Received: 31 January 2022 | Revised: 21 February 2022 | Accepted: 22 February 2022
DOI: 10.37917/ijeee.18.1.9 Vol. 18| Issue 1| June 2022

Open Access

*Iraqi Journal for Electrical and Electronic Engineering*
*Original Article*

# Secure Patient Authentication Scheme in the Healthcare System Using Symmetric Encryption

**Naba M. Hamed[*1], Ali A. Yassin[2]**
[1]College of Computer Science and Information Technology, University of Basrah, Basrah, 61004, Iraq
[2]Department of Computer science, Education College for Pure Sciences, University of Basrah, Basrah, 61004, Iraq

**Correspondence**
*Naba M.Hamed
Department of Computer science,
College of Computer Science and Information Technology,
University of Basrah, Basrah, Iraq
Iraq Email: nabawq12@gmail.com

***Abstract***
***Recently, the incorporation of state-of-the-art technology such as Electronic Healthcare Records (EHRs), networks, and cloud computing has transformed the traditional healthcare system. However, security problems have arisen as a result of the integration of technology. Secure remote user authentication is a core part of the healthcare system to validate the user's identification via an unsecure communication network. Since then, several remote user authentication schemes have been presented, each with its own set of pros and limitations. As a result, security, malicious attacks and privacy concerns are considered one of the main challenges related to the healthcare system. In this paper, we propose a safe user authentication scheme for patients in the healthcare system that overcomes these flaws and confirms the security of the proposed work using scyther, a formal security tool. In the healthcare environment, our work provides an effective means to construct an environment capable of setting, registering, storing, searching, analyzing, authentication, and verifying electronic healthcare information in order to protect the information of patients. Furthermore, our suggested scheme uses symmetric encryption based on the crypto-hash function for accessing the anomaly of the patient's identity and One-Time Password (OTP). Towards the end of the study, the performance analysis results indicate a delicate balance of security and performance that is frequently lacking in previous works.***

**Keywords:** Electronic Health Records, Malicious Attacks, Healthcare System, OTP Authentication.

## I. INTRODUCTION

The Internet has become an integral aspect of modern life. With the rapid advancement of Internet technology, we can now provide any service from anywhere and at any time. Remote user authentication is becoming a crucial aspect of accessing valuable services or resources in the healthcare system, cloud applications, multi-server environments, and mobile devices. Remote user authentication is an important part of any security design. Authorization grants Identity-Based Privileges and audit trails are not transparent without authentication. Secrecy and privacy will be breached if we are unable to distinguish between authorized and unauthorized parties. Likewise, in order to access resources situated in faraway locations, each user must have the necessary access privileges. The use of a password-based authentication technique is one of the most simple and convenient protection mechanisms. The healthcare system, E-business, Database Management Systems, and Smart Card applications are some instances of password-based authentication schemes. There are two major issues with the password process in the computer system. One example is that passwords are kept in database systems in plaintext that the database administrator may readily view. Another issue is that an attacker can impersonate a valid user by stealing the user ID and password from the password database. Individuals' e-health data is some of their most sensitive information. Privacy regulations such as the Health Insurance Portability and Accountability Act (HIPPA) and the General Data Protection Regulation (GDPR)[1]. The remote system should have the skill to authenticate the users. Otherwise, a discount could impersonate a legitimate user login to get access to the system[2]. They were intended to improve healthcare data governance; however, e-health data has frequently been violated. Furthermore, as the accessibility and usability of e-health data grows, so do the security attack vectors. Over the previous decade, 1.5 million medical devices have been affected owing to software flaws and wireless connections, and cloud computing services that store and analyze e-health data have become a target for massive e-health data. In 2019-2021, 41.4 million patient records

were compromised, according to the Protenus Breach Barometer [1, 3-5].

As a result, security and privacy concerns must be addressed in order to prevent e-health data intrusions. To adequately research how to protect e-healthcare systems, security challenges, and solutions must be recognized as referred to previously. In more details, Electronic healthcare records (EHRs) are a developing technology that plays an important role in patient care. This is a medical service that allows patients to have medical appointments outside of hospitals, follow their health cases, review their medical tests, and do other medical tasks using their EHR system. Despite these benefits, studies in the literature highlight drawbacks associated with EHRs, which include disruptions to protecting patient privacy and security. Supporting a system to authenticate patients in an electronic health record (EHR) is a critical step for preventing various security risks from gaining access to patients' identities and data. Existing authentication schemes continue to have security flaws. Exchanging medical-related information or data between clients and servers exposes them to intrusion by attackers since they can be transmitted across an unstable network [6-17].

In this paper, we present a secure scheme for authenticating EHR patients and the Healthcare Center Server based on genuine member identities and verification codes. To provide robust security while maintaining satisfactory speed, the proposed work employs a lightweight crypto-hash function for the generation of One-Time Passwords (OTP) and symmetric key encryption (Counter mode (CTR mode)). As a result, the major purpose of this study is to conduct a strong authentication scheme to overcome issues in the previous works. Because current e-healthcare systems often comprise of numerous components (e.g., e-health data, medical devices, medical components (Ex. patients, doctors, employees), and cloud-health computing), there are several security risks faced these components, and our solutions are focused on authentication and privacy of patients represented the heart of healthcare system. In addition, OTP-based authentication appears to be one of the fastest-growing authentication technologies to prevents several malicious attacks such as MITM, Reply, Insider. The study demonstrate that the majority scheme of OTP-based authentication and key management solves the problems associated with dynamic ID and password schemes, especially in healthcare systems. The proposed scheme has good metrics like mutual authentication, user's anomaly, un-linkability. In practical side, the Scyther security proof was used to demonstrate our scheme's high security and resist malicious attacks. The proposed scheme has a good balances between the complexity of security and performance, can applied in healthcare system, and deals with real world data associated with the patient part.

The remainder of the article is arranged as follows: Section 2 describes the primitive tools. Section 3 shows the related work. Section 4 focused on the proposed scheme. Section 5 includes formal analysis utilizing the Scyther tool as well as security analysis. Section 6 describes the performance results. Finally, section 7 denotes to the conclusion.

## II. Primitive Tools

### A. Counter mode (CTR mode)

Counter mode is also known as unsynchronized stream cipher mode, because the stream cipher is built from the block cipher. Here we provide a self-contained description. To encrypt using CTR mode, first, choose a uniform value $ctr \in \{0,1\}^n$. Then, by computing $y_i := F_k(\text{ctr} + \text{i})$, where $ctr$ and $i$ are integers and addition is modulo $2^n$, a pseudorandom stream is formed. So, $C_i := y_i \oplus m_i$ is the $i^{th}$ ciphertext block, and the $IV$ is transmitted as part of the ciphertext once more. It's worth repeating that $F$ doesn't have to be invertible or even a permutation to be decrypted. The created stream may be trimmed to exactly the plaintext length. Preprocessing can be used to generate the pseudorandom stream before the message is known, and the stateful variation of $CTR$ mode is secure, just like $OFB$ mode, another "streamcipher" method. In contrast to the other safe modes covered so far, the $CTR$ mode has the benefit of being able to fully parallelize encryption and decryption since all blocks of the pseudorandom stream may be calculated independently of one another. In contrast to $OFB$, it is also possible to decipher the cipher text's $i^{th}$ block using just one $F$ evaluation. If F is a pseudorandom function, then $CTR$ mode is secure. $CTR$ mode is appealing because of these qualities [18].

### B. Crypto Hash Function

The process of turning a string of characters into a fixed-length value or key that represents the original string is referred to as hashing. The hash function indexes the original value or key and then accesses the data associated with that value or key. These which are used in cryptography should be called "one-way hash functions" can use to figure out the hash value for a given input. In the opposite way, it must be impossible to find an input for a given value that has the same hash value as that value (this is referred to as a one-way characteristic). The SHA-2 hash algorithm is used to encrypt data such as passwords. SHA-2 is a fantastic technique to ensure the security of your data, but it takes a long time to complete [19, 20].

### C. The One-Time Pad

In 1917, Vernam invented the one-time pad, a totally private encryption technique. There was no indication that the proposal was absolutely hidden at the time Vernam presented it; in fact, no one knew what perfect secrecy meant. Shannon introduced the notion of complete secrecy and proved that the one-time pad delivers that degree of security some 25 years later. Use of the pad just once The assumption behind the OTP is that the encryption key must be at least as lengthy as the plaintext message and comprised of really random digits. Each letter of the plaintext is "added" to one element from the OTP using modulo-addition. When the key

is unknown, a cipher text is produced that has no relation to the plaintext. At the receiving end, the same OTP is used to retrieve the original plaintext [21].

## III. Related Works

Several techniques have been presented to overcome the issues associated with cloud authentication and access control. Currently, the practice of medicine applications has sparked an interest among researchers. One of the most important topics addressed is the confidentiality of patient data, since the patient's data is private and confidential. Similarly, the patient may wish to conceal their genuine identity in order to preserve their privacy [4]. The authors of [22] covered numerous security needs, such as EHR storage security, malicious code prevention, protected access rights management, and other factors to secure the health information system. However, they did not propose a feasible plan for a patient to move their EHR to a health information system. We may envisage a scenario in which a hospital uses just the aforementioned simple procedures to construct its own health information system with no security mechanism. Furthermore, under this method, it is not viable for each patient to execute their own EHR exchange. In contrast, the authors of [4, 23-25] proposed that each patient's health records might be portable and saved on a flash drive. This is an interesting concept, but it is currently challenging to execute. There are several security concerns to address, such as portable device security and patient medical information access privileges. More security methods, however, are required to address these types of security vulnerabilities. Furthermore, several patient authentication strategies for e-health systems have been developed [26-30]. The systems in [27, 28] were vulnerable to a user impersonation attack and did not provide session key establishment with formal security evidence. The authors of [3, 29] did not provide a forward secrecy proof for the establishment of the session key. For cloud-assisted wearable devices, Liu et al. [31] advocated local and distant authentication. To achieve mutual authentication between wearable device and a smartphone, the local authentication protocol employs a hash-based selective disclosure method and a Chebyshev chaotic map. Following local authentication, the cloud performs remote authentication of the device using a yoking-proof algorithm.

A mutual authentication procedure was developed in a few investigations [32-34]. Based on Chebyshev chaotic maps and Diffie–Hellman key exchange, Li et al. [35] suggested a mutual authentication protocol and key agreement technique. Only approved doctors and medical personnel would have access to patients' health data acquired by body sensors in the planned medical system. A digital signature was also used to assure non-repudiation of the doctor's diagnosis. Cheng et al. [36] used blockchain to bypass a mutual authentication scheme's reliance on a trusted third party.

As a result, the primary goal of this research is to develop a robust authentication method based on cryptosystem tools to address concerns that have arisen in the previous works. Because today's e-healthcare systems generally include several components (e.g., e-health data, medical devices, medical components, and cloud-health computing), security threats and demands differ, and our solutions are centered on patient authentication and privacy. Based on the foregoing notions, we present an improved anonymous user authentication and key agreement approach for health monitoring. In the following security analysis, we showed the security of our protocol using security analysis and the Syther tool. The results of the performance comparison and efficiency analysis reveal that the proposed scheme provides a higher level of security while preserving computational efficiency.

## IV. The Proposed Scheme

In this section, we present the strong healthcare authentication scheme based on five phases: Setup, Registration, Login and Authentication, Healthcare, and key management. Our work offers the healthcare scheme permitting to six main elements: Cloud Healthcare Server ($CHS$), Key Generator Center ($KGC$), Users ($U_i$), Patient ($P_i$), Administrator ($Adm$), and Doctor ($D_i$). The main goal of the current scheme is offered secure environment for exchanging components' data of the proposed scheme. Additionally, this work has numerous benefits such as mutual authentication, key management, password anonymity, as well as, can resist familiar malicious attacks such as insider, MITM, Reply, Impersonate, and other. The characters used in the current work are conversed in Table 1.

TABLE 1
NOTATION USED IN THE PROSED SCHEM

| Symbol | Description |
|---|---|
| $CHS$ | Cloud Healthcare Server. |
| $KGC$ | Key Generator Center. |
| $U_i$ | The user. |
| $P_i$ | Patient in the system. |
| $Adm$ | Administrator in the system. |
| $D_i$ | Doctor in the system. |
| $\oplus$ | XOR operation. |
| MITM | Man-In the middle attack. |
| CTR mode | Counter mode. |
| $EHR_i$ | Electronic healthcare record. |
| $h(.)$ | One-way hash function. |
| $ID_{P_i}$ | Identity of patient $P_i$. |
| $PW_{P_i}$ | Password of patient $P_i$. |
| $VC$ ,$VC''$,$VC'$ | Verification code. |
| $SK_{P_i}$ | Shared key between $P_i$ and $CHS$. |
| $OFB$ | Output Feedback mode. |

| | |
|---|---|
| $r_i$ | The one-time random number generated by user. |
| $\|\|$ | Concatenation operation. |

*A. Setup Phase*

The setup phase considers the first step of the presented work. The $KGC$ is a trust third party created all the security parameters and depends on one-way hash function $h(.)$, symmetric encryption $Enc()$ /decryption ( $Dec()$ ). Then, $KGC$ creates ($SK_{P_i} \in \mathbb{Z}$) to encrypt/ decrypt data between $P_i$ and $CHS$; where the symmetric key encryption is Counter mode (CTR mode). This type of encryption employs the block cipher algorithm, which offers significant efficiency gains over traditional encryption options without jeopardizing security. Its fitted security, in particular, has been proven. Second, the majority of the objections leveled against CTR mode are unfounded.

*B. Registration Phase*

User ($P_i$) registers his main information in $CHS$ by performing the following steps:

1. $P_i$ Chooses his identity ($ID_{P_i}$) and password $(PW_{P_i})$ by using the main website of health care institute. Also, $P_i$ records information about his doctor and relatives (Electronic HealthCare Record ( $EHR_i$ )). $EHR_i$ includes phone numbers of doctors and relatives, Name of patient, Pathological case, E-mail, and others.

2. $P_i$ computes the following anonymous parameters based on the following equations:

$$AID_{P_i} = h(ID_{P_i}||SK_{P_i}) \dots Eq(1)$$
$$APW_{P_i} = h(PW_{P_i}||SK_{P_i}) \dots Eq(2)$$

3. $P_i$ submits ($AID_{P_i}, APW_{P_i}, HCR_i$) to $CHS$.

4. $CHS$ verifies its database to check if $P_i$ is previously registered. If so, $CHS$ terminates this phase. Otherwise, the $CHS$ ds a new patient's information ( $AID_{P_i}, APW_{P_i}, EHR_i$) in the main secure database.

*C. Login and Authentication Phase*

The patient ($P_i$) wishes to login system for checking his $EHR_i$, receiving report from his doctor or sending quires to his doctor. Therefore, it is necessary to ensure from the authority of $P_i$ to allow him accessing to the system. The important steps that use in current phase as follows:

1. $P_i$ enters his username ($ID_{P_i}$) and password ($PW_{P_i}$), generates integer random number $r_i \in \mathbb{Z}$, and computes an anonymity of identity and anonymity one time password $AID_{P_i} = h(ID_{P_i}||SK_{P_i})$ and $APW_{P_i} = h(h(PW_{P_i}||SK_{P_i})||r_i)$, respectively.

2. $P_i$ encrypts $r_i$ using symmetric key encryption (CTR mode), $E_{P_i} = Enc_{SK_{P_i}}(r_i)$.

3. $P_i$ sends his login request $<AID_{P_i}, APW_{P_i}, E_{P_i}>$ to $CHS$.

4. In the cloud health server ($CHS$), he checks patient's; if he was found in the database of $CHS$ or no based on $AID_{P_i}$ for obtaining $SK_{P_i}$. If false, he terminates this phase. Otherwise, $CHS$ restores random number by decrypting $E_{P_i}$ where $r'_i = Dec_{SK_{P_i}}(E_{P_i})$.

5. $APW'_{P_i}$ and $APW_{P_i}$, if it is valid then $CHS$ sends challenge as verification code ($VC$) to the E-mail of $P_i$.

6. At this moment, $P_i$ restores verification code ($VC''$) via his E-mail and encrypts $VC''$ using $E'_{P_i} = Enc_{SK_{P_i}}(VC')$. Then, he sends $E'_{P_i}$ to $CHS$.

7. $CHS$ computes $VC'' = Dec_{SK_{P_i}}(E'_{P_i})$ and compares between $VC''$ and $VC$ ; if true then he gives permission to $P_i$ for entering the system and applying the main operations included healthcare services at the Healthcare phase. Otherwise, He terminate the current phase.

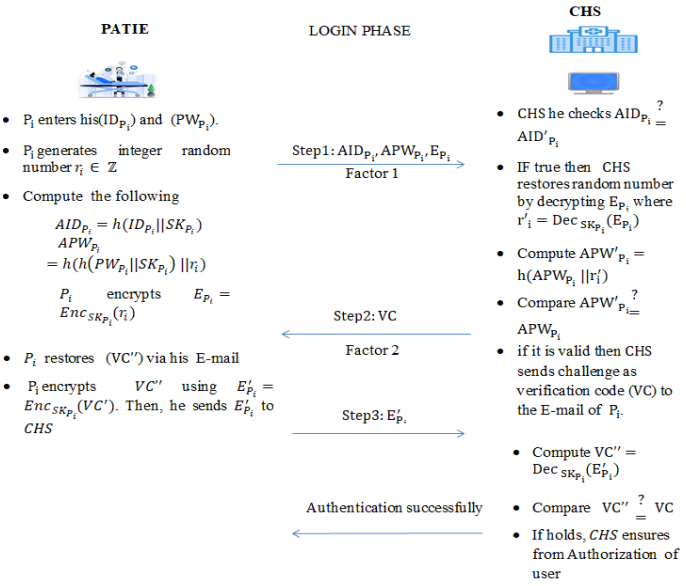


Fig.1: Login and Authentication phase

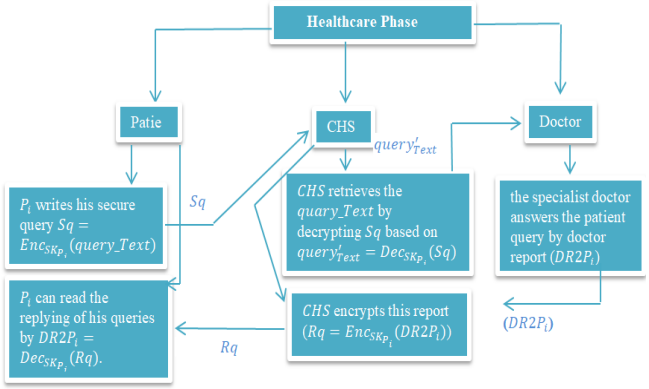


Fig.2: Flow chart of Healthcare phase for patient

*D. Healthcare Phase*

There are main medical services presented to each patient $P_i$, we can list these service in the below steps:

1. Health promotion: $P_i$ keeps the attachment with the health foundation.

2. Disease prevention: $P_i$ resists the disease based on devices of doctors $(D_1, D_2, D_3 \dots, D_n)$ and avoids all foods caused from the severity of chronic diseases.
3. Laboratory and diagnostic care: $P_i$ can receive the results of his test directly in his account $(EHR_i)$. In the other side, early examination through the symptoms associated with chronic diseases by sending his symptoms to the health foundation.
4. Remote emergency and inpatient services: $P_i$ can get full services to the case emergency to take first aid and treatment and prepare logistics before arriving at the hospital.
5. The mechanism of sending a query from $P_i$ to $CHS$ and vice versa. This query represents "*Inquiries about symptoms of a specific disease or other*". However, $P_i$ writes his secure query $Sq = Enc_{SK_{P_i}}(query\_Text)$ and sends $Sq$ to $CHS$.
6. In the side of $CHS$, he retrieves the $quary\_Text$ by decrypting $Sq$ based on $query'_{Text} = Dec_{SK_{P_i}}(Sq)$. Then, $CHS$ sends the $query'_{Text}$ to the concerned department in the health foundation. After that, the specialist doctor answers the patient query by doctor report $(DR2P_i)$ and then $CHS$ encrypts this report $(Rq = Enc_{SK_{P_i}}(DR2P_i))$ and resubmits $Rq$ to $P_i$.
7. Upon receiving $Rq$, $P_i$ can read the replying of his queries by $DR2P_i = Dec_{SK_{P_i}}(Rq)$.

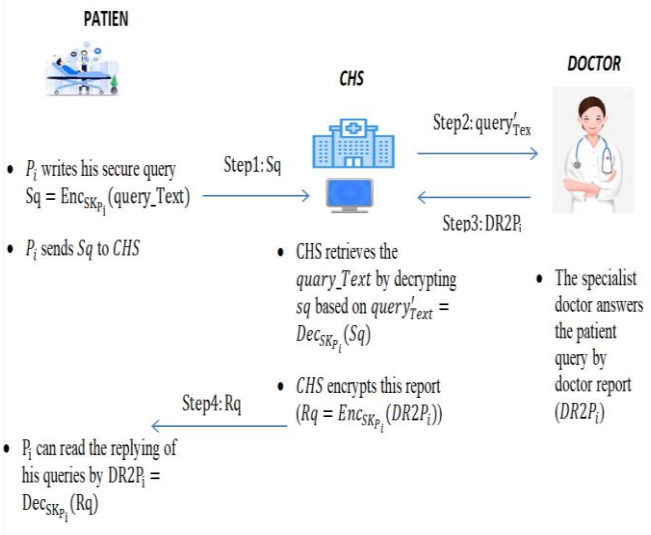


Fig.3: Healthcare phase for patient

**5. Key Management Phase**

Here, the main parties have an agreement to generate once key for each login request based on $(SK_{P_i}, r_i)$. In the moment of successful login of patient, the main parties $(P_i, CHS)$ performs the following points to apply this phase.

1. Patient $(P_i)$ side computes $SK_{P_i} = SK_{P_i} \oplus r_i$.
2. Cloud Healthcare Server $(CHS)$ side computes $SK_{P_i} = SK_{P_i} \oplus r'_i$.

## V. Formal Security Analysis with Scyther Tool

Currently, we are focusing on establishing that the suggested method can withstand severe assaults such as phishing, man-in-the-middle (MITM), replay attacks, and eavesdropping attacks. Furthermore, our work incorporates a number of security features. We do the following analysis of the suggested scheme. It considers as a cryptography tool used for formal security analysis and proof to ensure from security, resisting well-known malicious attacks, correctness of the messages via communication channel applied with the perfect cryptography functions such as hash function, EMAIL, encryption, and decryption. Finally, this tool gains the proposed scheme a guarantee to implement in the safe condition and can resist the familiar attacks until the attacker is accessible. Currently, the proposed scheme has been written in SPDL language and the viewed the results in the state of $(Automatic\ Claim)$ and $(Verification\ Claim)$.

1. ***Verification of Claim :*** Scyther's input language allows security features to be specified in terms of claimed events. For example, one may argue in a role definition that a particular value is confidential (confidentiality) and that certain traits should apply to communication partners (authentication). Scyther can be used to verify or disprove these traits.
2. ***Automatic of Claim:*** If the protocol specification lacks security assertions, Scyther can generate them automatically. Verification claims assert that the protocol's putative communication partners must have followed it as intended at the conclusion of each role. All parameters and locally produced values are likewise subject to confidentiality claims (nonce). Scyther evaluates the expanded protocol description, in the same manner, he did previously. This allows users to quickly study a protocol's characteristics. Based on the scyther tool, our work resists harmful attacks such as MITM, Insider, Replay, Spoofing, and Impersonation. The login and authentication phases are depicted in Figure 4 [37].

We notice that the proposed scheme has protect against malicious attacks as above mention. So, SPDL supports many major crypto functions like sending or receiving messages among components, and the roles of each component. When we strip the proposed system from security factions like crypto hash, encryption, we will notice the apparent weakness of the system, as Figures 5 and 6.

Figure 5 represents the result of an safe system that does not contain perfect cryptography functions. Therefore, this system becomes insecure and vulnerable to face the malicious attacks (see Figure 6).

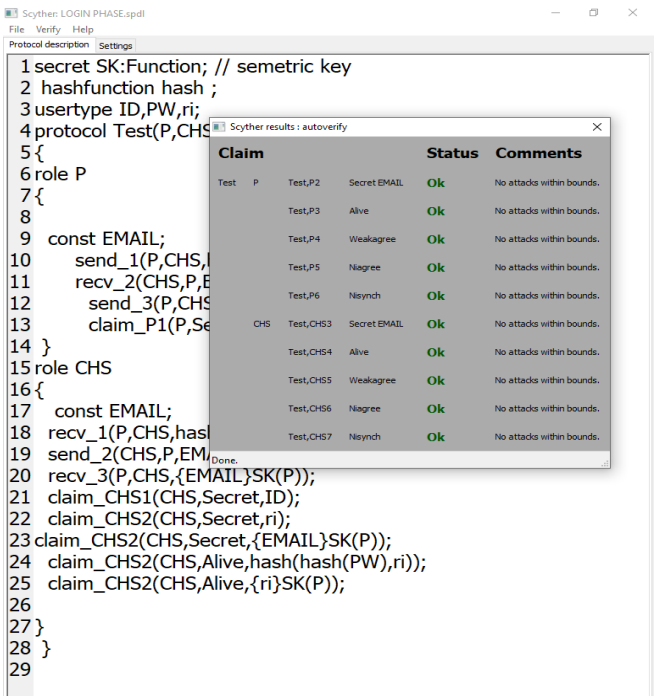


Fig.4: Login and Authentication phase that cannot be attacked

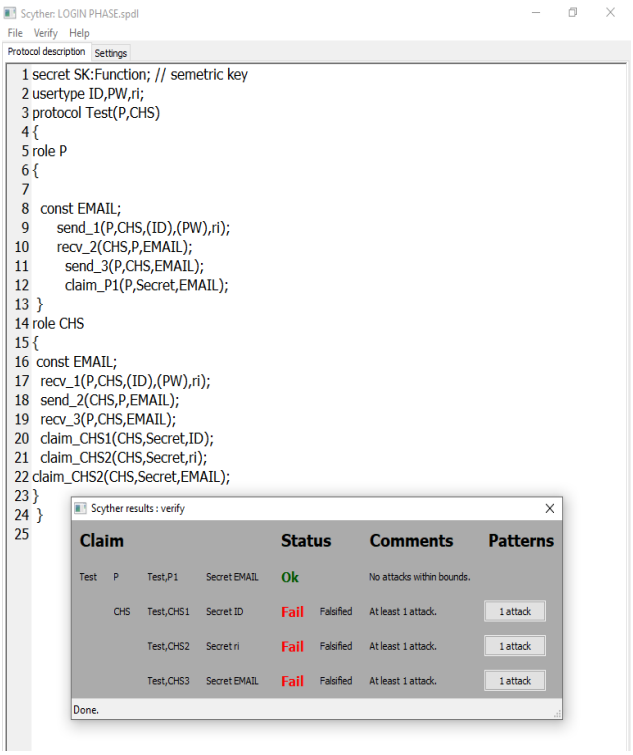


Fig. 5: Login and authentication phase that can be attacked

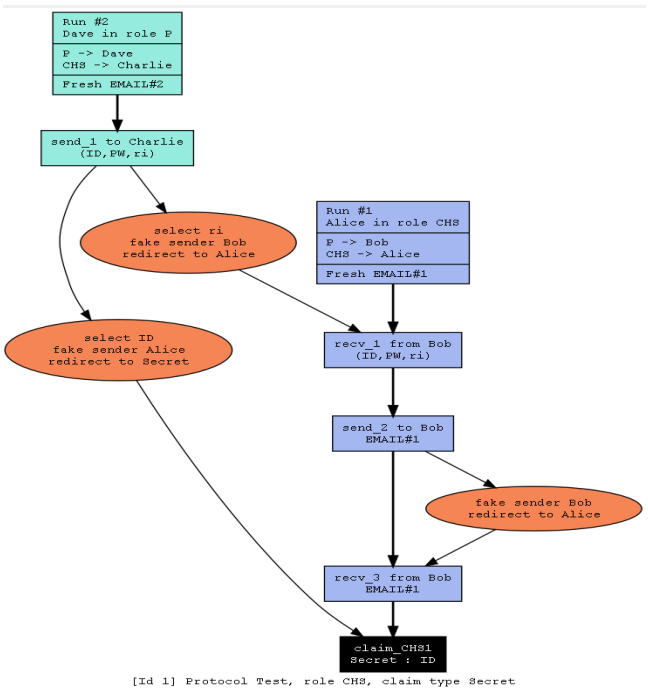


Fig. 6: Model checking of the login and authentication phase.

Figure 7 refers to the code of the login and authentication phase.


Fig. 7: The Proposed Scheme In SPDL-Scyther.

In the healthcare phase, we apply the same mechanism to check the correctness, security, verification of this phase. The figure 8 demonstrates the safety and security of the healthcare phase.

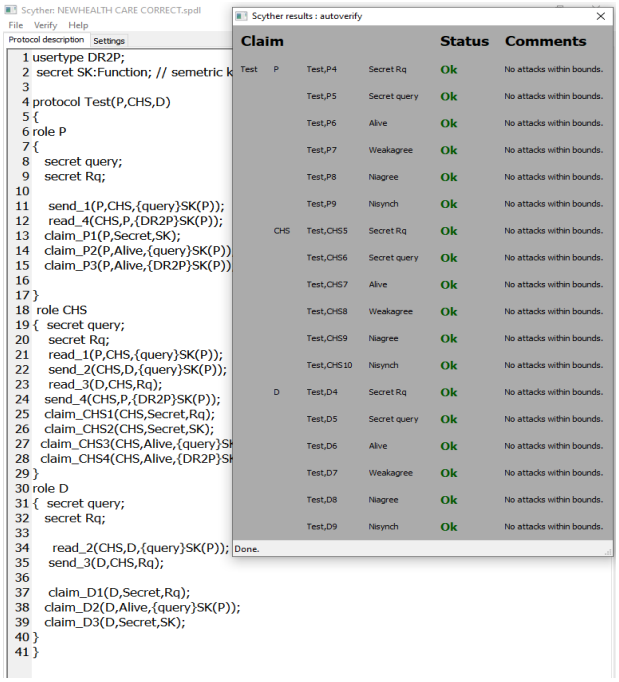


Fig. 8: Healthcare phase that cannot be attacked.

Figure 9 demonstrates the result of a safe system without faultless cryptographic mechanisms. As a result, this method becomes subject to malicious assaults and is rendered unsecure (see Figure 10).

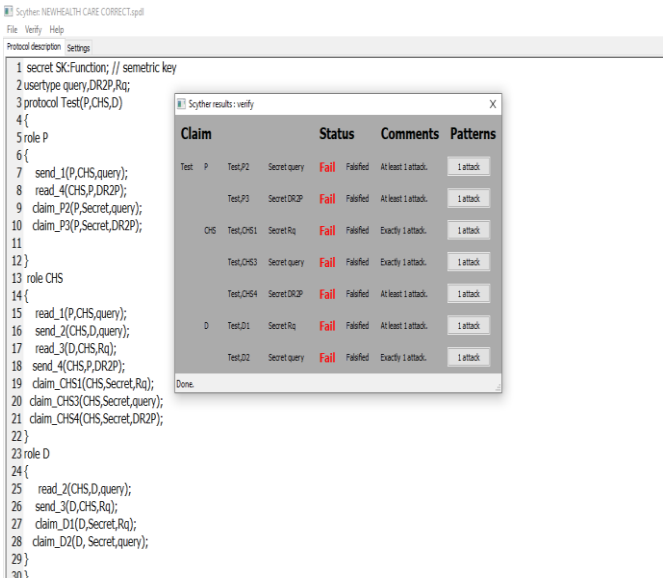


Fig. 9: Healthcare phase that can be attacked.


Fig.10: Model checking of the healthcare phase.

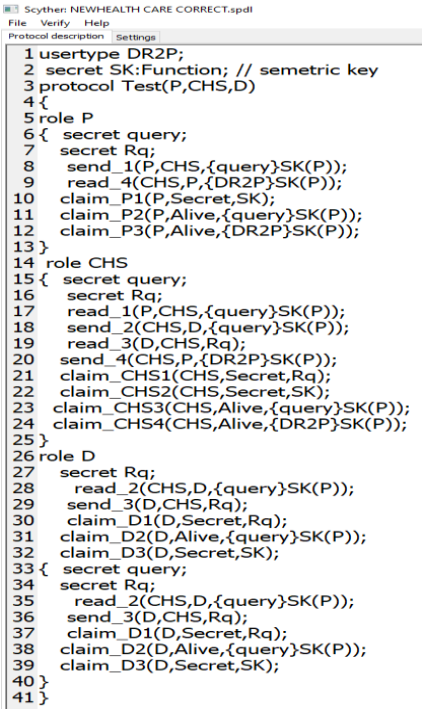


Fig. 11: The Proposed Scheme In SPDL-Scyther

## VI. Performance Analysis

### A. *Computation Cost*

The computational cost is used to determine the time complexity of the proposed scheme. Table 2 compares the computational costs of the most important related schem and our work and Figure 12, as well as our work with other related works. Table 3 shows key security feature comparisons between the proposed scheme and previous works. Moreover, depending on[38], the processing times for the basic functions are approximately as follows. Using the rules in the following:

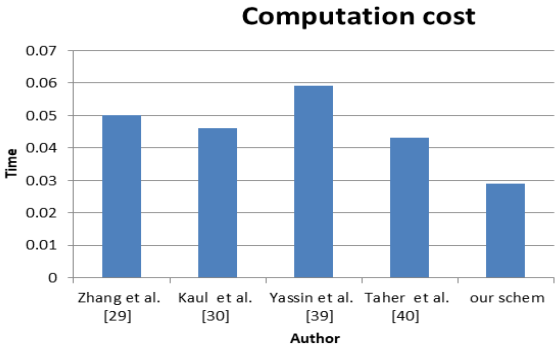


Fig. 12: Computation Cost Comparison

TABLE 2
COMPUTATION COST COMPARISION WITH OTHER RELATED WORKS

| Term | Meaning | Time needed |
|---|---|---|
| $T_h$ | The time allotted to the crypto hash function | 0.0023 ms |
| $T_{\oplus}$ | The processing time for the XOR operation | Negligible |
| $T_{Enc}$ | The processing time for a symmetric encryption function. | 0.0046 ms |
| $T_{Dec}$ | The processing time for a symmetric decryption Function. | 0.0046 ms |
| $T_{\|\|}$ | The processing time for the Concatenation operation. | Negligible |

According to the aforementioned comparisons, the suggested system has a lower time complexity ($5\,T_h + 2\,T_{Enc} + 5\,T_{\|} + 2T_{Dec}\,) = 0.0299$ than previous relevant studies. We see that the suggested system has a fair mix of performance and security aspects (see Table 3).

TABLE 3
COMPARING OF THE COMPUTATIONAL COST

| Scheme | Registration Phase | Login and Authentication Phases | Total Cost |
|---|---|---|---|
| Zhang et al. [29] | $4T_h + 5T_{\oplus} + 5T_{\|}$ | $18\,T_h + 27\,T_{\oplus} + 19T_{\|}$ | $22\,T_h + 32T_{\oplus} + 24T_{\|} \approx 0.0506$ |
| Kaul et al. [30] | $6\,T_h + 6\,T_{\oplus} + 6\,T_{\|} + 1T_{Dec} + 1T_{Enc}$ | $10\,T_h + 20\,T_{\oplus} + 10\,T_{\|}$ | $16\,T_h + 26\,T_{\oplus} + 16\,T_{\|} + 1T_{Dec} + 1T_{Enc} \approx 0.046$ |
| Yassin et al. [39] | $5\,T_h + 2\,T_{\oplus} + 1T_{\|}$ | $13\,T_h + 12\,T_{\oplus} + 6T_{\|} + 2T_{Dec} + 2T_{Enc}$ | $18\,T_h + 14\,T_{\oplus} + 7T_{\|} + 2T_{Dec} + 2T_{Enc} \approx 0.0598$ |
| Taher et al. [40] | $5\,T_h + 3\,T_{\oplus} + 4\,T_{\|}$ | $2T_{Dec} + 2T_{Enc} + 6\,T_h + 3\,T_{\oplus} + 5T_{\|}$ | $11\,T_h + 6T_{\oplus} + 9T_{\|} + 2T_{Dec} + 2T_{Enc} \approx 0.0437$ |
| Our Scheme | $2\,T_h + 2T_{\|\|}$ | $3T_h + 3\,T_{\|} + 2T_{Enc} + 2T_{Dec}$ | $5\,T_h + 2\,T_{Enc} + 5\,T_{\|} + 2T_{Dec} \approx 0.0299$ |

TABLE 4
COMPARISON WITH OTHER RELATED WORKS

| Security Features | [4] | [22] | [29] | [30] | [32] | [34] | Our |
|---|---|---|---|---|---|---|---|
| Mutual Authentication | YES | NO | YES | YES | YES | YES | YES |
| Anonymous& Untraceable | NO | NO | YES | NO | NO | YES | YES |
| Forward Secrecy | YES | NO | YES | NO | YES | YES | YES |
| Key Agreement | NO | NO | NO | NO | NO | NO | YES |
| Key Freshness | NO | NO | NO | NO | NO | NO | YES |
| MITM Attack | NO | YES | YES | NO | YES | YES | YES |
| Replay Attack | YES | YES | YES | YES | YES | YES | YES |
| Eavesdropping Attack | NO | NO | NO | NO | NO | YES | YES |
| Stolen Personal Device | NO | NO | NO | NO | NO | NO | YES |
| Healthcare Phase | NO | NO | NO | NO | NO | NO | YES |

### *B. Communication cost*

During the login and authentication step , the cost of sent messages is calculated. we assumed the identity size is 32 bit, the hash value's size is 160 bits[41], the cipher text value size is 128 bit, we also compare our proposed scheme with other related works based on Table 5 below.

TABLE 5
COMMUNICATION COST

| Authors | No of bits | No of messages |
|---|---|---|
| Zhang et al.[29] | 1568 | 4 |
| Kaul et al. [30] | 768 | 4 |
| Yassin et al. [39] | 576 | 2 |
| Taher et al.[40] | 1660 | 3 |
| Our Scheme | 608 | 3 |

## VII. CONCLUSIONS

EHRs enable authorized health stakeholders to share structured medical data in order to improve healthcare delivery quality. In these systems, privacy and security are critical, since if sensitive information is leaked, the patient might face serious consequences. Concerns about security and privacy are seen as important barriers in the healthcare system. Remote user authentication is a crucial step in authenticating a person's identity. There have been a number of techniques for remote user authentication, each with their own set of advantages and disadvantages. We propose a secure user authentication scheme for patients in the healthcare system that uses Scyther, a formal security tool, to confirm the security of the proposed work. In the healthcare setting, our work enables the creation of an environment capable of setting, registering, storing, finding, analyzing, authenticating, and validating electronic healthcare information in order to secure patient information. The suggested work uses a lightweight crypto-hash function for the creation of One-Time Passwords (OTP) and symmetric key encryption (Counter mode (CTR mode) to provide good security while maintaining adequate performance. As a result, the primary goal of this study is to develop a reliable authentication method based on cryptosystem tools in order to address the problems identified in the previous study. Because security threats and demands differ, our solutions focus on patient authentication and privacy. Keep this information private and away from unwanted access. The proposed system will be able to fight off attacks like Man-in-the-Middle, Insider, Replay, and more. It's safe to use features like mutual authentication, anomalies, key management, and other things that are safe. Achieve a balance between speed and security. In the future, we will focus on administrators using two-factor authentication. First-factor biometrics (password and user name) and second-factor biometrics (fingerprint) improve the security of electronic health records patient HER, which is more secure than traditional authentication factors.

## CONFLICT OF INTEREST

The authors have no conflict of relevant interest to this article.

## REFERENCES

[1] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE journal of biomedical and health informatics*, vol. 24, no. 8, pp. 2169-2176, 2020.

[2] E. T. Jasim and H. A. Younis, "Cryptanalysis and Security Enhancement of a Khan et al.'s Scheme," *IOSR Journal of Computer Engineering*, vol. 17, no. 2, pp. 08-16, 2015.

[3] V. Jaiman and V. Urovi, "A consent model for blockchain-based health data sharing platforms," *IEEE Access*, vol. 8, pp. 143734-143745, 2020.

[4] M. T. Chen and T. H. Lin, "A Provable and Secure Patient Electronic Health Record Fair Exchange Scheme for Health Information Systems," *Applied Sciences*, vol. 11, no. 5, p. 2401, 2021.

[5] S. Vishnu, S. J. Ramson, and R. Jegan, "Internet of medical things (IoMT)-An overview," in *2020 5th international conference on devices, circuits and systems (ICDCS)*, 2020: IEEE, pp. 101-104.

[6] T. Chakraborty, S. Jajodia, J. Katz, A. Picariello, G. Sperli, and V. Subrahmanian, "FORGE: A fake online repository generation engine for cyber deception," *IEEE Transactions on Dependable and Secure Computing*, 2019.
[7] D. He, N. Kumar, M. K. Khan, and J.-H. Lee, "Anonymous two-factor authentication for consumer roaming service in global mobility networks," *IEEE Transactions on Consumer Electronics*, vol. 59, no. 4, pp. 811-817, 2013.
[8] R. Fazal, M. A. Shah, H. A. Khattak, H. T. Rauf, and F. Al-Turjman, "Achieving data privacy for decision support systems in times of massive data sharing," *Cluster Computing*, pp. 1-13, 2022.
[9] J. Kaur, R. A. Dara, C. Obimbo, F. Song, and K. Menard, "A comprehensive keyword analysis of online privacy policies," *Information Security Journal: A Global Perspective*, vol. 27, no. 5-6, pp. 260-275, 2018.
[10] S. K. Mukhiya and Y. Lamo, "An HL7 FHIR and GraphQL approach for interoperability between heterogeneous Electronic Health Record systems," *Health Informatics Journal*, vol. 27, no. 3, p. 14604582211043920, 2021.
[11] P. C. Paul, J. Loane, F. McCaffery, and G. Regan, "Towards Design and Development of a Data Security and Privacy Risk Management Framework for WBAN Based Healthcare Applications," *Applied System Innovation*, vol. 4, no. 4, p. 76, 2021.
[12] S. T. Webb, "Hardening the Healthcare Industry Against Ransomware Attacks," Utica College, 2021.
[13] L. Faulconer, "The Danger of Dealer's Choice: Why State-by-State Regulation of Online Sports Betting Is Not Enough," *NCJL & Tech.*, vol. 21, p. 137, 2019.
[14] B. S. Dias, "Blip on The Radar: School Safety Synergy Through Early Warning and Information Sharing," Naval Postgraduate School, 2020.
[15] S. R. Oh, Y. D. Seo, E. Lee, and Y. G. Kim, "A Comprehensive Survey on Security and Privacy for Electronic Health Data," *International Journal of Environmental Research and Public Health*, vol. 18, no. 18, p. 9668, 2021.
[16] Q. Dong, "Cloud-Connected Medical Devices for Personalized Medicine: An ECG Ring Sensor and a Home Air Pollution Sensor," The George Washington University, 2021.
[17] B. A. Mensah, "Implementing Blockchain Technology to Develop a National Electronic Data Exchange System for Medical Records," Colorado Technical University, 2021.
[18] J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC press, 2020.
[19] C. Thomas and R. T. Jose, "A comparative study on different hashing algorithms," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 7, pp. 170-175, 2015.
[20] R. A. Muhajjar, "Use of genetic algorithm in the cryptanalysis of transposition ciphers," *Basrah Journal of Scienec A*, vol. 28, no. 1, pp. 49-57, 2010.
[21] G. Ganapathy and G. Kang, "An Efficient Multi-Layer Encryption Framework with Authentication for EHR in Mobile Crowd Computing," *International journal of advanced smart convergence*, vol. 8, no. 2, pp. 204-210, 2019.
[22] I. Chiuchisan, D.-G. Balan, O. Geman, I. Chiuchisan, and I. Gordin, "A security approach for health care information systems," in *2017 E-health and bioengineering conference (EHB)*, 2017: IEEE, pp. 721-724.
[23] B. Drohan, C. A. Roche, J. C. Cusack, and K. S. Hughes, "Hereditary breast and ovarian cancer and other hereditary syndromes: using technology to identify carriers," *Annals of surgical oncology*, vol. 19, no. 6, pp. 1732-1737, 2012.
[24] S. Shafqat, S. Kishwer, R. U. Rasool, J. Qadir, T. Amjad, and H. F. Ahmad, "Big data analytics enhanced healthcare systems: a review," *The Journal of Supercomputing*, vol. 76, no. 3, pp. 1754-1799, 2020.
[25] F. Shafqat, M. N. A. Khan, and S. Shafqat, "SmartHealth: IoT-Enabled Context-Aware 5G Ambient Cloud Platform," in *IoT in Healthcare and Ambient Assisted Living*: Springer, 2021, pp. 43-67.
[26] A. K. Das and A. Goswami, "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *Journal of medical systems*, vol. 37, no. 3, pp. 1-16, 2013.
[27] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Systems*, vol. 21, no. 1, pp. 49-60, 2015.
[28] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483-495, 2018.
[29] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795-2805, 2017.
[30] S. D. Kaul, V. K. Murty, and D. Hatzinakos, "Secure and privacy preserving biometric based user authentication with data access control system in the healthcare environment," in *2020 International Conference on Cyberworlds (CW)*, 2020: IEEE, pp. 249-256.
[31] H. Liu, H. Ning, Y. Yue, Y. Wan, and L. T. Yang, "Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices," *Future Generation Computer Systems*, vol. 78, pp. 976-986, 2018.
[32] C. T. Li, C. C. Lee, and C. Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of medical systems*, vol. 40, no. 5, p. 117, 2016.
[33] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *Journal of medical systems*, vol. 44, no. 2, pp. 1-11, 2020.
[34] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star

two-tier wireless body area networks," *Computer methods and programs in biomedicine*, vol. 135, pp. 37-50, 2016.
[35] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, "Anonymous authentication scheme for smart cloud based healthcare applications," *IEEE access*, vol. 6, pp. 33552-33567, 2018.
[36] X. Liu and W. Ma, "ETAP: Energy-efficient and traceable authentication protocol in mobile medical cloud architecture," *IEEE Access*, vol. 6, pp. 33513-33528, 2018.
[37] N. El Madhoun and G. Pujolle, "A secure cloud-based NFC payment architecture for small traders," in *2016 3rd Smart Cloud Networks & Systems (SCNS)*, 2016: IEEE, pp. 1-6.
[38] M. Kompara, S. H. Islam, and M. Hölbl, "A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs," *Computer networks*, vol. 148, pp. 196-213, 2019.
[39] A. A. Yassin, J. Yao, and S. Han, "Strong authentication scheme based on hand geometry and smart card factors," *Computers*, vol. 5, no. 3, p. 15, 2016.
[40] B. H. Taher, L. H. Wei, and A. A. Yassin, "Flexible and Efficient Authentication of IoT Cloud Scheme Using Crypto Hash Function," in *Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence*, 2018, pp. 487-494.
[41] M. H. Alzuwaini and A. A. Yassin, "An Efficient Mechanism to Prevent the Phishing Attacks," *Iraqi Journal for Electrical & Electronic Engineering*, vol. 17, no. 1, 2021.