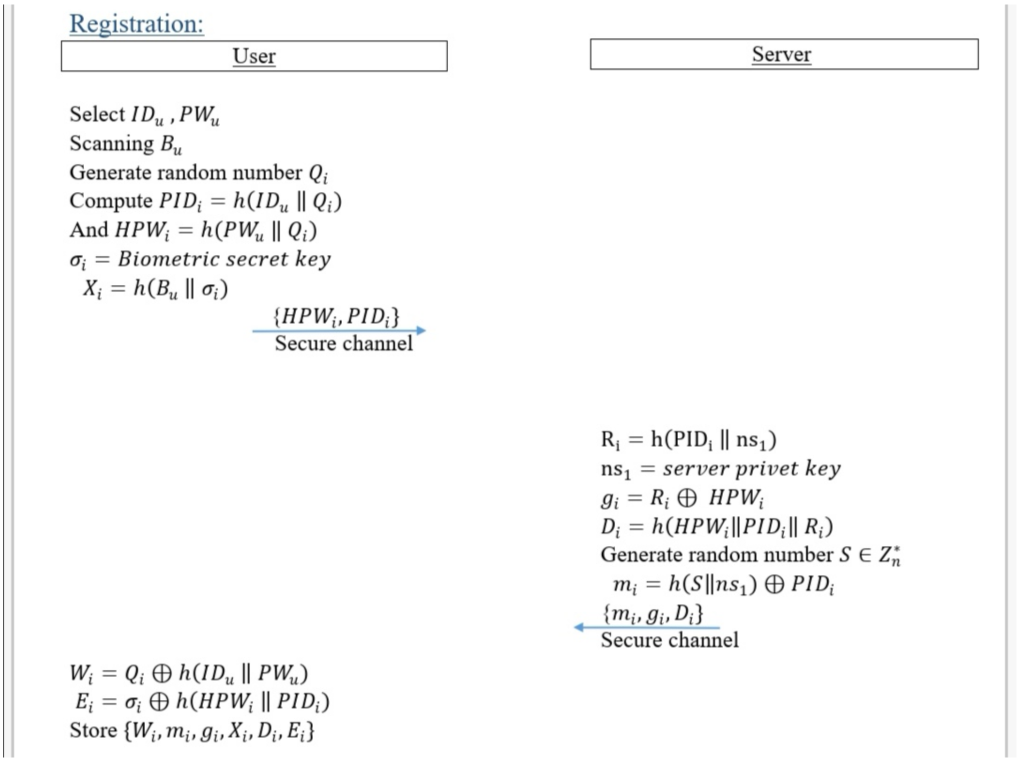
3.3 Authentication Phase

Step 3. As the server receives the request message from the Patient, it checks the authenticity of the time stamp, if $t_2 - t_1 > \Delta t$ that's mean is the timestamp that has not expired then the server will calculate

$$R_i' = h(PID_i \| ns_1) \tag{22}$$

$$L1{=}m_i \oplus PID_i \tag{23}$$

$$M_1' = h(R_i' \| L1 \| PID_i) \tag{24}$$



Registration:

User

Server

Select ID_u , PW_u

Scanning B_u

Generate random number Q_i

Compute $PID_i = h(ID_u \parallel Q_i)$

And $HPW_i = h(PW_u \parallel Q_i)$

$\sigma_i = Biometric\ secret\ key$

$X_i = h(B_u \parallel \sigma_i)$

$\{HPW_i, PID_i\}$

Secure channel

$\mathrm{R_i = h(PID_i \parallel ns_1)}$

$\mathrm{ns_1} = server\ privet\ key$

$g_i = R_i \oplus HPW_i$

$D_i = h(HPW_i \| PID_i \| R_i)$

Generate random number $S \in Z_n^*$

$m_i = h(S \| ns_1) \oplus PID_i$

$\{m_i, g_i, D_i\}$

Secure channel

$W_i = Q_i \oplus h(ID_u \parallel PW_u)$

$E_i = \sigma_i \oplus h(HPW_i \parallel PID_i)$

Store $\{W_i, m_i, g_i, X_i, D_i, E_i\}$

Fig 2. The registration phase for the proposed scheme.

and check if

$$M_1' = M_1 \tag{25}$$

then server generates a random number $ns_2 \in Z_n^*$ and compute

$$M_4 = ns_2 \oplus h(R_i' \| L1 \| PID_i) \tag{26}$$

$$M_5 = h(ns_2 \| R_i' \| L1 \| PID_i \| Z \| t_3) \tag{27}$$

After that server will send a message that contains the values $< M_4, M_5, t_3 >$ to the Patient. Otherwise, the session will terminate by the server.

Step 4. On the Patient side, it will get a time-stamp t_3 as well as checking the time interval; if $t_4 - t_3 > \Delta t$ and the session will terminate by the Patient if that condition is not verified, then calculate

$$ns_2' = M_4 \oplus h(R_i \| L \| PID_i) \tag{28}$$

$$M_5' = h(ns_2' \| R_i \| L \| PID_i \| Z \| t_3) \tag{29}$$

and then check if

$$M_5 = M_5' \tag{30}$$

then finally calculate the session key

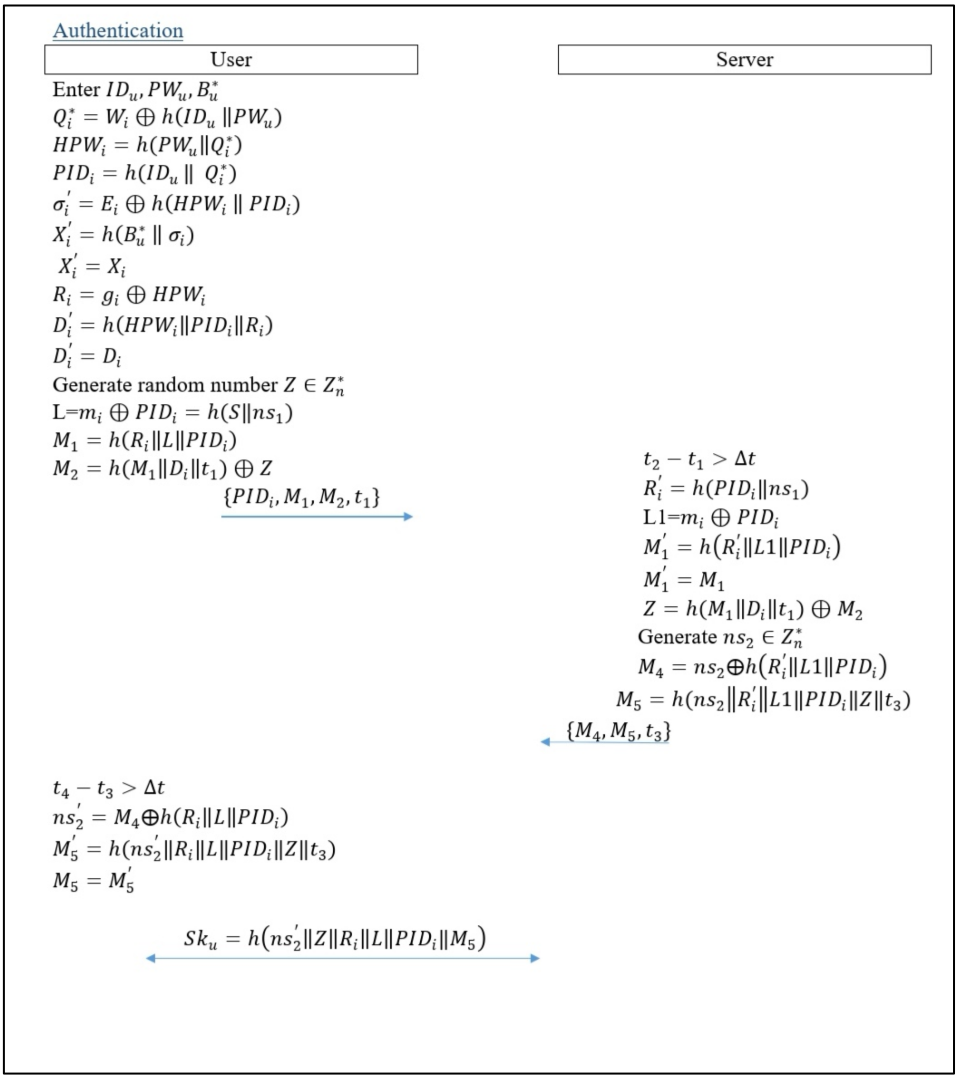
$$Sk_u = h(ns_2' \| Z \| R_i \| L \| PID_i \| M_5) \tag{31}$$

Else, the session will terminate by the Patient. The last two phases are shown as under in Fig 3.

4 Security Analysis

This checklist of security systems covers different security attacks as well as advantageous security properties, and it is generally used in the documentation of multi-factor user authentication as a valuation criteria, as shown in Table 2.

1. Offline Guessing The Password Attack: Over the unreliable channel, the password of patient PW_u and identity ID_u are never conveyed in plain text. Furthermore, the one-way hash functions and concatenation operations are secure the Patient's password, identity, and biometric that are a part of the components of the saved parameter $\{W_i, m_i, g_i, X_i, D_i, E_i\}$. Therefore, the attacker would be unable to reverse it and know the password. As a result, the proposed protocol is resistant to guessing the password.
2. Stolen Smart device Attack: Assume that the Adversary will steal the patient's smart device and retrieve the data stored on it $\{W_i, m_i, g_i, X_i, D_i, E_i\}$. Even in this case, Adversary is unable to retrieve the Patient's credentials password PW_u and identity D_u. Since the password is concealed throughout the values are stored in a smart device, that is secured using one-way hash functions, As a result, Adversary would not be able to retrieve the Patient's credentials in a polynomial amount of time



Enter ID_u, PW_u, B_u^*

$Q_i^* = W_i \oplus h(ID_u \| PW_u)$

$HPW_i = h(PW_u \| Q_i^*)$

$PID_i = h(ID_u \| Q_i^*)$

$\sigma_i^{'} = E_i \oplus h(HPW_i \| PID_i)$

$X_i^{'} = h(B_u^* \| \sigma_i)$

$X_i^{'} = X_i$

$R_i = g_i \oplus HPW_i$

$D_i^{'} = h(HPW_i \| PID_i \| R_i)$

$D_i^{'} = D_i$

Generate random number $Z \in Z_n^*$

L=$m_i \oplus PID_i = h(S \| ns_1)$

$M_1 = h(R_i \| L \| PID_i)$

$M_2 = h(M_1 \| D_i \| t_1) \oplus Z$

$\{PID_i, M_1, M_2, t_1\}$

$t_2 - t_1 > \Delta t$

$R_i^{'} = h(PID_i \| ns_1)$

L1=$m_i \oplus PID_i$

$M_1^{'} = h\left(R_i^{'} \| L1 \| PID_i\right)$

$M_1^{'} = M_1$

$Z = h(M_1 \| D_i \| t_1) \oplus M_2$

Generate $ns_2 \in Z_n^*$

$M_4 = ns_2 \oplus h\left(R_i^{'} \| L1 \| PID_i\right)$

$M_5 = h(ns_2 \| R_i^{'} \| L1 \| PID_i \| Z \| t_3)$

$\{M_4, M_5, t_3\}$

$t_4 - t_3 > \Delta t$

$ns_2^{'} = M_4 \oplus h(R_i \| L \| PID_i)$

$M_5^{'} = h(ns_2^{'} \| R_i \| L \| PID_i \| Z \| t_3)$

$M_5 = M_5^{'}$

$Sk_u = h\left(ns_2^{'} \| Z \| R_i \| L \| PID_i \| M_5\right)$

Fig 3. Login and Authentication phase for the proposed scheme.

3. Replay Attack: Replay attacks can resist the proposed protocol and ignore the data that have been replayed, and it guarantees this via the strength of random numbers and timestamps. To verify the novelty of the messages received, Time-stamps (t_1, t_3) are used.

4. Impersonation Attack: The protocol is designed to withstand imitation threats on both the Patient and the cloud server. An adversary will failure to vary the transmitted messages. The reason

for this is that median tokens require either the cloud server's or the patient's private key information. The intermediate tokens cannot be modified to impersonate the Patient's and server's identities without these values.

5. Privileged Insider Attack: At the registration process, and through the protected channel important information is transmitted from the patient side. Meanwhile, the Patient and the cloud server communication may intercept. even so, the intercepted information cannot be used to decipher the patient's identity (PID_i) and password (HPW_i) pseudo values. for the reason that The Adversary does not have access to the server's private key, nor does he have access to the random numbers.$\mathrm{ns}_1$and ns_2 respectively.

6. Temporary Information Attack on Known Session: Assume that the Adversary obtains information about the random numbers (ns_2 , Z) used during the processing of session keys (Sk_u). Although these numbers are available, Adversary cannot calculate the Sk_u unless knowing R_i , PID_i and L.

7. Perfect Forward Secrecy: With the impossibility of accessing the session keys unless the private key is known, perfect forward secrecy will ensure.

8. Maintains Patient Anonymity: The contact between the cloud server and the patient is grounded on the parameters (ID_u,PW_u and B_u). A Patient's personality is defined by the mixture of these values. nevertheless, these parameters cannot be derived from transmitted messages since they are sent in a secret structure over the channel.

9. Resistance to Denial of Service attacks: At each point of the protocol, timestamps and different tokens are used to validate received messages. As a result, the Adversary is unable to deceive the legitimate parties and consume their resources.

10. Mutual authentication: On receiving the request message, $\{PID_i, M_1, M_2, t_1\}$ the server authenticates the Patient side in the proposed protocol. When validating the t_1 timestamp and comparing the Eq. (24) with Eq. (20) $M_1' = h(R_i'\|L1\|PID_i) = M_1$. Also, the server returns a message $\{M_4, M_5, t_3\}$ to patient. Similarly, It validates the newness of the t_3 and Eq.(29) with Eq.(27) $M_5' = h(ns_2'\|R_i\|L\|PID_i\|Z\|t_3) = M_5$ The authentication will be done if all values are identical. As a result, the current protocol achieves mutual authentication.

11. stolen verifier attacks: In the server database, the proposed scheme would not construct or save a verifier table. However, On the cloud server-side, the proposed protocol does not store a verification table, However, also an adversary with entry to the database server would be unable to verifiers the Patient analyses data.

12. man-in-the-middle attack: Mutual authentication between the Patient and the server is provided by the proposed scheme. The parameter in Eq. (20) $M_1 = h(R_i\|L\|PID_i)$ is used to authenticate the Patient. On the other side, the patient authenticates the server using Eq. (27) $M_5 = h(ns_2'\|R_i\|L\|PID_i\|Z\|t_3\ )To$ compute M_1 and M_5, the adversary on both sides requires $\mathrm{R_i}$ or the secret key ns_1. As a result, no adversary can be both a cloud server and a patient. Also, the session key computation Eq.(31) $Sk_u = h(ns_2'\|Z\|R_i\|L\|PID_i\|M_5)$ which needs the secret parameter of a patient $\mathrm{R_i}$ in addition to the random numbers (ns_2 , Z) provided by each participating server and Patient. Any attacker behaving like a man in the middle would be unable to have these random numbers. As a result, the proposed scheme is highly resistant to MitM attacks. We reviewed the potential attacks and compared them between our protocol and other protocols, and the next table shows that.

Table 2. Security parameters comparison.

	proposed	[9]	[8]	[10]
Offline Password Guessing Attack	✓	✗	✓	✗
Stolen Smart device Attack	✓	✗	✓	✓
Replay Attack	✓	✓	✓	✓
Impersonation Attack	✓	✓	✓	✓
Privileged Insider Attack	✓	✓	✓	✗
Temporary Information Attack on Known Session	✓	✓	✓	✗
Perfect Forward Secrecy	✓	✗	✓	✗
Maintains Patient Anonymity	✓	✗	✓	✓
Resistance to Denial of Service (DoS) attacks	✓	✓	✓	✗
Mutual Authentication	✓	✗	✓	✓
Stolen Verifier Attacks	✓	✗	✓	✓
Man-In-The-Middle Attack	✓	✗	✓	✗

5 Performance Analysis

- The comparison of the proposed protocol has been accurate with current modern protocols such as [8],_and [9], not just for performance but also for computation and communication. The following are the notations that are involved:
  t_h : secure one-way hash function for Computation cost
  t_E : symmetric encryption/decryption for Computation cost

The following is the computational cost from the above processes, according to the experimental results. Tan et al.[9] scheme takes $4t_h$ at operations carried out during registration and $12t_h + 2t_E$ at operations carried out during authentication, Zahid et al.[8] performs $4t_h + 1t_E$ and $15t_h + 2t_E$ for registration and authentication processes respectively, Kisung et al.[10] needs the computation cost $20t_h$ for both registration and authentication phases and that takes around $0{:}\,08\ ms$. In our scheme, Assume that executing a hash function t_h takes around $0{:}\,004\ ms$ and symmetric encryption/decryption t_E takes around $0{:}\,008\,ms$. **Table 3.** shows that the comparison of the result between the proposed protocol to recent related protocols [9] and [8]. The Table demonstrates that the protocol of Zahid et al has around 36% in contrast to the proposed protocol, there is an additional overhead, in the same time that our protocol has around 10% In terms of computation cost, there is an additional overhead as compared to the Tan et al protocol. Though, our protocol is more secure than another alternative scheme.

- The communication cost is compared in **Table 3.** During the login and authentication processes, the total bandwidth used, and the number of messages exchanged, will derive the communication cost. Assuming the random numbers, one-way hash function output is (160-bits) each, while timestamps expend (32-bits). The login phase from the proposed protocol is $\{\,PID_i, M_1, M_2, t_1\}$ needs (160 + 160 + 160 + 32) = 512 whereas the authentication phase $\{M_4, M_5, t_3\}$content(160+160+32) = 352. As a result, the proposed scheme's total bit requirement is 864 bits.

From the previous analysis, we noticed that both protocols in [9] and [8] used encryption and this makes it possible to decrypt the data sent through the open channel between the server cloud and the patient, while on the other hand, in our protocol this cannot happen because we only use one-way-hash that cannot be decrypted, and this is what makes The proposed protocol is more lightweight and does not have high computational and communication overheads.

Table 3. Compare overheads and review proposed and current protocol.

Protocol	Computational cost		Running Time	Exchanged Messages	Communication cost
	Registration processes	Authentication processes			
Tan et al.[9]	4th	12th +2E	≈0:08ms	3	1184
Kisung et al.[10]	7th	13th	≈0:08ms	4	3008
Zahid et al.[8]	4th+1E	15th+2E	≈0:1ms	3	842
proposed scheme	8th	14th	≈0:088ms	2	864

6 Conclusion

In the proposed protocol, we have explained how it is resistant to many attacks like Offline Guessing the Password Attack, Stolen Smart device Attack, MitM Attack, Resistance to Denial of Service (DoS) attacks, and so on. against important patients' data, as it is transmitted through the open channel to the cloud server and vice versa. This paper also proved that Scheme. [9] has many security mistakes and does not prevent multiple attacks, including Stolen Smart device Attacks, Man-In-The-Middle attacks, Offline Password Guessing attacks, and so on. As well, the computation cost of [8] protocol has around 36% in contrast to the proposed protocol, there is an additional overhead. Therefore, to overcome these security flaws, we designed the protocol proposed in this paper.

References

[1] Rohit Ranchal, Paul Bastide, Xu Wang, Aris Gkoulalas-Divanis, Maneesh Mehra, Senthil Bakthavachalam, Hui Lei, Ajay Mohindra, "Disrupting Healthcare Silos: Addressing Data Volume, Velocity and Variety With a Cloud-Native Healthcare Data Ingestion Service,". In IEEE Journal of Biomedical and Health Informatics, Nov. 2020, vol. 24, no. 11, pp. 3182-3188.

[2] Zaid Alaa Hussien, Hai Jin, Zaid Ameen Abduljabbar, Mohammed Abdulridha Hussain, Ali A. Yassin, Salah H. Abbdal, Mustafa A. Al Sibahee, Deqing Zou, "Secure and efficient e-health scheme based on the Internet of Things,". In 2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 5-8 Aug. 2016, pp. 1-6.

[3] Pei Huang, Linke Guo, Ming Li, Yuguang Fang. "Practical Privacy-Preserving ECG-Based Authentication for IoT-Based Healthcare,". In IEEE Internet of Things Journal, Oct. 2019, vol. 6, no. 5, pp. 9200-9210.

[4] Sobhan Esmaeili, Seyed Reza Kamel Tabbakh, Hassan Shakeri. "A priority-aware lightweight secure sensing model for body area networks with clinical healthcare applications in Internet of Things,". In Pervasive and Mobile Computing, Nov. 2020, vol. 69, pp.1574-1192.

[5] Amal sammoud, Nicolas montavont, Mohamed Aymen chalouf, Ammar bouallegue, Omessaad hamdi, "A secure and lightweight three-factor authentication and key generation scheme for direct communication between healthcare professionals and patient’s WMSN,". In: 2020 IEEE Symposium on Computers and Communications (ISCC), 2020, pp. 1-6.

[6] Shehzad Ashraf Chaudhry, Husnain Naqvi, Muhammad Khurram Khan. "An enhanced lightweight anonymous biometric based authentication scheme for TMIS,". Multimed Tools Appl 77, 2018,5503–5524.

[7] Muhammad Ajmal Azad, Samiran Bag, Charith Perera, Mahmoud Barhamgi, Feng Hao. "Authentic Caller: Self-Enforcing Authentication in a Next-Generation Network,". in IEEE Transactions on Industrial Informatics, May 2020, vol. 16, no. 5, pp. 3606-3615.

[8] Zahid Mehmood, Anwar Ghani, Gongliang Chen, Ahmed S. Alghamdi. "Authentication and Secure Key Management in E-Health Services: A Robust and Efficient Protocol Using Biometrics,". In IEEE Access, 2019, vol. 7, pp. 113385-113397.

[9] Zuowen Tan, "An efficient biometrics-based authentication scheme for telecare medicine information systems,". In Network, 2013, vol. 2, no. 3, pp. 200-204.

[10] Kisung Park, Sungkee Noh, Hyunjin Lee, Ashok Kumar Das, Myeonghyun Kim, Youngho Park, Mohammad Wazid. "LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things,". in IEEE Access, 2020, vol. 8, pp. 119387-119404.