

# Secure two-factor mutual authentication scheme using shared image in medical healthcare environment

Husam A. Abdulmalik, Ali A. Yassin

Department of Computer Science, College of Education for Pure Science, University of Basrah, Basrah, Iraq

## Article Info

### Article history:

Received Jul 23, 2022

Revised Sep 30, 2022

Accepted Nov 2, 2022

### Keywords:

Healthcare

Key management

Mutual authentication

One-time password

## ABSTRACT

The cloud healthcare system has become the essential online service during the COVID-19 pandemic. In this type of system, the authorized user may login to a distant server to acquire the service and resources they demand, we need full security procedures that cover criteria such as authentication, privacy, integrity, and availability. The journey of security for any healthcare system starts with the authentication of users based on their privileges. Traditional user authentication mechanisms, such as password and personal identification number (PIN) typing, are vulnerable to malicious attacks like on/offline, insider, replay, guessing, and shoulder surfing. To address these issues, we proposed a secure authentication scheme that uses the authenticated delegating mechanism based on two factors: a one-time password and generating a secure variable vector from a legible user's digital image to enable the permission of a user through the back-end database of a cloud server. The proposed mutual authentication can protect the information against well-known attacks, ensure the user's privacy, and key management. Moreover, comparisons with existing schemes show that the proposed scheme supplies more privacy, security metrics, and resistance to attacks than the others while being more efficient in computation and communication costs.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Husam A. Abdulmalik

Department of Computer Science, College of Education for Pure Science, University of Basrah

Basrah, Iraq

Email: hussam.akif@uobasrah.edu.iq

## 1. INTRODUCTION

Security is an important aspect of information especially in those environments where information is sensitive and private, such as in healthcare systems. When health information is shared between people and their healthcare professionals, it can help with diagnosis and self-care, making health information systems (HIS) more useful. By giving health experts, patients, administrators, and developers a way to collaborate and communicate with one another, cloud computing improves the quality of healthcare services. On the other side, when cloud resources and services are made available to the general public, it is referred to as an untrusted cloud environment. As a result, security issues have become extremely essential in HIS and consider one of the most significant risks HIS faces. In 2018, HIS continues to be a common target for ransomware, crypto mining, data theft, phishing, and insider threats [1], [2].

In HIS, to ensure the preservation of sensitive and important patient data, security and privacy are crucial components. Privacy refers to safeguarding data against use and access by unauthorized parties, whereas security refers to maintaining data confidentiality during its transport, storage, gathering, and processing [3], [4]. Authentication is a crucial defense against unauthorized access to HIS and sensitive patient. Initially, a single factor was used for objects authentication and at that time, this type of

authentication was often utilized due to its ease of use and simplicity [5], [6]. The use of a password (or a personal identification number (PIN)) to verify the ownership of the user ID was the most common example of single factor authentication (SFA) and clearly is the weakest level of authentication for many reasons, for example, sharing the password can cause compromising the account immediately in addition to that, an unauthorized user can attempt to gain access by utilizing some type of known attacks like a dictionary attack, rainbow table or social engineering techniques [7]–[9]. As a second step forward, two-factor authentication (2FA) [10], [11] was proposed that combines the username/password combination with another factor which could come from one of the following categories: i) knowledge factor: something you know, this could be a PIN, a password, answers to “secret questions” or a specific keystroke pattern, ii) ownership factor: something you have, like a credit card, a smartphone, or a small hardware token, and iii) biometric factor: something you are, like biometric data or behavior pattern.

As a third step forward, multi-factor authentication (MFA) was proposed to provide advanced level security and protection of computing devices and key services from illegal access by using more than two factors of credentials [12], [13]. Authentication in HIS has included many schemes that were proposed by researchers in the past years using 2FA or MFA, most of which were dealing with known security problems like man-in-the-middle (MITM) attack, replay attack and impersonation attack and working to increase resistance against them. However, many of these schemes still contain security holes that can be exploited by attackers [14], [15]. Over the years, a number of research papers have been published in the healthcare sector to enhance the security and privacy of patients. Various smart healthcare systems are proposed for that but many security problems exist in these systems especially those based on passwords as the main authentication factor [16]. A number of important vulnerabilities of password building for smart healthcare are shown in [17] and present a password strength evaluation method. These vulnerabilities include password reuse and building passwords based on personal information. As a result, such passwords can easily be an easy target for some known attacks like dictionary attacks. On the other hand, several password authentication techniques based on the smart card for telecare medical information systems (TMIS) have been proposed. For instance in 2018, Radhakrishnan and Karupiah [18] show that Lee [19] technique is still vulnerable to offline password guessing and forgery attacks and that it is also unable to provide forward secrecy, user anonymity and mutual authentication.

Karthigaiveni and Indrani [20] proposed a 2FA scheme with key agreement using elliptic curve cryptography (ECC) with a smart card and password. Radhakrishnan and Muniyandi [21] show that Karthigaiveni and Indrani [20] scheme has security flaws such as offline password guessing attack and user anonymity. They proposed a 2FA scheme that uses ECC with smart cards, effective, secure, and overcomes security vulnerabilities. Their proposed scheme safeguards user privacy by enabling registered users to change their passwords without disclosing their identities to the server. Beside using the smart card, using biometrics in the healthcare environment has made it possible to determine the identity of patients in a new way. So, another authentication schemes based on biometric factors in healthcare systems have been proposed. Azeta *et al.* [22] developed a HIMS with fingerprint biometrics and password/pin as the main factors for authentication. The HIMS is called CareMed HIMS and a combination of technologies such as UML, biometrics, data management and computer programming have been used to develop the system. Mohammedi *et al.* [23] proposed a lightweight biometric-based authentication scheme for mobile healthcare environments. The suggested scheme converts the patient biometric data to ECC-based keys so there is no need to save or communicate the patient’s biometric template. The researchers show that in the context of RFID authentication protocols, their scheme is resistant to well-known attacks.

Adeli *et al.* [24] made a detailed analysis of the scheme in [23] and show that the proposed protocol is vulnerable to some known attacks like MITM attack and they also demonstrate that the protocol does not provide some important security features like anonymity, forward secrecy and untraceability. To overcome these weaknesses, they proposed an improved protocol that employs only elliptic curve scalar multiplication for both the reader and the tag. They show that their proposed scheme can withstand known attacks like MITM attack and requires 50% less communication cost and 23% less computation time than the Mohammedi *et al.* [23] scheme. Mason *et al.* [25] provide an advanced technique for securely identifying patients. They suggested a technique for patient authentication that combines the use of periocular biometrics with the electronic master patient index in healthcare information systems. Some security concerns that should be taken into consideration have been discussed in [26], [27] when designing and implementing the biometric system. Some of these security concerns are identified as the following:

- Hacking risk, as the use of biometrics increases, our biometric information can be available in more than one place where we may not find the same level of protection.
- Biometrics might be used so frequently. People may believe that biometrics will address all security issues, thus they may not take the kind of common sense security precautions that are necessary.
- Biometric databases are one type of database that may be more vulnerable than others where you can change your password but you can’t change any of your biometrics parameters.

In this paper, we proposed a two factors authentication scheme that has several security features like user privacy, anonymity of verification parameters, non-linkability, confidentiality, forward secrecy, and mutual authentication. The proposed scheme is based on a random vector of shared image points as a second authentication factor in order to provide a safe and secure authentication protocol that resists most of the known security attacks.

## 2. THE PROPOSED SCHEME

In this section, we present an authentication scheme based on using a random vector of points that will be extracted from an image to achieve the required authentication in the healthcare environment. The proposed scheme has three main elements: user ( $U_i$ ), admin ( $A_i$ ), and cloud server (CS). User represents the patient and the admin represents doctors and healthcare systems employees who have the privilege of reading and writing of patients records. According to that, we covered two types of authentication that can be applied in healthcare systems, user-cloud server authentication and admin-cloud server authentication. The first type of authentication consists of three phases: user setup/registration phase, user login phase and user authentication phase. The second type of authentication also consists of three phases: admin setup/registration phase, admin login phase, and admin authentication phase. The use of shared image points vector in the proposed scheme will be applied to admin-cloud server authentication part as it should be more secure according to the type of privileges that will be given to admin after allowing access to the system. The characters used in the current work have conversed in Table 1.

Table 1. The characters used in the proposed protocol

Symbol	Description
$U_i$	A legitimate user $U_i$
$A_i$	A legitimate administrator $A_i$
CS	A trustworthy cloud server
$Img_{A_i}, Img_{CS_i}$	Shared private images for both administrator and cloud server
$SK_{U_i}$	Shared private key between use $U_i$ and CS
$SK_{A_i}$	Shared private key between administrator $A_i$ and CS
$ID_{U_i}$	Identity of user $U_i$
$PW_{U_i}$	Password of user $U_i$
$h(PW_{U_i})$	Hashed password of user $U_i$
$index_{U_i}$	Index of secret sequence term on user side
$index_{CS_i}$	Index of secret sequence term on cloud server side
$index_{A_i}$	Index of secret sequence term on admin side
$Seq_{index_{U_i}}$	A term in generated secret sequence at position equal to index
$ENC_{SK_{U_i}}$	Symmetric encryption function based on key $SK_{U_i}$
$ENC_{SK_{A_i}}$	Symmetric encryption function based on key $SK_{A_i}$
$DEC_{SK_{U_i}}$	Symmetric decryption function based on key $SK_{U_i}$
$DEC_{SK_{A_i}}$	Symmetric decryption function based on key $SK_{A_i}$
$P_i, P'_i, N_i, N'_i, N''_i, E_i$	Other miscellaneous values that are applied in the verification
$V_i$	Vector of random points selected from $Img_{A_i}$
$V_{Pos_i}$	Positions of random points in $V_i$
$h(.)$	A cryptography one-way hash function
$\parallel$	The concatenation operation

### 2.1. User registration phase

The user (patient) must register in the cloud server CS to use this network healthcare system using the steps. Step 1: the user selects an identity  $ID_{U_i}$  and a password  $PW_{U_i}$  then computes the hash value of the selected password  $h(PW_{U_i})$  using hash function  $h$ . User sends registration request message  $M_{U_i} = (ID_{U_i}, h(PW_{U_i}))$  to CS through a secure channel. User and CS will use the same secret sequential and set  $index_{U_i} = 0$ . Step 2: the cloud server CS checks if an account with  $ID_{U_i}$  exists or not. If not, it stores the user's information and set  $index_{CS_i} = 0$ . A secret sequential generation rule will be given to each user.

### 2.2. User login and authentication phase

Step 1: the user input the identity  $ID_{U_i}$  and the password  $PW_{U_i}$  then generate the term  $Seq_{index_{U_i}}$  and set  $index_{U_i} = index_{U_i} + 1$ . After that, user computes  $P_i = h(PW_{U_i}) \parallel h(Seq_{index_{U_i}})$  and sends  $(ID_{U_i}, P_i)$  through a public channel. Step 2: the cloud server CS checks if an account with  $ID_{U_i}$  exists or not, if it exist, then CS

generates  $Seq_{index_{CSi}}$  and set  $index_{CSi}=index_{CSi}+1$  then it computes  $P'_i = h(PW_{ui}) || h(Seq_{index_{CSi}})$  and verifies that  $P'_i = P_i$ , if yes then the CS log in the user to the system. Otherwise, CS rejects user login.

**2.3. Admin registration phase**

Before admin (a doctor or healthcare system’s employee) registration. A third party should generate and distribute the following items for both admin and cloud server: i) an image  $Img$  with dimensions  $(n \times n)$ , ii) a symmetric secret key  $SK$ , and iii) a secret sequential generation rule. After that, admin can register in the cloud server CS using the following steps: step 1: the admin select an identity  $ID_{Ai}$  and a password  $PW_{Ai}$  then compute the hash value of the selected password  $h(PW_{Ai})$  using hash function  $h$ . Admin sends registration request message  $M_{Ai} = (ID_{Ai}, h(PW_{Ai}))$  to CS through a secure channel. Like user registration phase, admin and CS should also use the same secret sequential and set  $index_{Ai} = 0$ . Step 2: the cloud server CS checks if an account with  $ID_{Ai}$  exists or not, if not it stores admin’s information and set  $index_{CSi} = 0$ .

**2.4. Admin login and authentication phase**

Step 1: the admin inputs the identity  $ID_{Ai}$  and the password  $PW_{Ai}$  then generate the term  $Seq_{index_{Ai}}$  and sets  $index_{Ai}=index_{Ai}+1$ . After that, admin computes  $P_i = h(PW_{Ai}) || h(Seq_{index_{Ai}})$  and sends login request message  $M_{Ai} = (ID_{Ai}, P_i)$  to CS through a public channel. Step 2: the cloud server CS checks if an account with  $ID_{Ai}$  exists or not, if it exists, then CS generates  $Seq_{index_{CSi}}$  and sets  $index_{CSi}=index_{CSi}+1$  then it computes  $P'_i = h(PW_{Ai}) || h(Seq_{index_{CSi}})$  and verifies that  $P'_i = P_i$ , if yes then go to the next step. Otherwise, the CS discards the message and terminates the authentication process. Step 3: the cloud server CS generates a vector of random image points positions  $(x,y)$  within the range of image size  $V_{Posi} \in Img_{CSi}$  where  $V_{Posi} = \{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$  so the CS now can extract image points values as vector  $V_i \in Img_{CSi}$  and computes  $N_i = h(V_i)$ . After that CS encrypts  $V_{Posi}$  using the symmetric key  $SK$  and get  $E_{Posi} = ENC_{SK_{Ai}}(V_{Posi})$ . A message with  $E_{Posi}$  and  $N_i$  will be sent to admin.

Step 4: the admin decrypt  $E_{Posi}$  using symmetric key  $SK$  to get the vector of image points positions  $V'_{Posi} = DEC_{SK_{Ai}}(E_{Posi})$  then admin uses these positions to extract image points values vector  $V'_i$  form  $Img_{Ai}$  using  $V'_{Posi}$ . After that admin compute  $N'_i = h(V'_i)$  and verify that  $N'_i = N_i$ , if no then admin should terminate the session. Otherwise, the admin computes  $N''_i = h(V'_{Posi})$  and generates new key  $SK_{Ai} = SK_{Ai} \oplus Seq_{index_{Ai}}$ . This new key will be used in the next login session. Now admin sends  $(N''_i)$  to CS. Step 5: in this step CS verifies that  $N''_i = h(V_{Posi})$ , if yes then the CS log in the admin to the system and generates new key  $SK_{Ai} = SK_{Ai} \oplus Seq_{index_{CSi}}$  to be used next login session. Otherwise, CS rejects admin login. Figures 1 and 2 show the phases of the proposed protocol for both user and admin.

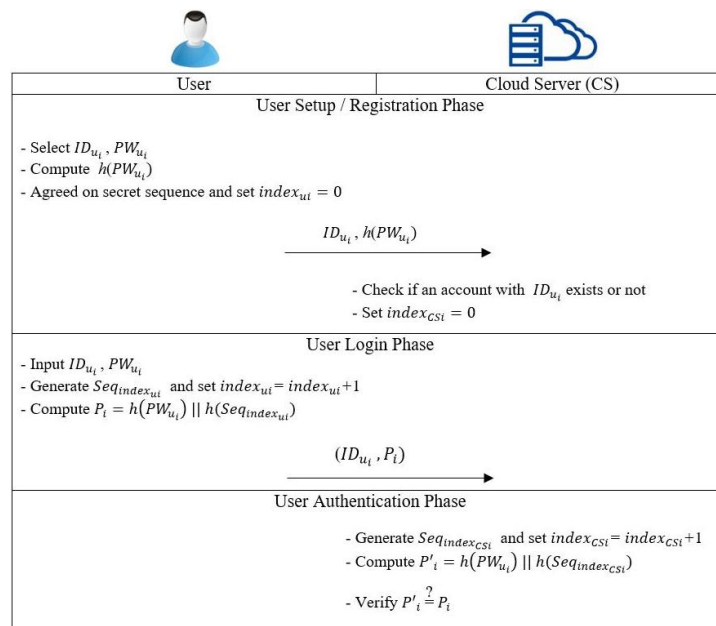


Figure 1. User registration, login, and authentication phases

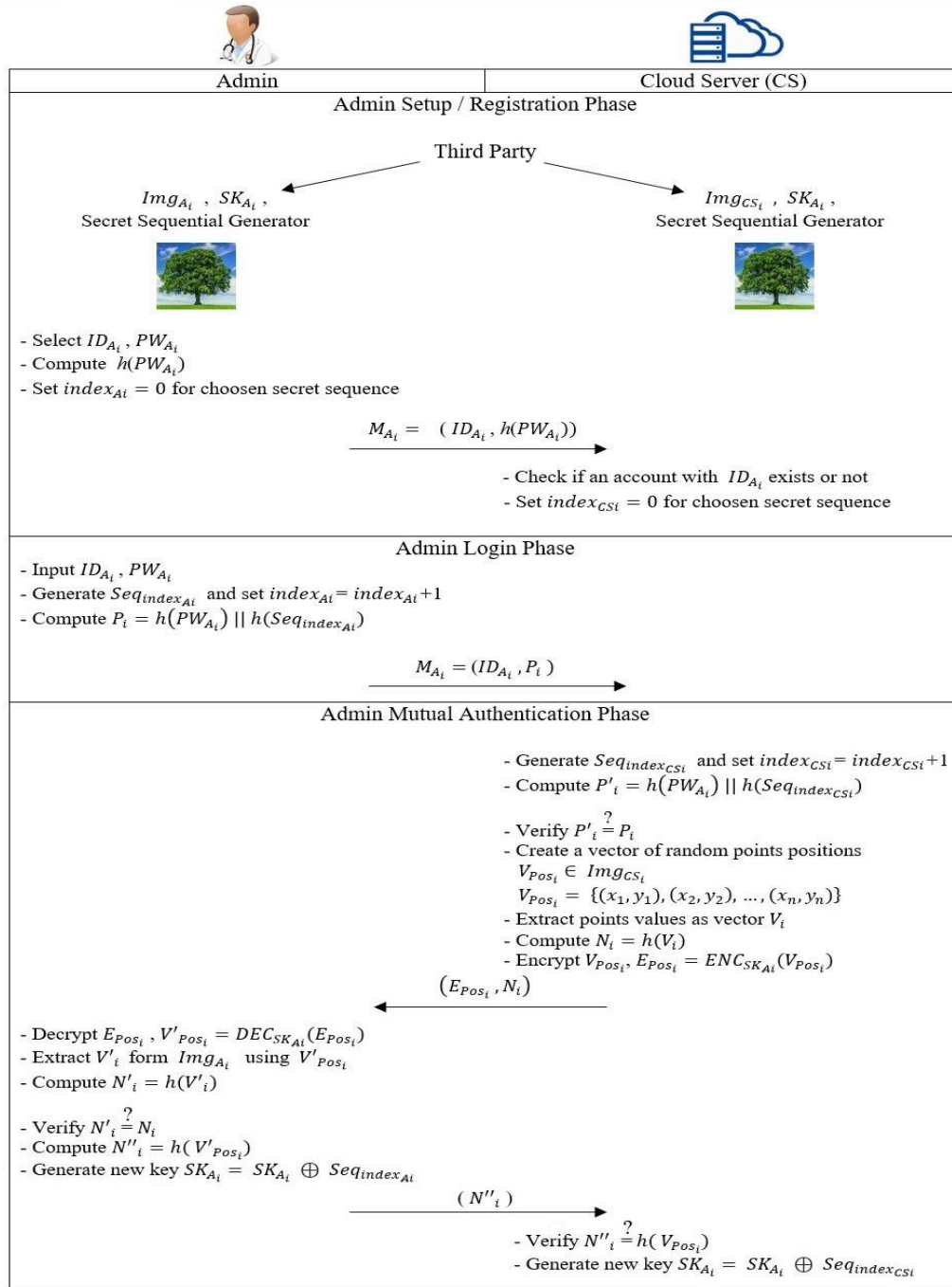


Figure 2. Admin registration, login, and mutual authentication phases

### 3. ANALYSIS AND RESULTS

In the following sub-sections we will perform two types of analysis on the proposed scheme. Security analysis against some significant known attacks and performance analysis in terms of computation cost and communication overhead. The analysis results will be discussed with a comparison with some related works.

#### 3.1. Security analysis

In this section, two types of security analysis will be applied to the scheme suggested in this work. The first is informal security analysis and the second is formal security analysis. Both types of security analysis are explained in detail against some significant known security attacks and the analysis results showed good resistance to these attacks.

### 3.1.1. Informal security analysis

In this section, we show some security features of the proposed scheme and its ability to resist famous attacks such as MITM, replay and impersonation attacks.

- User privacy:** because the encrypted data supplied was computed using random numbers created from the images ( $Img_{Ai}$ ,  $Img_{CSi}$ ) and ( $V_i, V_{Pos_i}, P_i, N_i$ ), the values were untraceable and generated once for each login request for all components. Furthermore, attackers cannot use the shared keys ( $SK_{u_i}, SK_{A_i}$ ) to identify the component's identity.
- Anonymity of verification parameters:** when an administrator first begins registering in the system, he uses his primary parameters (identity ( $ID_{A_i}$ ), password ( $h(PW_{A_i})$ ), which are stored in the database of  $CS$ . After that,  $CS$  replies to  $A_i$  by providing him ( $Img_{A_i}, SK_{A_i}$ ). In the login and authentication phase,  $A_i$  uses anonymity parameters ( $P_i, N''_i$ ) generated once for each login (where  $P_i = h(PW_{A_i}) || h(Seq_{index_{A_i}})$ ,  $N''_i = h(V'_{Pos_i})$ ). Assuming an attacker has the ability to access the main parameters ( $P_i, N''_i$ ), the attacker cannot know the details (like shared key, shared image points) of  $A_i$  or  $CS$  as these parameters have been saved in an anomalous way and they fail to use them again to login instead of  $A_i$ .
- Non-linkability:** the main parameters create different random numbers for each login request. On the administrator side, the variable parameters ( $Seq_{index_{A_i}}, Seq_{index_{CSi}}, V_i, V'_i$ ) have been generated in a secure manner, ensuring high level security and preserving privacy based on previous agreement between  $A_i$  and  $CS$ . The verification message ( $M_{A_i} = (ID_{A_i}, P_i)$ ) of  $A_i$  that should be computed  $P'_i = h(PW_{A_i}) || h(Seq_{index_{CSi}})$  and then checked  $P'_i = P_i$ ; if so,  $A_i$  sends a challenge ( $E_{Pos_i}, N_i$ ) to  $CSi$ . Then,  $A_i$  checks the validity of  $CS$  by computing  $N'_i = h(V'_i)$  and comparing it with the value  $N_i$ ; if it matches, he sends  $N''_i$  to  $CS$  as a second factor to ensure its validity of  $A_i$ . Thus, all response values ( $P_i, P'_i, N_i, N'_i, N''_i$ ) are different, making it impossible for attackers to determine whether data was sent from the same component.
- Confidentiality:** each secret key ( $SK_{u_i}, SK_{A_i}$ ) in the proposed scheme is shared with the cloud server's back-end database. If the users are not authorized, they cannot access the services and resources of the system because they do not have the secret keys.
- Perfect forward secrecy and key management:** we highlight this feature because it ensures that an attacker will not compromise the session keys. The suggested method makes use of dynamic authentication credentials that are based on ( $Seq_{index_{A_i}}, P_i, V_{Pos_i}, SK_{A_i}, N_i$ ), which continue to evolve during sessions in order to attain complete forward secrecy. Assume an attacker has the capacity to get the secret key  $SK_{A_i}$ , the adversary is still unable to obtain  $V_{Pos_i}$  and obtain a fresh key for a new login session  $SK_{A_i} = SK_{A_i} \oplus Seq_{index_{A_i}}$ . The reason for this is that the parameters ( $Seq_{index_{A_i}}, P_i, V_{Pos_i}, SK_{A_i}, N_i$ ) become outsourced after each successful session. Therefore, the proposed scheme provides this feature.
- Mutual authentication:** to avoid adversaries, all parties should authenticate each other's identities before transmitting data. Our proposed scheme provides mutual authentication between  $ADM$  and  $CS$ . For each login process, both parties must verify the other's credibility through a set of steps mentioned in the authentication phase. In the administrator side, the mutual authentication has been applied as follows:

$$\begin{array}{l}
 ADM \xrightarrow{\{M_{A_i}=(ID_{A_i}, P_i)\}} CS \\
 ADM \xleftarrow{\{E_{Pos_i}, N_i\}} CS \\
 ADM \xrightarrow{\{N''_i\}} CS
 \end{array}$$

We notice that each part should be posse the main parameters ( $ID_{A_i}, P_i, E_{Pos_i}, N_i, N''_i, Seq_{index_{A_i}}, V_{Pos_i}, SK_{A_i}$ ) to complete mutual authentication. Otherwise, the authentication will terminate. Therefore, our proposed work provides mutual authentication.

- MITM attack:** in administrator side, we assume that the adversary  $\hat{A}$  can obtain the exchanged messages  $\{M_{A_i} = (ID_{A_i}, P_i)\}$ ,  $\{E_{Pos_i}, N_i\}$ , and  $\{N''_i\}$  between  $ADM$  and  $CSP$  during login and authentication phases.  $\hat{A}$  tries to change these messages and sends it to the legal party, these messages cannot exceed the verification step because  $\hat{A}$  does not posse the real parameters ( $P_i, Seq_{index_{A_i}}, V_{Pos_i}, SK_{A_i}$ ).
- Replay attack:** in this type of attack, the adversary  $\hat{A}$  tries to get the original message and re-send it more than once. Also, this type fails in our scheme due to the use of parameters ( $P_i, Seq_{index_{A_i}}, V_{Pos_i}$ ) besides using a symmetric encryption algorithm and OTP feature, which makes the secure messages and changing every time.

- i. Impersonation attack: the server/user impersonation attack can be successful when the adversary  $\hat{A}$  creates a valid  $P_i, Seq_{index_{Ai}}, V_{Pos_i}, SK_{Ai}, N_i$  and sends these parameters with  $Seq_{index_{ui}}$ . However, this type of attack fails because  $ID_{Ai}$  should be shared with the original parameters  $P_i, Seq_{index_{Ai}}, V_{Pos_i}, SK_{Ai}$ .

### 3.1.2. Formal security analysis using scyther tool

The proposed authentication protocols for admin-CS are verified using the scyther verification tool to prove that our scheme is secure against significant attacks. Scyther has many useful features like unbounded verification, attack finding, and visualization, also it supports some other properties like secrecy, agreement, aliveness, and synchronization [28]–[30]. Figure 3 shows admin authentication protocol written in security protocol description language beside the scyther verification result. The verification result shows that our proposed protocol is secure against the significant attacks.

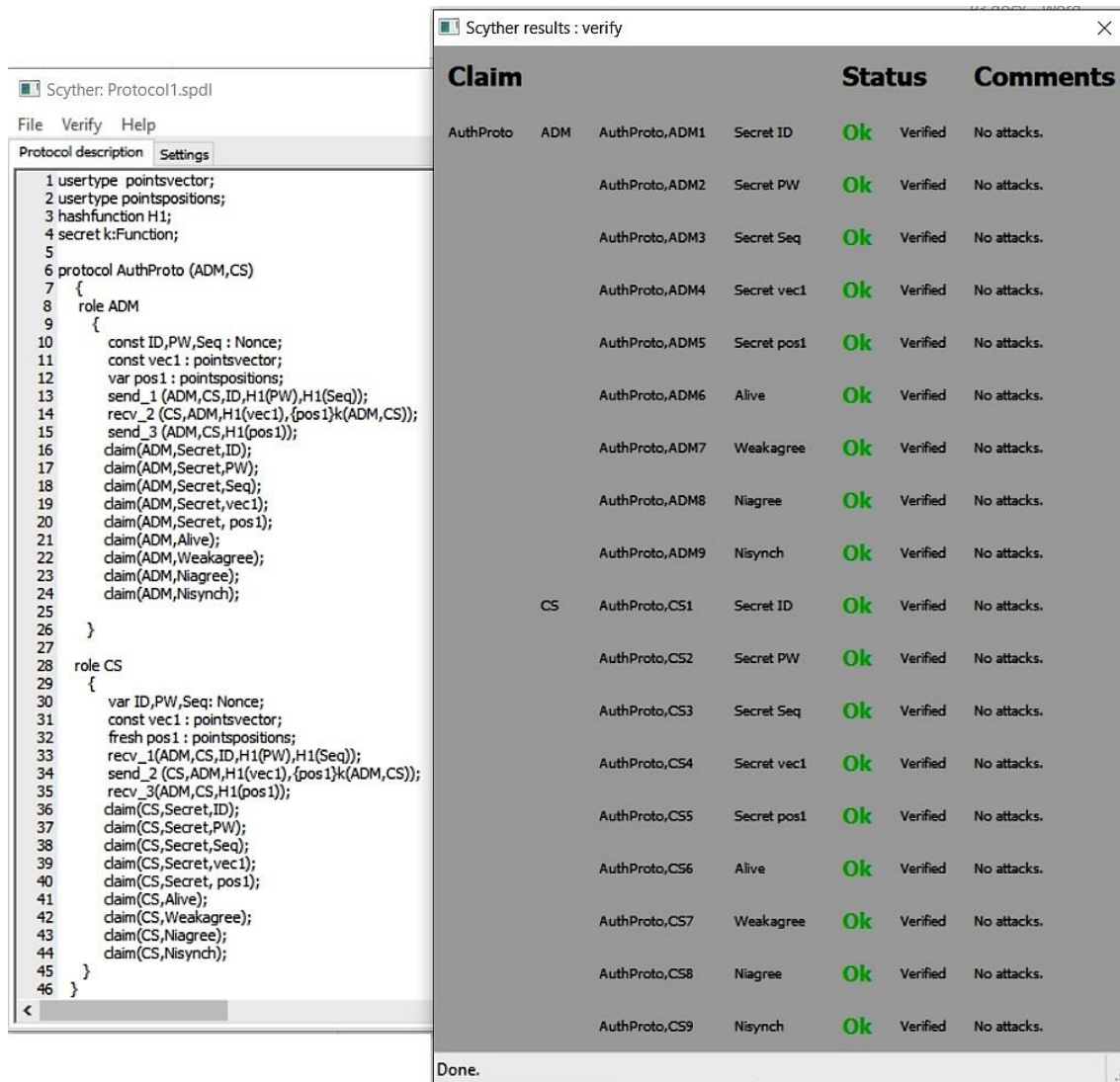


Figure 3. The proposed protocol in stochastic description process language (SPDL) with verification result

### 3.2. Performance analysis

In this section, we will provide the performance analysis of the proposed authentication protocol. The performance is evaluated in terms of computation cost and communication overhead. Our performance analysis includes comparisons with the performance of some other authentication schemes proposed for the same environment.



**3.2.1. Computation cost**

The computation cost is referred to the time which was consumed in the phase of message generation and verification. Table 2 shows the related notations that will be used to evaluate the computation costs of the proposed protocol. The execution time of exclusive OR ( $\oplus$ ) operation is computationally negligible, therefore we ignored it.

Since the login and authentication phase is the most important part of an authentication scheme, we focus on these phases and ignore the costs of the registration phase because it only runs a limited number of times in the initial stage of the proposed protocol. We compare the computation costs of the proposed scheme with four other authentication schemes designed for the same environment as our scheme [18], [31]–[33]. We depend on the measurements for computation cost in [34], [35] to evaluate the computation time for  $T_h$ ,  $T_{en}$  and  $T_{de}$  while depend on our implementation to evaluate the cost of  $T_{xp}$  and  $T_{xv}$ . The average running time of each operation is listed in Table 3. In our comparison we will focus on the admin-CS protocol as our proposed scheme of using a shared image is applied between these two partners. The computation cost for each partner of the proposed protocol and the total cost are shown in Table 4. Table 5 shows the comparisons of the proposed scheme's computation cost with those of related schemes. The results show that our proposed scheme required time is less than some related works results and a little higher than others and this is because our scheme provides more security requirements than other schemes.

Table 2. The related notations used in protocol evaluation

Notation	Execution time of the operation	Notation	Execution time of the operation
$T_h$	One-way hash function $h(\cdot)$	$T_{xv}$	Extract image points values
$T_{en}$	Symmetric encryption algorithm AES (128-bit key)	$T_{Sec}$	Generate new term of sequential
$T_{de}$	Decryption algorithm	$T_{mexp}$	Modular exponent operation. Used in [18] scheme
$T_{xp}$	Generate vector of random image points positions	$T_{pm}$	Executing a point multiplication operation. Used in [33] scheme

Table 3. The average running time of each operation

Operation	Running time (ms)	Operation	Running time (ms)
$T_h$	0.0023	$T_{xp}$	0.058
$T_{en}$	0.0046	$T_{xv}$	0.0055
$T_{de}$	0.0046		

Table 4. The computation cost for each partner in the proposed protocol

Partner	Computation cost	Partner	Computation cost
User	$2T_h$	Cloud server	$T_{Sec}+4T_h+T_{en}+T_{xp} T_{xv}$
Admin	$T_{Sec}+4T_h+T_{de}+T_{xv}$	Total (for admin-CS)	$2T_{Sec}+8T_h+T_{en}+T_{de}+T_{xp}+2 T_{xv}$

Table 5. Computation cost comparison with some related works

Scheme	Total cost	Time needed (ms)
Kaul <i>et al.</i> [31]	$16 T_h+26 T_{\oplus}+16 T_{\parallel}+1T_{Dec}+1T_{Enc}$	$\approx 0.046$
Hamed and Yassin [32]	$5 T_h+2 T_{Enc}+5 T_{\parallel}+2T_{Dec}$	$\approx 0.0299$
Radhakrishnan and Karupiah [18]	$15T_h+1T_{mexp}$	$\approx 530$
Qiu <i>et al.</i> [33]	$13 T_h+4 T_{pm}$	$\approx 270.39$
Ours (for admin-CS)	$2T_{Sec}+8T_h+T_{en}+T_{de}+T_{xp}+2 T_{xv}$	$\approx 0.0966$

**3.2.2. Communication costs**

According to [35] and [36], we assume that the identity and hash digest for SHA-1 are each 160 bits. Consequently, it is possible to calculate the suggested protocol's communication costs for both user-CS communication and admin-CS communication as follows: for user-CS communication we have one message in login/authentication phase,  $(ID_{u_i}, P_i)$  so it requires  $(160+160+160)=480$  bits. For admin-CS communication we have three messages in login/authentication phase.

- Message 1:  $(ID_{A_i}, P_i)$  requires  $(160+160+160)=480$  bits
- Message 2:  $(E_{POS_i}, N_i)$  requires  $(128+160)=288$  bits
- Message 3:  $(N''_i)$  requires 160 bits

As a result, the overall communication cost is  $480+288+160=928$  bits. Table 6 shows the comparisons of the proposed scheme's communication cost with those of related schemes. The results indicate that our scheme has acceptable communication costs compared with other related schemes.



Table 6. Communication cost comparison with some related works

Scheme	Communication cost (bits)
Kaul <i>et al.</i> [31]	768
Hamed and Yassin [32]	608
Radhakrishnan and Karupiah [18]	1024
Qiu <i>et al.</i> [33]	-----
Ours ( <i>for admin-CS</i> )	928

#### 4. CONCLUSION

The protection of e-healthcare information systems from security and privacy breaches became a challenge. There have been a number of techniques for remote user authentication, each one has some advantages and disadvantages. Our proposed work presents a 2FA scheme based on using random points of the shared image to authenticate the connection between the admin (doctors or healthcare system's employees) and the cloud server. The proposed scheme was analyzed informally and formally, the formal analysis shows that our scheme has several security features like user privacy, anonymity of verification parameters, non-linkability, confidentiality, forward secrecy, and mutual authentication. Formal analysis was made using scyther tool and the results obtained proved that the proposed scheme is safe and secure. We think that our research and analysis will be beneficial not only in healthcare environments but also in any place that needs to apply a secure authentication scheme.




#### REFERENCES

- [1] K. Hashizume, D. G. Rosado, E. Fe. -Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2013, doi: 10.1186/1869-0238-4-5.
- [2] I. Keshta and A. Odeh, "Security and privacy of electronic health records: concerns and challenges," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 177–183, Jul. 2021, doi: 10.1016/j.eij.2020.07.003.
- [3] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *Journal of Systems Architecture*, vol. 113, p. 101883, Feb. 2021, doi: 10.1016/j.sysarc.2020.101883.
- [4] M. Imdad, D. W. Jacob, H. Mahdin, Z. Baharum, S. M. Shaharudin, and M. S. Azmi, "Internet of things: security requirements, attacks and counter measures," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 3, pp. 1520–1530, Jun. 2020, doi: 10.11591/ijeecs.v18.i3.pp1520-1530.
- [5] R. K. Konoth, V. v. d. Veen, and H. Bos, "How anywhere computing just killed your phone-based two-factor authentication," in *Financial Cryptography and Data Security*, Berlin, Heidelberg: Springer, 2017, pp. 405–421, doi: 10.1007/978-3-662-54970-4\_24.
- [6] J.-J. Kim and S.-P. Hong, "A method of risk assessment for multi-factor authentication," *Journal of Information Processing Systems*, vol. 7, no. 1, pp. 187–198, Mar. 2011, doi: 10.3745/JIPS.2011.7.1.187.
- [7] D. Wang and P. Wang, "Offline dictionary attack on password authentication schemes using smart cards," in *Information Security*, Cham: Springer, 2015, pp. 221–237, doi: 10.1007/978-3-319-27659-5\_16.
- [8] M. C. A. Kioon, Z. Wang, and S. D. Das, "Security Analysis of MD5 algorithm in Password Storage," in *Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation*, 2013, pp. 706–709, doi: 10.2991/isccca.2013.177.
- [9] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys*, vol. 48, no. 3, pp. 1–39, Feb. 2016, doi: 10.1145/2835375.
- [10] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, "Two-factor authentication: is the world ready?," in *Proceedings of the Eighth European Workshop on System Security*, Apr. 2015, pp. 1–7, doi: 10.1145/2751323.2751327.
- [11] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, Jul. 2015, doi: 10.1109/TDSC.2014.2355850.
- [12] A. B. -Spantzel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino, and S. J. Elliott, "Privacy preserving multi-factor authentication with biometrics," *Journal of Computer Security*, vol. 15, no. 5, pp. 529–560, Jul. 2007, doi: 10.3233/JCS-2007-15503.
- [13] R. K. Banyal, P. Jain, and V. K. Jain, "Multi-factor authentication framework for cloud computing," in *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation*, Sep. 2013, pp. 105–110, doi: 10.1109/CIMSim.2013.25.
- [14] A. Kogetsu, S. Ogishima, and K. Kato, "Authentication of patients and participants in health information exchange and consent for medical research: a key step for privacy protection, respect for autonomy, and trustworthiness," *Frontiers in Genetics*, vol. 9, no. 167, pp. 1–6, Jun. 2018, doi: 10.3389/fgene.2018.00167.
- [15] B. Patil and S. R. Biradar, "An efficient authentication and key-distribution protocol for wireless multimedia sensor network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 1, pp. 347–354, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp347-354.
- [16] N. E. -Bakkouri and T. Mazri, "Security threats in smart healthcare," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 19, pp. 209–214, Nov. 2020, doi: 10.5194/isprs-archives-XLIV-4-W3-2020-209-2020.
- [17] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, "Privacy in the internet of things for smart healthcare," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 38–44, Apr. 2018, doi: 10.1109/MCOM.2018.1700809.
- [18] N. Radhakrishnan and M. Karupiah, "An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems," *Informatics in Medicine Unlocked*, vol. 16, pp. 1–35, 2018, doi: 10.1016/j.imu.2018.02.003.
- [19] T.-F. Lee, "An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine




- information systems,” *Journal of Medical Systems*, vol. 37, no. 6, pp. 1–9, Dec. 2013, doi: 10.1007/s10916-013-9985-9.
- [20] M. Karthigaiveni and B. Indrani, “An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–12, Oct. 2019, doi: 10.1007/s12652-019-01513-w.
- [21] N. Radhakrishnan and A. P. Muniyandi, “Dependable and provable secure two-factor mutual authentication scheme using ECC for IoT-based telecare medical information system,” *Journal of Healthcare Engineering*, vol. 2022, pp. 1–15, Feb. 2022, doi: 10.1155/2022/9273662.
- [22] A. A. Azeta, D.-O. A. Iboroma, V. I. Azeta, E. O. Igbekele, D. O. Fatinikun, and E. Ekpunobi, “Implementing a medical record system with biometrics authentication in E-health,” in *2017 IEEE AFRICON*, Sep. 2017, pp. 979–983, doi: 10.1109/AFRCON.2017.8095615.
- [23] M. Mohammedi, M. Omar, and A. Bouabdallah, “Secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 5, pp. 1527–1539, Oct. 2018, doi: 10.1007/s12652-017-0574-5.
- [24] M. Adeli, N. Bagheri, and H. R. Meimani, “On the designing a secure biometric-based remote patient authentication scheme for mobile healthcare environments,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 3075–3089, Feb. 2021, doi: 10.1007/s12652-020-02465-2.
- [25] J. Mason, R. Dave, P. Chatterjee, I. G. -Allen, A. Esterline, and K. Roy, “An investigation of biometric authentication in the healthcare environment,” *Array*, vol. 8, p. 100042, Dec. 2020, doi: 10.1016/j.array.2020.100042.
- [26] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, “Security and accuracy of fingerprint-based biometrics: a review,” *Symmetry*, vol. 11, no. 2, pp. 1–19, Jan. 2019, doi: 10.3390/sym11020141.
- [27] Z. Rui and Z. Yan, “A survey on biometric authentication: toward secure and privacy-preserving identification,” *IEEE Access*, vol. 7, pp. 5994–6009, 2019, doi: 10.1109/ACCESS.2018.2889996.
- [28] C. J. F. Cremers, “The scyther tool: verification, falsification, and analysis of security protocols,” in *Computer Aided Verification*, Berlin, Heidelberg: Springer, 2008, pp. 414–418, doi: 10.1007/978-3-540-70545-1\_38.
- [29] R. Patel, B. Borisaniya, A. Patel, D. Patel, M. Rajarajan, and A. Zisman, “Comparative analysis of formal model checking tools for security protocol verification,” in *Recent Trends in Network Security and Applications*, Berlin, Heidelberg: Springer, 2010, pp. 152–163, doi: 10.1007/978-3-642-14478-3\_16.
- [30] A. H. Aly, A. Ghalwash, M. M. Nasr, and A. A. A.-E. Hafez, “Formal security analysis of lightweight authenticated key agreement protocol for IoT in cloud computing,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 1, pp. 621–636, Oct. 2021, doi: 10.11591/ijeecs.v24.i1.pp621-636.
- [31] S. D. Kaul, V. K. Murty, and D. Hatzinakos, “Secure and privacy preserving biometric based user authentication with data access control system in the healthcare environment,” in *2020 International Conference on Cyberworlds (CW)*, Sep. 2020, pp. 249–256, doi: 10.1109/CW49994.2020.00047.
- [32] N. Hamed and A. Yassin, “Secure patient authentication scheme in the healthcare system using symmetric encryption,” *Iraqi Journal for Electrical and Electronic Engineering*, vol. 18, no. 1, pp. 71–81, Jun. 2022, doi: 10.37917/ijeee.18.1.9.
- [33] S. Qiu, G. Xu, H. Ahmad, and L. Wang, “A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems,” *IEEE Access*, vol. 6, pp. 7452–7463, 2018, doi: 10.1109/ACCESS.2017.2780124.
- [34] J. Zhang, Q. Zhang, Z. Li, X. Lu, and Y. Gan, “A lightweight and secure anonymous user authentication protocol for wireless body area networks,” *Security and Communication Networks*, vol. 2021, pp. 1–11, Jul. 2021, doi: 10.1155/2021/4939589.
- [35] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. H. Islam, and D. Giri, “A robust authentication and access control protocol for securing wireless healthcare sensor networks,” *Journal of Information Security and Applications*, vol. 52, p. 102502, Jun. 2020, doi: 10.1016/j.jisa.2020.102502.
- [36] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park, “Physically secure lightweight anonymous user authentication protocol for internet of things using physically unclonable functions,” *IEEE Access*, vol. 7, pp. 85627–85644, 2019, doi: 10.1109/ACCESS.2019.2926578.

## BIOGRAPHIES OF AUTHORS



**Husam A. Abdulmalik**    received his Bachelor's degree in Computer Science from University of Basrah, Iraq in 1994. He received the Master degree in Computer Science (Cryptography and Computer Security) from University of Basrah, Iraq in 1996 and completed his Ph.D. in Network Security (Intrusion Detection Systems) from University of Basrah, Iraq in 2007. Currently, he is a lecturer at the Department of Computer Science, Education College for Pure Science, University of Basrah since 2009. His research interests include networks and computer security, particularly intrusion detection systems, and authentication techniques. He can be contacted at email: hussam.akif@uobasrah.edu.iq.



**Ali A. Yassin**    is a Professor with the Department of Computer Science, College of Education for Pure Science, University of Basrah. He received the bachelor's and master's degrees from the University of Basrah, Basrah, Iraq, and the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, China. His research interests include the security of cloud computing, image processing, pattern recognition, biometrics, data integrity, DNA cryptography, steganography, sharing data, graphical password, QR code, and soft computing. He can be contacted at email: ali.yassin@uobasrah.edu.iq.