International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 15 (2023) pp. 522-530

Received: 22 July 2022; Accepted: 15 May 2022; Published: 9 July 2023

Virtual SmartCards-based Authentication in Healthcare Systems and Applications

Abdulla J. Y. Aldarwish[1], Dr. Kalyani Patel[2], Ali A. Yassin, Aqeel A. Yaseen

[1]*Department of Computer Science, Gujarat University, Ahmedabad, 380009, India*
abdullajas@uobasrah.edu.iq

[2] K.S. School of Business Management and Information Technology, Gujarat University, Ahmedabad, India
kalyanipatel@gujaratuniversity.ac.in

***Abstract*: Secure and dependable sensing is a critical point for access control, which includes user authentication by using biometric recognition of each patient in a healthcare system. In recent years, there has been a surge of interest in biometric authentication from both the academic and business sectors. Traditional security and privacy approaches in this sector are not viable alternatives for providing both security and performance efficiency. Because of this, some cutting-edge authentication systems are open to attacks from intruders and do not work well in terms of communication and computation costs. This paper presented a unique, lightweight, multi-factor user authentication method that gets around these problems and checks its security with Scyther, a formal verification tool. Our research focuses on using an asymmetric encryption function with a biometric factor, a passwordless feature, and a QR code to make a secure virtual smart card that can be used to grant the users safe access to the healthcare system. Furthermore, our suggested approach surpasses existing proposed symmetric encryption or biometric authentication techniques. Additionally, our work supports many fields, such as the Internet of Things (IoT) in healthcare, E-banking healthcare transactions, and others.**

***Keywords*:** Authentication, passwordless, QR Code, Virtual SmartCards, Scyther**.**

I. Introduction

The advent and proliferation of Internet apps and the widespread use of the latest smartphones have revolutionized all spheres of our lives and made it more important than ever to keep information and privacy safe. Additionally, as technology progresses, security is becoming increasingly important. Therefore, when the Server is hacked, the present technique of entering an ID and password is quite likely to disclose all information. Then, several approaches for safe authentication have been investigated. The process of authentication serves as a critical measure to prevent unauthorized entry into a device or any other confidential online or offline application. Initially, a single criterion was used to confirm the subject's identification. The community extensively adopted Single-Factor Authentication (SFA) at the time because of its simplicity and user-friendliness. Also, it was shown that authentication with a single factor is not enough to protect against a wide range of security problems, such as dictionary attacks, phishing attacks, and social engineering techniques[1].

After that, Two-Factor Authentication (2FA) was recommended as a logical step forward to pair the representative data (username/password) and something a person owns, like a phone or a smartcard, as a second factor. Subsequently, the Multi-Factor Authentication (MFA) concept was introduced to enhance security measures and provide continuous protection to computing devices and critical services against unauthorized access. MFA achieves this by incorporating more than two types of credentials for authentication. Conventional elements like something you know, something you have, and something you are used in the method of multi-factor authentication technique[2]. Figure (1) shows the Multi-Factor Authentication parameters. On smart devices and wearables, users prefer authentication protocols that are easy to use. So, developers of smart systems face numerous challenges, including tackling issues like intelligent authentication, safeguarding information during transmission, and implementing user verification based on attributes.[3]. Furthermore, user information intended for registration in a sensitive system (such as E-banking and E-healthcare) must be protected from intruders[4, 5].

MFA primarily relies on user biometrics, which involves the automated recognition of individuals based on their biological and behavioral characteristics. On the biometric side, the authentication methods suffer from impersonation attacks and high costs from some biometrics and others[6]. However, the MFA substantially improves access to most electronic devices in terms of both security and user experience. MFA applications can be categorized into three

major market segments:

1. Commercial applications encompass various use cases like account login, e-commerce, ATM transactions, physical access control, and more.
2. Governmental applications include identity documents, government IDs, passports, driver's licenses, social security systems, border control, and related functions.
3. Forensic applications include criminal investigation, identification, and so on.

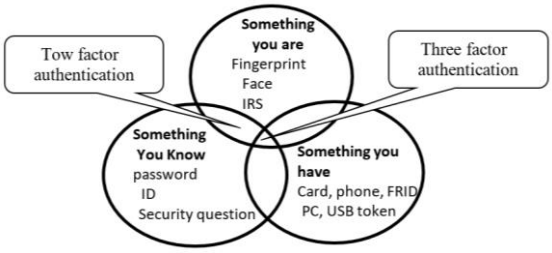

Figure 1:Multi-Factor Authentication

Several articles address the difficulties and concerns of IoT security. These articles evaluate the performance of suggested algorithms regarding their security, privacy, power, time, and usability for systems [8, 9]. Therefore, enhanced authentication procedures are still required for IoT systems [10, 11]. Our proposed scheme relies on mobile devices and server multi-factor and mutual authentication. However, it is essential to recognize that potential attackers may be able to eavesdrop on connections between network components. Eavesdropping poses significant risks to the system, as the perpetrator may use the collected information for nefarious purposes, posing a substantial threat to the system's integrity. [12].

The main contributions of our paper are listed in the following points:

The proposed scheme can resist famous attacks such as impersonation insider, hub node spoofing, replay, tracing, key escrow, and Man-in-the-middle. At the same time, the proposed work has many security metrics like mutual authentication, secure key management, and strong verification.

Our work has been proofed in formal (Scyther tool) and informal ways. Also, the proposed scheme has a good balance between performance and complexity of security. We use a symmetric encryption method, QR code, and virtual smartcard.

The user does not need to use multi-factor authentication to login into the system each time he keeps logging in to the same device. We pay attention to work with smart factor authentication.

We recommend using the passwordless feature in the proposed scheme that depends on the preferring factor being either biometric or password used for extracting secret factors to perform the authentication phase. BTW, our proposed scheme can support several types of biometrics, such as fingerprints, faces, and hand geometry. As well as is suitable for IoT applications.

The rest of the paper is structured in the following manner. Section 1 includes the introduction. Section 2 reviews related work. Section 3 presents the proposed scheme with details. Section 4 presents formal and informal security analyses. Section 5 explains the comparison and performance. Finally, section 6 concludes this paper.

II. RELATED WORK

Authentication processes are required when users access systems to ensure they are attempting to get access as the intended user and safeguard users' sensitive data[12]. Recently, several researchers have worked on securing authentication for E-healthcare systems [13, 14]. Many studies on mobile application authentication systems are the ones listed below.

A one-time password is a mechanism used in several systems (banks, government, etc.) that generates a new password for each user's login request [4]. Nevertheless, it is susceptible to sophisticated phishing assaults, and its work suffers from repetition and fails to resist familiar attacks [15]. Many authors continuously proposed MFA schemes, beginning with incorporating biometrics (physical and behavioral) into authentication schemes, such as face recognition, eye recognition methods, fingerprints, etc. [13, 16]. There was an issue with the difficult-to-modify biological agents, which impacted system security.

In more detail, Tan and Lee [17] proposed authentication systems based on fingerprint biometrics. These methods encrypt biological pictures before transferring them to authentication systems, boosting network secrecy. Unfortunately, this scheme has no balance between performance and protection [18].

Hassan and Shukur [15] proposed an electronic framework for payment systems using multi-factor authentication. The system depends on user biodata, passwords, and fingerprints. But they can be attacked in several ways, such as by switching SIM cards, intercepting SMS_OTP messages wirelessly, using malware, etc.

Rahman et al. [19] proposed using an advanced encryption protocol and a hashed message authentication code to enhance the security of fog computing. However, the scheme encountered difficulties in effectively mitigating privileged insider attacks and lacked a secure environment for such attacks. Additionally, the scheme exhibited a heavier computational and communication burden due to its reliance on more complex processes.

Reese et al. [20] performed comparative tests of the usability of five two-factor authentication methods: SMS, OTP, push notifications, printed-out codes, and Universal 2nd Factor (U2F) with Security Key. The purpose was to give a more comprehensive comparison of various methodologies. According to their results, users found all five ways to be workable, and most participants deemed the additional effort to be worth the security advantages. But one-third of the people who participated in the study said that they do not

always have access to their second factor, which causes problems.

Most recently, Sadri and Asaar [21] proposed a two-factor authentication protocol based on smart card and biometric passwords with anonymous user information and allowed offline passwords locally. Still, the protocol does not resist user impersonation attacks and stolen smart card attacks[22].

We propose an MFA scheme to tackle the abovementioned threat. This authentication system uses a virtual smart card with a QR code rather than SMS. Our work can allow the user to enter using password or biometrics. Additionally, the proposed protocol includes a passwordless feature, allowing the user to access the system without a password. Also, we resist malicious attacks and depend on mutual authentication. Each login includes a new once-secure session key, user information anonymity, the ability to unlink, protection if a mobile device is lost or stolen, and the ability to change passwords offline.

III. Proposed Scheme

In this section, we propose the multi-factor mutual authentication of a security system that consists of two components: user data entry (U_i), and the cloud server center (S). In addition, our work is based on four phases: registration, login, authentication, and password change. Table 1 defines and compiles the symbols and their corresponding meanings and interpretations in this paper.

TABLE 1. Notation.

Notation	Description
U_i	User
ID_i	User U_i Identity
PW_i	User U_i Password
$PBoi$	The biometric of User U_i
S	The remote Application server
x	The server S secret key
e	The server S public key
N	Number of registrations with S by user U_i
T_i	User timestamp
T_s	Server timestamp
$E_Q(m)$	Encryption of message m using key Q
$D_Q(m)$	The decryption of message m using key Q
R	User Role (default is normal user)
SK	Session key
$\oplus$	XOR Bitwise operation
$h(.)$	A secure one-way hash function
$\|\|$	Concatenation operation

A. *Registration Phase*

During this phase, the mobile user is registered with the Access Control Unit using the authentication application. The user U_i produces his or her ID_i and password PW_i and sends just the ID_i to Server S. The latter verifies the legitimacy of ID_i . If it is determined to be valid, the server S generates and stores a virtual card number VC_i in its database:

$(ID_i; RID_i) = (ID_i ; E_x (VC_i; ID_i ; \mathrm{N})$, where N is the number of registered users . If $\mathrm{N} = 0$, that means first registration. Otherwise, compute N as $(\mathrm{N}+1)$. Then, calculates the following in the Server:

The Server generates random number (b), then computes $AID_i = E_x (ID_i \,||\, b)$.

$G = h(x \,||\, ID_i || \mathrm{N} \,||\, VC_i)$, where G is represent, the data utilized to verify the validity of the entered data exchanged between the mobile device and the server.

After that, the Server saves $\{AID_i, VC_i, \mathrm{N}, G, n, e; h(.), EQ(.), DQ(.)\}$ in a database and sends it through a secure channel to the authorized mobile application.

Upon receiving the aforementioned information from the server, the mobile device computes the following:

Generates r as a random number, then computes $RPW_i = h(PW_i || r)$.

$L = G \oplus RPW_i$.

In addition, the user can use his biometrics Bo_i in the registration phase.

Compute $RBo_i = h(Bo_i || r)$.

$LBio = G \oplus RBo_i$,

Finally, the authorized mobile application replaces $\boldsymbol{L}$ with $\boldsymbol{G}$ and binds $\boldsymbol{LBio}$ with information received from the Server, then saves it in a new secure storage space in mobile known as Virtual Smart Card ($\boldsymbol{VSC}$). Figure (2) shows the flowchart of the registration process, and Figure (3) depicts the sequence of message exchanges between user devices and the server during the registration phase.

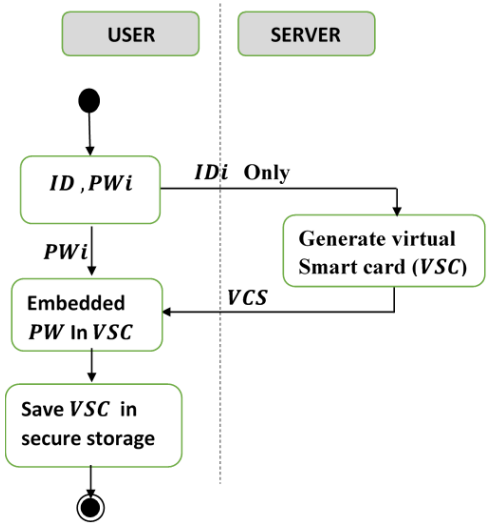

Figure 2. Registration process

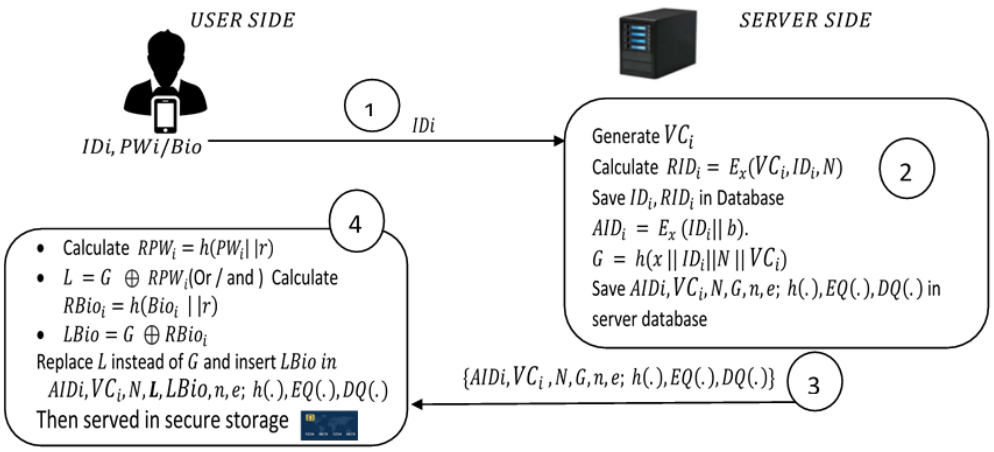

Figure 3. Details of the registration process.

A. Login Phase

The valid user should enter his identity ID_i and password PW_i / his biometric through an authorized mobile application. Then the mobile provides a virtual smart card (VSC) and retrieves the random number r. Afterward, performs the following calculations:

$RPW_i = h(PW_i||r)$

$RBio_i = h(Bio_i||r)$

Retrieval form $G = L \oplus (RPW_i)$ or ($G = LBio \oplus (RBio_i)$) (G is calculated by utilizing the password provided by the user during the request for a new connection).

$F = G^a \bmod n$ (a: is a random number)

$C_1 = h(T_i || G || F)$

$D = C_1^e \bmod n$

$IZ_i = E_{C_1}(AID_i, \mathrm{N}, VC_i, F)$

The mobile application generates and sends messages. $m = \{IZ_i, T_i, D\}$.

B. Authentication Phase

When the authentication server receives the login message (m), first compute ΔT if $\{T_i - T' > \Delta T\}$ when (T') is a current timestamp and (ΔT) is the correct interval time. Then reject the login request if the above inequality is valid. Otherwise, the Server implements the following operations:

obtain C_1 using: $C_1 = D^x \bmod n$ (decrypts D by using secret key x)

decrypts IZ_i with C_1 to retrieve the values of $AIDi, \mathrm{N}, SC_i, F$ using: $D_{C_1}(IZ_i) = (AID_i, \mathrm{N}, VC_i, F)$

Decrypts AID_i using: $D_x(AID_i) = (ID_i, b)$ to obtain ID_i

Decrypts RID_i to obtain N, VC_i, ID_i.

Subsequently, the viability of the database is examined. If confirmed, the virtual smart card number is decrypted and compared with the stored information in the database. The number's validity is checked to ensure it does not belong to a virtual smart card reported as lost, stolen, or frozen. Additionally, the user type is verified. Following these checks, the system proceeds to compute:

$G' = h(x||ID_i||\mathrm{N}||SC)$

$C'_1 = h(Ti||G'||F)$

If $C'_1 = C_1$, the user is authenticated, then Server generates a random number d and computes:

$V = G^d \bmod n$

$W = F^d = G^{ad} \bmod n$

$SK = h(T_i || W || T_S)$

$C_2 = E_{C_1}(V, W, T_S)$

Eventually, the Server a generates QR code depending on $m' = \{C_2, V, T_s\}$ and sends it to the user, so the QR code is another authentication factor based on a private, secure channel between the user and the authentication server. Hence, this channel is fully safe against malicious attacks.

Finally, the user receives a QR code and then auto-scans it to get the message m' at that time T'', then check if $\{T_s - T'' < \Delta T\}$. If the inequality holds, compute the following:

$W = V^a = G^{ad} \bmod n$

$C'_2 = E_{C_1}(V, W, T_s)$

If $C_2 = C'_2$ the server S is authenticated, and the user $U_i$calculates his session key $SK = h(T_i || W || T_S)$

Figure (4) shows the login and authentication process, and Figure (5) provides a summary of the message steps involved in the login and authentication process between user devices.

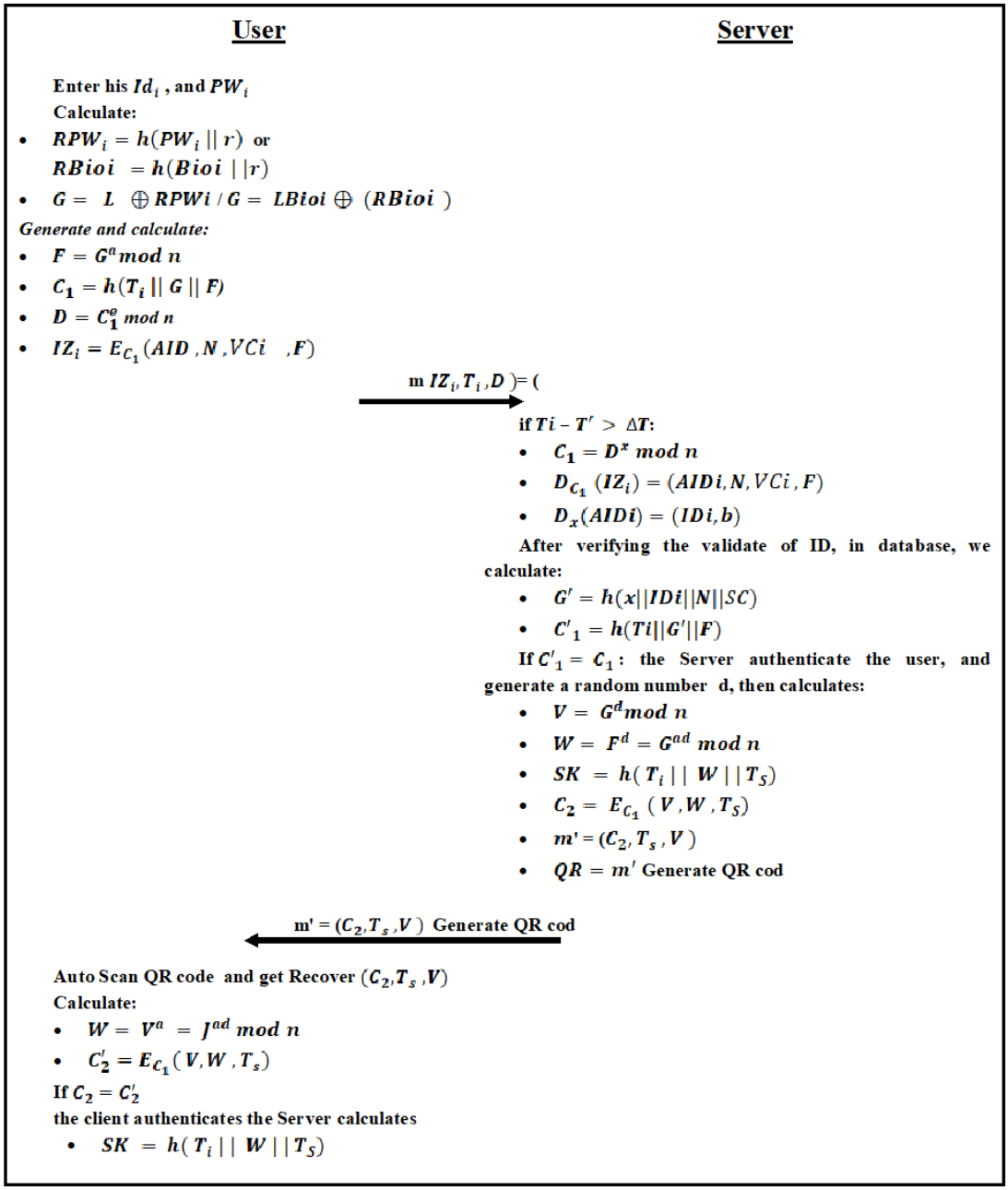

Figure 5. Login and authentication Details process

.

A. Password Change Phase

The user can change his password or biometric by providing an old password/ biometric (PW_i / Bio_i) and choosing a new password PW_i' /Bio_i' , then compute:

$RPW_i' = h(PW_i \| r)$ and $L' = L \| h(RPW_i)$

$RBio_i' = h(Bio_i \| r)$ and $LBio_i' = LBio_i \| h(RBio_i)$

Thence, the L and $LBio_i$ are substituted in the virtual smart card with the $L' and\ LBio_i'$.

IV. SECURITY ANALYSIS

By Using multi-factor mutual authentication, our proposed scheme was able to stop the most common known attacks, as shown below:

A. User Anonymity

By "anonymous user," we mean that only Server S and the user himself know what U_i is. As ID_i is concealed inside AID_i, RID_i, and IZi, the adversary must decode AID_i and RID_i. The Server is the only one who knows the private key x. Thus, and the attacker is unable to determine which user initiated the authentication session with the Server. Consequently, the suggested approach guarantees anonymity.

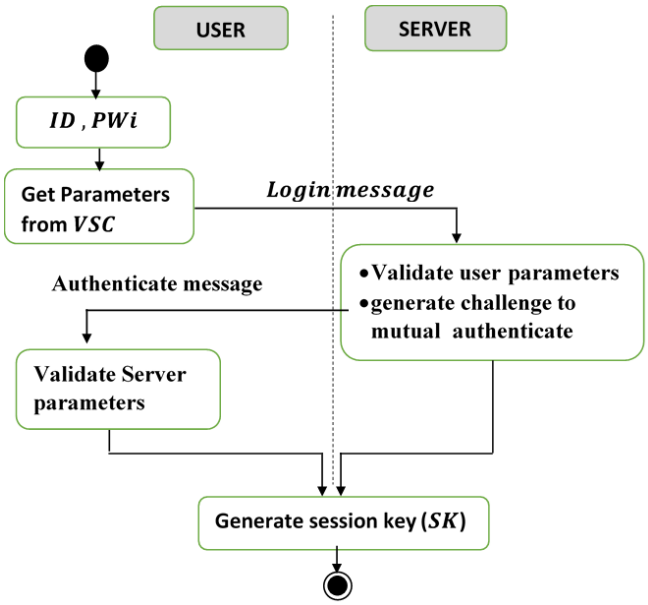

Figure 4. Login and authentication process.

B. Untraceability of Users

This feature implies that an adversary can't ascertain whether multiple executions of the scheme are linked to the same user. In the proposed scheme, every component of the login message, including $m = IZ_i, T_i, D$, is specific to the session, as the calculation of IZ_i and D relies on session-specific random nonces a and b. During the registration process, the user's identity is encrypted using the secret key x and securely sent to the user. AID_i is encrypted asIZ_i during the login phase using the key C_1, computed using the random variable a. Therefore, each ID_i is encrypted uniquely for each session, despite the usage of the same secret key x. Since the attacker is unaware of the secret key x, he cannot determine if two different AID_i numbers belong to the same ID_i . In addition, since C_1has a unique value for each session and is connected with the timestamp T_i, an attacker cannot determine if two executions of the technique are tied to the same user. Thus, the property of user anonymity is met.

C. Stolen-Verifier Attack

In this attack scenario, an adversary illicitly acquires or modifies verification data stored on the server, including sensitive information such as plain-text or hashed passwords. In this scheme, only the Server can verify the authentication information $G = h(x||ID_i\ ||N||VC_i)$ since it has the secret key x. In addition, there is no method to extract password or verification information from server-stored RPW_i. Consequently, this property is met.

D. User Impersonation Attack

To impersonate a valid user U_i, an attacker must then establish his identity by calculating $C_1 = h(T_i||G||F)$. However, the attacker cannot determine the correct value of C_1 because he lacks the secret key x or $G = h(x||ID_i\ ||N||VC_i\ )$, which are acquired from L and RPW_i. Therefore, this strategy is resistant to this assault.

E. Server Impersonation Attack

To impersonate the Server, an attacker must generate a legitimate response $C_2 = E_{c1}(V, W, T_s)$. However, the attacker does not know C_1, which is calculated from the server-only value G He cannot thus compute $C_2$and provide a legitimate answer. Consequently, the technique is resistant to server impersonation attacks.

F. Mutual Authentication

This feature signifies that the server and the user can authenticate each other's identities. Only the server possessing the correct secret key can successfully pass the user-level verification utilizing C_2, as mentioned earlier. Similarly, only legitimate users with valid passwords can pass the server-level C_1 verification. As a result, mutual authentication is ensured.

V. Formal Verification

The proposed scheme has been validated using the Scyther Security Simulation Tool, an efficient tool to evaluate and identify possible threats and weaknesses in network security protocols [23]. Using Scyther Security, We implemented the proposed scheme without using security functions that work in other systems. Figure (6) shows the system's vulnerability without security protocol.

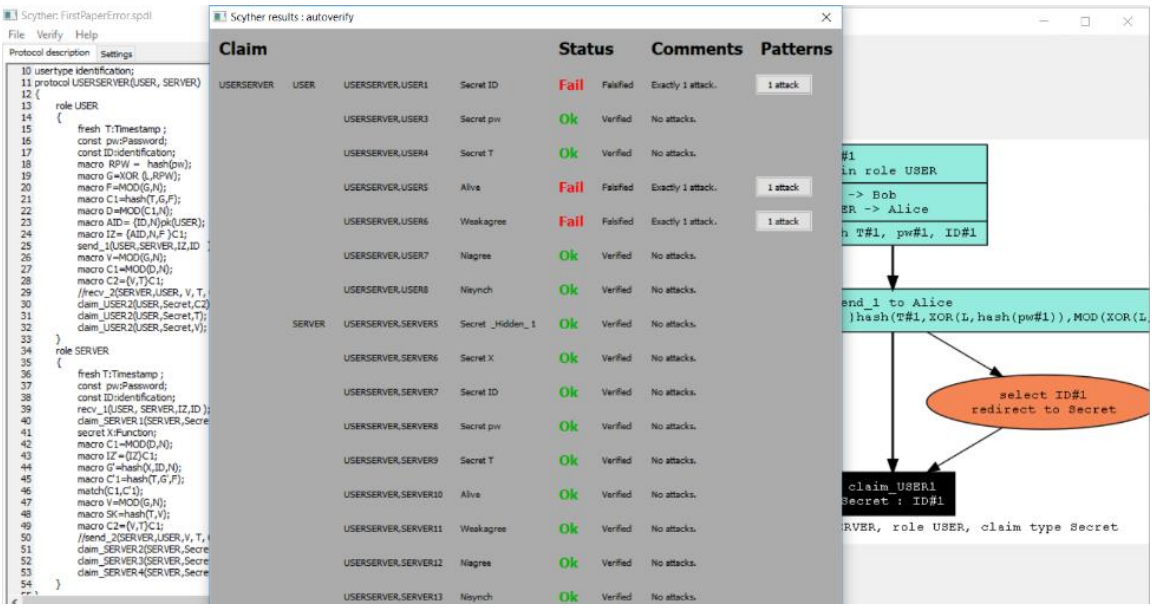

Figure 6. Shows protocol weaknesses in the security analysis.

We showed that the scheme could resist different kinds of cryptographic attacks. Figure. 7 shows the security verification analysis result, and Figure. 8 displays the security characterization result of our proposed scheme using the Scyther security tool. The analysis of the claims shows that the proposed scheme has no cryptographic flaws that could be used to break it.

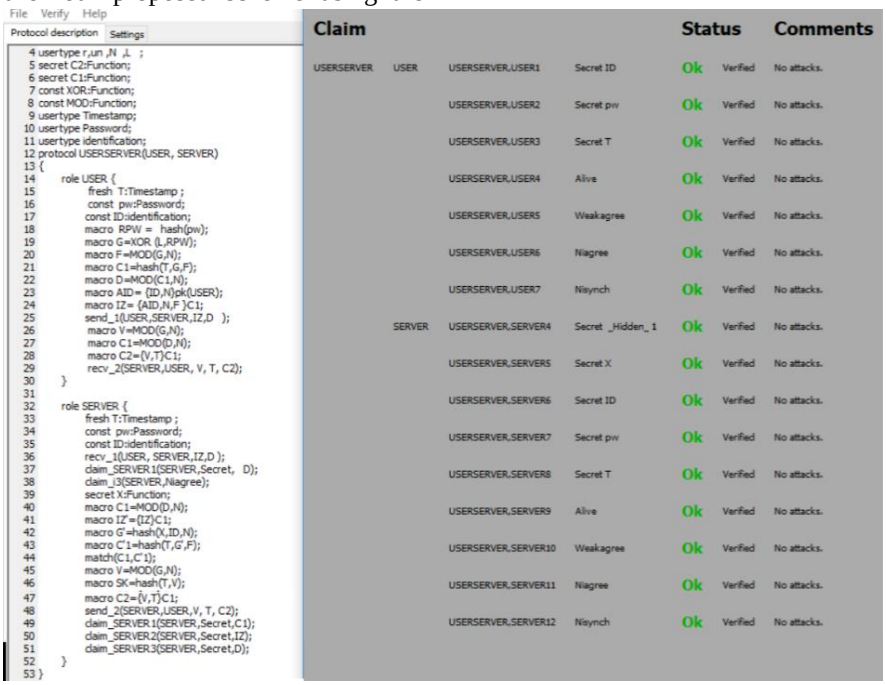

Figure 7. Show the security analysis

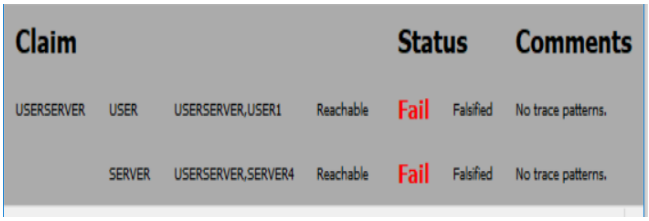

Figure 8. Display the security characterization result.

I. COMPARISON OF SECURITY PROPERTIES

Experimental Results

Figure 9 explains the mechanism of the registration phase works; the user enters his own information and sends an ID to the S. Then the S generates smart card parameters and reverts them. Upon receiving the parameters, the application replaces L with G and packets all the parameters with the Bio to

generate VSC. Finally, VSC is stored in a secure storage area on the mobile device

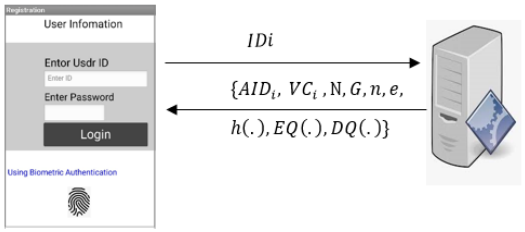

Figure 9. Registration phase mechanism

Figure 10 depicts the login and authentication process; when a user wants to access the system via the mobile application, he must enter his password (PW_i) or biometric (Bio_i) to retrieve parameters from VSC and compute $m = \{IZ_i, T_i, D\}$. After receiving m, the S checks the user's validity and then generates $m' = \{C_2, V, T_s\}$ to be embedded in the QR code as mutual user authentication. Lastly, the mobile application auto-scan the received QR code to ensure the reliability of the Server. Eventually, the Server and mobile application deduce the session key ($SK = h(T_i || W || T_S)$).

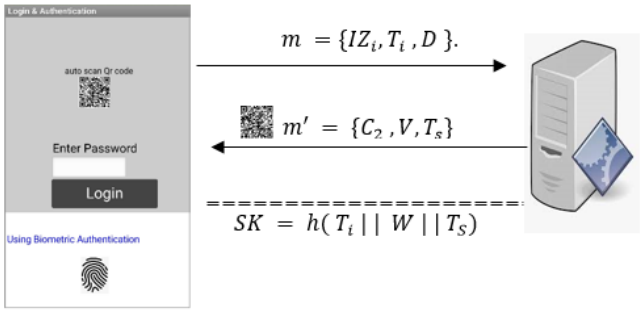

Figure 10. login and authentication proses

Security Features

In table 2, we compared the security features of our proposed scheme with some protocols from previous studies.

Table 2. Comparison between the proposed scheme and other related work

scheme	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14
Chen et, al. [12]	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	Y
Sadri & Asaar [21]	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Ali et, al. [16]	Y	Y	Y	N	Y	N	Y	Y	N	N	N	N	Y	Y
Ayub et, al. [14]	Y	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	N	Y
Nikravan, et, al.[24]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	Y
Mohammed & Yassin [13]	N	N	Y	N	Y	N	Y	Y	N	Y	Y	N	N	Y
Our proposed scheme	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

F1: Ensure user anonymity, F2: Ensure user untraceability, F3: Resist online password guessing attack, F4: Resist offline password guessing attack, F5: Resist stolen-verifier attack, F6: Resist modification attack, F8: Resists replay attack, F8: Resist user Impersonation Attack, F9: Resist server Impersonation Attack, F10: Ensure mutual authentication, F11: Ensure password change, F12: Ensure smart card revocation, F13: QR code. F14: Biometric.

Performance Comparisons

In this section, we compare the performance of our protocol with [13, 14, 21, 24] to compute the computation and communication overhead. The basic processing times of the functions are approximate, as shown in table 3 and table 4, depending on[25, 26].

Table 3. Processing times

Operation	Meaning	Process Time
T_{ED}	encryption decryption function	**0.0046**
T_h	hash function	**0.0023**
T_m	Mathematical operation	**0.005**
$T_{\oplus}$	XOR operation	***negligible***
$T_{\|\|}$	Concatenation	***negligible***

Protocol	**Verification's Time Complexity**	**Result**
Sadri & Asaar [21]	$10T_{\oplus} + 30T_h + 65T_{\|\|} 6T_{ED}$	0.0966
Mohammed & Yassin [13]	$4T_{\oplus} + 7T_h + 14T_{\|\|} + 5T_{ED} + 4T_{mod}$	0.0575
Nikravan, et, al.[24]	$15T_{\oplus} + 19T_h + 54T_{\|\|} + 6T_m$	0.0737
Ayub et, al. [14]	$9T_{\oplus} + 18T_h + 34T_{\|\|} 8T_{ED}$	0.0782
Proposed	$4T_{\oplus} + 8T_h + 15T_{\|\|} + 5T_{ED} + 5T_{mod}$	0.0713

Table 4. computation of communication costs.

I. Conclusion

In this paper, we introduce a lightweight multi-factor authentication scheme to authenticate user and Server communication. The proposed scheme has many security features such as multi-factor mutual authentication, user anonymity, unlinkability, virtual smart factor authentication, and using QR code in mutual authentication. Furthermore, the proposed approach resists password guessing (online/offline), user/server impersonation, MITM, replay attacks, and insider attacks. The proposed scheme not only presents an authentication protocol but also reduces the cost. According to the comparison result, it is considered more efficient than other existing authentication schemes. Additionally, our protocol resists well-known security threats depending on the informal security analysis. Moreover, the formal security analysis and performance also proved that the proposed protocol facilitates the login process in a secure manner. Consequently, our protocol has been proven to be effective, dependable, and safe.

References

[1] S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating user perception of multi-factor authentication: A systematic review," arXiv preprint arXiv:1908.05901, 2019. https://doi.org/10.48550/arXiv.1908.05901

[2] 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: IEEE.

[3] M. Sajid, A. Harris, and S. Habib, "Internet of Everything: Applications, and Security Challenges," in *2021 International Conference on Innovative Computing (ICIC)*, 2021, pp. 1-9: IEEE.

[4] S. P. Krishna, D. Tejasri, B. Soumya, and M. Madhuri, "Bank Application: One-Time Password Generation," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2022, pp. 855-859: IEEE.

[5] V. Rajasekar, J. Premalatha, K. Sathya, and M. J. Saračević, "Secure remote user authentication scheme on health care, IoT and cloud applications: a multilayer systematic survey," vol. 18, no. 3, pp. 87-106, 2021.

[6] Y. Li, X. Yun, L. Fang, and C. Ge, "An Efficient Login Authentication System against Multiple Attacks in Mobile Devices," vol. 13, no. 1, p. 125, 2021.

[7] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," vol. 2, no. 1, p. 1, 2018.

[8] W. K. Ahmed and R. S. Mohammed, "Lightweight Authentication Methods in IoT: Survey," in *2022 International Conference on Computer Science and Software Engineering (CSASE)*, 2022, pp. 241-246.

[9] A. Hameed and A. Alomary, "Security Issues in IoT: A Survey," in *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2019, pp. 1-5.

[10] A. K. Tyagi and A. Abraham, "Internet of Things: Future Challenging Issues and Possible Research Directions," International Journal of Computer Information Systems and Industrial Management Applications. ISSN, pp. 2150-7988, 2020.

[11] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646-1685, 2020.

[12] F. Chen, Z. Xiao, T. Xiang, J. Fan, H.-L. Truong, and S. Computing, "A Full Lifecycle Authentication Scheme for Large-scale Smart IoT Applications," 2022.

[13] A. J. Mohammed and A. A. Yassin, "Efficient and flexible multi-factor authentication protocol based on fuzzy extractor of administrator's fingerprint and smart mobile device," vol. 3, no. 3, p. 24, 2019.

[14] M. F. Ayub, K. Mahmood, S. Kumari, A. K. Sangaiah, and Networks, "Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology," vol. 7, no. 2, pp. 235-244, 2021.

[15] M. A. Hassan and Z. Shukur, "A secure multi factor user authentication framework for electronic payment system," in *2021 3rd International Cyber Resilience Conference (CRC)*, 2021, pp. 1-6: IEEE.

[16] G. Ali, M. A. Dida, and A. J. F. I. Elikana Sam, "A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications," vol. 13, no. 12, p. 299, 2021.

[17] T. N. Tan and H. J. I. Lee, "High-secure fingerprint authentication system using ring-LWE cryptography," vol. 7, pp. 23379-23387, 2019.

[18] P. Duong-Ngoc, T. N. Tan, and H. J. Lee, "Efficient NewHope cryptography based facial security system on a GPU," vol. 8, pp. 108158-108168, 2020.

[19] G. Rahman, C. Wen, and Applications, "Mutual authentication security scheme in fog computing," vol. 10, no. 11, 2019.

[20] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A Usability Study of Five {Two-Factor} Authentication Methods," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019, pp. 357-370.

[21] M. J. Sadri and M. R.Asaar, "An anonymous two-factor authentication protocol for IoT-based applications," vol. 199, p. 108460, 2021.

[22] C.-M. Chen, S. Liu, X. Li, S. Kumari, L. J. S. Li, and C. Networks, "Design and Analysis of a Provable Secure Two-Factor Authentication Protocol for Internet of Things," vol. 2022, 2022.

[23] M. Fareed, A. A.Yassin, and Informatics, "Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system," vol. 11, no. 4, 2022.

[24] M. Nikravan and A. J. W. Reza, "A multi-factor user authentication and key agreement protocol based on bilinear pairing for the internet of things," vol. 111, no. 1, pp. 463-494, 2020.

[25] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, V. J. Odelu, and p. i. biomedicine, "Secure anonymous mutual authentication for star two-tier wireless body area networks," vol. 135, pp. 37-50, 2016.

[26] H. H. Kilinc, T. J. Yanik, and tutorials, "A survey of SIP authentication and key agreement schemes," vol. 16, no. 2, pp. 1005-1023, 2013.