Indonesian Journal of Electrical Engineering and Computer Science
Vol. 23, No. 1, July 2021, pp. 140~149
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i1.pp140-149

Password authentication scheme based on smart card and QR code

Mushtaq Hasson[1], Ali A.Yassin[2], Abdulla J. Yassin[3], Abdullah Mohammed Rashid[4], Aqeel A. Yaseen[5], Hamid Alasadi[6]
[1-3,6]Computer Science Department, Education College for Pure Science, University of Basrah, Basrah, Iraq
[4]Education College for Human Science, University of Basrah, Basrah, Iraq
[5]Al Kunooz University College Computer Engineering Techniques, Basrah, Iraq

Article Info

Article history:

Received Feb 13, 2021
Revised Apr 28, 2021
Accepted May 1, 2021

Keywords:

Biometric
Cloud computing
Dynamic authentication
QR-code
Smart card
User anonymity

ABSTRACT

As a hopeful computing paradigm, cloud services are obtainable to end users based on pay-as-you-go service. Security is represented one of the vital issues for the extended adoption of cloud computing, with the object of accessing several cloud service providers, applications, and services by using anonymity features to authenticate the user. We present a good authentication scheme based on quick response (QR) code and smart card. Furthermore, our proposed scheme has several crucial merits such as key management, mutual authentication, one-time password, user anonymity, freely chosen password, secure password changes, and revocation by using QR code. The security of proposed scheme depends on crypto-hash function, QR-code validation, and smart card. Moreover, we view that our proposed scheme can resist numerous malicious attacks and are more appropriate for practical applications than other previous works. The proposed scheme has proved as a strong mutual authentication based on burrows-abadi-needham (BAN) logic and security analysis. Furthermore, our proposed scheme has good results compared with related work.

Corresponding Author:

Abdulla J. Yassin
Computer Science Department, Education College for Pure Science
University of Basrah, Iraq
Email: abdullajas@uobasrah.edu.iq

1. INTRODUCTION

Parallel and distributed systems have essentially changed the manner entities and enterprises share, procedure and store information today. Furthermore, security issues play a principal role in parallel and distributed systems, as better obtainability and access to information, in turn, involve that there is a greater need to keep them. To solve these issues, there are many security skills, tools and systems have been presented [1]-[10] during the years from 1985-2020. For instance, several access control methods such as trust management systems that have been offered over these time period.

In recent times, cloud computing [2] considers the on-demand service model for information technology provides, often depended on parallel and distributed computing technologies. With the fast growth of cloud computing models, service providers gradually put their services in clouds for users and customers. Cloud computing has preserved a lot of well-merited attention lately due to the fluctuant advantages its service-oriented manner has existing, such as pay-as-you-go, on-demand services. In the cloud environment, customers can access the resources and services without knowing the location of data, computing devices, and platforms. With the acceptance of cloud computing services, authorization,

authentication and security concerns of cloud computing have become major research topics. Authentication is the core of the security field, whether in the cloud or any network. Managing identities and authentication are the main challenges of corporate networks and cloud computing. Additionally, these challenges became more important in the e-commerce world for the purpose of distribution resources thru governmental lines [9].

Customers prefer the security to be smooth and transparent. Customers' top preferability is access-the facility to obtain the information they need to acquire their work finished, as rapidly and opportunely as possible. The main issue is that security and accessibility will always take opposite ends of a continuum. Consequently, illegitimate users can feat these security faults and either misappropriate secret information or interrupt the usual operation of the Internet using different kinds of malicious attacks and threats. Accordingly, sturdy user authentication does not have high abilities in cloud environments [9], [11]-[13].

Nowadays, a multi-factor authentication scheme supports meaningfully more security but is suffered from slowly of implementation, even within local united networks, much less in the cloud. Commonly, there are three kinds of authentication factors: i) Knowledge factor based on something user's known, such as personal identification number (PIN); ii) Possession factor that depends something user's has, such as smart cards; iii) Inheritance factor that depends on biometric characteristics, such as face recognition, voiceprint and iris recognition [14].

On the positive side, the typical scheme for strong authentication deal between legal user and the cloud service provider is to employ static identity for each user's login phase, which can be exposed some important information about a real user's login message to an adversary and then fail to prevent the peril of identity robbery or impersonating [15]. To avoid aforementioned faults, remote user authentication based on user anonymity is a vital topic issue for confirming the privacy of the legitimate user and dynamic identity (ID)-based schemes are worthy to attract attention. For numerous transaction-oriented services like remote commercial service and e-payment based on the smart card, the central goal of user anonymity is to support a way for preserving identity information during authentication phase and no one has the ability to keep track of a particular user through the exchanging messages between entities.

Khan *et al.* [16] demanded that Wang et al.'s scheme is still vulnerable to some faults like an absence of user anonymity throughout authentication phase, a privation of session key agreement, and does not support revocation feature. Li *et al.* [17] focus on Khan *et al.* scheme [16], which cannot provide anonymity of a login user and does not resist insider attacks. Moreover, in 2012, Madhusudhan [18] exhibited that Khan *et al.* scheme suffers from withstanding the insider attack and cannot provide the forward secrecy of the session key throughout the authentication phase.

In this paper, we utilize the user's QR code of his fingerprint as a biometric-knowledge factor with the smart card in a good method that does not require extra hardware and software in the user's login phase. Our advanced scheme enjoys in several features like efficiency, user anonymity, flexible password-based remote mutual authentication, a one-time password for each login session, users can freely select and change their passwords, a cloud server and the user can build authenticated sessions' keys and our proposed scheme produces once a key for each user's login request in the authentication phase. Furthermore, our work can be applied to verify a genuine user and authenticated cloud server without illuminating users' passwords whenever it is judged to be necessary. Moreover, our scheme can withstand several types of attacks such as DOS attack, replay attack, insider attack, forgery attack, off-line attack, and reflection attack. Constantly, compared with the previous works, our scheme is yet powerful both in computation and communication cost. In the other hand, we compare our work with Khan's scheme and another multi-factor authentication schemes. As viewed in Figure 1. Organization paper section 2 presents QR code, Fingerprint factor. The proposed scheme and security analysis are showed in section 3. Section 4 contains the discussion and comparison with the related works. Section 5 gives our conclusions.

2. DESIGN ISSUES

In this section, we demonstrate the QR Code, feature extraction of fingerprint, design issues of proposed scheme, and main comparison with the other related works.

2.1. Quick respond code

A quick response code (QR code) considers a type of two-dimensional array barcode much faster than old-style UPC barcodes (see Figure 2). QR codes represent incoming cultural zeitgeists–now they are applied in e-business promotions such as discount coupons, announcements, and resource chain management, areas far outside their original imagined use states like tracking automobile portions in the auto industrial industry. QR codes support a cheap, simple, easy, and secure technique to transfer information in a "push" design to individuals that have the skill to read the symbol. Furthermore, open source libraries occur for

producing QR codes from a variability of data sources, as long as the information can appropriate into a stable number of letterings (alphanumeric strings) based on the preview version of the QR code [19].

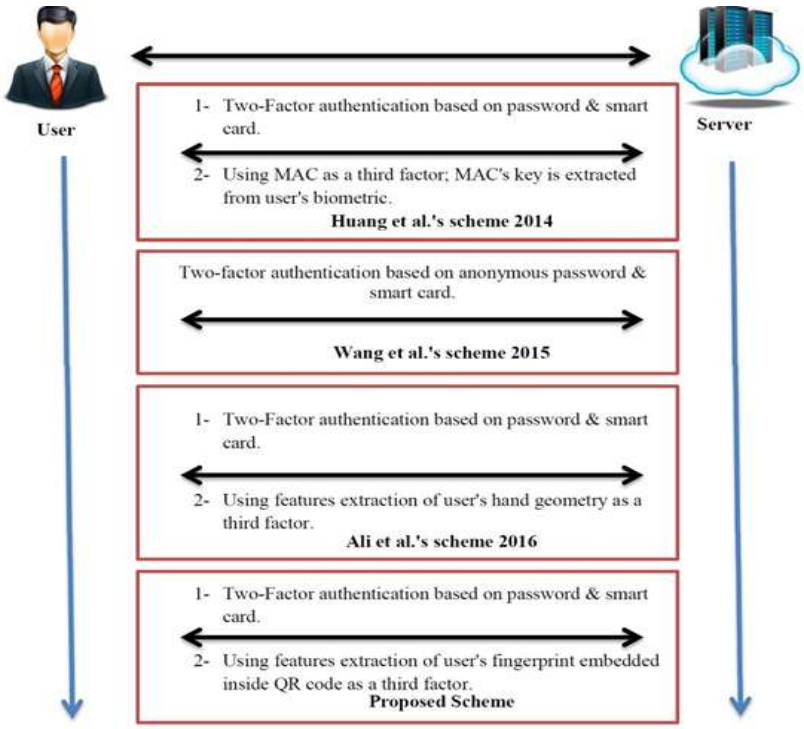

Figure 1. Compare our work with another scheme

(a) (b) (c)

Figure 2. demonstrates of example QR codes; (a) coordinates, (b) URL, (c) URI

2.2. Feature extraction of fingerprint

In fact, the fingerprint is one of the most widespread of biometric techniques as well as is unique and stays unchanged during the life. A fingerprint consists of the pattern of ridges on the surface of the finger. A ridge is represented by a single curved section, and a valley is posited in the region between two neighboring ridges. The minutiae, which are the local abruptions in the ridge streaming pattern, support the features that will be used in the identification phase. Details of the orientation, type, and location of minutiae are occupied into account when implementing minutiae extraction [20].

3. PROPOSED SCHEME

Our work employs the symbolizations prepared at in Table 1. In our work, the user (U_i) needs to register as a first step in the remote server (S) that has been found in cloud service provider (CSP). Thereafter, the user gains his personal smart card from the authenticated server (S). After that, U_i pushes smart card into the machine to obtain the services from the server, on ensuring from credentials information of the user at login phase. Briefly, the proposed scheme needs five phases as below. The symbols used in our proposed scheme are discussed in Table 1.

Table 1. Notations used in our proposed scheme

Symbol	Description
U_i	A real user.
S	An authenticated server that is found in CSP.
CSP	Cloud Service Provider
IDU, PW	Identity and password of U_i.
PWU_i	Anonymous of password.
h()	The hash function.
FPU_i	User's fingerprint.
FXU_i	Features extraction in level 3 of user's fingerprint.
X	The secret key of S.
N	It is random integer random.
I	It is the registration count of user
Y	A primitive element which is used in login phase.
IDU_i	Anonymous of user's identity.
GenQR()	The function is used to generate user's QR image QRU_i.
SC	The smart card of a user.

3.1. Registration phase

To obtain benefits of from a legitimate server, U_i should be completed the registration phase. The details of main steps are shown as follows:

- **Step R1:** $U_i \xrightarrow{IDU, PWU_i, FPU_i} \boldsymbol{S}$, U_i enters his identity IDU and selects a password PW, then calculates $PWU_i = h(PW)$. Additionally, U_i imprints his fingerprint FPU_i. Finally, U_i sends his (IDU, PWU_i, FPU_i) with registration request to an authenticate server S in a secure channel.
- **Step R2**: $S \rightarrow FXU_i, X, IDU_i, Y, QRU_i$, in this step, S checks the validity of U_i's identity. If IDU is already found in users' database, S request from a user to use a new identity. Otherwise, S computes feature extraction of user's fingerprint in level3 $FXU_i = \text{ExtractL3}(FPU_i)$, selects secret key $X \in Z_n$, where $n = p \times q$; p and q large prime numbers. After that, S computes $IDU_i = h(IDU \,||\, N \,||\, I \,||\, X)$, where N is integer random that selected from FXU_i, I is a count related by the registration of each user, if U_i is the first registered user at the system, I =0, else, $I = I + 1$. Furthermore, S adds $< IDU_i, I >$ for each new user in registered user's database. Finally, S computes $Y = h(FXU_i)^{PWU_i} \bmod p \oplus X$ and QR image based on an embedded crypto hash function of FXU_i inside the QR image $QRU_i = \text{GenQR}(h(FXU_i))$.
- **Step R3:** $\boldsymbol{S} \xrightarrow{SC, QRU_i} U_i$, S embeds the main values { IDU_i, Y, p, N } existed inside his smart card (SC) and then pushes SC and QRU_i to U_i.
- **Step R4:** $U_i \xrightarrow{QRU_i} \boldsymbol{Smart\ Phone}$, U_i keeps (SC) and saves QRU_i in his smartphone.

3.2. Login phase

In this phase, U_i should be inserted his SC into a card reader. Then, he inputs the identity IDU_i', password PW. U_i also extracts $h'(FXU_i)$ from his QR code image QRU_i' which saved on his smartphone. SC manages the login phase as viewed in the Figure 3.

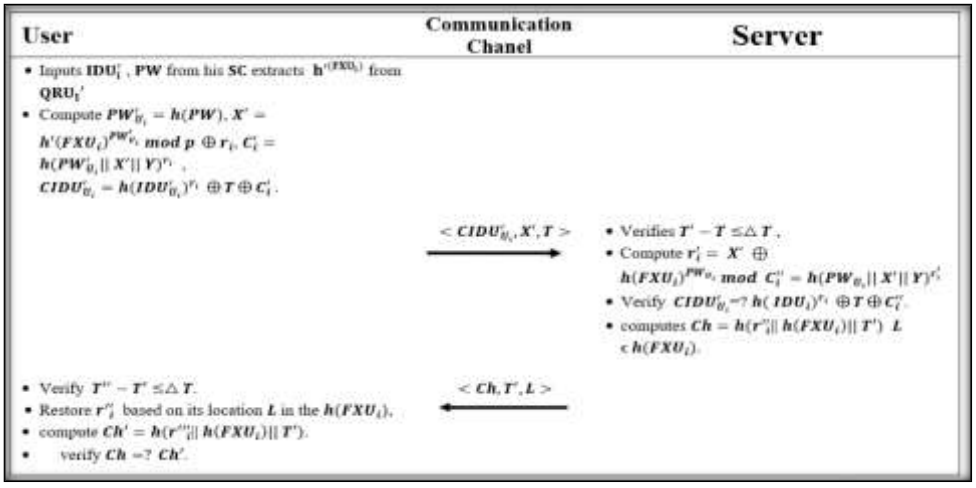

Figure 3. Login and authentication phases

- **Step L1.** Calculate $PW'_{U_i} = h(PW),\ X' = h'(FXU_i)^{PW'_{U_i}} mod\ p \oplus r_i,\ C'_i = h(PW'_{U_i} || X' || Y)^{r_i}$. Where $r_i \in Z_N^*$ is integer random number.
- **Step L2.** Compute $CIDU'_{U_i} = h(IDU'_{U_i})^{r_i} \oplus T \oplus C'_i$, where T is the U_i's current timestamp.
- **Step L3.** The user's smart card submits his login request message M to the remote server; $\boldsymbol{SC} \overset{M}{\rightarrow} \boldsymbol{S}: M = \{ CIDU'_{U_i}, X', T\}$.

3.3. Mutual authentication phase

In the end of login user's moment at time T', S completes the following steps (see Figure 3):

- **Step A1:** S checks the validity of the time-stamp T. If $T' - T \leq \triangle T$, then a genuine server S accepts user's login request and then implements the next step. Else, S dismisses this phase.
- **Step A2**: S retrieves $r'_i = X' \oplus h(FXU_i)^{PW_{U_i}} mod\ p$ and compute $C''_i = h(PW_{U_i} || X' || Y)^{r'_i}$, and checks whether $CIDU'_{U_i}$ is equal to $h(\ IDU_i)^{r_i} \oplus T \oplus C''_i$. If so, S gives permeation to accept the login request.
- **Step A3**: S computes $Ch = h(r'_i || \ h(FXU_i) || \ T')$, where r'_i is random integer number which selected from $h(FXU_i)$ in the position L(see Figure 4). Then, S sends (Ch, T', L) to U_i's SC.
- **Step A4**: upon receiving S's message (Ch, T', L) at time T'', SC checks the verification of $T'' - T' \leq \triangle T$. If the time delay of sending message is unacceptable, dismiss this phase. Else, SC restores r''_i based on its location L in the $h(FXU_i)$, and computes $Ch' = h(r''_i || \ h(FXU_i) || \ T')$. As the last step, it verifies $Ch =?\ Ch'$. If verification hold, S is an authenticated by U_i. Otherwise, terminate the mutual authentication phase.

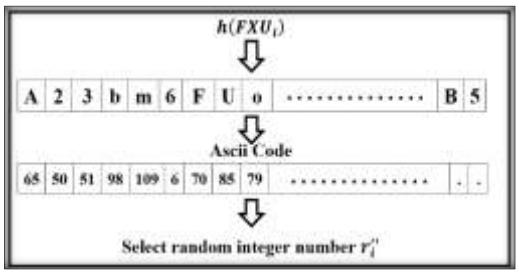

Figure 4. Shows the mechanism to extract r''_i

3.4. Password change phase

In our proposed scheme, this phase has performed in independently manner without interacting with remote server. Furthermore, the user doesn't need to change his fingerprint's information and QR Code image. The following steps detail the working of this phase:

- **Step C1.** U_i adds SC into the machine and enters IDU'_i, previous password PW'_i. After that, U_i should be implemented in the above aforementioned phases login and mutual authentication. The server S checks the validity of old password of user PW'_i.
- **Step C2.** U_i enters a new password $PW_{new\,i}$ and computes $PW_i = h(PW_{new\,i})$. Then, he retrieves his fingerprint's information $h(FXU_i)$ from his QR Code image (QRU_i) which has been saved in user's smartphone.
- **Step C3.** SC computes $Y_{new\,i} = h(FXU_i)^{PW_{new\,i}} mod\ p \oplus X$ and replaces the old Y with a new $Y_{new\,i}$.

3.5. Smart card revocation phase

To prevent an attacker from using U_i's smart card when he lost his smart card, this phase will apply the following steps:

- **Step V1.** U_i selects his identity IDU and picks a new password PW_{new}, then calculates $PWU_i = h(PW_{new})$, retrieves his FPU_i from QRU_i. Finally, U_i sends his (IDU, PWU_i, FPU_i) with revocation request to the server S in a protected communication.
- **Step V2.** Upon receiving the U_i's registration request, S validates of U_i's identity. If IDU is already found in users' database based on his FPU_i. If both IDU and FPU_i of U_i are found, S computes $I = I + 1$ as a first step and calculates $IDU_i = h(IDU\ ||\ N||\ I||\ X)$, where N is integer random that picked from FXU_i. In the second step, S updates $< IDU_i,\ I >$ with $< IDU_i,\ I + 1 >$ in registered users' database.
- **Step V3.** Finally, S computes $Y = h(FXU_i)^{PWU_i} mod\ p \oplus X$ and embeds the main values $\{ IDU_i, Y, p, N \}$ inside SC and then returns SC to U_i.

4. PROOF OF CRYPTO-SECURITY

In this section, Burrows-Abdi-Needham (BAN) logic is used to prove the security of the mutual authentication phase between U_i and S. There are some parameters applied in this section as below:

- $P| \equiv A$: P principle believes A's declaration.
- $P \lhd A$: P notes A; it is mean that P has the ability to receive message combined with A.
- $P|\sim A$: P sent A.
- $\#(A)$: The message A is a new.
- $P \overset{K}{\leftrightarrow} Q$: P and Q communicate based on shared key K.
- (A, B): A or B is one part of (A, B).
- $(A)_K$: The crypto-hashed value of A using shared K.
- $(A, B)_K$: The crypto-hashed value of A and B based on key K.
- $< A >_B$: A combined with B.
- $\{A\}_K$: A is encrypted by using shared key K.
- $\{A, B\}_K$: A and B are encrypted by using shared key K.

The fundamental rules of BAN-logic postulates are as viewed below:

- Rule (1): Message meaning instruction.

$$\frac{P|\equiv P\overset{K}{\leftrightarrow}Q, P\lhd(A)_K}{P|\equiv Q|\sim A}$$

- Rule (2): Nonce-verification instruction.
-

$$\frac{P|\equiv\#(A), P|\equiv Q|\sim A}{P|\equiv Q|\equiv A}$$

If P sees that the fresh message A has been expressed newly (freshness) and P confirms that Q once said A, thereafter P believes that Q believes A.

- Rule (3): Freshness instruction.

$$\frac{P|\equiv\#(A)}{P|\equiv\#(A,B)}$$

If one part (Message A or B) is identified to be new, formerly the complete formula is new.

- Rule (4): Jurisdiction instruction.

$$\frac{P|\equiv Q|\Rightarrow A, P|\equiv Q|\equiv A}{P|\equiv A}$$

The main two parties user (U_i) and remote server (S) that is located at cloud service provider (CSP). We are aimed to view the major aims of our proposed scheme as follows:

- $Goal_1$: $U_i| \equiv (U_i \overset{SK}{\leftrightarrow} S)$.
- $Goal_2$: $S| \equiv (U_i \overset{SK}{\leftrightarrow} S)$.

Next, we apply BAN logic on the proposed scheme. The proposed scheme generic types are viewed in the following:

Message1. $U_i \rightarrow S :< CIDU'_{U_i}, X', T >$

Message 2. $S \rightarrow U_i :< Ch, T', L >$

where U_i represents the smart card SC side. The typical forms of our proposed scheme are as follows:

Message1. $U_i \rightarrow S :< h\left(IDU'_{U_i}\right)^{r_i} \oplus T \oplus h(PW'_{U_i}|| X'|| Y)^{r_i}$

$$, h'(FXU_i)^{PW'_{U_i}} \bmod p \oplus r_i, T >$$

Message 2. $S \rightarrow U_i :< h(r''_i|| h(FXU_i)|| T'), T', L >$

To analyze our work, the following assumptions are also required:

(A1:) $U_i| \equiv \#(T)$;

(A2:) $S| \equiv \#(T'')$;

(A3:) $U_i| \equiv (U_i \overset{SK}{\leftrightarrow} S)$;

(A4:) $S| \equiv (U_i \overset{SK}{\leftrightarrow} S)$;

(A5:) $U_i| \equiv S| \equiv (U_i \overset{SK}{\leftrightarrow} S)$;

(A6:) $S| \equiv U_i| \equiv (U_i \overset{SK}{\leftrightarrow} S)$;

We use BAN logic instructions and the assumptions to evaluate the idealized form of our work protocol. The basic crypto-proofs are characterized as below:
Depending on the message 1, we could conclude:
S1: $\triangleleft$ $((\mathrm{IDU}'_{\mathrm{U_i}},\ \mathrm{r_i}, \mathrm{X}', \mathrm{Y}, \mathrm{PW}'_{\mathrm{U_i}})_{\mathrm{h}}, \mathrm{X}', \mathrm{T})$
Depending on A4, we perform the message meaning instruction to obtain:
$\mathrm{S}|\ \equiv (\mathrm{U_i} \overset{(\mathrm{Ch},\mathrm{T}',\mathrm{L})}{\longleftrightarrow} \mathrm{S})$
S2: $\mathrm{S}|\ \equiv (\mathrm{U_i}|{\sim}\mathrm{T}')$
Depending on (A1), we perform the freshness conjuncatenation instruction to obtain:
S3: $\mathrm{U_i}|\ \equiv \#(\mathrm{IDU}'_{\mathrm{U_i}}, \mathrm{r_i}, \mathrm{X}', \mathrm{Y}, \mathrm{PW}'_{\mathrm{U_i}})_{\mathrm{h}}$
Depending on (S2) and (S3), The proposed scheme performs the nonce verification rule to obtain:
S4: $\mathrm{S}| \equiv \mathrm{U_i}| \equiv (\mathrm{IDU}'_{\mathrm{U_i}}, \mathrm{r_i}, \mathrm{X}', \mathrm{Y}, \mathrm{PW}'_{\mathrm{U_i}})_{\mathrm{h}}$
Depending on A4 and S4, our work uses the jurisdiction instruction to obtain:
S5: $\mathrm{S}| \equiv \mathrm{T}'$
Depending on $\mathrm{K} = (\mathrm{h}(\mathrm{r}'_{\mathrm{i}}|| \mathrm{h}(\mathrm{FXU_i})|| \mathrm{T}'), \mathrm{L})$, S5, and A2, we could get:
S6: $\mathrm{S}| \equiv (\mathrm{U_i} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{S})$ (Goal 2).
Depending on the message 2, we could get:
S7: $\mathrm{U_i} \triangleleft (\mathrm{IDU_i}, \mathrm{FXU_i})_{\mathrm{h}}, \mathrm{T}''$
Depending on A3, our works uses the message meaning instruction to conclude:
S8: $\mathrm{U_i}| \equiv \mathrm{S}|{\sim}\mathrm{T}''$
Depending on A2, our work employs the freshness -conjuncatenation instruction to conclude:
S9: $\mathrm{U_i}| \equiv \#(\mathrm{IDU_i}, \mathrm{FXU_i})_{\mathrm{h}}, \mathrm{T}''$
Depending on the S8 and S9, the proposed scheme uses nonce verification instruction to conclude:
S10: $\mathrm{U_i}| \equiv \mathrm{S}| \equiv (\mathrm{IDU_i}, \mathrm{FXU_i})_{\mathrm{h}}, \mathrm{T}''$
Depending on the assumption A3 and 10 , we use the jurisdiction instruction to conclude:
S11: $\mathrm{U_i}| \equiv \mathrm{T}''$
Depending on $\mathrm{SK} = (\mathrm{CIDU}'_{\mathrm{U_i}}, \mathrm{X}', \mathrm{Ch})$, S11 and A1, we could conclude:
S12: $\mathrm{U_i}| \equiv (\mathrm{U_i} \overset{\mathrm{SK}}{\leftrightarrow} \mathrm{S})$ (Goal 1)

5. SECURITY ANALYSES AND DISCUSSION ON THE POSSIBLE ATTACKS

In this part, we analyze our work and demonstrate that the proposed scheme can resist some of the familiar attacks. Additionally, the proposed has good security characteristics.

Proposition 1. Our work can provide secure mutual authentication.

Proof. It means both the remote server and legal user to authenticate each other. In this paper, authentication of U_i to S has used three steps as follows (see Figure 2):

- $U_i \overset{M}{\rightarrow} S: M = \{ CIDU'_{U_i}, X', T\}$. So, $U_i$computes the main parameters $(CIDU'_{U_i}, X')$one time for each login phase based on $h'(\mathrm{FXU_i})$, r_i, p, Y that saved in QR image and smart card.
- $S \overset{M}{\rightarrow} U_i: M = \{ Ch, T', L\}$. S checks the authority of U_i based on the time-stamp T and exams whether $CIDU'_{U_i}$ is equivalent to $h(IDU_i)^{r_i} \oplus T \oplus C''_i$ where $C''_i = h(PW_{U_i}|| X'|| Y)^{r'_i}$. If the result is true, S ensures from authenticating of U_i and sends challenge $\{ h, T', L\}$ to U_i.
- U_i checks the validity of S based on verifying $T'' - T' \leq \triangle T$ and compares $Ch ? = h(r''_i|| h(FXU_i)|| T')$. If so, U_i ensures from authenticating of S.

Proposition 2. Our proposed scheme can provide perfect forward secrecy.

Proof. In our work, the common session key depends on $\mathrm{FXU_i}$ saved on user's smartphone that uses to generate $\mathrm{X}' = \mathrm{h}'(\mathrm{FXU_i})^{\mathrm{PW}'_{\mathrm{U_i}}} \bmod \mathrm{p} \oplus \mathrm{r_i}$ in login phase. In the same time, the server extracts the random r'_{i} is a random integer number which selected from $\mathrm{h}(\mathrm{FXU_i})$ in the position L. After that, S computes $\mathrm{Ch} = \mathrm{h}(\mathrm{r}'_{\mathrm{i}}|| \mathrm{h}(\mathrm{FXU_i})|| \mathrm{T}')$ and then sends it to $\mathrm{U_i}$ to check the authority of S.

Even if the secret key Y and three values p, q and $\mathrm{r_i}$ are compromised for some reason, an adversary fails to compute any previous X' without getting $\mathrm{FXU_i}$ and $\mathrm{PW}'_{\mathrm{U_i}}$ because obtain $\mathrm{FXU_i}$ is very difficult which embeds inside QR image $\mathrm{QRU_i}$ saved in $\mathrm{U_i}$'s smartphone. Additionally, if an adversary can eavesdrop all transmitted messages $\mathrm{CIDU}'_{\mathrm{U_i}}, \mathrm{X}', \mathrm{Ch}, \mathrm{L}$, he fails to use again for logging in the system instead legal user $\mathrm{U_i}$. Because these messages are generated one time for each user's login request. Therefore, our proposed scheme ensures perfect forward secrecy.

Proposition 3. Our work offers robust login and password change phase.

Proof. Upon receiving the inputs, identity IDU_i', password PW. U_i also extracts $h'(FXU_i)$ from his QR code image QRU_i' which saved on his smartphone. The smart card completes $CIDU_{U_i}' = h(IDU_{U_i}')^{r_i} \oplus T \oplus C_i'$ based on $C_i' = h(PW_{U_i}' || X' || Y)^{r_i}$ and then verifies $CIDU_{U_i}' =? h(IDU_i)^{r_i} \oplus T \oplus C_i''$. If not verified, dismiss the phase. The main condition $CIDU_{U_i}' =? h(IDU_i)^{r_i} \oplus T \oplus C_i''$ includes important information which can only be completed in the case of retrieving the biometric information $h'(FXU_i)$ from user's QR code image QRU_i' . Consequently, if the user inputs incorrect values, the session is stopped.

Proposition 5. Our work prevents an adversary from establishing session key.

Proof. If user's keys (C_i', Y) are compromised, then an adversary fails to build key $X' = h'(FXU_i)^{PW_{U_i}'} \bmod p \oplus r_i$, as to generate the session key, the QR code image QRU_i' to retrieve $h'(FXU_i)$ and PW_{U_i}', p, r_i are needed to compute X'. Even, if an adversary eavesdrops to get the value X' during user's login phase, he cannot use it again because X' enables one time for each user's login request. Additionally, the information biometric $h'(FXU_i)$ embeds inside QRU_i' saved in user's smartphone.

Proposition 6. Our work can support revocation of smart cards and also does not need to use extra hardware and software.

Proof. In the case of user's smart card has been lost or stolen, the attacker cannot obtain or change the password because he fails to get information of biometric $h'(FXU_i)$ embedded inside QRU_i' which stored in user's smartphone. If an adversary U_j has the ability to steal the user U_i's smart card, then U_j can extract the secret information $\{ IDU_i, Y, p, N \}$ saved in SC. So as to try deriving U_i's password or login into the remote system based on the stolen smart card, U_j should be computed $PW_{U_i}' = h(PW)$, $X' = h'(FXU_i)^{PW_{U_i}'} \bmod p \oplus r_i$, $C_i' = h(PW_{U_i}' || X' || Y)^{r_i}$, but U_j cannot compute X' and C_i', because he is unable to achieve $h'(FXU_i)$ and QRU_i'. In the login phase, the user needs to use his QR image QRU_i' saved on his smartphone. Compared with Chuang et al.'s scheme in [9], their scheme requires extra hardware and software to complete the verification of a user's biometric. Our proposed scheme needs a QR reader apps that is available free download in IOS for iPhone mobiles or Google play for Android mobiles. As a result, our proposed scheme provides revocation of smart cards and does not needs extra hardware and software for biometric information.

Proposition 7. The proposed scheme resists insider attacks.

Proof. In cloud computing environment that is consists of many servers, U_i may be used his password PW_i to register on cloud's servers for his convenience. In this attack, a privileged-insider of S may attempt to get U_i's real password PW_i and then use user's password to login other cloud's servers. In our proposed scheme, step R1 of registration phase that U_i registers to S by sending $PWU_i = h(PW_i)$ and FXU_i instead of plain text PWU_i. The login phase depends on U_i's password and QR Code image. So, because of the complexity under the assumption of crypto-hash function a privileged-insider of S is unable to obtain the real password of user PWU_i without achieving to the feature' extraction of user's fingerprint $h'(FXU_i)$.

Proposition 8. Our proposed scheme can withstand a forgery attack.

Proof. If an attacker attempts to impersonate a real user's account U_i, he should be had the main keys to get the legitimate login message $\{ CIDU_{U_i}', X', T \}$. It is necessary to compute the following operations by an attacker:

- Compute $PW_{U_i}' = h(PW), X' = h'(FXU_i)^{PW_{U_i}'} \bmod p \oplus r_i, C_i' = h(PW_{U_i}' || X' || Y)^{r_i}$.
- Compute $CIDU_{U_i}' = h(IDU_{U_i}')^{r_i} \oplus T \oplus C_i'$.

An attacker fails to obtain $\{QRU_i', r_i, Y, h(FXU_i), PW, IDU_{U_i}', p \}$. As a result, an attacker cannot forge legal login messages and fails to apply the forgery attack.

6. DISCUSSION

This section compares our proposed scheme with previous works based on Tables 2-4. In Table 4, T_h and T_E represent the time complexity of computation of hash function and the exponential of modulo operations, individually. Table 2 describes the major comparison of various conventional authentication methods as follows:

C1: Mutual authentication;
C2: Forward secrecy;
C3: Preserve user anonymity;
C4: Efficient password change;
C5: Session key computation;
C6: Pre-smart card authentication;
C7: Revocation by using personal biometrics based on QR code;

Table 3 describes the significant comparison of various conventional attacks methods as follows:

T1: Withstand user's impersonation attack;
T2: Withstand insider attack;
T3: Withstand replay attack;
T4: Withstand offline password guessing;
T5: Withstand forgery attack;
T6: Withstand temporary information attack;
T7: Withstand DOS attack.

In performance evaluation, we compare the proposed scheme with previous works in [15], [21]-[24] that are specified in Tables 2 and 3. In addition, the schemes of Li *et al.* [21], Lee *et al.* [22] suffer from the revelation of user's password and did not prevent attacks. Karuppiah and Saravanan' scheme [23] can professionally resist insider and forgery attacks, however, it fails to view mechanism for preserving and privacy of session key. Li *et al.* [24] scheme suffers from off-line password guessing and replay attacks. Table 5 explains that performances of different schemes were also compared with our proposed scheme. The details of communication and computation costs are showed in Tables 4 and 5, respectively. We use the same standards for computing and communication cost in [25]. The authors assumed that the size of hash function matches 128 bits. For more details, they also assumed that the lengths of of ID_i and PW_i are closed with 128 bits. As a final point, the sizes of both time-stamps and random numbers equivalent 64 bits.

Table 2. The main authentication methods

Scheme	C1	C2	C3	C4	C5	C6	C7
Li & Hwang [21]	Y	Y	N	N	Y	N	N
Lee *et al.* [22]	Y	Y	N	N	Y	N	N
Khan *et al.* [16]	Y	N	N	Y	Y	Y	N
Li *et al.* [24]	Y	Y	N	Y	Y	Y	N
Karuppiah [23]	Y	--	N	Y	Y	N	N
Ankita *et al.* [15]	Y	Y	Y	Y	Y	Y	N
Our proposed scheme	Y	Y	Y	Y	Y	Y	Y

Table 3. The main attacks methods

Scheme	T1	T2	T3	T4	T5	T6	T7
Li & Hwang [21]	Y	N	N	Y	N	Y	N
Lee *et al.* [22]	Y	N	N	N	N	Y	N
Khan *et al.* [16]	Y	N	Y	Y	Y	Y	Y
Li *et al.* [24]	Y	Y	N	Y	Y	N	Y
Karuppiah [23]	Y	Y	Y	N	Y	Y	Y
Ankita *et al.* [15]	Y	Y	Y	Y	Y	Y	Y
Our proposed scheme	Y	Y	Y	Y	Y	Y	Y

Table 4. Computation cost

Scheme	Login Phase	Authentication Phase	Total
Lee *et al.* [22]	$3T_h$	$9T_h$	$12\ T_h$
Khan *et al.* [16]	$3T_h$	$7T_h$	$10\ T_h$
Li *et al.* [24]	$2T_h + T_E$	$T_h + 5T_E$	$3T_h + 6T_E$
Karuppiah [23]	$3T_h + 5T_E$	$2T_h + T_E$	$5T_h + 6T_E$
Ankita *et al.* [15]	$3T_h + 2T_E$	$6T_h + 4T_E$	$9T_h + 6T_E$
Proposed scheme	$3T_h + T_E$	$4T_h + T_E$	$7T_h + 2T_E$

Table 5. Performance comparison among relevant authentication schemes

Scheme	Login Phase		Authentication Phase			Total
	Login message	Cost	Authentication messages	Cost $S \rightarrow U_i$	Cost $U_i \rightarrow S$	
Li & Hwang [21]	ID_i, M_2	576	$((M_6, M_5), (M_8))$	448	256	1280
Lee *et al.* [22]	$TID_i, T, A_i \oplus Q_i$	256	$((B_i, h(K_i, A_i)), h(K'_i, B_i))$	192	128	576
Khan *et al.* [16]	CID_i, C_i, d, T	384	C_2, T_s	192	----	576
Li *et al.* [24]	ID_u, M_1, M_2	320	$((M_6, M_7), (M_9))$	256	256	832
Karuppiah [23]	B_2, M, C	512	$(h(C_1), r, T_s), (M_1, T))$	640	320	1472
Ankita *et al.* [15]	NID, A_1, C_u, T_1	320	(C_s, A_4, T_3)	256	---	576
Proposed scheme	$CIDU'_{U_i}, X', T$	320	Ch, T', L	256	----	576

7. CONCLUSION

We present a developed scheme using multi-factors: password, smart card, biometric, and QR code image. The proposed scheme has the ability to resist well-known attacks compared with the related works. Our work offers effective login, robust authentication, and password change phases where an incorrect input is directly detected, and a legal user can freely change his password by using his smart card and QR code image without server assistant. Furthermore, our work keeps user anonymity and ensures multi-factor authentication. Additionally, our proposed scheme is more robust and appropriate for using in many services and applications like e-banking, online payment systems, election system.

REFERENCES

[1] R. Kumar, and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Computer Science Review*, vol. 33, pp. 1-48, 2019, doi: 10.1016/j.cosrev.2019.05.002.

[2] L. Coppolino, S. D'Antonio, G. Mazzeo, L. Romano, "A comprehensive survey of hardware-assisted security: From the edge to the cloud," *Internet of Things*, vol. 6, 2019, Art. no. 100055, doi: 10.1016/j.iot.2019.100055.

[3] A. M. Simplicio Jr, M. V. M. Silva, R. C. A. Alves, and T. K. C. Shibata, "Lightweight and escrow-less authenticated key agreement for the internet of things," *Comp. Communic.*, vol. 98, pp. 43-51, 2017, doi: 10.1016/j.comcom.2016.05.002.

[4] R. D. Panda, S. K. Behera, and D. Jena, "A Survey on Cloud Computing Security Issues, Attacks and Countermeasures," *Advances in Machine Learning and Computational Intelligence*, 2021, pp. 513-524, doi: 10.1007/978-981-15-5243-4_47.

[5] H. Tabrizchi, and M. K. Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *The journal of supercomputing*, vol. 76, no. 12, pp. 9493-9532, 2020, doi: 10.1007/s11227-020-03213-1.

[6] M. Saadeh, A. Sleit, K. E. Sabri, W. Almobaideen, "Object Authentication in the Context of the Internet of Things: A Survey," *Journal of Cyber Security and Mobility*, vol. 9, no. 3, pp. 385-448, 2020, doi: 10.13052/jcsm2245-1439.932.

[7] V. Agarwal, A. K. Kaushal, and L. Chouhan, "A Survey on Cloud Computing Security Issues and Cryptographic Techniques," *Social Networking and Computational Intelligence*, vol. 100, 2020, pp. 119-134, doi: 10.1007/978-981-15-2071-6_10.

[8] Z. C. Xu, J. Rao, and X. Bu, "URL: A unified reinforcement learning approach for autonomic cloud management," *Journal of Parallel and Distributed Computing*, vol. 72, no. 2, pp. 95-105, 2012, doi: 10.1016/j.jpdc.2011.10.003.

[9] D. He, "An efficient remote user authentication and key agreement protocol for mobile client-server environment from pairings," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1009-1016, 2012, doi: 10.1016/j.adhoc.2012.01.002.

[10] B. Sumitra, C. Pethuru, and M. Misbahuddin, "A survey of cloud authentication attacks and solution approaches," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 10, pp. 6245-6253, 2014.

[11] A. A. Yassin, J. Yao, and S. Han, "Strong authentication scheme based on hand geometry and smart card factors," *Computers*, vol. 5, no. 3, 2016, doi: 10.3390/computers5030015.

[12] W. A. R. W. M. Isa, A. I. H. Suhaimi, N. Noordin, A. Harun, J. Ismail, R. A. Teh, "Cloud computing adoption reference model," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 16, no. 1, pp. 395-400, 2019, doi: 10.11591/ijeecs.v16.i1.pp395-400

[13] T. Mehraj, M. A. Sheheryar, S. Ahmed, A. H. Mir "A critical insight into the identity authentication systems on smartphones," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 13, no. 3, pp. 982-989, 2019, doi: 10.11591/ijeecs.v13.i3.pp982-989

[14] A. A. Yassin, M. A. Hasson, and H. S. Ridha, "A New Message Authentication Code Scheme Based on Feature Extraction of Fingerprint in Cloud Computing," *International Journal Of Engineering Research & Technology (IJERT)*, vol. 3, no. 11, 2014.

[15] A. Chaturvedi, A. K. Das, D. Mishra, S. Mukhopadhyay, "Design of a secure smart card-based multi-server authentication scheme," *Journal of Information Security and Applications*, vol. 30, pp. 64-80, 2016, doi: 10.1016/j.jisa.2016.05.006.

[16] K. M. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme," *Computer Communications*, vol. 34, no. 3, pp. 305-309, 2011, doi: 10.1016/j.comcom.2010.02.011.

[17] T. C. Li, C. C. Lee, and C. Y. Weng, "A dynamic identity-based user authentication scheme for remote login systems," *Security and Communication Networks*, vol. 8, no. 18, pp. 3372-3382, 2015, doi: 10.1002/sec.1264.

[18] R. Madhusudhan, and R. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review," *Journal of Network and Computer Applications*, vol. 35, no. 4, pp. 1235-1248, 2012, doi: 10.1016/j.jnca.2012.01.007.

[19] Y. Y. Chang *et al.*, "A mobile medical QR-code authentication system and its automatic FICE image evaluation application," *Journal of applied research and technology*, vol. 13, no. 2, pp. 220-229, 2015, doi: 10.1016/j.jart.2015.06.020.

[20] A. A. Yassin *et al.*, "Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing," *2012 Second International Conference on Cloud and Green Computing*, 2012, pp. 282-289, doi: 10.1109/CGC.2012.91

[21] T. C. Li, and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010, doi: 10.1016/j.jnca.2009.08.001.

[22] C. C. Lee, C.-Ta Li, K.-Y. Huang, S.-Y. Huang, "An improvement of remote authentication and key agreement schemes," *Journal of Circuits, Systems, and Computers*, vol. 20, no. 04, pp. 697-707, 2011, doi: 10.1142/S0218126611007554

[23] M. Karuppiah, and R. Saravanan, "A secure remote user mutual authentication scheme using smart cards," *Journal of Information Security and Applications*, vol. 19, no. 4-5, pp. 282-294, 2014, doi: 10.1016/j.jisa.2014.09.006.

[24] X. Li, J. Niu, Z. Wang, C.-M. Chen, "Applying biometrics to design three-factor remote user authentication scheme with key agreement," *Security and Communication Networks*, vol. 7, no. 10, pp. 1488-1497, 2014, doi: 10.1002/sec.767.

[25] E. J. Yoon, and K. Y. Yoo, "Improving the dynamic ID-based remote mutual authentication scheme," *OTM Confederated International Conferences, On the Move to Meaningful Internet Systems-OTM 2006*, vol. 4277, 2006, pp. 499-507, doi: 10.1007/11915034_73.