Received: October 31, 2022. Revised: December 2, 2022. 50

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Towards for Designing Educational System Using Role-Based Access Control

Maha Kadhim Kabier[1]* Ali A. Yassin[1] Zaid Ameen Abduljabbar[1]

[1]*Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq*
* Corresponding author's Email: eduppg.maha.kabier@uobasrah.edu.iq

Abstract: During the COVID-19 pandemic, online electronic educational systems have been used in most schools and universities as they were forced to move their operations from classrooms to online settings. However, these systems face a serious security issue. Access control considers the core of data security for any implemented system. This paper presents the well-known role-based access control (RBAC) approach to enhance system security and improve user role and system privilege. This study also addresses the issues faced by extant schemes, such as security risk tolerance, by proposing a privacy-preserving educational system that utilizes RBAC and smart multi-factor authentication. This approach uses an asymmetric cryptosystem based on the Elgamal digital signature operation to provide multi-factor authentication while relying on low-complexity cryptographic hash functions. RBAC manages system security via the "user classification, role authorization, and unified management" approach. By limiting the amount of data that users can access, RBAC is particularly suited for multi-level applications. This approach also uses informal analysis and the Scyther tool to conduct extensive formal security proofs. RBAC offers many benefits, including mutual authentication, identity anonymity, forward secrecy, key management, and high resistance to well-known attacks, such as phishing, replay, Man-In-The-Middle (MITM), and insider attacks. Compared with other schemes, RBAC offers more security features and boasts higher cost effectiveness in processing and communication. Furthermore, our work achieves a good balance between performance and security complexity when compared to the state-of-the-art. So, we get good results at a cost of 0.253 ms for computing and 1326 bits for communication.

Keywords: Educational system, Role-based access control, Multi-factor authentication, Elgamal digital signature.

1. Introduction

Following its rapid growth in recent years, the Internet has completely invaded contemporary life. Enabled by such technology, people can now provide services regardless of time and location constraints. The educational system is one of the most important benefactors of such technology. Educational administration systems need to be secure to support teaching and learning for both teachers and students [1, 2].

Each user needs to be authenticated before s/he can access services or resources in educational systems, cloud applications, multi-server setups, and mobile devices, thereby underscoring the importance of restricting the access of these users to these systems; such restriction is an essential component of any security architecture [3].

An educational system contains modifiable tasks that alter the rights of each user and place restrictions on the security of the system [4].

As its defining feature, the role-based access control (RBAC) approach assigns each user with an appropriate role, and each role has an associated set of permissions. RBAC allows systems to be controlled such that users are granted access to the permissions associated with certain roles by identifying themselves as members with the appropriate roles. As a result, roles are established for a range of job functions inside a system and are being utilized to manage permissions [5].

RBAC provides a framework for managing the access of users to resources based on their assigned roles. Each user has a certain role allocated to them,

and each position has a set of privileges to which they alone have access. As a result, the resource management strategy needed for an educational system may be provided by RBAC [6].

The entire educational system is facing challenges in the form of the COVID-19 pandemic and the technological breakthroughs that have affected schools, colleges, and other educational institutions, thereby triggering a shift from traditional classroom learning to e-learning. Although more efficient and productive than traditional classroom learning, e-learning lacks secrecy, hence exposing the information passed between parties to the risk of interception. As a result, the access of unauthorized users to the system needs to be restricted [7].

In this paper, we propose RBAC, whose fundamental tenet is that roles are made up of operations that correspond to the actions performed by users who have been correctly assigned to these roles as well as to the relationships among users, roles, and operations [8]. We propose a verification scheme to protect the system from some of the most well-known cyberattacks, including phishing, MITM, insider, and reply attacks. Compared with other relevant systems, such as strong verification, key management, message enforceability, and anomaly of user identification, the proposed scheme offers many security benefits to the system.

This scheme is divided into four primary phases, namely, the registration phase, role privileges management phase, permission to configure phase, and login and authentication phase. Each of these phases ensures a safe and secure information transfer among the three main components of the system (i.e., user, cloud server provider, and authentication server) using the Elgamal digital signature, SHA-512 hash function, and smart-factor authentication. The proposed scheme is safe against common attacks by using security analysis and the Scyther tool [9]. The proposed scheme also outperforms the extant ones in terms of computational and communication costs.

This work contributes to the literature by outlining a strong security plan that emphasizes how easily access control and authentication factors may be integrated into an educational system. The proposed scheme aims to distribute the policies and privileges among the constituents of the system, including the administrator and users. Specifically, the user has the right to enjoy all or some of the primary system operations, including adding, deleting, and modifying, depending on the permission granted to him/her by the administrator. We rely on formal (Scyther tool) and informal security analyses to demonstrate how immune our proposed scheme is to well-known attacks, including insider, reply, and MITM attacks.

The proposed scheme also has strong features, such as secure mutual authentication, anomaly, and perfect forward secrecy, and is based on smart-factor authentication. The privacy of users is also dependent on the cloud service provider, which creates secret keys for the administrator and users.

The rest of this paper is structured as follows. Section 2 reviews the related work. Section 3 presents the primitive tools. Section 4 describes the proposed scheme. Section 5 presents the security analyses and discusses the possible attacks. Section 6 concludes the paper.

2. Related works

Users may want to protect their privacy and hide their true identities when using sensitive data. Accordingly, this topic has attracted much attention from researchers in recent years. In this section, we analyse numerous studies that concern the same topic.

In 2017, Lin et al. [10] introduced a secure scheme for cloud-based smart learning applications. Their system registers the user with the authentication server based on his/her identity. The user symmetrically encrypts his/her data before sending to the authentication server. This server then decrypts the password and obtains its hash value. This method is resistant to MITM attacks but is susceptible to fishing due to the sharing of passwords among communication entities.

In 2018, Binu et al. [11] proposed the broker authentication scheme, which employs a two-factor authentication system in which the user password serves as the first factor and a crypto-token kept in the database serves as the second factor. The user must present both the password and crypto-token to the authentication server to prove his/her identity. However, without intervention from the servers, the user can manage his/her password and verification data. The Scyther tool was used to test whether this system can guard itself from well-known attacks. Results show that the sharing of passwords between users and the authentication server renders this scheme vulnerable to phishing attacks.

In 2019, Foulidi et al. [12] proposed a study to determine whether there are any issues with the Directorate's coordination and communication with the schools, as well as what steps the educational managers take to develop an effective communication system. However, there are issues faced in this study, such as the operation of the

instructional network, and the absence of current information technology (IT) equipment and technological apparatus

In 2019, T. Snoussi [13] proposed an LMS usage in higher education in the UAE, due to the numerous benefits when using this method in emirate educational institutions provides such as the simplicity of setting up and delivering online courses, carrying out evaluations online, having access to and availability of learning resources, the potential for students and faculty to save time and money, and communication and interaction. But technical issues and users' computer competence are the main barriers to integrating technology into education. In his most recent study, Al Samarraie [14] believed freshmen students may not have the necessary prior technical skills to use the LMS efficiently. It may still be difficult for students to coordinate and handle various concepts in a way that enables them to connect and share their unique tacit knowledge.

In 2021, Pulgar et al. [15] used social network analysis (SNA) to visualize student relationships, academic standing, and teamwork in classes. One of the study's limitations is the absence of data on topics like internet availability, accessibility, and teacher and student ICT training, given how important these tools are for remote learning. Additionally, we acknowledge that the conducted study does not take into account the individual experiences of students as they switch from in-person to online instruction.

In 2022, Dr. Kasumu et al. [16] offered descriptive survey research to look into the use of learning management systems in education. The study's findings suggest that students can maintain their autonomy, excitement, and motivation by using a learning management system. But teachers should make sure to regularly use learning management systems in order to construct lessons that are suited to their students' needs. However, this study did not look into the security issue surrounding data transmission between users in the e-learning system.

In this paper, we propose a robust verification scheme based on the SHA-512 function and Elgamal digital signatures. This scheme offers many benefits, including protection against user-identity-related anomalies, smart-factor authentication, and resistance to well-known attacks, including impersonation, phishing, replay, MITM, and insider attacks. The proposed scheme is independently and officially tested using cryptography proofs and Scyther. The proposed scheme outperforms the extant ones in terms of computation/communication cost and security analysis. Table 1 presents the comparison results. The proposed scheme achieves ten factors F1, F2, F3, F4, F5, F26, F7, F8, F9, and F10, when compared with other previous works, reflecting excellent precision and security as follows:

Table1. The security comparison with other schemes

Factors	[10]	[11]	[12]	[13]	[15]	[16]	our
F1	N	N	N	N	Y	N	Y
F2	Y	Y	Y	Y	N	N	Y
F3	Y	Y	Y	N	Y	N	Y
F4	N	Y	N	Y	N	N	Y
F5	Y	Y	N	N	N	N	Y
F6	Y	Y	N	N	N	N	Y
F7	N	N	Y	Y	Y	N	Y
F8	N	Y	N	N	N	N	Y
F9	Y	Y	N	N	N	N	Y
F10	N	Y	N	N	N	N	Y

F1: Secure mutual authentication, F2: Perfect forward secrecy, F3: Supports users' identity anonymity, F4: Resists insider attacks, F5: Resists MITM attacks, F6: Resists replay attacks, F7: Resists phishing attacks, F8: Strong verification, F9: Login and authentication phase efficiency, F10: Formal verification with Scyther.

3. Primitive tools

3.1 The Elgamal algorithm

In 1984 a public key technique based on discrete logarithms was proposed by Taher Elgamal [17]. The ElGamal encryption/signature algorithm, which is based on the Diffie-Hellman key exchange, is an asymmetric key encryption algorithm for public-key cryptography [18]. This probabilistic signature algorithm assigns different legal digital signatures to the same message. The Elgamal algorithm mainly includes three phases, namely, the secret key generation, digital signature generation, and digital signature verification phases [19].

3.1.1. Key generation

Let P be a large prime number. The discrete logarithm cannot be easily solved in $P \in Z^*$ Therefore, select a generator $g \in Z$ and a random number that is a primitive root of P. The sender then generates Private (S_K) and Public (P_K) keys as follows:

• Generate a random integer $P \in Z_P^*$.
• Compute $Y = g^X \, mod \, P$.
• The public key is (Y, g, P), and the private key is X

3.1.2. Digital signature generation

Suppose that the message to be signed is$M$. first compute the hash m=$h(M)$ and digital signature are initially computed as follows:

• Choose a random integer $K \in Z_{P-1}^{*}$and gcd$(K, P-1)=1$, K a primitive root of $P-1$.

• Compute $S_1 = g^K \, mod \, P$ and $S_2 = \big(K-1(m - X\, S_1)\big) mod\ (P-1)$.

• The signature consists of (S_1, S_2)

3.1.3. Digital signature verification

The receiver of the signature has the public key (P_K) $(Y$,g,$P)$ and parameter signature (S_1, S_2) of the message M. The hash is initially computed as m= (M), and then the verification proceeds as follows:

• Compute $V_1 = (M) mod\ P$

• Compute $V_2 = (Y)^{S_1}\ (S_1)^{S_2}$

• If $V_1 = V_2$, then the signature is valid.

3.2 SHA-512

SHA-512 is a hashing algorithm that divides the information into three parts, namely, the original message, the padding bits, and the size of the original message. The combined size of these three parts should be a multiple of 1024 because the formatted message will be processed as 1024-bit blocks [20].

3.3 Scyther

Scyther is a tool for analysing and verifying security protocols. Apart from demonstrating cutting-edge performance, Scyther also offers a number of unique capabilities that are not offered by other tools. Some of its novel features include the potential for unbounded verification with guaranteed termination, support for multi-protocol analysis, and analysis of infinite sets of traces in terms of patterns [9].

As a tool for the formal analysis of security protocols, Scyther can quickly investigate the characteristics of a protocol. Scyther protocols are written using the SPDL programming language. Many important cryptographic operations, such as message sending and receiving between components and the functions played by each component, are supported by SPDL. This tool can be used to (1) confirm that the security claims in the protocol description are true, (2) automatically generate and confirm suitable security claims for a protocol, and (3) fully characterize the protocol for an analysis.

4. The proposed educational system

This section presents the suggested design of the Role-Based Access Educational System (RBAES). An electronic educational system depends on a model of role-based access control. The proposed system consists of two parts: Users and Resources. The first one is represented by Administrators divided into two parts: the main Administrator (ADM)and the Head of Departments ($HD_1, HD_2, HD_3, \dots, HD_n$),Teachers ($T_1, T_2, T_3, \dots, T_n$), Students ($S_1, S_2, S_3, \dots, S_m$), Examination committee (EC), and Cloud Service Provider (CSP) while the second one refers to Subjects ($Sb_1, Sb_2, Sb_3, \dots, Sb_k$), Scores $(Sc_1, Sc_2, Sc_3, \dots, Sc_k)$. The proposed design system is divided into four main phases: Registration Phase, Role Privileges Management Phase, and Permission to configure Phase, login, and Authentication Phase. The major aim of our work is to build a strong system that can resist malicious attacks such as MITM, Reply, and Insider. Table 2 explains the essential notations applied and is defined to assist our work's presentation and analysis to meet the requirements of secure data transmission over RBAES.

Table2. Notation used in the proposed scheme

Symbol	Description
ADM	Main Administrator
HD_i	Head of Department
T_i	Teacher
S_i	Student
EC_i	Examination committee
CSP	Cloud Service Provider
AS	Authentication Server
S_b	Subject
UN	Username
PW	Password
h(.)	hash function
PN	Phone number
MD	Mobile Device
S_K	Private Key
P_K	Public key
S_1, S_2	Parameters of singing Digital signature (ElGamal)
V_1, V_2	Parameters of Verification Digital signature (ElGamal)
Z	Set of Integer Number
R_S	Resources Server
ECT_i	Examination Committee Teacher
PT_i	Position Teacher
NT_i	Normal Teacher
V_i, V_i', V_i''	Verification code

4.1 Registration phase

In this phase, we pay more attention to users' registration based on the Administrator, Head of Departments, Teachers, and Students.

4.1.1. Administrator registration side

The ADM wishes to register in the educational system that requires sending the personal information to the CSP. The ADM has a unique attribute to register as the first one in the system for distributing the privileges/roles to remaining users such as Students and Teachers. The personal information is Username ($UN_{ADM} = h(UN_{ADM})$), Password ($PW_{ADM} = h(PW_{ADM})$), Phone number (PN_{ADM}), Mobile Device (MD_{ADM}). The $h(.)$ refers to the cryptographic hash function (SHA-512).

The CSP checks the identity of ADM in the database exists or not, CSP then sends requests for ADM to the Authentication Server (AS) for gaining the main keys. After that, AS generates Public Key (P_{KADM}) and Private Key (S_{KADM}) to use in ElGamal digital signature as follows:-

1- Generate a random integer number $X_{ADM} \in Z^*_{P-1}$ and compute $Y = g^{X_{ADM}} \ mod\ P$; where P is a large prime number and $g \in Z_P$.
2- Generate Private Key ($S_{KADM} = X_{ADM}$) and Public Key ($P_{KADM} = Y, g, P$). Then sends these Keys ($S_{KADM}.P_{KADM}$) to CSP.
3- CSP after the Keys($S_{KADM}.P_{KADM}$) receiver, declares P_{KADM} and sends S_{KADM} to ADM.

4.1.2. Teachers registration side

The teacher (T_i) should be registered in the educational system via permission gained from

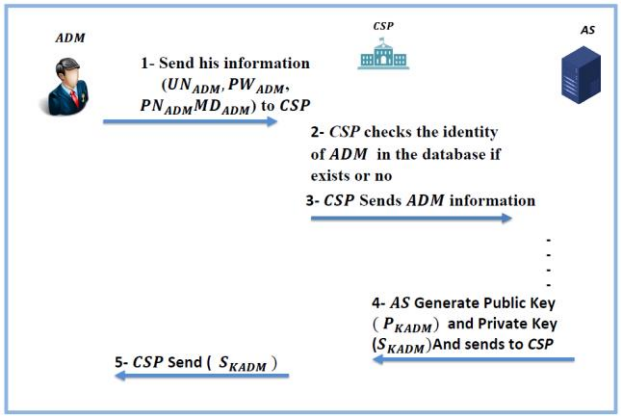


Figure. 1 Illustrates the administrator's registration in the educational system

ADM. In our work, the role of the teacher can be divided into three levels: Normal Teacher (NT_i), Examination Committee Teacher (ECT_i), and Position Teacher (PT_i). Fig. 2 explains the roles of teachers gained from ADM.

T_i sends his personal information (Username($UN_{T_i} = h(UN_{T_i})$), Password ($PW_{T_i} = h(PW_{T_i})$), Phone number (MD_{T_i}), Mobile Device (PN_{T_i})) to the CSP that checks teacher's information in the database if exists or no. We divide this stage into three levels as follows:

Level1. The normal teacher can log in to the system using Username ($UN_{NT_i} = h(UN_{NT_i})$), Password ($PW_{NT_i} = h(PW_{NT_i})$).

Level2 and Level3. Each Examination Committee Teacher (ECT_i) and Position Teacher (PT_i) have the same privileges as the administrator (ADM). Therefore, the gait of public and private keys is the same way as administrators based on CSP and AS.

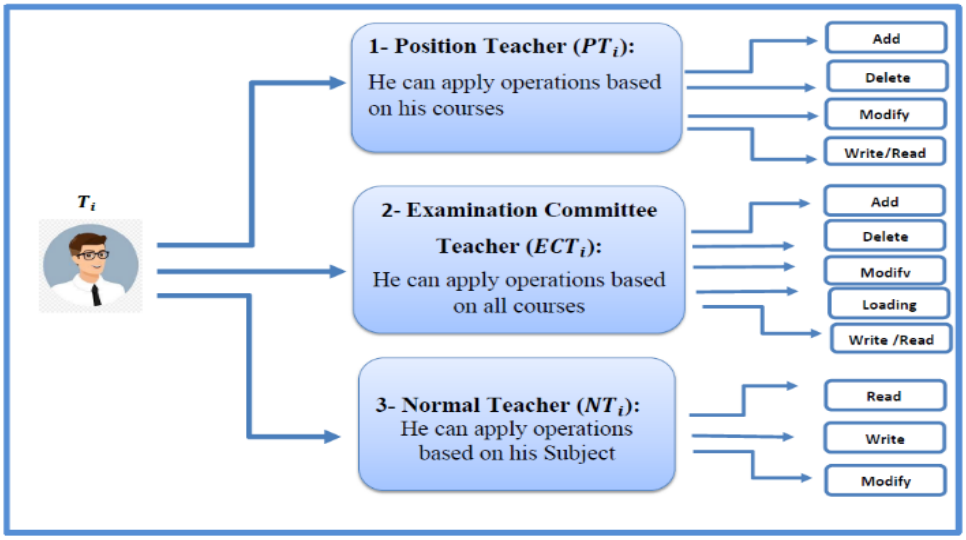


Figure. 2 Describes the roles/privileges of teachers obtained from ADM

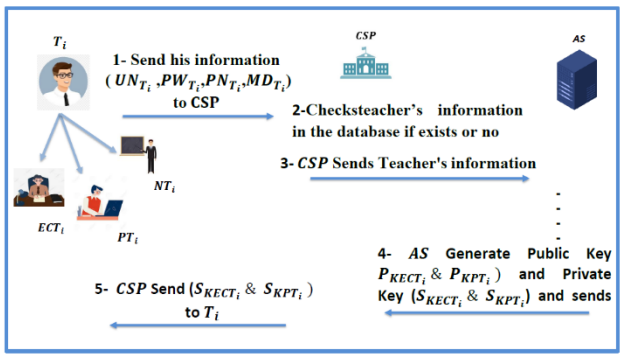


Figure. 3 Shows teacher's registration in the educational system

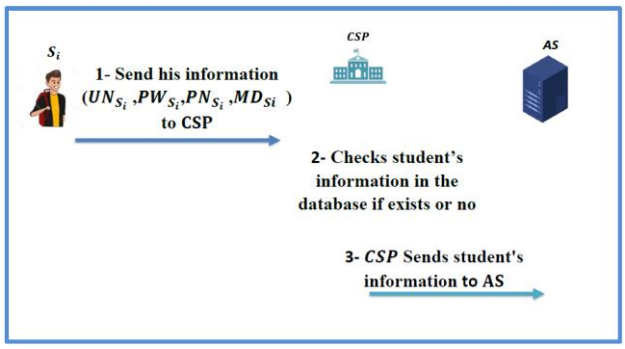


Figure. 4 Explains student registration in the educational system

The following steps describe the mechanism of obtaining keys for ECT_i and PT_i.

1. $ECT_i \rightarrow \ CSP: Requestion\ for\ keys$
2. $CSP \rightarrow \ AS: Requestion\ of\ ECT_i$
3. $AS \rightarrow \ CSP: S_{KECT_i}, P_{KECT_i}$
4. $CSP \rightarrow \ ECT_i: < S_{KECT_i}, UN_{ECT_i}, PW_{ECT_i}, PN_{ECT_i}, MD_{ECT_i} >$

In the PT_i, we perform the following steps:

1. $PT_i \rightarrow \ CSP: Requestion\ for\ keys$
2. $CSP \rightarrow \ AS: Requestion\ of\ PT_i$
3. $AS \rightarrow \ CSP: S_{KPT_i}, P_{KPT_i}$
4. $CSP \rightarrow \ ECT_i: < S_{KPT_i}, UN_{PT_i}, PW_{PT_i}, PN_{PT_i}, MD_{PT_i} >$

4.1.3. Students registration side

The student (S_i) should be registered in the educational system via permission gained from ADM. In our work, the role of the student is read-only, S_i Send his personal information Username ($UN_{S_i} = h(UN_{S_i})$), Password ($PW_{S_i} = h(PW_{S_i})$), Phone number (Mobile Device (MD_{S_i}) to *CSP*, that checks student's information provided from his school's manager in the database; it exists or no. After that, the student can log in to the system by using his/her Username ($UN_{S_i} = h(UN_{S_i})$) and Password ($PW_{S_i} = h(PW_{S_i})$), and verification code (VC_{S_i}) which applies smart factor authentication in the changing his devices to ensure from the authority of student.

4.2 Role privileges management phase

In RBAC, the users are associated with roles gained by the system manager, and roles linked with the services. The administrator of the educational system is responsible for assigning the roles to components of the educational environment such as schools that perform some functions like determining various roles and restricting roles based on privileges and services. In this phase, we focus on the school's environment; each user has privileges based on his position/role in the school (see Fig. 6). We can divide the role of each user into two levels as follows:

1) High – Level includes Administrator, Head of Departments, and Examination committee.

2) Low–Level includes Teachers T_i and StudentsS_i. Where the student can read his scores while the normal teacher can read/write scores of his classes. Fig. 5 explains the working mechanism of these levels. Additionally, we use a role hierarchy model that includes the operations, constraints, and objects. Therefore, each component can inherence some privileges his parents; for example, the role of the high-level authorization is more flexible, in addition to its authority can be granted directly, but also inherit other roles permissions.

Table 3. Explain type of roles

Role	Assigned permissions
R1	Read Scores & Read Subjects
R2	Read & Write Scores &Modify of Classes
R3	Add &Delete &Modify &Read &Write of Corse
R4	Add &Delete &Modify &Read &Write of all Corse

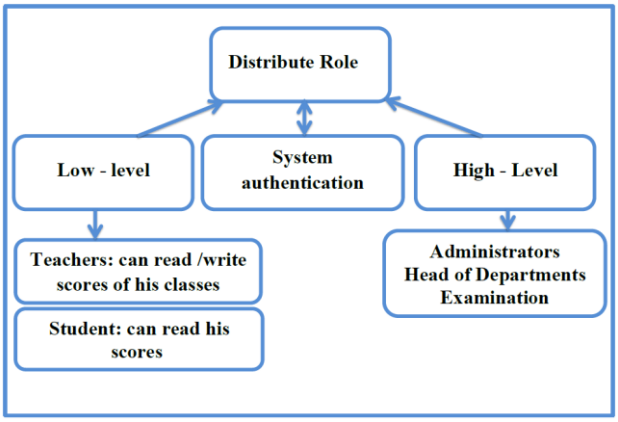


Figure. 5 Describes the working mechanism of these levels

4.3 Permission setting phase

In this phase, we divide the authority of users into three types:

4.3.1. Departmental authority

This type of authority commonly be appropriate to the departmental role. For instance, the academic administrator of the school management owns the authority over the classrooms' resources in the educational system and fails to control/operate the resources of classrooms' in the other school.

4.3.2. Function permission

This type of authority refers to which system function module that offers to the user to use or not use.

4.3.3. Data permissions

These kinds of permissions are essentially applied to limit the operation of the data in the database, and used to detect several data objects (data tables, views, etc.) for using the permissions (search, insert, entry, update, delete, etc.). Fig. 6 explains the of authority in the educational administration system as follows:

4.3.3.1. Task set

the decomposition of the system functions refers to task division and function mention to the need to perform the task.

4.3.3.2. Role set

Based on the executed task set the role and the permissions are granted to the role.

4.3.3.3. Permission setting

Role of the system permissions are determined by the role of the corresponding set of tasks, and the role of the corresponding set of permissions on the several modules of the call.

4.4 Login and authentication phase

After a successful registration phase, system users wish to login into the educational system for accessing the resources of the server and benefit from the facilities of the system:

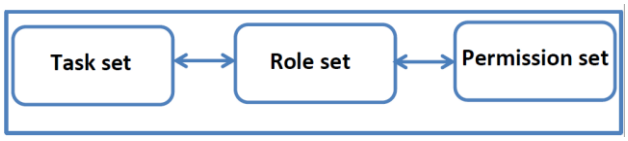


Figure. 6 Explains the of authority in the educational administration

4.4.1. Students side

In this phase, the student (wishes are login into CSP , and he inputs his credentials data UN_{S_i} and PW_{S_i} and then applies the following steps:

1- Generate integer random number ($r_i \in Z_x$); where $x = p \times q$, q , and p are prime numbers. Furthermore, he computes $UN'_{S_i} = h(UN_{S_i})$, $PW'_{S_i} = h(PW_{S_i}) \oplus r_i$, and $r'_i = h(PW_{S_i}) \oplus h(UN_{S_i}) \oplus r_i$.

2- Send his credential information ($UN'_{S_i}, PW'_{S_i}, r'_i$) to CSP.

3- Upon receiving credential information from S_i, CSP checks the UN'_{S_i} with $h(UN_{S_i})$ in his database,

4- if it does not exist, terminate this phase. Otherwise, CSP computes $r''_i = h(PW_{S_i}) \oplus h(UN_{S_i}) \oplus r'_i$. Finally, he computes $PW''_{S_i} = h(PW_{S_i}) \oplus r''_i$ and compares PW''_{S_i} with PW'_{S_i}, if holds, CSP gains permission to S_i for using services and resources inside educational system based on student's role, otherwise, CSP terminates the current phase.

In the change user's device case, the student should be performed the up-mentioned steps (1-3) and then he applies the following steps:

5- CSP sends verification cod (V_i) as SMS to the student's phone number.

6- S_i computes $V'_i = h(V_i) \oplus r_i$ and sends V'_i to CSP

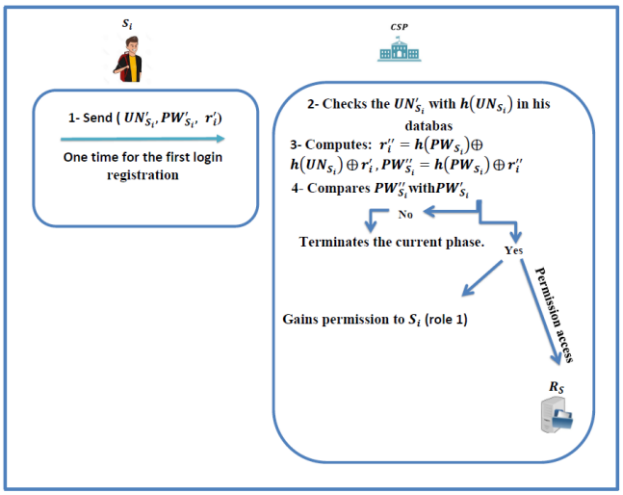
7- CSP computes $V''_i = h(V_i) \oplus r'_i$ and compares V''_i with V'_i, if holds, CSP gains permission to S_i for using services and resources inside educational system based on student's role, otherwise, CSP terminates the current phase.

In this phase, the mechanism of the login and authentication phase works based on smart-factor authentication that does not require from student to enter his creational information in each login request while he does not change his device. The figure explains smart-factor authentication.

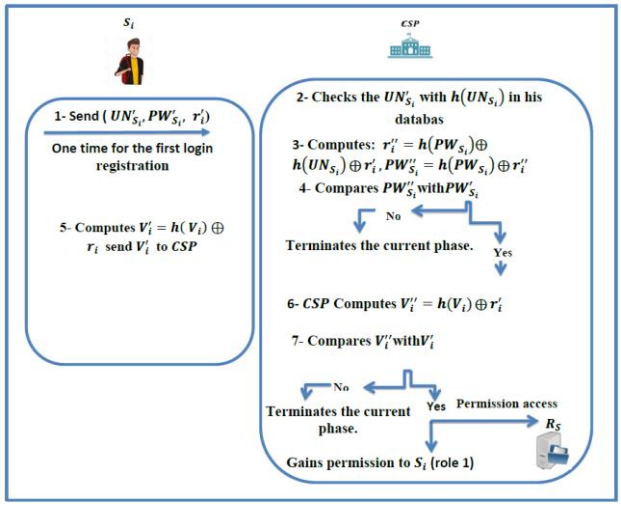
4.4.2. Administrator side

In this phase, the ADM inputs his credentials data UN_{ADM} and PW_{ADM} and then applies the following steps:

1- Generate integer random number ($r_i \in Z_x$); where $x = p \times q$, q and p are prime numbers. Furthermore, he computes $UN'_{ADM} = h(UN_{ADM})$,

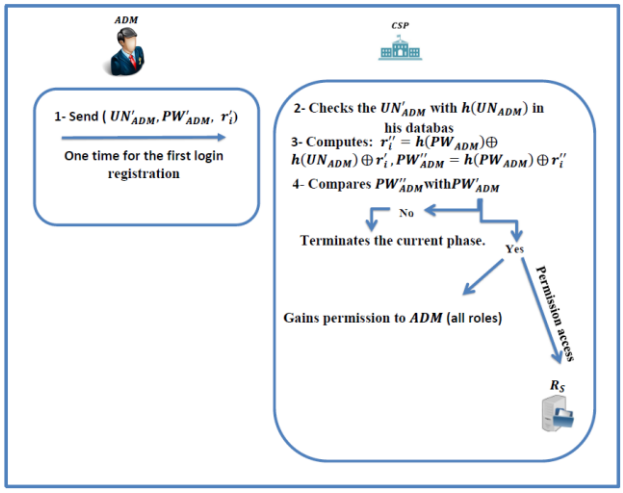


(a)

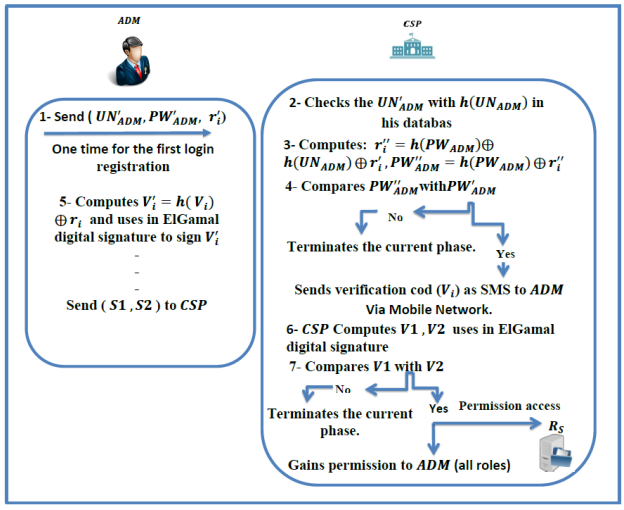


(b)

Figure. 7 Illustrates the student login and authentication in the educational system: (a) using the same user's device case and (b) using the not same user's device case



(a)



(b)

Figure. 8 Describes the administrator login and authentication in the educational system: (a) using the same user's device case and (b) using the not same user's device case

$PW'_{ADM} = h(PW_{ADM}) \oplus r_i$,and$r'_i = h(PW_{ADM}) \oplus h(UN_{ADM}) \oplus r_i$.

2- Send his credential information ($UN'_{ADM}, PW'_{ADM}, r'_i$) to CSP.

3- Upon receiving credential information from ADM, CSP checks the UN'_{ADM} with $h(UN_{ADM})$ in his database. If it does not exist, he terminates this phase. Otherwise, CSP computes $r''_i = h(PW_{ADM}) \oplus h(UN_{ADM}) \oplus r'_i$. Finally, he computes $PW''_{ADM} = h(PW_{ADM}) \oplus r''_i$ and compares PW''_{ADM} with PW'_{ADM}, if holds, CSP gains permission to ADM for using full services and resources inside educational system based on administrator role, otherwise, CSP terminates the current phase.

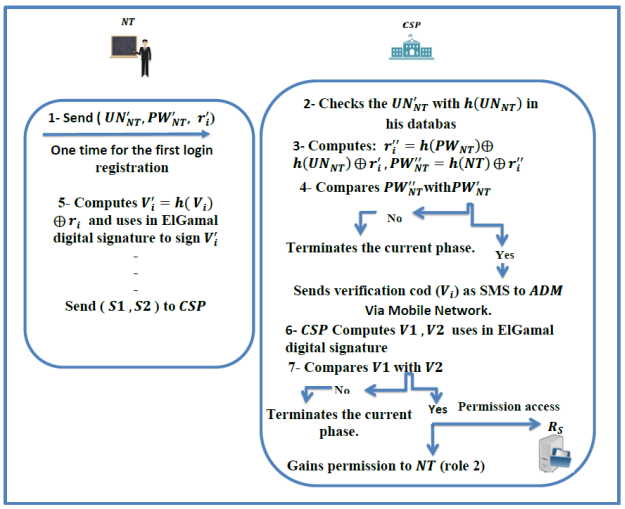
In the change user's device case or login in the system for the first time, the ADM should be performed the up-mentioned steps (1-3) and then he applies the following steps:

4- CSP generates and sends verification cod (V_i) asana SMS to theADM's phone number.

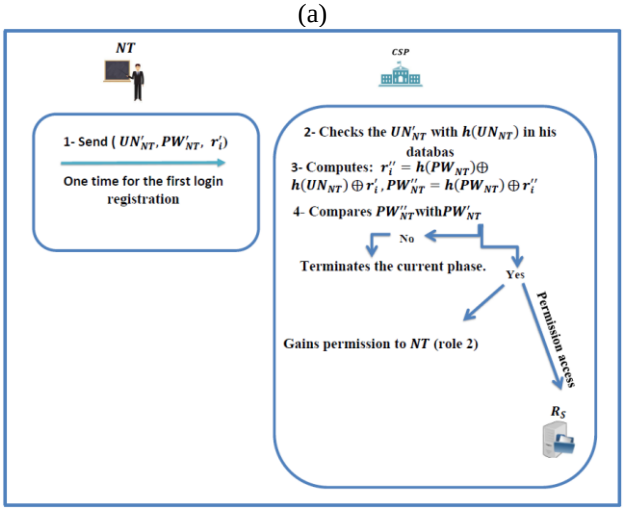
5- Up on receiving the verification code, ADM computes $V'_i = h(V_i) \oplus r_i$ and uses in ElGamal digital signature to sign V'_i based on the following steps:-

- ADMchooses a random integer $K \in Z^*_{p-1}$
- Computes $S_1 = g^k \bmod P$, $S_2 = ((k^{-1}(V'_i - r_i S_1))) mod (P-1)$.
- ADM sends ($S1, S2$) to CSP.

6 - Up on receiving the ($S1, S2$), CSP computes $V_1 = g^{h(V_i)} \bmod P$ and $V_2 = (Y)^{S_1}(S_1)^{S_2} \bmod P$. checks are $V_1 = V_2$, If holds, CSP gains permission to ADM for using services and resources inside the educational system based on the Position of the administrator's role. Otherwise, CSP terminates the current phase.

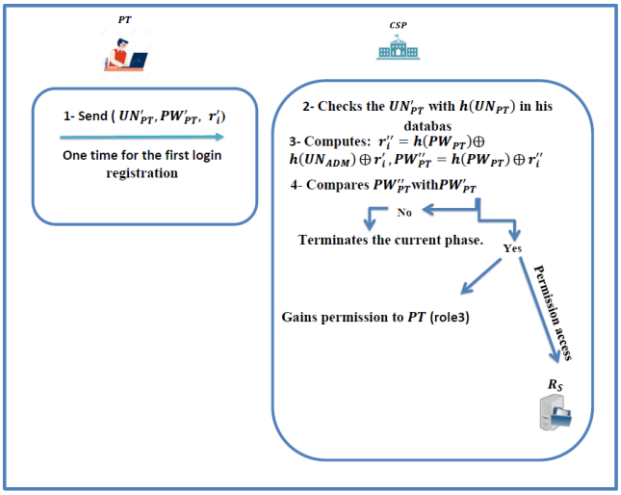


(a)

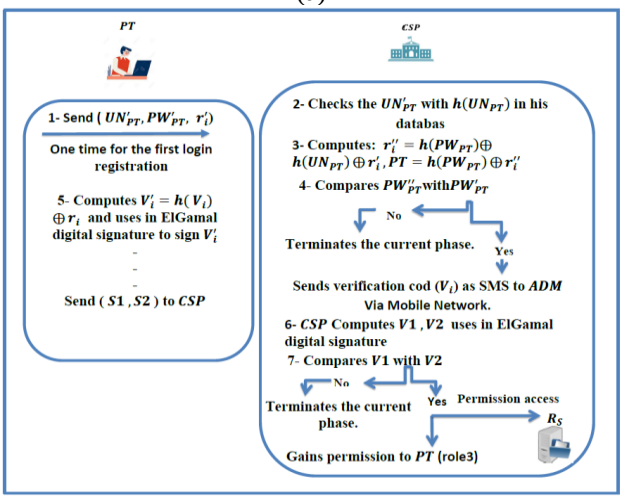


(b)

Figure. 9 Illustrates the normal teacher login and authentication in the educational system: (a) using the same user's device case and (b) using the not same user's device case



(a)



(b)

Figure. 10 Explains the position teacher login and authentication in the educational system: (a) using the same user's device case and (b) using the not same user's device case

4.4.3. Teacher side

4.4.3.1. Normal teacher (NT_i)

We follow the same steps used in the student's case and we use the symbol (NT_i) instead of (S_i), CSP gains permission to NT_i for using services and resources inside the educational system based on normal teacher's role, Read\Write and Add Scours on his subject.

4.4.3.2. Examination committee teacher (ECT_i) and position teacher (PT_i) Side

We follow the same steps used in the administrator's case and we use the symbol (ECT_i) to the examination committee and (PT_i) to position the teacher instead of (ADM), CSP gains permission to (ECT_i) and (PT_i) for using services and resources inside the educational system based on examination committee and Position teacher's role, role: Read\Write and Add, Delete, Modify Scours on all course for examination committee and Read\Write and Add, Delete, Modify Scours on his course for position teacher.

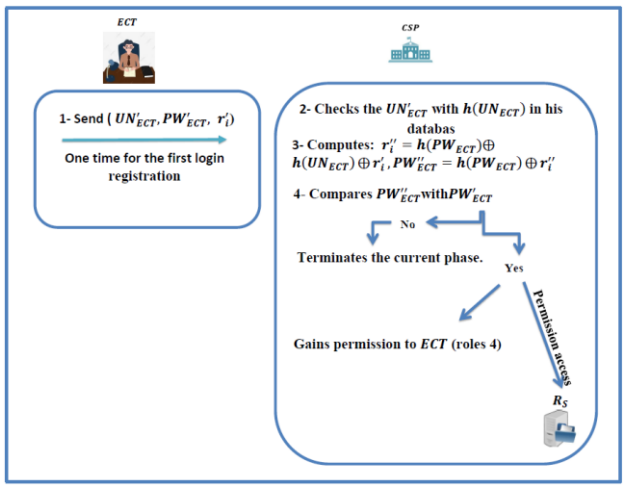
5. Security analyses and discussion on possible attacks

In this section, we analyse the security properties of the proposed scheme and compare this scheme with related ones.

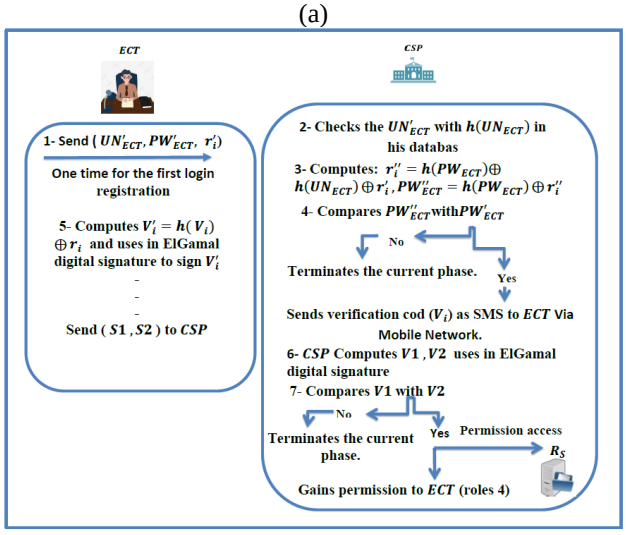
5.1 Informal security analysis

Proposition1. Our work can provide a secure mutual authentication.

Proof. CSP and users can authenticate each other, The authentication of CSP to ADM involves the following step



(a)



(b)

Figure. 11 Illustrates the examination committee teacher login and authentication in the educational system: (a) using the same user's device case and (b) using the not same user's device case

•$ADM \xrightarrow{M_1} CSP$:$M$={ UN'_{ADM},r_i}. The ADMcomputes the main parameters (UN'_{ADM},PW'_{ADM}) at once for each login phase based on $h(UN'_{ADM} \oplus r_i)$, $h(UN'_{ADM} \oplus r_i$).

• $CSP \xrightarrow{M_2} ADM$:$M$={ V_i }, where CSP sends V_i via a mobile network, and ADMcomputes $V'_i = h(V_i) \oplus r_i$ and sends it to the CSP.

•After receiving the credentials data (CSP), compute for $V''_i = h(V'_i) \oplus r'_i$ and compare V''_{ADM} with V'_{ADM}. If the result is true, then ADM ensures from authenticating of CSP.

The mechanism of the login and authentication phase works based on smart-factor authentication that does not require a student to enter his/her information per login request. We observe that values for two delivered messages ($M1$, $M2$) are only generated once and are difficult to detect by attackers, thereby ensuring that there will be a procedure of mutual authentication between two parties.

Proposition2. Our proposed scheme can guarantee perfect forward secrecy.

Proof. The keys generator depends on the digital signature verification of Elgamal. In the registration phase, the complexity of computing Xi from Y is treated as a discrete logarithm problem where the use generates $Y = g^{X_i} \, mod \, P$ in the login phase, whereas the server extracts a random integer number (r_i) after that user (for example, ADM) computes $S_1 = g^k \, mod \, P$, $S_2 = ((k^{-1} (V'_i - r_i \, S_1)) mod (P - 1)$.and sends (S_1 , S_2) to CSP. Upon receiving the (S_1 , S_2), the CSP computes $V_1 = g^{h(V_i)} \, mod$ and $V_2 = (Y)^{S_1} (S_1)^{S_2} \, mod \, P$. To confirm the authority of ADM even if the secret key Y and three values $p, q,$ and r_i are compromised for some reason, an adversary fails to compute any previous X_{ADM} because obtaining $XADM$ is very difficult and depends on the discrete logarithm problem.

Correctness

The correctness of the verification digital signature (Elgamal) between V_2 and $V_2$is calculated as

Where $h(m) = S_1 \, X_i + S_2 \, k \, mod \, (P - 1)$ then

$$\begin{aligned} V_1 &= g^{S_1 \, X_i + S_2 \, k} \, mod \, (P - 1) \\ &= g^{S_1 \, X_i} \, g^{S_2 \, k} \, mod \, (P - 1) \\ &= (g^{x_i})^{S_1} \, (g^k)^{S_2} \, mod \, (P - 1) \\ &= (Y)^{S_1} \, (S_1)^{S_2} \, mod \, (P - 1) \\ &= V_2 \end{aligned}$$

Proposition3. The proposed scheme supports the anonymity of users.

Proof. In the login phase, the identity of all users (e.g., a normal teacher) is saved using the SHA-512 hash function(UN'_{NT} =h(UN_{NT}), PW'_{NT}'=h(PW_{NT})$\oplus r_i$) and sent to CSP, thereby preventing adversaries from learning about the identity of these users as they would need to break the hash function, which is not possible. Therefore, the proposed scheme guarantees the anonymity of users.

Proposition4. The proposed scheme resists insider attacks.

Insider attacks are particularly devastating for both users and organizations given that the insiders of organizations can easily conduct information breach [21].

Proof. If a user (e.g.,ADM) logs into the educational system to access many services using the same username and password (UN'_{ADM} , PW'_{ADM}), then insider assaults are likely to happen. The proposed scheme prevents any service-providing server from

learning the username and password of users by sharing such information in encrypted form $UN'_{ADM} = h(UN_{ADM}) \oplus r_i$, $PW'_{ADM} = h(PW_{ADM}) \oplus r_i$ in the CSP. Therefore, the proposed scheme is resistant to insider attacks.

Proposition5. The proposed scheme resists MITM attacks

Proof. The adversary needs to know the $(UN'_{ADM}P, PW'_{ADM}, r'_i)$ to masquerade as ADM and the challenge message (SMS) to preteens as CSP. In our work, the brief secrets are denoted by r_i and SMS. An adversary fails to obtain $(UN'_{ADM}P, PW'_{ADM}, r'_i)$ to calculate these useful parameters because such parameters always generate once for each login request. When an adversary has access to the random number r_i and login information to compute the S_{KADM} key, s/he cannot have PN_{ADM} to receive an SMS from the CSP. Therefore, our proposed system resists MITM attacks.

Proposition6. The proposed scheme resists replay attacks.

Proof. In the proposed scheme, the CSP generates a unique random number r_i for each login session. Therefore, the message request for one session is only valid for this particular session and is unique from the message requests for other sessions. In other words, the adversary A' cannot intercept and use these messages to gain access to the services available in the system because the proposed scheme can resist replaying attacks due to the random number mechanism.

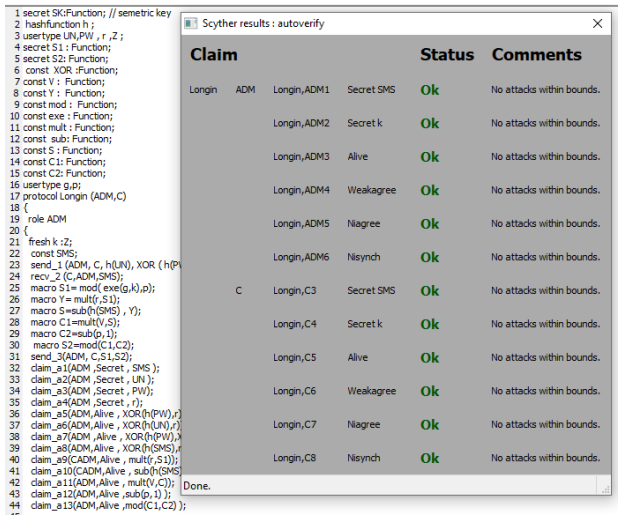
Proposition7. The proposed scheme resists phishing attacks.

Phishing attacks come in the form of fraudulent e-mail messages that appear to have been sent by legitimate enterprises to access private information and to commit identity theft [22].

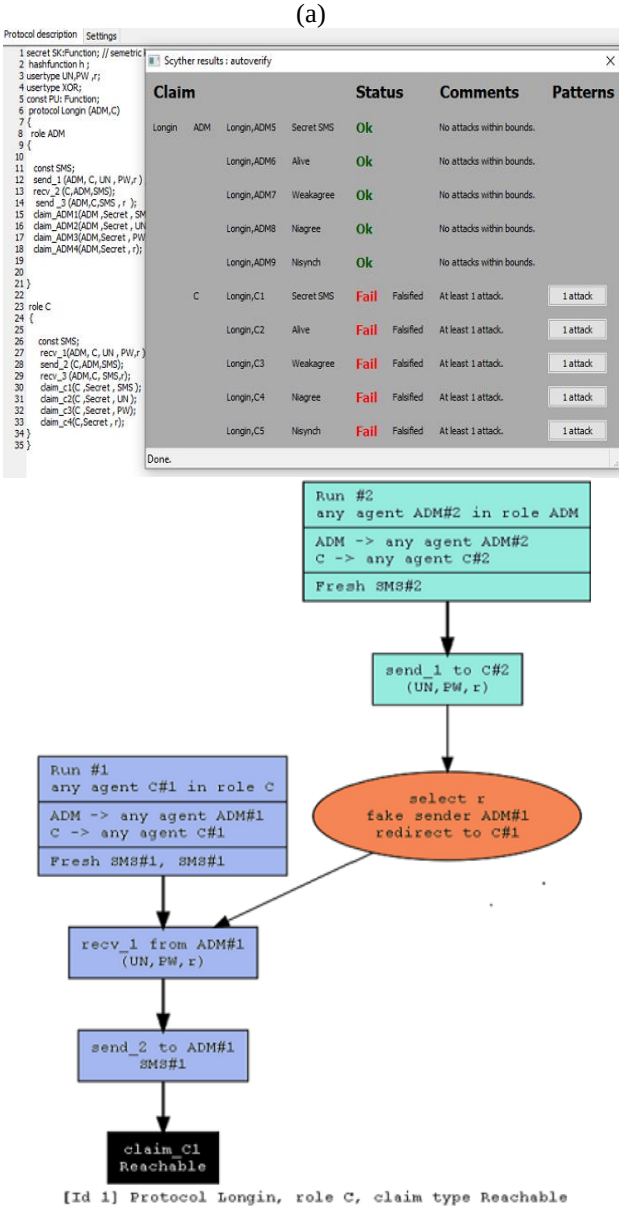
Proof. The user identity (e.g.,ADM) is encrypted during the login phase using the SHA-256 hash function $UN'_{ADM} = h(UN_{ADM}) \oplus r_i$, $PW'_{ADM} = h(PW_{ADM}) \oplus r_i$ and sent to the CSP, who will then verify the identity of the user by sending an SMS to ADM. In this way, adversaries are unable to phish password and login details from the education system.

5.2 Security analysis of the proposed approach using Scyther

Scyther uses an unbounded model checking technique whose protocol is safe for all potential behaviours, even when an advanced insider attack is present. Fig. 12 illustrates the results of the system scheme verification using Scyther.



(a)



(b)

Figure. 12 Illustrates the results of the system scheme verification: (a) cannot be attacked and (b) can be attacked

5.3 Performance analysis

5.3.1. Computation cost

The time complexity of the suggested scheme is calculated using the computational cost, and the crypto hash function is identified as the commonly used operation in previous research. Table 4 compare the computational cost of the proposed scheme with other important schemes [23-26]. The processing times for the fundamental operations are roughly set as follows [28]:
Crypto hash function (T_h) = 0.023ms.
Exclusive OR operation ($T_{\oplus}$)= negligible.

Furthermore, our work achieves a good trade-off between performance and security complexity when compared to the state-of-the-art. Because it only has eight Exclusive OR operations and thirteen hash operations, the proposed scheme takes less time than other works. Additionally, because digital signature operations (sign and verify) do not necessitate additional time for encryption and decryption, using them yields the greatest results, and since the data sent between the mobile device and the server is crucial, it requires higher efficiency and confidentiality.

5.3.2. Computation cost

To calculate the communication cost during the login and authentication phases in practical implementation, we use the following assumptions based on [29-31]
- The size of the random nonce is 160 bits.
- The used hash function is a secure hash. Therefore, the size of the digested hash is 32 bits.
- The identities are 160 bits in size.
- The size of the Elgamal digital signature algorithm is 750 bits.
- The cipher text size is 128 bits.
-The time stamps are equal to 32 bits.
Table 5 compares the same methods in terms of their communication cost.

Table 4. Computation cost comparison with other works

Scheme	Registration	Login and Authentication	Total Cost
Our Scheme	$4T_{h(\text{for ADM})}$	$7T_h + 8T_{\oplus(\text{for ADM})}$	0.253
Our Scheme	$4T_{h(\text{for user})}$	$7T_h + 8T_{\oplus(\text{for user})}$	0.253
[23]	$2T_h + 6T_{\oplus}$	$16T_h + 29T_{\oplus}$	0.414
[24]	$6T_h + 2T_{\oplus}$	$24T_h + 10T_{\oplus}$	0.46
[25]	$3h + 2T_{\oplus}$	$25T_h + 26T_{\oplus}$	0.644
[26]	$4T_h + 5T_{\oplus}$	$18T_h + 27T_{\oplus}$	0.506

Table 5. Communication cos comparison with other related works

Protocol	No of messages	No of bits
Our scheme	$3_{(for\ ADM)}$	1326
Our scheme	$3_{(for\ User)}$	576
[23]	5	2688
[24]	3	1536
[25]	4	2688
[26]	4	1568

Three exchange messages are employed in the proposed system for communication processes: data transferred from the U_i to the CSP using symmetric key encryption, data sent from the U_i to the CSP using an Elgamal digital signature, and vice versa. The outcome depends on the potential of digital signatures to lower the transferred messages (three messages) between primary components, and the total cost is 1326 bits, the lowest among comparable systems.

6. Conclusions

The rapid development of the Internet and information technology has substantially affected all life aspects, of which the educational system stands as one of the most important. The online educational system is facing several forms of danger, such as security threats, malicious attacks, and unauthorized access to instructional resources, which can be resolved by combining a dependable, secure, and scalable multi-factor authentication method with the RBAC method, which is a widely used secure and adaptable role-based access control technique. We explore the design of the RBAC model, which assesses and adjusts the responsibilities and permissions in the school administration system. Results show that the RBAC scheme successfully safeguards the operational security of the educational administration system, satisfies the security criteria, demonstrates a superior control access capability, and meets the system security needs. This scheme was then formally examined using the Scyther tool, and results highlight the usable security properties and safety of this scheme.

References

[1] L. Dongdong, X. Shiliang, Z. Yan, T. Fuxiao, N. Lei, and Z. Jia, “Role-based access control in educational administration system”, *MATEC Web Conf.*, Vol. 139, pp. 1-8, 2017.
[2] C. Ruan and S. Shahrestani, “Role based access control for web-based teaching systems”, In: *Proc. of 2010 Int. Conf. Comput. Intell. Softw. Eng. CiSE 2010*, pp. 0-3, 2010.

[3] M. K. Khan, S. K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'", *Comput. Commun.*, Vol. 34, No. 3, pp. 305-309, 2011.

[4] Q. Li and L. Zhao, "Research and implementation of educational management system based on role access control technology", In: *Proc. of 2015 6th International Conference on Manufacturing Science and Engineering*, pp. 456-459, 2015.

[5] D. Ferraiolo, J. Cugini, and D. R. Kuhn, "Role-based access control (RBAC): Features and motivations", In: *Proc. of 11th Annu. Comput. Secur. Appl. Conf.*, pp. 241-248, 1995.

[6] A. Onashoga, A. A. Alli, and T. Ogunseye, "Enhanced Role Based Access Control Mechanism for Electronic Examination System", *Int. J. Comput. Netw. Inf. Secur.*, Vol. 6, No. 3, pp. 1-9, 2014.

[7] C. J. F. Cremers, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", *Comput. Aided Verif.*, Vol. 5423, pp. 414-418, 2008.

[8] N. Hamed and A. Yassin, "Secure Patient Authentication Scheme in the Healthcare System Using Symmetric Encryption", *Iraqi J. Electr. Electron. Eng.*, Vol. 18, No. 1, pp. 71-81, 2022.

[9] G. Kambourakis, D. P. N. Kontoni, A. Rouskas, and S. Gritzalis, "A PKI approach for deploying modern secure distributed e-learning and m-learning environments", *Comput. Educ.*, Vol. 48, No. 1, pp. 1-16, 2007.

[10] A. Lee, "Authentication scheme for smart learning system in the cloud computing environment", *J. Comput. Virol. Hacking Tech.*, Vol. 11, No. 3, pp. 149-155, 2015.

[11] S. Binu, M. Misbahuddin, and P. Raj, "A Strong Single Sign-on User Authentication Scheme Using Mobile Token Without Verifier Table for Cloud Based Services", *Computer and Network Security Essentials*, pp. 237-261, 2018.

[12] X. Foulidi, "Issues on Effective Communication in Educational Administration : A Local Survey", *Linguistics and Literature*, Vol. 2, No. 11, pp. 89-92, 2019.

[13] T. Snoussi, "Learning Management System in Education: Opportunities and Challenges", *Int. J. Innov. Technol. Explor. Eng.*, Vol. 8, No. 12S, pp. 664-667, 2019.

[14] H. A. Samarraie and N. Saeed, "A systematic review of cloud computing tools for collaborative learning: Opportunities and challenges to the blended-learning environment", *Comput. Educ.*, Vol. 124, pp. 77-91, 2018.

[15] J. Pulgar, D. Ramírez, A. Umanzor, C. Candia, and I. Sánchez, "Student networks on online teaching due to COVID-19: Academic effects of strong friendship ties and perceived academic prestige in physics and mathematics courses", *arXiv preprint arXiv:2109.06245*, 2021.

[16] D. K. R. Oluwayimika, "Learning Management System in Education: Benefits and Drawbacks", *Int. J. Trendy Res. Eng. Technol.*, Vol. 07, No. 01, pp. 17-23, 2022.

[17] D. Logarithms, "a Public Key Cryptosystem and a Signature based on Discrete Logarithms", *System*, pp. 10-18, 1976.

[18] D. Karima and M. Lamine, "Two dimensional ElGamal public key cryptosystem", *Inf. Secur. J.*, Vol. 28, No. 4-5, pp. 120-126, 2019.

[19] G. F. Elkabbany and M. Rasslan, "ENHANEMENT OF ELGAMAL SIGNATURE SCHEME USING MULTI-PROCESSING SYSTEM The Proposed Parallel Design of ElGamal Signature Algorithm", In: *Proc. of 2017 Intl Conf on Advanced Control Circuits Systems (ACCS) Systems & 2017 Intl Conf on New Paradigms in Electronics & Information Technology (PEIT)*, pp. 179-186, 2017.

[20] M. Sumagita, I. Riadi, J.P.D.S. Sh, and U. Warungboto, "Analysis of secure hash algorithm (SHA) 512 for encryption process on web-based application", *International Journal of Cyber-Security and Digital Forensics*, Vol. 7, No. 4, pp.373-381, 2018.

[21] S. Rajamanickam, S. Vollala, R. Amin, and N. Ramasubramanian, "Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC", *IEEE Syst. J.*, Vol. 14, No. 2, pp. 1972-1983, 2020.

[22] S. Bojjagani, D. R. D. Brabin, and P. V. V. Rao, "PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification", *Procedia Comput. Sci.*, Vol. 171, No. 2019, pp. 1110-1119, 2020.

[23] A. M. Koya and D. P. P., "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network", *Comput. Networks*, Vol. 140, pp. 138-151, 2018.

[24] S. Challa and A. K. Das, V. Odeiu , N. Kumar, S. Kumari, M. K. Khan, and A. Vasilakos, "An efficient ECC-based provably secure three-

factor user authentication and key agreement protocol for wireless healthcare sensor networks", *Comput. Electr. Eng.*, Vol. 69, pp. 534-554, 2018.

[25] X. Liu, R. Zhang, and M. Zhao, "A robust authentication scheme with dynamic password for wireless body area networks", *Comput. Networks*, Vol. 161, pp. 220-234, 2019.

[26] 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 Trans. Ind. Electron.*, Vol. 65, No. 3, pp. 2795-2805, 2018.

[27] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook", *J. Syst. Archit.*, Vol. 97, pp. 185-196, 2019.

[28] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes", *IEEE Commun. Surv. Tutorials*, Vol. 16, No. 2, pp. 1005-1023, 2014.

[29] E. Munivel and A. Kannammal, "New Authentication Scheme to Secure against the Phishing Attack in the Mobile Cloud Computing", *Secur. Commun. Networks*, Vol. 2019, 2019.

[30] Y. Zheng, "Signcryption or How to Achieve Cost Signature & Encryption Cost Signature + Cost Encryption", *Annu. Int. Cryptol. Conf.*, 1999.

[31] A. Chaturvedi, A. K. Das, D. Mishra, and S. Mukhopadhyay, "Design of a secure smart card-based multi-server authentication scheme", *J. Inf. Secur. Appl.*, Vol. 30, pp. 64-80.

[32] H. I. Nasser and M. A. Hussain, "Provably curb man-in-the-middle attack-based ARP spoofing in a local network", *Bulletin of Electrical Engineering and Informatics*, Vol. 11, No. 4, pp. 2280-2291, 2022.

[33] A. I. Abdulsada, D. G. Honi, and S. A. Darraji, "Efficient multi-keyword similarity search over encrypted cloud documents", *Indones. J. Electr. Eng. Comput. Sci.*, Vol. 23, No. 1, pp. 510-518, 2021.