

Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system

Mohammad Fareed^{1,2}, Ali A. Yassin¹

¹Department of Computer Science, Education College for Pure Science, University of Basrah, Basrah, Iraq

²Communication Media and Commission, Basrah, Iraq

Article Info

Article history:

Received Jan 30, 2022

Revised May 9, 2022

Accepted Jun 1, 2022

Keywords:

Asymmetric cryptosystem

Healthcare system

Multi-factor authentication

Privacy-preserving

Role-based access control

Schnorr digital signature

ABSTRACT

E-healthcare assists medical specialists in remotely collecting patient health data and providing remote health diagnoses. The roles are distributed among the system's users, contrasted between admin to data entry within certain rules and policies. Role-based access control (RBAC) is a technique of advanced access control that restricts key operations of users (addition, deletion and modification) access based on a user's role within a healthcare system. This paper proposes a privacy-preserving using RBAC and smart multi-factor authentication for the healthcare system to overcome the limitation flaw in previous schemes such as security risk tolerance, scalability and dynamism. This work relies on low-complexity cryptographic hash functions and symmetric operations to authenticate users while using an asymmetric cryptosystem based on the Schnorr digital signature lightweight operation to authenticate the administrator to provide multi-factor authentication. The administrator represents the system's core, and any his information leak could attack the entire system and its components. The proposed scheme conducted two thorough formal security proofs for the proposed work based on informal analysis and the Scyther tool. Furthermore, comparisons with other schemes reveal that the proposed scheme provides greater security features, and resisting attacks than the others while also being efficient in computing 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:

Mohammad Fareed

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

Basrah 61004, Iraq

Email: pedupg.m.fareed@uobasrah.edu.iq

1. INTRODUCTION

In the world of safe technology, the first step in the journey of login system according to identify a customer/administrator using a multi-factor authentication scheme that is an umbrella term for checking an unauthorized customer or robot based on certain factor/s, such as password, token, biometric. Today, there are three traditional classes of multi-factor authentication: something you have (e.g., smart mobile, USB token-driver), something you are (e.g., hand geometry, fingerprint), and something you know (e.g., username and password). Additionally, *somewhere you are* or location has been included as an additional factor to detect or track the user's location from a tracking device (e.g., global positioning system (GPS), WiFi locator, and RFID reader location), although it is not as widely undesirable as in the other traditional three factors [1]. Commonly, single-factor authentication (SFA) was most widely used by society due to its easiness and user approachability. Seemingly, SFA is the most unsuccessful in resisting malicious attacks like dictionary attacks, man-in-the-middle (MITM) attacks, social engineering techniques [2]. As a result, the single factor fails to support adequate protection due to a set of security threats [3], [4]. As an obvious step forward, the researchers

focused on the combination of the username/password with the second factor like personal identification number (PIN) [5] called two-factor authentication (2FA). Here, 2FA adds a shield layer of security to the authentication procedure, making it a solidier for attackers to access online accounts. Even if the victim's password is a breakthrough, a password alone is not enough to pass the authentication check in 2FA.

Additionally, the role of this process is to control access to the systems and data. Online service providers prefer to use 2FA to preserve the security of their users' credentials against being used by adversaries who are increasingly using 2FA to protect their users' credentials from being used by hackers who plunder a password database to gain user passwords. Authentication occurs once the user logs in to the system, determining his authorization level. A user's authorization may specify what resources they have access to and the tasks they may do. RBAC decides whether or not to provide access based on the traits and resources of the requesting party. It means that the user's access rights will vary depending on their position in the organization. An administrator establishes the criteria for each position's access and who gets to have that access. Additionally, RBAC can control users' privileges and distribute their authority according to the work methodology of the proposed system. Users can hence be made members of a certain role depending on their responsibilities or corporate position and can be later be reassigned to another role without impacting the underlying access control infrastructure.

This work contributes by proposing a good security scheme that stresses the usability of integrating authentication factors in a healthcare system and access control. The proposed scheme aims to distribute the policies and privileges among the system's components: administrator and users; the user has the right to enjoy all or some of the main system operations adding, deleting, and modifying according to the permission given to him by the administrator. In our solution, we depend on formal (Scyther tool) and informal security analyses to prove the immunity of the proposal work towards well-known attacks like Insider attacks, reply attacks, MITM attacks, impersonate attacks; the proposed scheme has powerful features such as anomaly, perfect forward secrecy, unlinkability. Additionally, users' privacy relies on the healthcare center responsible for generating secret keys of the administrator and users.

The rest of the paper is structured as follows: section 2 discusses the latest related work. Section 3 presents the proposed healthcare authentication schemes followed by its security analysis in section 4. Finally, section 5 concludes this paper.

2. RELATED WORK

Multi-factor authentication is one of the most schemes of security's world that applies in many systems, which depend on two or more factors, attempts to improve information security, preserving privacy, and trust management in sophisticated contexts like the internet of things and smart devices [1]. Significantly, users need simple user-friendly authentication procedures in smart hyper-connected devices and wearable devices. Consequently, several challenges face the developers of smart systems such as smart login, secure exchange information, and attributes-based user's authentication [3]. The privacy of user information wishing to register in a sensitive system (e.g., E-bank and E-healthcare) must be protected against opponents [1], [6], [7].

According to research, multi-factor authentication is more extensively utilized in mobile environments and E-healthcare. The one-time password (OTP) and security token are frequently recommended in the financial transaction attendance system [8]. Numerous research papers have attempted to offer strong multi-factor authentication schemes such as face recognition and unique hardware identification used in city and community street monitoring [9]. These schemes focused on feeding the people with prior information. Then they use the same information to answer some questions used as something you know to factor in the login system [10]. In the ATM card field, some schemes embedded chip and iris recognition [11] have been offered as a realistic way to authenticate ATM customers [12].

In recent research articles, we have seen the need for multi-factor authentication, which should be required to avoid impersonation attributes. Traditional factors such as *something you have*, *something you know*, and *something you are* used in the three-factor technique. It has been suggested that something you have is automatic for mobile users because it is always with the user's smartphone [13]. Some authors use a dynamically near-field communication (NFC) code as an additional factor in their scheme to increase security [14]. Symmetric keys can be used with other components such as passwords and biometric data [15]. All three factors can be successfully combined, taking into account addressing the balance between complexity and performance must be addressed [11]. In addition to the three traditional features. The fourth factor is where you are or your location [16]. Low-cost locators like Bluetooth and GPS can be used to track or locate a person while authenticating to the system [17].

The more factors are added, the more confident a system is; nonetheless, usability must be considered. People use these systems frequently and cannot devote the time and effort required to log on or do any difficult authentication step many times per day [18]. SELAMAT, a robust multi-factor authentication scheme, works easy

to assist users in accessing cross-platform systems in different geographical areas [19]. Similarly, using a third-party authentication tool like Google Authenticator to generate PIN code and OTP can save consumers time and effort, supporting a single sign-on (SSO) experience [18]. Users do not need to memorize a password or token in a security system focused on usability and deploy ability; instead of restoring passwords, scan a dynamically generated quick response code with their smartphone (QR code) [20]. Unlike traditional multi-factor authentication, which requires users to use specific factors without allowing them to choose which ones they prefer, (t, n) threshold authentication allows users to choose which authentication factors they want to use [21].

Several multi-factor authentication techniques have been introduced so far. However, the practical deployment observes to be limited since they require too much work from the user and do not provide the security level expected [22]. Also, since it requires a high level of user proficiency and may not have authentication devices everywhere, adopting some hostile, high-tech aspects may deter users from acquiring and implementing these systems [23]. This is in line with a study [24] indicating that more user-friendly multi-factor authentication is relatively important; even though very few previous publications focused on user evaluation of different objectives, attendance systems have sometimes been developed with security mechanisms to prevent impersonation or spoofing have been developed. During the COVID-19 crisis, the multi-factor scheme became popular in many systems, depending on QR code identification and face verification factors [25].

In addition, it's necessary to specify the responsibilities of each user when granting access. Role-based access control (RBAC) allows us to create and restrict our needs' access to functionality and information. System access may be restricted depending on a user's job within the organization using the RBAC technique [26]. To be specific, four primary contributions of the paper are summarized as: i) design a secure Multi-Factor authentication scheme based on the management and support of large-scale healthcare systems and scalability; ii) access to data must be secured and protected in real-time over a public communication channel; iii) the registration phase allows authorized administrators and users to access current and future resources based on their permissions; iv) perform formal and informal analysis to ensure the security system sturdiness, effectiveness, and resistance to common malicious attacks.

3. PROPOSAL SCHEME

In this section, we propose the strong authentication of the administrator in the healthcare system consist of three components: administrator (ADM), user data entry (U_i), the healthcare center (HCC). In addition, our work is based on five phases: initialization phase, registration phase, authentication (administrator, user) phase, and trust management phase.

3.1. Initialization phase

Step1: the administrator (ADM) plays the primary role of managing and accessing control of the components. Therefore, he needs to register his information (full name (FN_{ADM}), address (AD_{ADM}), administrator's identity (ID_{ADM}), phone number (PNO_{ADM}), username (UN_{ADM}), password (PW_{ADM})) in the HCC for one time. Then, HCC ($PW'_{ADM} = H(PW_{ADM} || UN_{ADM})$) is computed to preserve the privacy of Admin's identity in an anomalous manner. However, HCC uses $H(.)$ as a crypto-hash secure hash algorithm (SHA) 256, where hashing considers the core principles of additional security modules and works as one side function. SHA 256 is a part of the SHA 2 family of algorithms. The significance of the 256 in the name attitudes for the final hash digest value, i.e., irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits.

Step 2: generate public and private keys (Pr_{ADM}, Pu_{ADM}) to encrypt $Enc(.)$ /decrypt $Dec(.)$ based on public-key encryption.

Step 3: HCC generates the shared key ($SK_{ADM} \in \mathbb{Z}$) to encrypt $Enc(.)$ /decrypt $Dec(.)$ data based on symmetric key encryption counter mode (CTR mode).

Step 4: HCC stores the IP information of the Internet service provider (HCC_{ip}) for HCC in the database.

3.2. Registration phase

Step 1: ADM registers U_i 's information (full name (FN_{U_i}), address (AD_{U_i}), phone no. (PN_{U_i}), email (EM_{U_i}), username (UN_{U_i}), password (PW_{U_i})), to HCC . Then, HCC saves PW_{U_i} as anomaly method by using $UN'_{U_i} = H(PW_{U_i} || UN_{U_i})$.

Step 2: generate public and private keys (Pr_{U_i}, Pu_{U_i}) to sign data from the U_i to the HCC based on Schnorr digital signature as below:

U_i selects two large primes p and q such that: $(p - 1) \bmod q = 0$.

U_i chooses $g \in \mathbb{Z}_p$ of order q , $g \neq 1$ & $g^q = 1 \bmod p$.

U_i picks $x_{U_i} \in \mathbb{Z}_q$ and $g^{x_{U_i}} \bmod p$.

$Pr_{U_i} = x_{U_i}$ and $Pu_{U_i} = g^{x_{U_i}} \text{mod } p$.

Step 3: after completing the registration process of P_i and determining his health status by HCC_{DP_k} , ADM uploads FF_{P_i} to C_i .

Step 4: finally, HCC sends (Pu_{ADM}, SK_{ADM}) to the U_i .

3.3. Administrator authentication phase

At this point, the main dialogue will take place between two main components HCC and the administrator of the system (ADM). All system privileges are linked by ADM . We notice that ADM can access and manage the major processes and system components. Therefore, it is necessary to provide a secure and immunogenic authentication phase for ADM as shown in Figure 1. The steps below refer to the mechanism of the current phase:

Step 1: ADM enters his login credentials (UN_{ADM}, PW_{ADM}) and selects $r \in \mathbb{Z}$.

Step 2: ADM calculates $L = H(UN_{ADM} || PW_{ADM}) \oplus r$, and encrypts $E_r = Enc_{SK_{ADM}}(r)$.

Step 3: ADM sends (L, E_r) to HCC .

Step 4: HCC computes $r' = Dec_{SK_{ADM}}(E_r)$ and retrieves PW'_{ADM} from database.

Step 5: HCC calculates $L' = PW'_{ADM} \oplus r'$, and compares $L \stackrel{?}{=} L'$.

Step 6: If the comparison result is hold, then HCC generates and sends SMS token (SMS_T) via PNO_{ADM} to ADM .

Step 7: ADM restores SMS_T from HCC by SMS on his PNO_{ADM} and enters SMS'_T in the dialogue box and resubmits to HCC .

Step 8: HCC compares $SMS_T \stackrel{?}{=} SMS'_T$; if matches, then ADM is authorized. Then, ADM can fully manage the system completely through operations (adding, modifying, deleting data, and decrypting of some data stored in the global database based on the Pr_{ADM}) as well as manages the U_i and HCC_{DP_k} .

Step 9: HCC computes $SK'_{ADM} = SK_{ADM} \oplus r'$ and saves a new SK'_{ADM} with each successful login request. To make the shared key change dynamically.

3.4. User authentication phase

Here, the login information of users (data entry) that is entered with each patient's data so that they can manage their tasks in HCC after their identities according to the following steps:

Step 1: U_i enters his login credentials (UN_{U_i}, PW_{U_i}) and calculates $U_{H_i} = H(UN_{U_i} || PW_{U_i})$.

Step 2: U_i computes $U_{i_{ip}} = Enc_{Pu_{ADM}}(IP \text{ device})$. Next, he sends $(U_{H_i}, U_{i_{ip}})$ to HCC .

Step 3: HCC receives the data and compares $U'_{H_i} \stackrel{?}{=} UN'_{U_i}$; if the result is accurate, go to Step4; otherwise, it terminates the current phase.

Step 4: HCC generates and sends SMS token (SMS_{TU}) via PNO_{U_i} to U_i .

Step 5: U_i retrieves SMS_{U_i} from HCC by SMS on his PNO_{U_i} and enters SMS'_{U_i} in the dialogue box and resubmits to HCC .

Step 6: HCC compares $SMS_{U_i} \stackrel{?}{=} SMS'_{U_i}$; if matches, then U_i is authorized.

Figure 2 Explains the user authentication phase.

3.5. Role based access control phase

This phase is responsible for securing the managed operations between HCC and users supervised by ADM . So, the users need permissions from ADM to apply some operations such as adding, deleting, and updating to the EHRs. Therefore, the current phase depends on the positive results (U_i and ADM must be authorized) of the previous phase as follows:

Step 1: HCC decrypts $U_{i_{ip}}$ to check whether $Dec_{Pr_{ADM}}(U_{i_{ip}})$ is equal to the stored $HCC_{i_{ip}}$. If so, the login was within the health institution. Otherwise, all data sent by U_i to the HCC which must be signed because U_i has been login outside the organization.

Step 2: U_i want to add a new P_i data. Firstly, he should be computed $P_{info} = (FN_{P_i} || AD_{P_i} || PN_{P_i} || EM_{P_i} || FCI_{P_i} || TD_{P_i} || UN_{P_i} || PW_{P_i})$. Secondly, the user side checks his location based on the next steps.

Step 3: check the location of U_i , if it exists inside the health organization, the communication channel is secure because he works directly on the HCC . Hence, Step8 will be performed.

Step 4: if U_i is outside the health organization. The communication channel is not secure because he works (anywhere/anytime) indirectly on the HCC .

Step 5: this step works forward secrecy of the data transferred between U_i and HCC . In addition to ensuring that the attackers do not change it through the digital signature.

Step 6: at this step, U_i should be contributed to the decision making of sending the patient's information to HCC . U_i performs the following steps:

Choose a random integer number $k_{U_i} \in \mathbb{Z}_q^*$ and set $r_{U_i} = g^{k_{U_i}}$.

Compute $e_{U_i} = H(r_{U_i} || P_{info})$ and $s_{U_i} = k_{U_i} + Pr_{U_i} * e_{U_i}$.

Send $Sign_{Pr_{U_i}}(P_{info}) = \langle P_{info}, s_{U_i}, e_{U_i} \rangle$ to *HCC*.

Step7: upon receiving the data in Step 6, *HCC* verifies whether the $Sign_{Pr_{U_i}}(P_{info})$ is valid or not by running $Verify_{Pr_{U_i}}(P_{info}, s_{U_i}, e_{U_i})$ as follows.

Set $r'_{U_i} = g^{s_{U_i}} y^{-e_{U_i}}$.

$r'_{U_i} = g^{k_{U_i} + Pr_{U_i} * e_{U_i}} * g^{-Pr_{U_i} * e_{U_i}}$.

$r'_{U_i} = g^{k_{U_i}}$.

Compare $e_{U_i} \stackrel{?}{=} H(r'_{U_i} || P_{info})$; if equals, go to Step8; Otherwise, terminate and exit the current phase.

Step 8: *HCC* creates EHR_{P_i} to the new P_i and saves P_{info} in the EHR_{P_i} .

Step 9: sometime, U_i Maybe needed to run main operations like delete/modify. Therefore, there are robust restrictions that should execute for gaining user's permission to apply operation that can be performed directly if the (modification /deletion) process is immediately after the insertion. However, if the modification/deletion operations are done after a time, the operations cannot execute proximately. Thus, *HCC* sends SMS token (SMS_{TU_i}) via PNO_{U_i} to U_i for making secure operations.

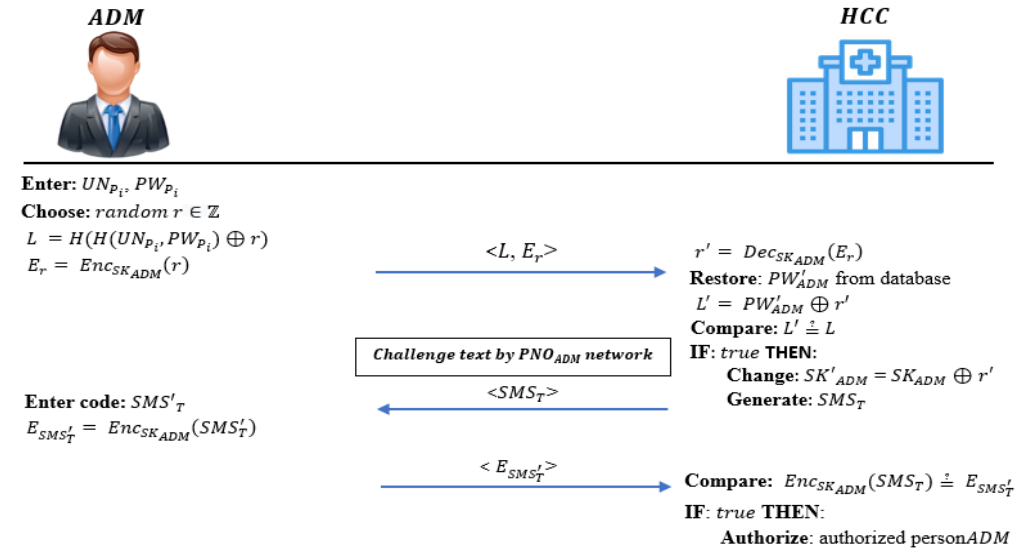


Figure 1. Administrator authentication phase

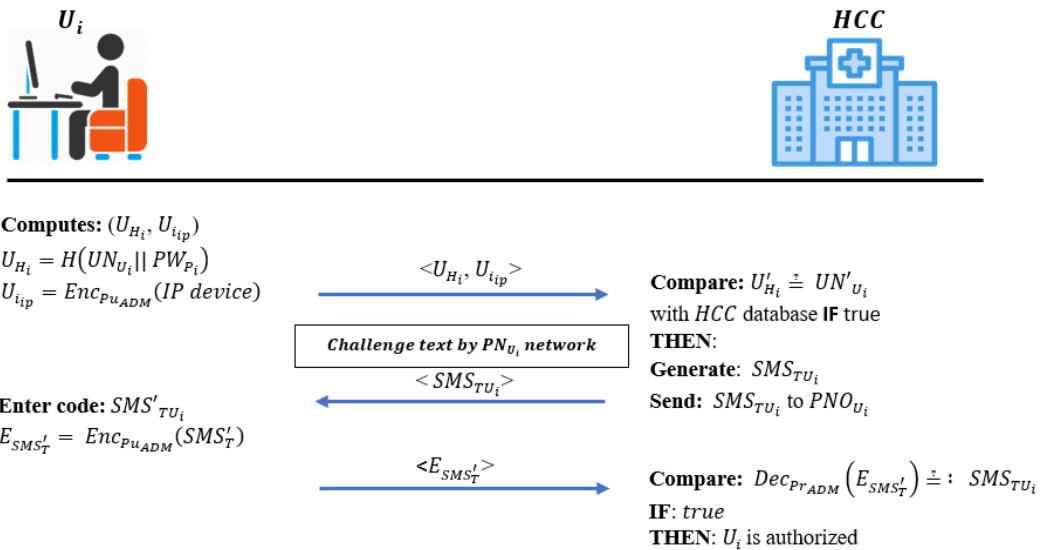


Figure 2. User authentication phase

4. SECURITY ANALYSIS

This section evaluates security analysis of the proposed scheme in terms of formal and informal security analysis as the follows:

4.1. Formal security analysis

As the internet and other open networks have grown in popularity, many security tools have been created and used to ensure safe communication for the proposed system. Scyther is a tool for evaluating the security and vulnerabilities of schemes. Two steps explain the working of the tool. Scyther is guaranteed to finish in the first step while enabling an indefinite number of sessions to establish protocol soundness. The option is to produce the proof tree (using the backend). The second step, Scyther, aids graphical user interface analysis by offering attack behavior classes [26]. Any proposed scheme should be expressed in the security protocol description language (SPDL), which specifies protocols and schemes and supports expressions for encryption, decryption, and signature, as well for sending and receiving events [27]. We write the proposed scheme using SPDL language and display the results in the cases of automatic claim and verification claim. We perform the proposed system without using security functions that work in the same traditional systems. We note that Figure 3 refers to the traditional system and its weakness.

This paper, proposed the idea a secure system that has overcome the weakness of traditional systems using symmetric key encryption (), crypto-hash function. Figure 4 show the proposed system's result resisting well-known malicious attacks.

4.2. Informal security analysis

As stated in the CK threat model, previous papers over the last ten years have denoted that in the related work section, a security proof suffers from an inadequate security model that does not succeed in detecting all the genuine capabilities of an attacker. Therefore, according to the CK threat model, we prove the security of a proposed system as follows.

4.2.1. Mutual authentication

We use this feature among main components (HCC and ADM, HCC and U_i). Our work focuses on multi-privilege authentication associated with the messages: 1) from HCC and to ADM and vice versa; 2) from HCC to U_i and vice versa. Here, ADM considers the highest privilege while managing all components of the healthcare system, including U_i , C_i and others. ADM requires to be original by HCC based on (L, E_r, VC) , which is a message from ADM to HCC . HCC in the proposed system could authenticate only the legal ADM because a CK adversary needs to guess the login information (UN_{ADM}, PW_{ADM}, r) and compute $L = H(UN_{ADM} || PW_{ADM} || r)$, and the adversary must know the ADM 's shared-key to encrypt r using $E_r = Enc_{SK_{ADM}}(r)$. Here, HCC can be considered a trusted party.

Although the adversary faces difficulty to obtain $(UN_{ADM}, PW_{ADM}, r, SK_{ADM})$ as the first step to login HCC . Therefore, we assume the adversary can obtain $(UN_{ADM}, PW_{ADM}, r, SK_{ADM})$ and login as an administrator ADM' . Hence, ADM must be trusted by HCC based on $(SMS\ TOKEN)$, and also the login information must be correct, HCC decrypts $r' = Dec_{SK_{ADM}}(E_r)$ and gets PW'_{ADM} with the ADM 's information is stored in the system database then compares L to $(PW'_{ADM} || r')$; if so, HCC generates and sends SMS token (SMS_T) via PNO_{ADM} to ADM , ADM' fails to receive SMS_T from HCC by SMS because he does not have ADM 's device phone number PNO_{ADM} . After that, HCC terminates the authentication phase. In case ADM is legitimate; he enters SMS'_T in the dialogue box and computes $VC = Enc_{SK_{ADM}}(SMS'_T)$ and then send it back it to HCC . Finally, HCC compares $Enc_{SK_{ADM}}(SMS_T) \stackrel{?}{=} VC$; if matches, then ADM is the authorized.

4.2.2. Session key agreement

The session key is used to create a protected communication channel between ADM and HCC to support secrecy on data. They agree on a once session key $SK_{ADM} = SK_{ADM} \oplus r$ after responsive authentication. It is unattainable for CK adversary to obtain any information of SK_{ADM} based on r .

4.2.3. Perfect forward secrecy

we note this feature that proves guarantees that an adversary fails to compromise the session keys. The proposed system uses dynamic authentication credentials based on (SK_{ADM}, r, SMS_T) , which continue evolving in sessions to achieve perfect forward secrecy. Here, assume an adversary has the ability to obtain SK_{ADM} , the adversary still unable to obtain $L = H(H(UN_{ADM} || PW_{ADM}) \oplus r)$. The reason is that after each successful session, the values SK_{ADM} , r and SMS_T generate once using crypto hash function. Therefore, the proposed system enjoys this feature.

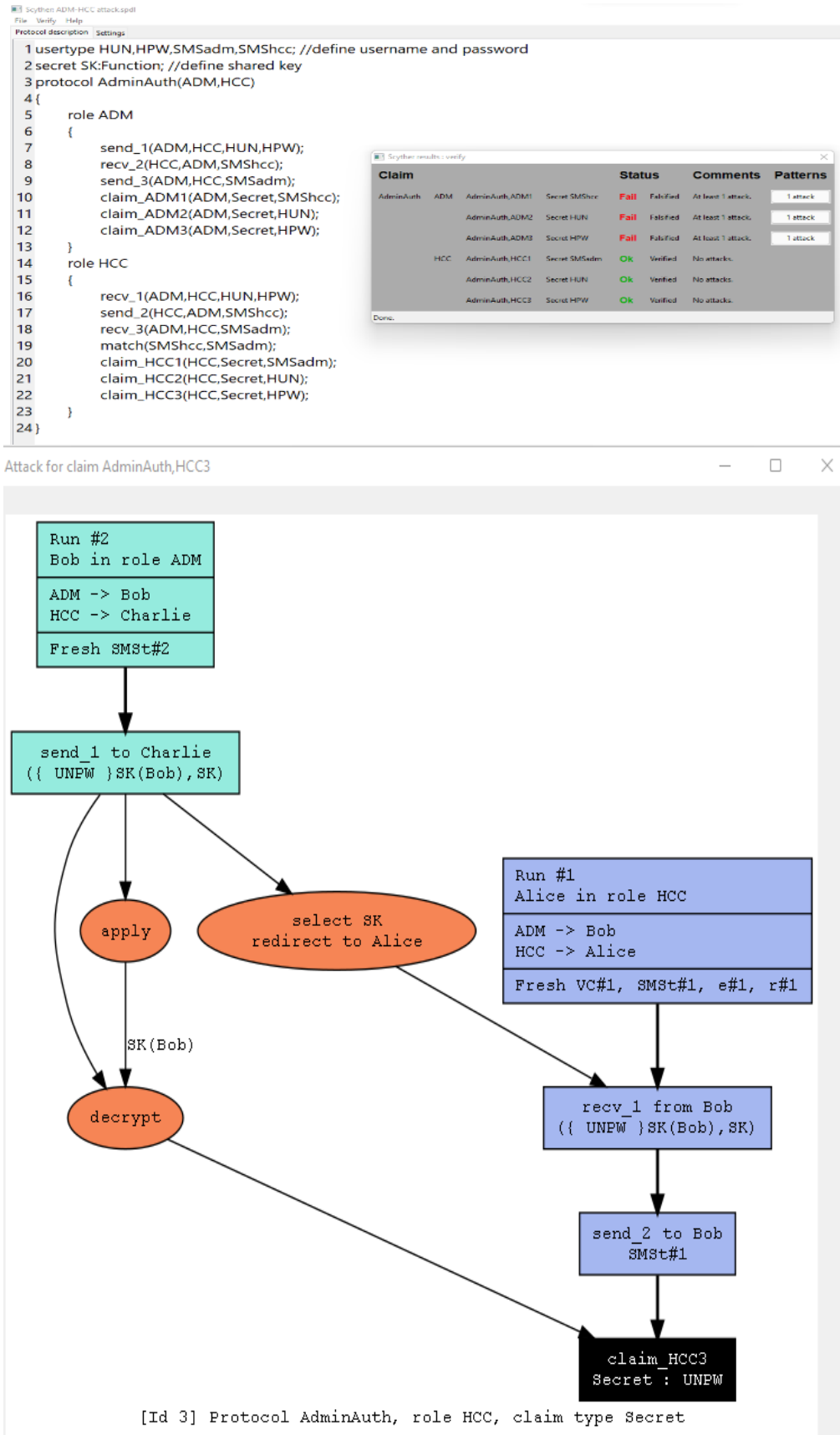


Figure 3. Traditional system

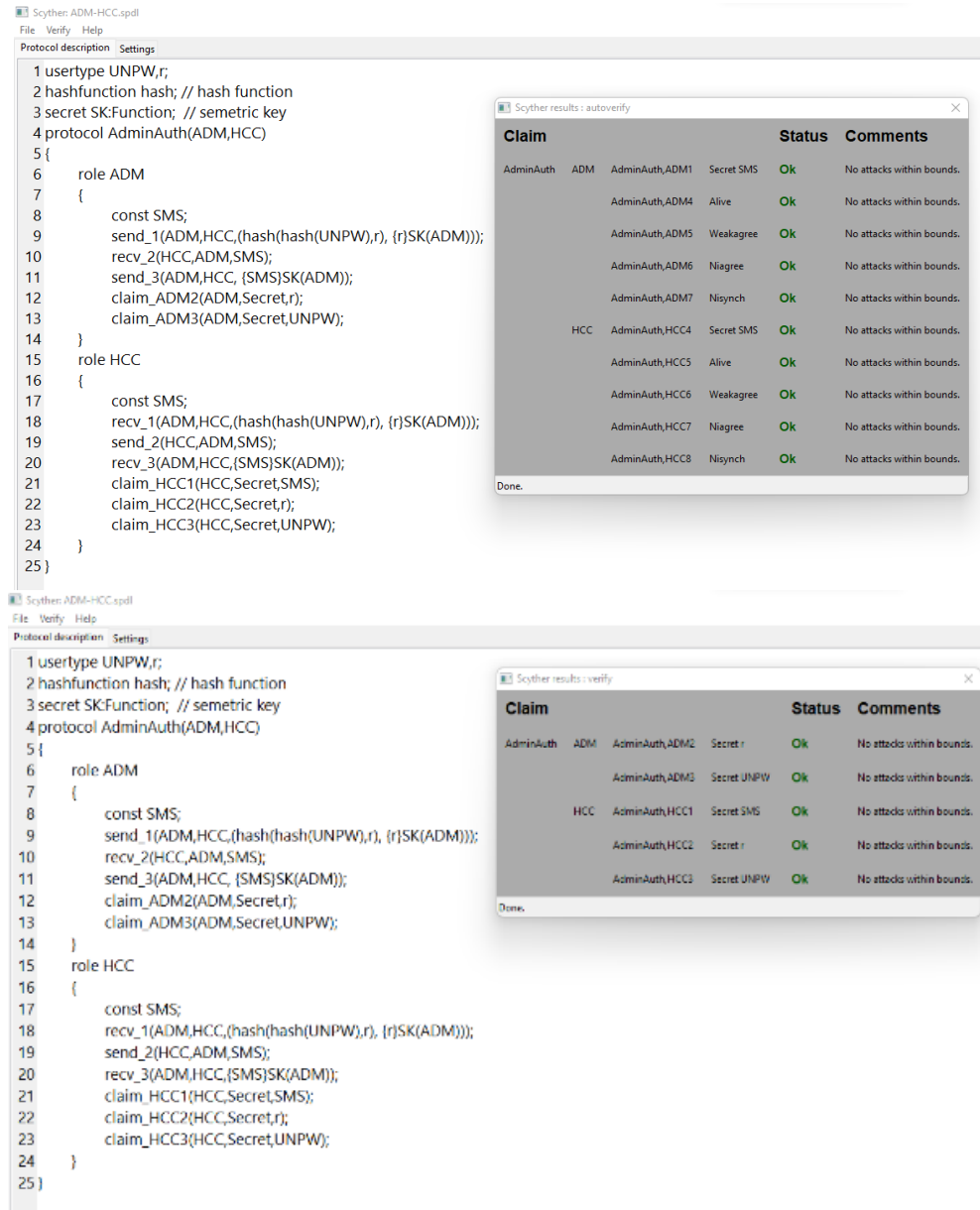


Figure 4. Verification system and verification auto system

4.2.4. Attack resistance

We could argue that any attack is positive if a CK adversary locates any technique to run several malicious attacks, such as impersonation, man-in-the-middle (MITM), replay, and insider. Most of all, an impersonation attack has a direct relationship with mutual authentication; the adversary needs to know the first-factor message (L , E_r) to masquerade as ADM and the challenge message (SMS_T) to pretence as HCC , respectively. Conversely, these messages are linked to the knowledge of login information. So, the proposed system could prevent impersonation attacks. Additionally, the *MITM* attack works in the same manner as active eavesdropping; the adversary constructs autonomous connections with the components of the network and dispatches messages between them to make them trust they are communicating directly to each other but actually, the adversary organizes this communication. Here, we denoted the mutual authentication provision, the shared key (SK_{ADM}) associated information to only registered ADM and HCC . In the CK model, the session key of the system is necessary not to be compromised even in the case of temporary secret leakage.

Our work, the brief secrets are r and SMS_T . An adversary fails to obtain both UN_{ADM} and PW_{ADM} to calculate L because these useful parameters (UN_{ADM} , PW_{ADM}) generate once for each login request. Assume that an adversary has access to the short-lived random number r and login information to compute L and get

SK_{ADM} key, but the adversary cannot have PNO_{ADM} to receive the SMS_T From HCC as shown in Figure 4. Therefore, our proposed system resists MITM, dictionary, impersonate, replay, sniffing, hijacking, and eavesdropping attacks because an adversary cannot access any benefits from exchanged parameters between ADM and HCC . So, an adversary fails to apply an insider attack because the SMS_T connects with the legal-administrator's phone number (PNO_{ADM}). Finally, DoS adds to the list of resisting attacks by the proposed system using timestamps for exchanging information.

4.2.5. Anonymity

An adversary faces difficulty to reveal the user's identity/password using CK adversary's perspective. Currently, it is obligatory to check the identity of login information transmitted among system components to reflect anonymity. We notice that all information in HCC saved using SHA-256 hash function $H(PW_{ADM}||UN_{ADM})$, which has a strong relationship with the identity of entities. To do so, the adversary should know break SHA-256, which is not feasible. Therefore, the proposed system provides anonymity.

4.2.6. Unlinkability

This feature focuses on preventing HCC from detecting ADM that has logged previously or not. We applied to feature in the proposed system by changing the values (SK_{ADM}, r, PW_{ADM}) each time ADM attempts to login. Consequently, HCC cannot link different logins with the same ADM .

4.2.7. Role-based access control

RBAC regulates access based on users' roles in the system and the rules that govern what access is granted to which users in which roles. In this paper, the users need permissions from ADM to apply some operations such as add, delete, update on EHRs. Here, U_i needs permission from ADM to delete, update or add new information on the EHR. The following steps describe the mechanism of gain role in more potential to U_i for apply some operation. The operation can be performed directly if the (modification /deletion) process is immediately after the insertion. However, if the modification/deletion operations are done after a time, the operations cannot be executed proximately. So, HCC sends SMS token (SMS_{TU}) via PNO_{U_i} to U_i for promoting him to a higher role. Then, U_i can apply operations when he uses SMS_{TU} as a code verification and gains permission for a limited time.

The results have confirmed the correctness of our proposed scheme in a realistic simulated environment. The authentication process was done secure and automatically for each factor. Thus, each user's time to check-in was short and depended only on the OTP. The first two-factor (something you know and have) authentication process is automatic and works in the smart factor principle. The second process using OTP data (something you have) takes approximately the speed of reading and input data to verify the user. This user-friendly scenario encourages employees to use it since they only feel authenticated by OTP verification. The other two factors are automatically authenticated instead of existing systems requiring several actions from the user. In terms of attempts to spoof, the results above show the possibility of spoofing one factor. Still, it takes too much effort to spoof all factors in a real situation. So, the proposed system has many good features such as location authentication factor "something you where" using ISP-IP, RBAC that depends on distributing the privilege among system's components. The summarised results are presented in Table 1. Our scheme implements multi-factor security to ensure that leaking data of all factors does not occur. Our work distinguishes to achieve all features in the Table 2 compared with other related work.

Table 1. The experiment's overall findings

| Results | Factors/attributes |
|--|--|
| Something you know (username/ password) (F1) | 100% accurate (like to our healthcare management system) |
| Something you have (smart device) (F2) | 100% accurate (the user's device is used to register in the system, and other users cannot register from the same device; as well as, we add the user's phone number to use as a second factor to receive SMS) |
| Something you where (location) (F3) | 100% accurate (when users wishes to work from outside the healthcare center, the transferred data should be protected by adding extra factor depending on ISP-IP) |
| Attempt for spoofing (F4) | The spoofing attack is possible to apply in any system, and it relies on the security sturdiness of authentication factors. On our practical side, the adversary can still not access the target's OTP crypto hash unless the victimized user willingly specifies it. Moreover, the adversary still needs to obtain extra information about other factors and gain the victim's device. Today, users feel reluctant to lend their mobile devices, even for a short time. |

Table 2. Demonstrates the main comparison between our work and related works

| Schemes/systems | Number of factors | Security | Accuracy | ISP IP Verification | Formal Verification |
|---------------------|----------------------|----------|----------|---------------------|---------------------|
| [27] | 2 (F1, F2) | Medium | Medium | No | No |
| [18] | 2 (F1, F2) | Medium | Medium | No | No |
| [20] | 2 (F2, F3) | Medium | Medium | No | No |
| [17] | 3 (F1, F2, F4) | Medium | Medium | No | No |
| [28] | 2 (F1, F2 or F2, F3) | Medium | Medium | No | No |
| [13] | 3 (F1, F2, F3) | High | High | No | No |
| [11] | 3 (F1, F2, F3) | High | High | No | No |
| [14] | 3 (F1, F2, F3) | High | High | No | No |
| [29] | 2 (F2, F3) | Medium | High | No | No |
| [30] | 2 (F2, F3) | Medium | High | No | No |
| [31] | 1 (F4) | N/A | High | No | No |
| The proposed system | 4 (F1, F2, F3, F4) | High | High | Yes | Yes |

One of the essential features of the proposed work is determining location via IP address (ISP IP Verification), which compares the user's IP address with the IP of the health server to determine whether the person works from inside or outside the health institution. Since operating from outside, the institution is more vulnerable to malicious attacks, as the data goes through the Internet, we should secure the data (encryption and digital signature) before sending it by the user's device to the HCC. Finally, the proposed scheme achieves four factors (F1, F2, F3, and F4) that reflect high accuracy and security compared with other previous works.

5. CONCLUSION

Security and privacy concerns are key roadblocks to large-scale healthcare system implementations. The authentication represents the core of this type of system. According to past studies, there are essentially no robust authentication schemes fit for this type of system. We propose a reliable, secure, and scalable multi-factor anonymous authentication technique as a first step in the right direction and follows by the second step focused on gaining privileges to all components of E-health system based on role for each one. The proposed scheme allows a legal component user/administrator to mutually authenticate with a healthcare center (cloud server) by using multi-factor technique such as OTP, SMS-token, ISP IP verification, and secure key management. Additionally, our work has good matrices like anonymity, unlinkability, and attack resistance. In the future, the security of the proposed scheme is explicitly demonstrated using the well-established Scyther tool and security analysis.




REFERENCES

- [1] M. A. A. Sibahee *et al.*, "Promising Bio-Authentication Scheme to Protect Documents for E2E S2S in IoT-Cloud," *2020 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 2020, pp. 1-6, doi: 10.1109/ICSPCC50002.2020.9259519.
- [2] M. A. A. Sibahee *et al.*, "Towards Iris-Based Authentication for Smart Devices in the Cloud," *Proceedings of Sixth International Congress on Information and Communication Technology. Lecture Notes in Networks and Systems*, vol. 216, pp. 953-964, 2022, doi: 10.1007/978-981-16-1781-2.
- [3] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018, doi: 10.3390/cryptography2010001.
- [4] K. Thomas *et al.*, "Protecting accounts from credential stuffing with password breach alerting," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 1556-1571.
- [5] D. Damopoulos and G. Kambourakis, "Hands-Free one-Time and continuous authentication using glass wearable devices," *Journal of Information Security and Applications*, vol. 46, pp. 138-150, 2019, doi: 10.1016/j.jisa.2019.02.002.
- [6] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, "A survey on multi-factor authentication for online banking in the wild," *Computers & Security*, vol. 95, p. 101745, 2020, doi: 10.1016/j.cose.2020.101745.
- [7] C. Vorakulpipat, E. Rattanalardnusorn, S. Sirapaisan, V. Savangasuk, and N. Kasisopha, "A Mobile-Based Patient-Centric Passive System for Guiding Patients Through the Hospital Workflow: Design and Development," *JMIR Mhealth Uhealth*, vol. 7, no. 7, p. e14779, 2019, 10.2196/14779.
- [8] B. Maciej, E. F. Imed and M. Kurkowski, "Multifactor Authentication Protocol in a Mobile Environment," *IEEE Access*, vol. 7, pp. 157185-157199, 2019, doi: 10.1109/ACCESS.2019.2948922.
- [9] B. -W. Kwon, P. K. Sharma, and J. -H. Park, "CCTV-Based Multi-Factor Authentication System," *J Inf Process Syst*, vol. 15, no. 4, pp. 904-919, 2019, doi: 10.3745/JIPS.03.0127.
- [10] A. Ullah, H. Xiao, and T. Barker "A multi-factor authentication method for security of online examinations," in *International Conference on Smart Grid and Internet of Things*, 2018, pp. 131-138, doi: 10.1007/978-3-030-05928-6_13.
- [11] N. A. K. Abiew, M. D. Jnr., and S. O. Banning, "Design and Implementation of Cost Effective Multi-factor Authentication Framework for ATM Systems," *Asian Journal of Research in Computer Science*, pp. 7-20, 2020, doi: 10.9734/ajrcos/2020/v5i330135.
- [12] E. Akinola Kayode, Y. Adekunle, A. Adebayo, "Multi-factor authentication model for integrating iris recognition into an automated teller machine," *International Journal of Computer Applications*, vol. 181, no. 45, pp. 1-8, 2019, doi: 10.5120/ijca2019918530.




- [13] A. Bissada and A. Olmsted "Mobile multi-factor authentication," in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2017, pp. 210-211, doi: 10.5120/ijca2019918530.
- [14] A. A. Alghamdi "A verification system for multi-factor authentication for E-healthcare architectures," *Arab Journal for Scientific Publishing (AJSP)*, vol. 2663, p. 5798, 2021.
- [15] Y. Liu, Q. Zhong, L. Chang, Z. Xia, D. He, and C. Cheng, "A secure data backup scheme using multi-factor authentication," *IET Information security*, vol. 11, no. 5, pp. 250-255, 2017, doi: 10.1049/iet-ifs.2016.0103.
- [16] S. Choi and D. Zage, "Addressing insider threat using "where you are" as fourth factor authentication," *2012 IEEE International Camahan Conference on Security Technology (ICCST)*, 2012, pp. 147-153, doi: 10.1109/CCST.2012.6393550.
- [17] K. I. Ramatsakane and W. S. Leung, "Pick location security: Seamless integrated multi-factor authentication," *2017 IST-Africa Week Conference (IST-Africa)*, 2017, pp. 1-10, doi: 10.23919/ISTAFRICA.2017.8102391.
- [18] G. Sciarretta, R. Carbone, S. Ranise, and L. Viganò "Design, formal specification and analysis of multi-factor authentication solutions with a single sign-on experience," in *International Conference on Principles of Security and Trust*, 2018, pp. 188-213, doi: 10.1007/978-3-319-89722-6_8.
- [19] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudhary, "SELAMAT: A New Secure and Lightweight Multi-Factor Authentication Scheme for Cross-Platform Industrial IoT Systems," *Sensors*, vol. 21, no. 4, p. 1428, 2021, doi: 10.3390/s21041428.
- [20] S. Jindal and M. Misra, "Multi-factor Authentication Scheme Using Mobile App and Camera," in *Advances in Communication and Computational Technology*, 2021, pp. 787-813, doi: 10.1007/978-981-15-5341-7_60.
- [21] W. Li, H. Cheng, P. Wang and K. Liang, "Practical Threshold Multi-Factor Authentication," in *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3573-3588, 2021, doi: 10.1109/TIFS.2021.3081263.
- [22] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," *Computers & Security*, vol. 88, p. 101619, 2020, doi: 10.1016/j.cose.2019.101619.
- [23] A. Ali, M. Ahmed, A. Khan, A. Anjum, M. Ilyas, and M. Helfert, "VisTAS: blockchain-based visible and trusted remote authentication system," *PeerJ Computer Science*, vol. 7, p. e516, 2021, doi: 10.7717/peerj-cs.516.
- [24] S. Das, B. Wang, Z. Tingle, L. J. Camp, "Evaluating user perception of multi-factor authentication: A systematic review," *arXiv preprint arXiv*, 2019, doi: 10.48550/arXiv.1908.05901.
- [25] S. Pichetjamroen, E. Rattanalerdnusorn, C. Vorakulpipat and A. Pichetjamroen, "Multi-Factor based Face Validation Attendance System with Contactless Design in Training Event," *2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, 2021, pp. 637-640, doi: 10.1109/ECTI-CON51831.2021.9454779.
- [26] M. A. de Carvalho Junior, "Health information system role-based access control current security trends and challenges," *Journal of Healthcare Engineering*, vol. 2018, p. 6510249, 2018, doi: 10.1155/2018/6510249.
- [27] T. P. Abayomi-Zannu, A. Odun-Ayo, and T. F. Barka, "A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication," in *Journal of Physics: Conference Series*, vol. 1378, p. 032104, 2019, doi: 10.1088/1742-6596/1378/3/032104.
- [28] N. A. Shaji and S. Soman, "Multi-factor authentication for net banking," *International Journal of System and Software Engineering*, vol. 5, no. 1, pp. 11-14, 2017.
- [29] R. A. Kurniawan, "Radio Frequency Identification and Image-Based Facial Identification as an Employee Attendance System," *Technology and Natural Sciences*, vol. 2, no. 1, pp. 18-26, 2020, doi: 10.46923/ijets.v2i1.67.
- [30] C. Vorakulpipat, S. Pichetjamroen, and E. Rattanalerdnusorn, "Usable comprehensive-factor authentication for a secure time attendance system," *peerJ computer science*, vol. 7, p. e678, 2021, doi: 10.7717/peerj-cs.678.
- [31] Y. Liu, L. Chen, Z. Ou, J. Chen and J. Wu, "A Crowdsourcing based Multi-modal Attendance Tracking System for Smartphone Users," *2020 International Symposium on Computer Engineering and Intelligent Communications (ISCEIC)*, 2020, pp. 61-64, doi: 10.1109/ISCEIC51027.2020.00021.

BIOGRAPHIES OF AUTHORS



Mohammad Fareed    is MSc student at University of Basrah, Education College for Pure Sciences, Computer Department. He received his BSc in computer science from University of Basrah, College of Science, Department of Computer Science, Iraq in 2016. His research interests include cyber security, cryptography, information technology, and security of systems. He can be contacted at email: my4irq@gmail.com and pedupg.m.fareed@uobasrah.edu.iq.



Prof. Dr. 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: alihas@upm.edu.my and Ali.Yassin@uobasrah.edu.iq.