Journal of Basrah Researches (Sciences) **49**(1), 85 (2023)
DOI: https://doi.org/10.56714/bjrs.49.1.8

Role Based Access Control Using Biometric the in Educational System

Maha K. Kabier[1], Ali A. Yassin[1,2*], Zaid A. Abduljabbar[1,2,3], Songfeng Lu[3,4]

[1]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq.
[2]Technical Computer Engineering Department, Al-Kunooze University College, Basrah, Iraq.
[3]Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen, China.
[4]School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan, China.

A R T I C L E I N F O

Received 08 April 2023
Accepted 29 April 2023
Published 30 June 2023

K e y w o r d s :

E-learning, Fingerprint, Biometrics, Multifactor Adaptive Authentication Techniques, Asymmetric Scalar Product Preserving Encryption.

Citation: M.K. Kabier et al., J. Basrah Res. (Sci.) **49**(1), 85 (2023). DOI:https://doi.org/10.56714/bjrs.49.1.8

A B S T R A C T

The purpose of a secure e-learning system based on cloud computing is to allow instructors and students to access their accounts at any time and from anywhere. These types of systems work to ensure that their users (instructors and students) are truly enrolled in the school or institute to prevent unauthorized users from accessing the resources and components of the system. Furthermore, the traditional authentication techniques used in the majority of educational systems suffer from several issues, such as cyber security attacks and weak management of resources. So, some students could be eager to take advantage of such a system's flaw in an effort to cheat. User authentication and end-user monitoring are more difficult in this situation. Multifactor adaptive authentication techniques are used to implement a system with simultaneous authentication. The proposed scheme system offers an effective, affordable, and human intervention-adaptive authentication and monitoring solution for e-learning environments. Additionally, our work can resist cyber security and contains some good metrics like mutual authentication, user anomalies, and others. In this paper, the proposed scheme system uses a two-factor authentication system based on Asymmetric Scalar Product Preserving Encryption (APSE) and fingerprint biometrics for managing and generating a user's account in a secure way. Our work also achieves a good balance between performance and security complexity compared to the state-of-the-art. So, we achieve good results for 1.69 ms for computation and 1280 bits for communication.

1. Introduction

E-learning environments based on the Internet are becoming increasingly popular as a result of the rapid improvements in communications and information technologies. The learning process is

*Corresponding author email : ali.yassin@uobasrah.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq

concentrated on traditional methods in our educational institutions, where the teacher considers books and whiteboards to be the only trustworthy sources of knowledge and is more concerned. Moreover, the interest in the theoretical side is more acceptable than the application side. When e-learning becomes an important part of our educational lives, utilizing state-of-the-art techniques for information integration, can be connecting information and sharing files between teachers and students, regardless of place or time [1]. Google, which provides the G-suite applications and the Google Classroom platform, is one of the best companies for providing the software and electronic services that educators and students needed. These systems include a variety of features, including the ability to send files and information between the teacher and the student quickly, efficiently, and securely by taking advantage of cloud computing services, especially in the educational sector [2]. At the same time, the Google Classroom suffers from several issues, such as hard-to-handle accounts, the management of many activities, and security issues that take first place in Google applications. The infrastructure for the Google Cloud's shared responsibility model, as a service (IaaS) layer where only the hardware, storage, and network are the provider's responsibility, up to software as a service (SaaS) where almost everything except the content and its access is up to the provider. Platform as a service (PaaS) layers like GKE. [3]. Cloud computing is a cutting-edge concept in the vast field of information technology, which offers a variety of services that work in many different ways. Due to cloud computing involves the storage of data on faraway servers; unauthorized access to such sensitive information becomes a significant risk. Without reliable security safeguards and flexibility, the benefits of cloud computing lose their legitimacy [4].

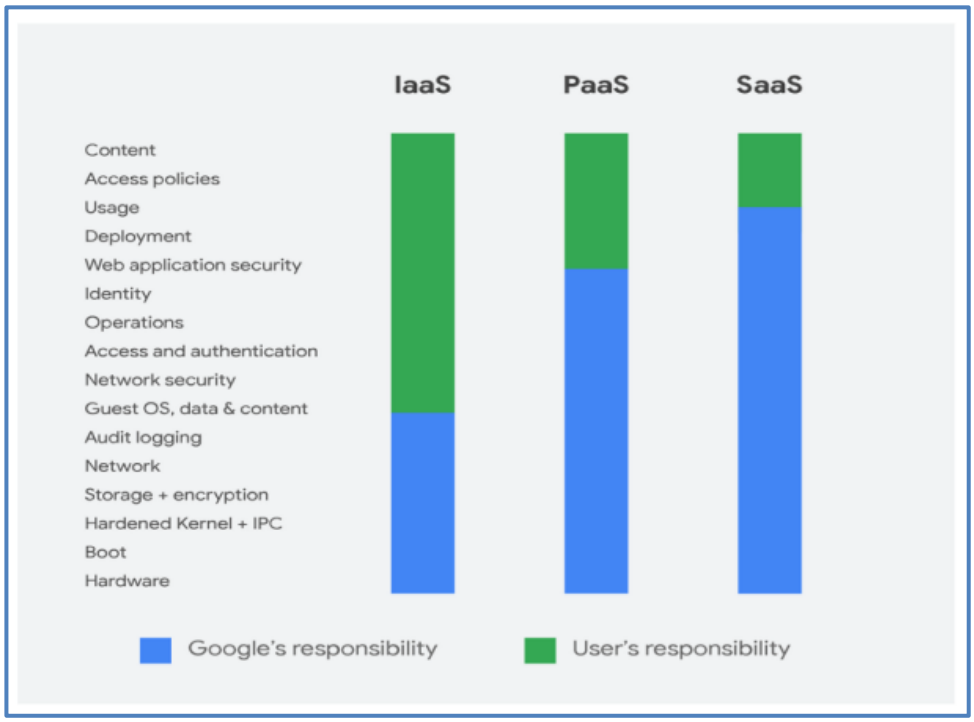


Fig. 1. Explains challenges faced google classroom [3]

Authentication is the key component of cloud computing security, because of this; only authorized users should be able to access the stored data [8]. Although text-based password scheme is the most applied authentication systems popular, they have a number of security flaws. These flaws demonstrate that people have trouble remembering lengthy or complex passwords, and that relying on short, basic passwords users at risk for security breaches [9].Dictionary and brute-force attacks have harmed passwords. The only characters that can be used as passwords are those found on keyboards. As a result, an attacker may try every combination until they find the right password; this kind of assault is known as a brute-force attack. Additionally, the majority of users choose straightforward passwords like their name, phone number, or favorite game. These concepts are

simple to remember. As a result, by creating a database of important terms, adversaries can launch a dictionary attack against the system. Password-based authentication is still plagued by malicious attacks like the Man-in-the-Middle (MITM) attack and replay attack [10].Personal physiological processes have developed as an effective way of addressing the aforementioned concerns, and are now used in many parts of daily life, such as financial security and verification [11].The term biometric operator refers to the method of identifying a person using specific physiological qualities, such as facial recognition, fingerprints, and iris. The most common biometric is still fingerprints [12, 13].There is a variety of security issues that can affect educational systems, including, data breaches educational systems often contain sensitive information, such as student records, grades, and financial data. If this information is not properly protected, it can be vulnerable to data breaches or unauthorized access. Security and privacy, The issue with system security and privacy, data transmission from the personal device to the authenticated server faced different types of attacks, including replay attacks, MITM attacks, and others. Additionally, there is a chance that the teacher's and student's privacy will be violated.However, biometrics is not the best option for the cloud environment because they call for specialized and expensive equipment, such as a fingerprint scanner, which raises the cost and causes problems when combined with the cloud computing environment. The method will also run slowly when numerous clients are being confirmed at once.Cloud authentication concepts work better with two-factor authentication (2FA). A user enters his login and password on the cloud server to authenticate. The cloud server asks the user to provide a second factor after checking the user's login and password against its database [14].

In this research, we offer an effective and safe password-based two-factor mutual authentication technique that makes use of feature extraction from the user's fingerprint and asymmetric scalar product-preserving encryption (ASPE).

This work contributes to the literature by offering an effective and safe password-based two-factor mutual authentication system, Using the proposed scheme system uses technology to enhance security, such as using the user's fingerprint (feature extraction) and asymmetric scalar product-preserving encryption (ASPE) to secure access to resources and systems. Furthermore, the proposed scheme system designing an educational system that can manage and control in a safe manner and build an integrated structure belonging to the academic institution without the need to take a ready-made structure such as google classroom, and G-suite applications. So, our work has the flexibility to done with the requirements or period conditions of the education ministry because it works in an open code environment. It can also be used as an applied system to work in all regions of Iraq. Additionally, it manages data security and can withstand attacks such as Insider attacks, reply attacks, MITM attacks, and other attacks. The system's proposed scheme system is built on smart-factor authentication and contains strong features including mutual authentication, anomaly, and forward secrecy, supports users' identity anonymity. Comparing our work to the state-of-the-art, we also manage to strike a good balance between performance and security complexity. The rest of this paper is organized as follows: In Section 2, we provide related work. In Section 3, we present primitive tools. In Section 4, we provide the proposed scheme system. Section 5, presents Security analyses and a discussion on possible attacks. Section 6, gives our conclusions.

2. Related Work

Users may want to protect their privacy and hide their true identities when using sensitive data. As a result, researchers have recently shown a lot of interest in this topic. The incorporation of biometric technologies into educational systems is motivated by various use cases. Several studies on the same topic are examined in this section. We give a summary of the most pertinent works on the application of biometric technologies in educational systems

In 2016, Alsadoon et al. [15] proposed a scheme for biometric authentication in online learning that was made for both teachers and students. Creating a sophisticated and more secure method of user authentication for E-learning systems is made by combining biometrics. Unfortunately, this project is not free of restrictions one of the main constraints is the amount of time available for research has

been. Additionally, this project must take into account learners with special requirements (such as those who are blind or deaf) and how to validate their access to e-learning portals.

In 2017, Al shehri et al. [16] a safe mobile learning system built on a cloud infrastructure. A secure mobile learning framework was developed to ensure mutual authentication and end-to-end security. Although the integrity and privacy of this method were good, its implementation in the simulated environment was unsuccessful.

In 2020, Ennouamani et al. [17] proposed a context-aware mobile learning system that suggests, for effective learning for each student, a dynamic mobile adaptable learning content and format (D-MALCOF). Additionally, this strategy received supportive comments and favorable impressions. However, this strategy failed short in the activity of collecting feedback activity.

In 2020, Alin et al. [18] proposed a method based on the dynamics of real-time typing as a biometric mechanism that prevents fraudulent identification and incorrect authentication. The vulnerability is observed, this authentication method faces criticism because students can only be identified if they have intense activity on the platform; this operation is required for the student profile to be created in the database.

In 2021, Labayen et al. [19] propose a framework based on the authentication of different biometric technologies and an automated proctoring system (systems work, now as well as AI algorithms). Unless taking into account, this framework needs more robust biometric models for a quality warrant by accounting for variations in face posture, light, and noise conditions.

In 2022, Dr. Kasumu et al. [20] provided a descriptive survey study to investigate the utilization of learning management systems in education. The study's conclusions imply that employing a learning management system can help students keep their independence, interest, and drive. But in order to create lessons that are appropriate for their students' needs, teachers should make sure to frequently use learning management systems. However, the security issue affecting data transmission between users in the e-learning system was not examined in this study.

In this research, we suggest a reliable verification method based on biometrics (fingerprints) and the SHA-512 function of asymmetric scalar-product-preserving encryption (ASPE). This system has several advantages, including smart-2-factor authentication, defines against user identity-relate abnormalities, and resistance to well-known threats including impersonation, phishing, and replay, MITM, and insider attacks. Scyther and cryptography proofs are used to independently and formally evaluate the proposed scheme system in terms of computation/communication costs and security analyses.Table1. Compares security attributes based on the primary security features as follows:
C1: Secure mutual authentication, C2: Perfect forward secrecy, C3: Supports users' identity anonymity, C4: Resists insider attacks, C5: Resists MITM attacks, C6: Resists replay attacks, C7: Resists phishing attacks, C8: Login and authentication phase efficiency, C9: Formal verification with Scyther.

Table 1. Comparison of authentication schemes.

Scheme	C1	C2	C3	C4	C5	C6	C7	C8	C9
Our	Y	Y	Y	Y	Y	Y	Y	Y	Y
[15]	Y	Y	N	N	N	Y	Y	Y	N
[16]	N	Y	Y	N	Y	N	N	Y	N
[17]	N	N	Y	N	N	Y	N	N	N
[18]	N	Y	N	Y	N	Y	Y	Y	N
[19]	Y	N	N	Y	N	N	Y	N	N
[20]	N	N	Y	N	N	N	N	Y	N

3. Primitive Tools

3.1. Asymmetric Scalar-Product-Preserving Encryption ASPE

One of the most effective encryption strategies is ASPE [21]. The adversary can access point-to-point encrypted data. ASPE overcomes this limitation by providing an encryption function that forbids the disclosure of actual distance information.

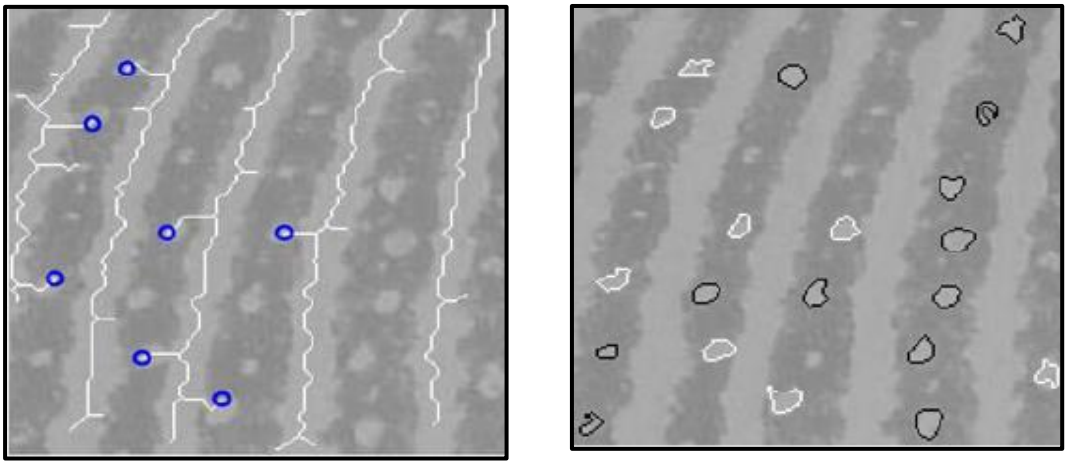
1. CSP sets up $n = pq$, where p , q are two large primes, and he selects (M_i , M_i' , $K_i \in Z_n^*$) .
2. CSP uses a cryptographic hash function $H(.)$, a symmetric key encryption $Enc(.)$ and then computes important information($p_i\ id_i , W_i$) , where $p_i = H\ (Un_i , K_i$) , $W_i = PW_i^T M_i M_i^{-1}\ PW_i$
3. $PW_i = M_i^{-1} PW_i$ .Where T transposes function
4. CSP selects a secret number S_i between [1 - ($n - 1$)] as user's private key and computes
5. $PK_i = S_i^{p_i}\ mod\ n$ as user's public key. The public system parameters contain (($P_s =$ ($K_i , n , h(.), Enc(), p_i , id_i$)).
6. $CSP \rightarrow U_i :$ (P_s , M_i, S_i , K_i).
7. $CSP \rightarrow AS :$ (P_s , PW_i , W_i , PK_i).

The following mathematical proof demonstrates how CSP ensures from matching values of $Y'_{ADM}\ and\ Y''_{ADM}$: $Y'_{ADM} = (\ Dec_{K_{ADM}}\ (E_{ADM2}\ ))^{p_{ADM}} = (Y_{ADM}\ )^{p_{ADM}}$ $(rS_{ADM}^c\ )^{p_{ADM}} = r^{p_{ADM}}\ S_{ADM}^{cp_{ADM}} = r^{p_{ADM}}\ \left(S_{ADM}^{p_{ADM}}\right)^c = Z_{ADM}\ PK_{ADM}^c = Y''_{ADM}$.

By providing an encryption option that inhibits the revelation of actual distance information, you may help stop data leakage.

3.2. SHA-512

Is a hashing algorithm that separates the data into three components: the original message, the padding bits, and the size of the original message. Given that the prepared message will be processed as 1024-bit blocks, the sum of the sizes of all three components should be a multiple of 1024. The way message processing works is as follows: structured input typically splits into blocks, like words, every 1024 bits because it can't completely divide without a remnant [22].Our scheme uses a hashing algorithm to check passwords because the hash values can be saved and used to compare user input to the hash values to see if it is correct or not. This means that users don't have to write down their passwords.



(a) (b)

Fig.2. (a) Detection of open pores and valleys the skeleton of valleys, represented by a white outline (b) Shows the pore localization algorithm's results. In black, closed pores were discovered. Open pores could be seen in white.

3.3. Scyther

Is a tool for assessing the security and weaknesses of schemes The tool's operation is explained in two steps. Scyther promises to complete the initial phase while allowing an infinite number of sessions to confirm protocol soundness. Creating the evidence tree is an option (using the backend). By providing attack behavior classifications, the second phase, Scyther, facilitates graphical user interface analysis [23]. The Security Protocol Description Language (SPDL), which defines protocols and schemes and enables phrases for encryption, decryption, and signature as well as for sending and receiving events, should be used to represent any proposed scheme system.

3.4. Features Extraction of Fingerprint

In order to locate the sweat pores, we first use a local threshold method to binaries the original grayscale image [24]. The sweat pores (or rather, their imprints) can generally be divided into two categories: closed and open. At first, we extract the pores that are completely surrounded by the ridge. These are the closed pores. They show a hole in a ridge in the binary image. We concentrate on regions of white pixels completely encircled by black pixels. We specify the upper (T_{max}) and lower (T_{min}) thresholds. If the surface of a suspect pore is below T_{min} or above T_{max} , it is eliminated. Smaller-sized objects are eliminated because they are typically noise artifacts, while larger-sized objects are eliminated because they are less likely to have level 3 characteristics. Empirically, we selected the T_{min} and T_{max} values. Typically, the ridge does not completely encompass a large number of pores (the open pores). They develop in the ridge like a hook. We first skeletonize the valleys of the original binaries image in order to locate them. The spurs then start to show up where the pores were. We calculate the separation between each spur's terminus and the valley skeleton. If this distance is great enough and there are enough white pixels around the spur location, we consider the spur's end to be the location of a pore (Figure 2). The total outcome of the pore detection is shown in Figure 3. The set of level 3 features that we keep are the pore coordinates [24].

Table 2. Notations of our proposed scheme system

Symbol	Description
ADM	Main Administrator
CSP	Cloud Service Provider
UN_i	Username
PW_i	Password
$h(.)$	hash function
PN	Phone number
S_K	Private Key
P_K	Public key
Z	Set of Integer Number
R_S	Resources Server
ECT_i	Examination Committee Teacher
PT_i	Position Teacher
$FP3_i$	level 3-features of the user's fingerprint extraction
K_i	The authenticated session key between each user and server
id_i	The anonymity of user's identity has been supported from to in registration phase CSP to U_i
p_i	Password anonymity has been provided from to in registration phase CSP to U_i
AS	Authentication Server

4. Proposed Scheme

In this section, we provide a good authentication and privacy protection applied on the educational system. Our proposed scheme system is involved three components: Cloud Service Provider (CSP), user set ($U_1, U_2, \dots, U_n$), and Authentication Server (AS). There are four phases make up our work: registration, login, authentication, and education. We are explained the proposed scheme system in more details as follows:

4.1. Registration Phase

During the registration process, a user sends the hash of his username, password, and fingerprint by secure channel to the data owner inside the cloud server, along with. The data owner returns the user's credentials, which are keys created from the user's username, password, and features' fingerprint extraction. During registration, the user U_i sends his Username ($UN_{U_i} = h(UN_{U_i})$), Password ($PW_{U_i} = h(PW_{U_i})$), Phone number (PN_{U_i}), and Fingerprint ($FP3_{U_i}$) to CSP that saves them in his database. After that, CSP forwards theU_i's requesting to AS while his information has been corrected based on rules of the proposed scheme system (See Table 2). The h (.) refers to the cryptographic hash function (SHA-512), and $FP3_i$ refers to the level 3-features of the user's fingerprint extraction. In this phase, we use ASPE to generate the main keys and data encryption. The following steps describe the mechanism for this phase (see fig.3):

1. $U_i \rightarrow CSP$: ($UN_{U_i}, PW_{U_i}, PN_{U_i}, FP3_{U_i}$).
2. CSP → sets up the main keys uses ASPE .
3. CSP sets up $n = pq$, where p , q are two large primes, and he selects (M_{U_i} , $M_{U_i}^{-1}$, $K_{U_i} \in Z_n^*$) .
4. CSP uses a cryptographic hash function h(.) , a symmetric key encryption Enc(.) and then computes important information(p_{U_i} , id_{U_i} , W_{U_i}),where $p_{U_i} = h(PW_{U_i}, K_{U_i})$, $W_{U_i} = PW_{U_i}^T M_{U_i} M_{U_i}^{-1} PW_{U_i}$,$PW_{U_i} = M_{U_i}^{-1} PW_{U_i}$, $id_{U_i} = h(UN_{U_i}, K_{U_i})$. Where T transpose function
5. CSP selects a secret number S_{ADM} between [1 - (n − 1)] as user's private key and computes
6. $V_{U_i} = S_{U_i}^{p_{U_i}} \bmod n$ as user's public key. The public system parameters contain ($(PK = (K_{U_i}, n, h(.), Enc(), p_{U_i}, id_{U_i}))$.
7. CSP → U_i : $(PK, M_{U_i}, S_{U_i}, K_{U_i})$.
8. CSP → AS : $(PK, PW_{U_i}, W_{U_i}, V_{U_i})$.

4.2 Login Phase

During the login process, the user inserts a username, enters a password, and his fingerprint to utilize educational system resources and services based on the user's roles.

In this phase the U_i sends a request to the CSP during the login phase for mutual authentication, which is done as follows:

1. U_i : Choose a random number r_i , he computes , $Un'_{U_i} = h(Un_{U_i}) \oplus r_i$, $PW'_{U_i} = h(PW_{U_i}) \oplus r_i$.
2. $U_i \rightarrow CSP$: $(Un'_{U_i}, PW'_{U_i}, r_i)$ as a first factor . CSP: Checks the UN'_{U_i} with $h(UN_{U_i})$ in his database. If it does not exist, he terminates this phase. Otherwise, CSP computes $r_i'' = h(PW_{U_i}) \oplus h(UN_{U_i}) \oplus r_i'$.
3. CSP: Computes $PW''_{U_i} = h(PW_{U_i}) \oplus r_i''$ and compares PW''_{U_i} with PW'_{U_i}, if holds, stop. As depicted in the figure(see fig.4)

4.3 Authentication Phase

The user sends his initial factor to the cloud server during the login phases, verifying its legitimacy. The cloud server then sends the user a request asking him to provide the second factor. The user will then supply his second factor to the cloud server after having his identity validated by the cloud server first. When a user's second factor is accepted by a cloud server,

1. finally granted access to that server's resources. Upon receiving credential information fromU_i, CSP performs the following operations:
2. CSP sends verification cod (V_i) as SMS to the use's phone number.
3. U_i computes $V_i' = h(V_i) \oplus r_i$ and sends V_i' to CSP.
4. CSP computes $V_i'' = h(V_i) \oplus r_i'$ and compares $V_i''$with V_i', if holds, CSP Requesting enter the $FP3_{ADM}$ to U_i .
5. ADM computes $FP3'_{U_i} = h(FP3_{U_i}) \oplus r_i$ and sends to the CSP , Upon receiving $FP3_i'$ from U_i, CSP computes $FP3''_{U_i} = h(FP3'_{U_i}) \oplus r_i''$ and compares $FP3''_{U_i}$ with $FP3'_{U_i}$. If holds, CSP compares Un'_{U_i} with $h(Y_{U_i}, r_i)$. If these values are congruent, then checks whether PW'_{U_i} and $h(X_{U_i}, r_i)$. If so, CSP will provide U_i by $c \in Z_n^*$,this is generated at random each time U_i tries to log in. If not, CSP is aware that the user is not authorized. The secret keyK_{U_i}, which is generated for each user's login request, is also used by CSP to encrypt c. So, $K_{U_i} = |r_i - K_{U_i}|$, where ‖ is absolute function .
6. CSP $\rightarrow U_i : E'_{K_{U_i}}(c)$.
7. U_i : Computes $K_{U_i} = |r_i - K_{U_i}|$, $c = Dec_{K_{U_i}}(E'_{K_{U_i}})$,and computes the response $Y_{U_i} = r_i S_{U_i}^c$, $E_{U_i1} = E_T(PW_{U_i}^T, M_i) = PW_{U_i}^T M_{U_i}$, $E_{U_i2} = Enc_{K_{U_i}}(Y_{U_i})$ and $h_{U_i} = h(Y_{U_i}, c)$.
8. $U_i \rightarrow$ CSP : (E_{U_i1} , E_{U_i2} , h_{U_i}) as a second factor .
9. CSP upon receiving the information in the step 4 , performs the following steps :-

- CSP computes $W'_{U_i} = E_{U_i1} PW'_{U_i} = PW_{U_i}^T M_{U_i} M'_{U_i} PW_{U_i}$ to check whether W'_{U_i} equals the stored W_{U_i} . If so. CSP computes $Y'_{U_i} = \left(Dec_{K_{U_i}}(E_{U_i2}) \right)^{p_{U_i}}$, $Y'' = r_i' PK_{U_i}^c$.
- The CSP first checks whether $Y'_{U_i} = Y''_{U_i}$. If so, CSP checks whether $h'_{U_i} = h(Y'_{U_i}, c)$ equals h_{U_i} . If so, CSP ensures from authenticating of the user.

Once an U_i's legitimacy has been successfully verified, the U_i is regarded as a legitimate user and is permitted to utilize the services and resources offered by the educational system in accordance with their role, in the event that this is not the case, CSP ends the current phase.(See fig.5)

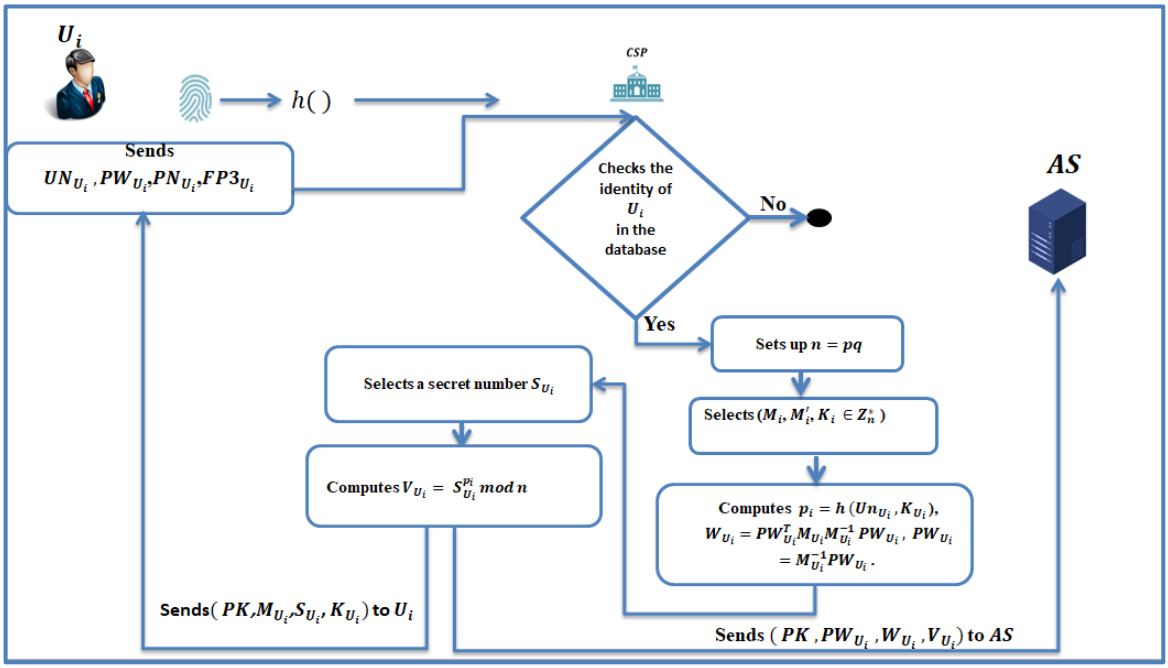


Fig.3. Show the user registration in the educational system

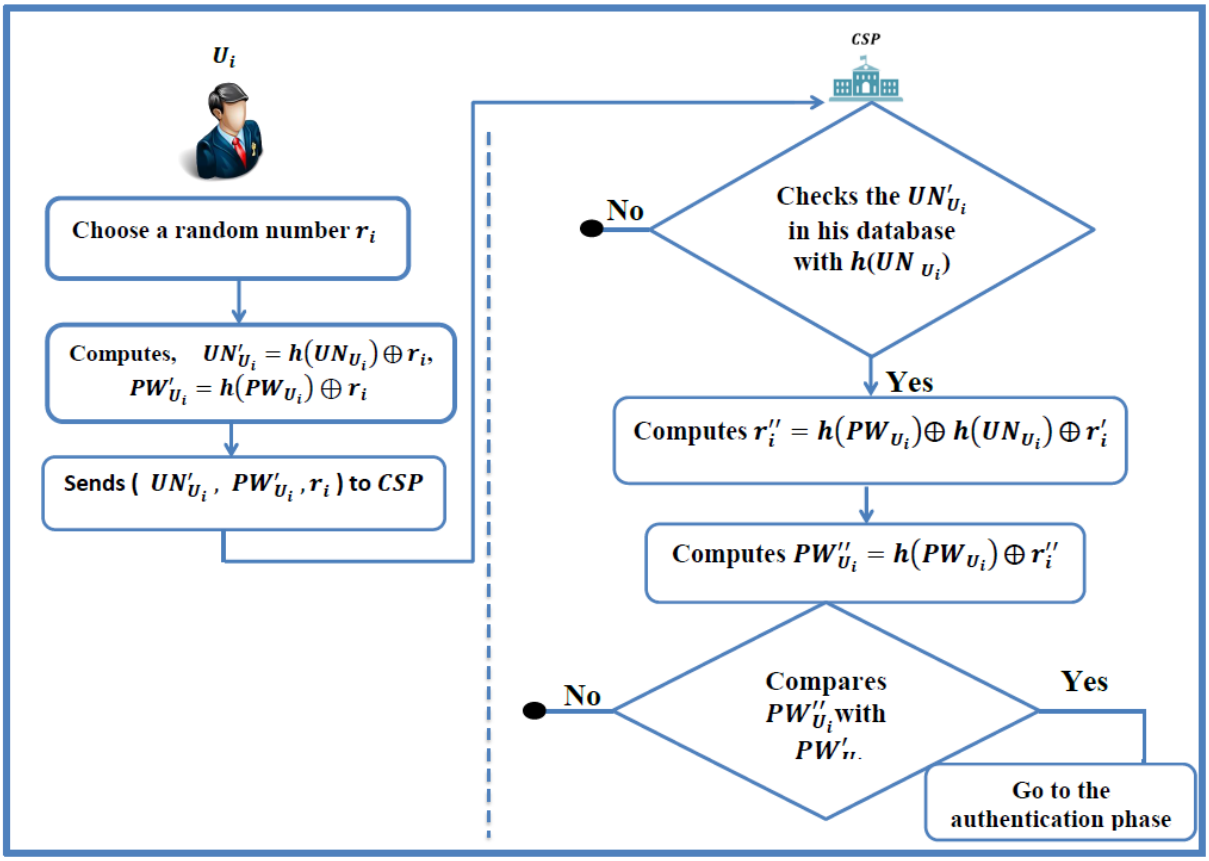


Fig.4. Illustrates user login in the educational system

4.4 Education phase

Role-based access control under the foundation of identity identification makes up the security framework of the educational administration system. Therefore, only users who successfully complete the authentication process can access the role privilege and the associated system resources. After successful authentication, the user gains access to their role and the authority that goes along with it. They can also request access to resources based on the privileges of this role. The Educational Administration System resources include both the numerous visible components of the system window, such as menus, buttons, etc. Table 3. Demonstrates the services the system offers customers in conformity with the rules.

Table 3. Demonstrates the services the educational system

No	Objects	Roles
1	Administrators	Read / Write of all objects system
2	Examination committee Teacher	Read / Write of all course
3	Position Teacher	Read / Write of his course
4	Normal Teacher	Read / Write of his classes
5	Students	Read only of his scores and View Schedule , download from subjects

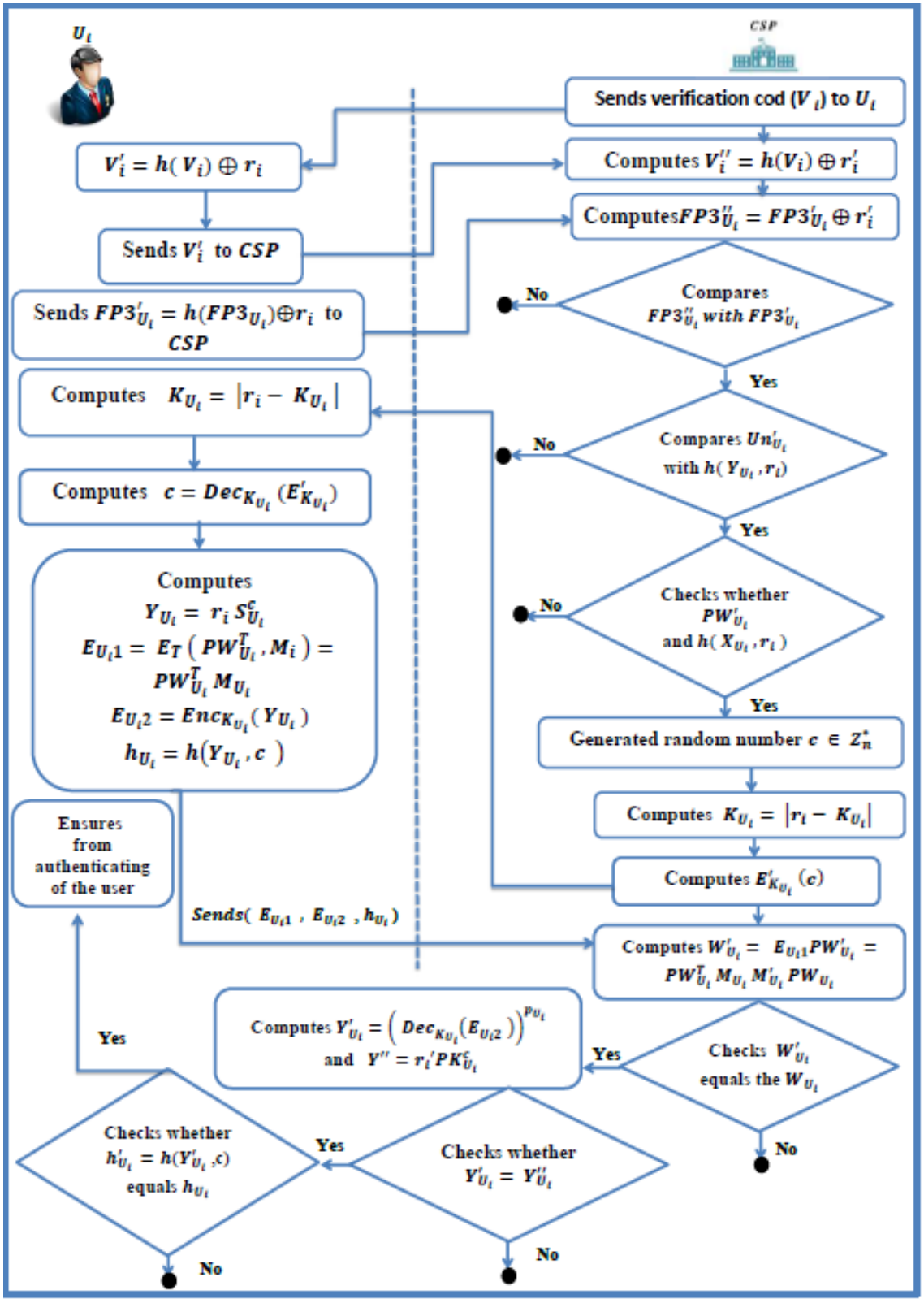


Fig.5. Illustrates user authentications in the educational system

5. Security Analysis

In this section, we outline our proposed scheme's security analysis. We will discuss how our system is safe against well-known threats like MITM, replay, and insider attacks. Additionally, there are several advantages to our suggested approach, such as user anonymity, mutual authentication, and session key agreement.

5.1. Formal Security Analysis with Scyther tool

Using the Scyther tool, we conducted an analysis showing that the proposed scheme can achieve greater privacy and security than the alternatives. The GUI is made for anyone who wants to examine or comprehend a protocol. We operate the proposed scheme without utilizing the security features employed by the same conventional solutions.

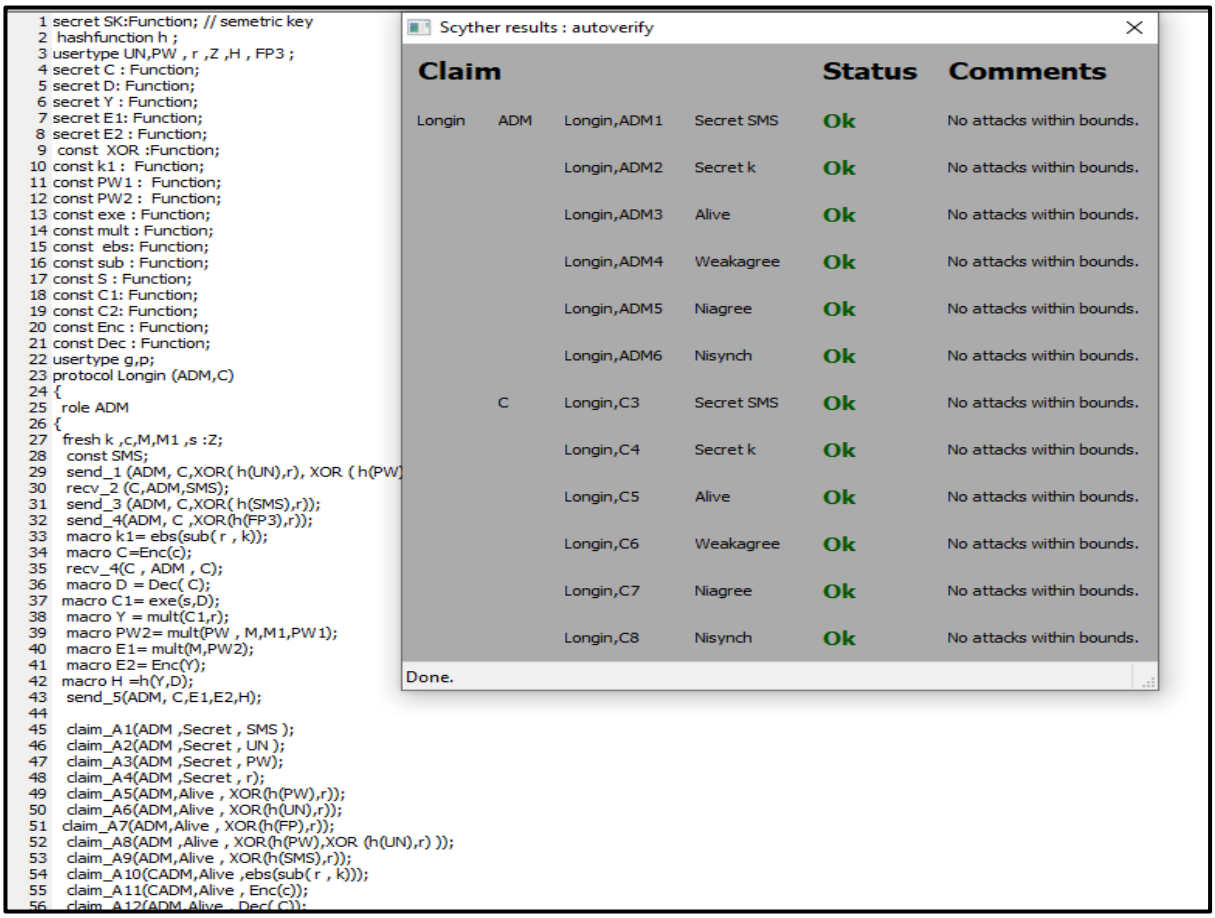


Fig. 6. Illustrates the results of the system scheme verification can be attacked

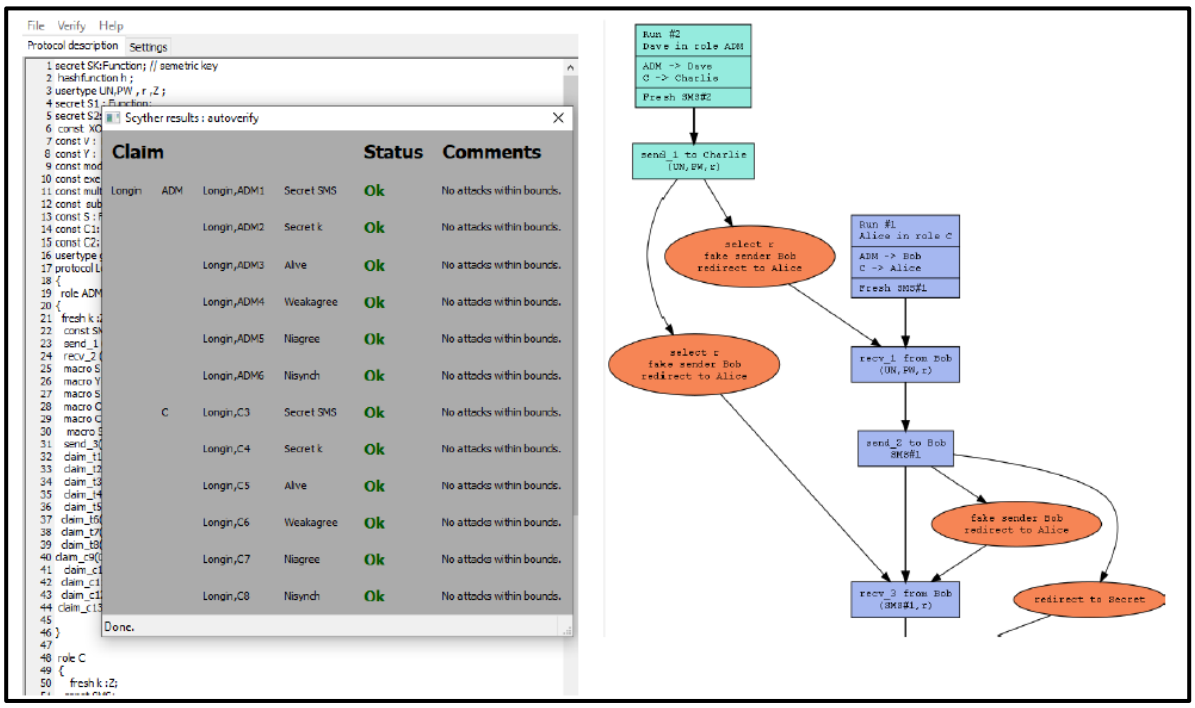


Fig.7. Illustrates the results of the system scheme verification cannot be attacked

5.2. Informal Analysis

- **Proposition1. Our proposed scheme can provide secure mutual authentication.**

Proof. The user and the server can authenticate one another thanks to a mutual authentication mechanism. In our work, the two factors (Un'_{U_i}, PW'_{U_i}, r_i) and ($E_{U_{i1}}$, $E_{U_{i2}}$, h_{U_i}) are used to authenticate user (for example) to CSP. An enemy is unable to produce ($E_{U_{i1}}$, $E_{U_{i2}}$, h_{U_i}, Z_{U_i}, S_{U_i}, W_{U_i}). These are unaffordability of (h_{U_i}, Z_{U_i}, S_{U_i}, W_{U_i}). Additionally, an adversary cannot decode E'_{U_i} in order to access c, which should be decrypted using a shared key K_{U_i}. So, K_{U_i} generates once for each user's login request, Furthermore dependent on the feature extraction of the user's fingerprint $FP3_{U_i}$, which was made available to the actual user and CSP via the secure channel by the database. As a result, our proposed scheme successfully accomplishes mutual authentication between two entities.

- **Proposition2. Our proposed scheme can present user anonymity**

Proof. Since the major parameters (h_{U_i}, Z_{U_i}, K_{U_i}) are altered with each user's login request and the second factor is encrypted with K_{U_i} which is anonymous to the adversary. Also, r_i generates once for each user's login request. So, it has been encrypted by shared key K_{U_i} which is existed just in U_i and CSP, he will be unable to determine the user's identity from the first factor (Un'_{U_i}, PW'_{U_i}, r_i) and second factor ($E_{U_{i1}}$, $E_{U_{i2}}$, h_{U_i}). In contrast, it is impossible due to the one-way cryptographic hash function characteristic and random values (h_{U_i}, Z_{U_i}, S_{U_i}, W_{U_i}, Un'_{U_i}, PW'_{U_i}). As a result, the approach we've suggested can support user anonymity.

- **Proposition3. Our proposed scheme can forward secrecy**

Proof. Even if the secret key is revealed or leaked, the password is still protected by our suggested system. If the adversary discloses the secret keyK_i, the system's authentication is not impressed, and he is unable to use this key during the subsequent login phase. In addition, it is very difficult for an adversary to extract the secret key based on Z_i, which necessitates that they have knowledge of(p_i , r_i), as well as the initial K_i that is supported from CSP to U_i during the registration step. As a result, our work upholds the forward secrecy.

- **Proposition4. Our proposed scheme can supply security of the password.**

Proof. The authentication messages (Un'_{U_i}, PW'_{U_i}, Z_i) and (E_{U_i1} , E_{U_i2}, h_{U_i}) in the suggested system only contain data pertaining to Z_i and h_i. They don't contain any data regarding the password. As a result, the values (Z_i , h_i) of the mutual authentication stage are generated at login time for each user, indicating that the authentication and password messages are entirely unique. The system can be protected from offline password dictionary searches using this isolation. Additionally, we observe the use of the password for anonymous mutual authentication. Our effort thus helps the password's security.

- **Proposition5. The proposed scheme can withstand MITM attack.**

Proof. In this type of attack, an adversary is intended to be able to intercept messages transferred between users and the server. When the user signs out of the server, he then utilizes this message[25]. The factors are delivered to the service provider securely encrypted in our suggested approach. The sensitive data (Z_{U_i} , id_{U_i} , p_{U_i}, Y_{U_i} , E_{U_i1} , E_{U_i2}, h_{U_i}), created by U_i as a login request (second factor) to CSP is used to generate the random value r_i. As soon as U_i logs out of the server, this private data are useless. As a result, an opponent who discovers communication between U_i and SP can only learn the value of r_i, which is utilized once, and cannot compute Z_{U_i}. However, an adversary cannot compute (Y'_{U_i} , c) to estimate a new (h_{U_i} , E_{U_i1}) for impersonating the user after U_i signs out of the server.

- **Proposition6. The proposed scheme can withstand replay attack.**

Proof. Our proposed scheme substitutes a random Z_{U_i} for the timestamp in the user's (U_i) login request message. Even if the opponent discovers the previous secret, say (Un'_{U_i} , PW'_{U_i}), theoretically he is still unable to launch a replay attack during the subsequent authentication session. As a result, an enemy is unable to acquire (p_{U_i} , S_{U_i} , M_{U_i} , V_{U_i} , r_i) for producing both elements. It is obvious that the enemy is unable to use the repeat assault

- **Proposition7. The proposed scheme can withstand insider attack.**

Proof. In our approach, instead of submitting (U_i , PW_i) as in other schemes, CSP must submit (U'_i , PW'_i) when U_i desires to register with a service provider for remote access services. The service provider is unable to determine the user's identification in U_i from id_i or the user's password ipw from ip. Additionally, an enemy is unable to acquire $PW_i^T M_i$ andh_i. As a result, the suggested system can withstand an insider attack.

5.3. Performance Analysis

In this section, we contrast our protocol with those in [29, 30, 31, 32] in order to understand how it operates in terms of computation and communication overheads as opposed to spending a lot of time and money on data collection.

5.3.1. Computational Cost

The suggested protocol consists of four phases: registration phase, login phase, authentication phase, and educational phase. Since the authentication phase of the proposed system is the one that is used the most, we shall concentrate on its computation requirements.In order computation analysis we define the computational requirements of a mathematical operation as T_m, a one-way hash function as T_h, symmetric key encryption, and decryption as T_{sym}, but we do not take into account the overhead of the exclusive-or operations as $T_{\oplus}$, elliptic curve cryptosystem T_{ecc} ,Bilinear pairing operation T_{bp}, random number generatorT_{rng}, point multiplication T_{pm} [26][27], which requires a relatively low overhead than any other operations. Table 4 shows a comparison of communication cost protocols[29, 30, 31, 32].Furthermore, compared to prior efforts, our scheme achieves a solid trade-off between performance and security complexity, and the proposed scheme is the most efficient. Additionally, since asymmetric encryption produces the best results and since the data transferred between a mobile device and a server is crucial, it requires good efficacy and confidentiality.

5.3.2. Communication Cost

Table 6 provides information on communication expenses in detail for our communication analysis. For the purpose of getting cumulative communication costs, we rely on the bandwidth values [33]. For the sake of comparison, they assumed that a cryptographic one-way hash function has an output size of 128 bits and that a user's identification is also 128 bits long. Finally, the sizes of the time stamps and random integers are equal at 64 bits, and symmetric key encryption is 256 bits. Table 5 compares the same methods in terms of their communication cost.

Table 4. Computation cost value

Operation	General Meaning	Time
T_m	Mathematical operation	0.005
T_h	One-way hash function	0.08
T_{sym}	A symmetric key encryption/decryption operation	0.14
$T_{\oplus}$	Exclusive OR operation	Negligible
T_{ecc}	Elliptic curve cryptosystem	4.31
T_{bp}	Bilinear pairing operation	14.48
T_{rng}	Random number generator	0.539
T_{pm}	Point multiplication	2.226

Table 5. Computation cost comparison result

Protocol	Verification's Time Complexity	Result
Proposed	$12\mathrm{T_h} + 8T_{\oplus} + 5\mathrm{T_{sym}} + 6\mathrm{T}_m +$	1.69
[29]	$9T_h + 2T_{bp} + 2T_{sym} + 5T_{ecc}$	51.51
[30]	$14T_h + 2T_{sym} + 4T_{ecc}$	18.64
[31]	$5T_h + 4T_{expo} + 2T_{rng}$	8.2459
[33]	$6T_h + 4T_{pm} + 1T_{rng}$	4.9561

Table 6. Comparing the cost of communication to other work

Protocol	Message length	Number of messages
Proposed	1280 bits	5 messages
[29]	1472 bits	2 messages
[30]	2528 bits	2 messages
[31]	1792 bits	4 messages
[33]	2304bits	5 messages

The result is dependent on the asymmetric encryption's ability to reduce the cost of messages exchanged (five messages) between the primary components. The cost is 1280 bits, the lowest among comparable systems.

6. Conclusion

The development of cloud computing technology and its widespread use made it possible to do away with all current methods of storing past data, which allowed users to store their digital files and made it possible for all data to be saved in a single cloud on the internet servers. In this article, we primarily concentrated on the usage of cloud computing in eLearning. Cloud computing has certain negatives, such as data and security concerns, access to the data, and infringing on rights to privacy, intellectual property, and data ownership. To process this important problem, we focus mainly on the infringing authentication issue by the proposed scheme to address password breach threats specific to a cloud environment. Through the use of a two-factor authentication system that depends on ASPE technology and level-3 feature extraction from the fingerprint. The proposed system operates in an open-code environment, is capable of managing data and controlling it securely, and is adaptable to the establishment's needs. Furthermore it runs without synchronized clocks between the service provider and user because we employ random numbers rather than timestamps to save software programs or data. The proposed scheme contains a number of components, including mutual authentication, anomaly, and forward secrecy, supports users' identity anonymity, and resistant's to all known malicious assaults, including replay attacks, MITM attacks, and other attacks.

References

[1] Montazer, G. Ali, Y. K. Al-Rikabi, International Conference on Web Research (ICWR), 34 (2021).

[2] Q. Alajmi, R. A. Arshah, A. Kamaludin, A. S. Sadiq, M. A. Al-Sharafi, Electr. Comput. Technol.**2018**(6),9(2017).
[3] https://cloud.google.com/blog/products/containers-kubernetes/exploring-container-security-the-shared-responsibility-model-in-gke-container-security-shared-responsibility-model-gke.
[4] Q. Alajmi, A. S. Sadiq, A. Kamaludin, M. A. Al-Sharafi, Adv. Sci. **24**(6), 4044 (2018).
[5] Z. A. Hussien, Z. A. Abduljabbar, M. A. Hussain, M. A. Al Sibahee, S. Lu, H. A. A. Al-Asadi. *CSAE*, 155(2019).
[6] M. A. Al Sibahee, S. Lu, Z. A. Abduljabbar, A. Ibrahim, Z. A. Hussien, K. A. Mutlaq, M. A. Hussain. *International Journal of Distributed Sensor Networks* **14**, 2 (2018).
[7] A. A.Yassin, Z. N. Hikmat, Z. A. Abduljabbar, H. Sh. Hashim. *International Journal of Engineering and Advanced Technology* **1**, 133 (2013).
[8] S. Subashini, V. Kavitha, Netw. Comput. Appl., **34**(1), 11(2011).
[9] M. Zhou, R. Zhang, W. Xie, W. Qian, A. Zhou, Conf. Semant. Knowl. Grid, 112(2010).
[10] M. Abdalla, D. Pointcheval, Notes Comput. Sci. **3376**(1), 208(2005).
[11] Kamesh, N. Sakthi Priya, Secur. Commun. Networks, **5**,(1), 437(2012).
[12] K. Upendra, S. Singh, V. Kumar, H. K. Verma, Med. Eng. Technol., **31**(1), 45(2007).
[13]M. Abdalla, M. Izabach, D. Pointcheval, International Conference, CANS **2008**(7), 148(2008).
[14]A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, D. Zou, International Parallel and Distributed Processing Symposium Workshops, 1217(2016).
[15]A. Alsadoon, L. Pham, A. Elchouemi, International Conference on Advances in Electrical, 16(2017).
[16]A. Majmaah, International Journal of Advanced Computer Science and Applications, **8**(10), 11(2017).
[17]S. Ennouamani, Z. Mahani, L. Akharraz, Education and Information Technologies, (2020).
[18]A. Zamfiroiu, D. Constantinescu, M. Zurini, C. Toma, Appl. Sci., **10**(21), 13(2020).
[19]M. Labayen, R. Vea, J. Florez, N. Aginako, B. Sierra, IEEE Access, **9**, 72411(2021).
[20]D. K. R. Oluwayimika, Trendy Res. Eng. Technol, **7**(1), 23(2022).
[21]A. Abdellaoui, Y. I. Khamlichi, H. Chaoui, Procedia Comput. Sci, **85**(9), 300(2016).
[22]M. Sumagita, I. Riadi, Cyber-Security Digit. Forensics, **7**(4), 381(2018).
[23] C. J. F. Cremers, International Conference, **7**(20), 418(2008).
[24]K. Kryszczuk, A. Drygajlo, P. Morier, Signal Pro-cessing Institute,(5), 88(2004).
[25]H. I. Nasser, M. A. Hussain. G. Honi, Comput. Sci, **30**(3), 628(2022).
[26]S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, A. Jamalipour, IEEE Commun. Surv. Tutorials,**16**(3),1686(2014) .
[27]S. Majumder, T. Mondal, M. J. Deen, Sensors, **17**(1), 130(2017).
[28]H. H. Kilinc, T. Yanik, IEEE Commun. Surv. Tutorials, **16**(2), 1023(2014).
[29]S. Khatoon, S. M. M. Rahman, M. Alrubaian, A. Alamri, IEEE Access, **7**, 47971(2019).
[30]A. Ostad-Sharif, D. Abbasinezhad-Mood, M. Nikooghadam, Commun. Syst., **32**(5), 23(2019).
[31]C. C. Yang, R. C. Wang, W. T. Liu, Comput. Secur, **24**(5), 386(2005).
[32 L. Wu, Y. Zhang, F. Wang, Comput. Stand. Interfaces, **31**(2), 291(2009).
[33]E. J. Yoon, K. Y. Yoo, Notes Comput. Sci, **4**(3), 507(2006).

Journal of Basrah Researches (Sciences) **49**(1), 85 (2023)
DOI: https://doi.org/10.56714/bjrs.49.1.8

التحكم في الوصول المستند إلى الدور باستخدام المقاييس الحيوية و التوقيع الرقمي في النظام التعليمي

مها كاظم خابر[1]، علي عادل ياسين[1,2] *، زيد أمين عبد الجبار [1,2,3]، Songfeng Lu [3,4]

[1]قسم علوم الحاسوب ، كلية التربية للعلوم الصرفة ، جامعة البصرة ، البصرة، العراق.
[2] قسم هندسة الحاسوب التقنية ، كلية الكنوز الجامعة ، البصرة، العراق.
[3] كلية العلوم والهندسة الالكترونية، جامعة هواتشونغ للعلوم والتكنولوجيا، ووهان، الصين.
[4] معهد بحوث جامعة شينزين هواتشونغ للعلوم والتكنولوجيا، شنتشن ، الصين.

معلومات البحث

الاستلام 08 نيسان 2023
القبول 28 نيسان 2023
النشر 30 حزيران 2023

الكلمات المفتاحية

التعلم الإلكتروني ، والقياسات الحيوية لبصمات الأصابع ، وتقنيات المصادقة التكيفية متعددة العوامل ، والتشفير غير المتماثل للحفاظ على المنتجات العددية.

Citation: M.K. Kabier et al., J. Basrah Res. (Sci.) **49**(1), 85 (2023).
DOI:https://doi.org/10.56714/bjrs.49.1.8

الملخص

الغرض من نظام التعلم الإلكتروني الآمن القائم على الحوسبة السحابية هو السماح للمدرسين والطلاب بالوصول إلى حساباتهم في أي وقت ومن أي مكان. تعمل هذه الأنواع من الأنظمة على ضمان أن المستخدمين (المدرسين والطلاب) مسجلين بالفعل في المدرسة أو المعهد لمنع المستخدمين غير المصرح لهم من الوصول إلى موارد ومكونات النظام. علاوة على ذلك ، فإن تقنيات المصادقة التقليدية المستخدمة في غالبية الأنظمة التعليمية تعاني من العديد من المشكلات, مثل هجمات الأمن السيبراني وضعف إدارة الموارد. لذلك ، قد يكون بعض الطلاب متحمسين للاستفادة من عيب مثل هذا النظام في محاولة للغش. تعتبر مصادقة المستخدم ومراقبة المستخدم النهائي أكثر صعوبة في هذه الحالة. تُستخدم تقنيات المصادقة التكيفية متعددة العوامل لتنفيذ نظام مصادقة متزامنة. يقدم النظام المقترح حلاً فعالاً وميسور التكلفة وقابل للتكيف مع التدخل البشري للتوثيق والرصد لبيئات التعلم الإلكتروني. بالإضافة إلى ذلك ، يمكن أن يقاوم عملنا الأمن السيبراني ويحتوي على بعض المقاييس الجيدة مثل المصادقة المتبادلة وحالات المستخدم الشاذة وغيرها. في هذا البحث ، يستخدم المخطط المقترح نظام مصادقة ثنائي يعتمد على التشفير غير المتماثل للحفاظ على المنتج (APSE)والقياسات الحيوية لبصمات الأصابع لإدارة وإنشاء حساب المستخدم بطريقة آمنة. يحقق عملنا أيضًا توازنًا جيدًا بين الأداء وتعقيد الأمان مقارنةً بأحدث ما توصلت إليه التكنولوجيا. لذلك ، نحقق نتائج جيدة لـ 1.69 مللي ثانية للحساب و 1280 بت للاتصال.

*Corresponding author email : ali.yassin@uobasrah.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq