How to Cite:
Alkhaldi, S., AlZain, M. A., & Masud, M. (2022). SCES proposed model for data protection in cloud educational system in Saudi Arabia. *International Journal of Health Sciences*, *6*(S3), 5090–5126. https://doi.org/10.53730/ijhs.v6nS3.7018

SCES proposed model for data protection in cloud educational system in Saudi Arabia

Sanaa Alkhaldi

Mohammed A. AlZain

Mehedi Masud

***Abstract*---**Education is the basis for the development of peoples and the progress of countries, so the Saudi government has made great efforts to develop education, and made this development one of the most important goals of the 2030 vision, and among the most prominent of these efforts and most in keeping with the current local and global conditions is what it provided during the Corona pandemic from the transformation to e-learning and the adoption of education platforms that enable its users to access and benefit from its services. Since the data of this systems users must be kept confidential and secure, this paper was made. This paper focuses on the security aspects of data protection in educational system in the Kingdom of Saudi Arabia in cloud computing environment. This paper involves data protection aspects by protecting data of Saudi educational systems and maintaining their integrity and confidentiality. It also proposes a secure model called SCES (Secure Cloud Educational System) based on Attribute-based encryption as an access control technique to avoid tampering with data when unauthorized people try to access it, and to protect data the proposed model applies combined encryption system using AES and RSA encryption algorithms. The performance of SCES proposed model will be discussed based on influencing factors and result analysis and its efficiency in maintaining the security of users' data.

***Keywords*---**cloud computing, access control, attribute-based encryption, data protection, time performance.

Introduction

The world is witnessing great development in all fields, especially technical ones. Based on the large and recent developments in the technical fields, especially with regard to information technology, including computing models that include grid,

distributed and parallel computing, cloud computing can be considered the best among these models. Cloud computing can be defined as the application and development of computing technologies that can be accessed via the Internet. Since the term cloud computing is a new term, no specific definition has been provided for it. There are some definitions of it, one of the most famous and comprehensive of which is: According to the National Institute of Standards and Technology (NIST), cloud computing is defined as: “Cloud computing is a model for convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. As cloud computing facilitates the management and sharing of resources, it has become important in many areas such as education systems, Enterprise resource planning (ERP), E-Governance.

Cloud Security includes methods that help ensure that data is protected from potential threats **Error! Bookmark not defined.** ."In fact, the security services implemented by security mechanisms execute security policies". One of the most powerful driving reasons behind a user's choice to move to a cloud computing system or remain with their traditional system is their trust in service provider and their offers. Trust is determined by determining if a service provider has addressed all concerns, including data security, virtual machine security, and other compliance issues and government. Computer and information security is achieved by providing confidentiality, integrity, availability, authentication and non-repudiation services. Thus, the security aspects in educational system in cloud computing environment related to data protection, access control, and time performance will be examined in the proposed model.

The remainder of this paper is organized as follows: Section 2 presents a review of cloud computing including: definition and cloud computing applications. Section 3 discusses cloud security from aspect of: security service and data security issues. Section 4 shows access control as a security mechanism for cloud computing. 5th section shows data protection techniques, security practices of data protection, and protect data by cryptography. Section 6 discusses our proposed model namely SCES model. Then, an analysis and experimentation of the SCES model will be presented in the 7th section. Finally, a conclusion and future work of this thesis will be in the sections 8 and 9.

Cloud computing overview

Based on the large and recent developments in the technical fields, especially with regard to information technology, including computing models that include grid, distributed and parallel computing, cloud computing can be considered the best among these models. This model has allowed its users to have minimal involvement with a third party to reduce or increase their demands by enabling them to access its services with a seamless connection to cloud resources, The following figure (Figure 1) shows how different entities are connected to cloud computing.

Figure 1. 1 Cloud computing

Cloud computing definition

Cloud computing can be defined as the application and development of computing technologies that can be accessed via the Internet. As one of the modern computing methods, this definition means that multiple technological services are provided to the user in an information technology-based space via the Internet without the user needing to know detailed information about any services or technologies and without knowledge of the infrastructure on which these services are based. This general definition is used to express the provision of the necessary modern technologies that are provided to users, such as web services and software as a service, and with issues related to them, so that they provide all the requirements that users need in an area that is accessed via the Internet. When users want to access any resources quickly and with less effort and without interaction with the provider, here cloud computing can be considered the ideal model to enable users to easily access when they need any configurable pool of computing resources.

Since the term cloud computing is a new term, no specific definition has been provided for it. There are some definitions of it, one of the most famous and comprehensive of which is: According to the National Institute of Standards and Technology (NIST), cloud computing is defined as: “Cloud computing is a model for convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. Cloud computing facilitates the tasks of users and solving their problems, and since the Internet does not show much detail to its users, it is likened to the cloud, so the word “cloud” was used to denote the Internet. It sets an abstract separation between users and technical details.

Cloud computing applications

Due to the characteristics of cloud computing, and the benefits and facilities it provides, its use has spread in many technologies and fields, including, for example: Social Networking, Business, Cloud Storage, health care, and educational systems.

Using cloud computing at educational system

Education services in the cloud computing environment provide an enjoyable and attractive environment for teachers, researchers and students, where they can access to their organization cloud to use their data, and take advantage of the facilities provided by these services such as: virtual classrooms, virtual labs, class recording, E-mail, files broadcasting, simulation tools, education forums, surveys etc.

Saudi educational system in cloud computing environment

Education in the Kingdom of Saudi Arabia is a guaranteed right for every individual in it, and the Saudi government has endeavored to develop education in all respects in terms of educational curricula, professional development for teachers, and provision of buildings and support with what they need for the educational process. The Kingdom of Saudi Arabia in supporting education despite the difficult circumstances that occurred during the COVID-19 pandemic. Whose impact was not limited to education, but to the entire natural life in all countries of the world, which prompted the world to take preventive measures to limit its spread, and these measures reached the enforce of distance education in all educational levels. This pandemic was not an obstacle to completing education. Rather, the Saudi government, represented by the Ministry of Education, provided electronic education systems based on cloud computing so that students could continue to receive their education and communicate with their teachers through it.

At the time when Saudi schools were closed on March 8, 2020, the Ministry of Education transferred its students to these electronic systems represented in the 'Madrasati' platform, which is an integrated educational platform that was created in cooperation with Microsoft, which provided accounts for all users of this platform, including students, teachers, administrators and parents, and the student logs into his account On the platform, he can obtain the academic courses in their electronic copies, as well as enter the virtual classes and perform assignments and tasks. The transition to distance education put students, teachers and parents in front of many challenges **Error! Bookmark not defined.**, perhaps the most prominent of which are the permissions to enter the platform and other problems related to the privacy and confidentiality of their data. Even before the Corona pandemic, the Ministry of Education provided a set of electronic systems that serve the educational process in terms of managing grades and results, as well as the administrative aspects of the ministry’s employees. The next screenshot shows the main interface of some educational systems in Saudi Arabia like: Mardasti platform, Noor System, and Faris system.

Figure 2. Educational systems in Saudi Arabia

Cloud security

This section shows security aspect for cloud computing including security service and data security issues.

Security service

Security includes methods that help ensure that data is protected from potential threats."In fact, the security services implemented by security mechanisms execute security policies". One of the most powerful driving reasons behind a user's choice to move to a cloud computing system or remain with their traditional system is their trust in service provider and their offers. Trust is determined by determining if a service provider has addressed all concerns, including data security, virtual machine security, and other compliance issues and government. Computer and information security is achieved by providing confidentiality, integrity, availability, authentication and non-repudiation services.

Data security issues

Based on the requirements of each aspect of the CIA standard, this study. provided a classification for each aspect in terms of data and Virtualization. We will discuss from them what is related to the data in terms of confidentiality and integrity, as it is the focus of our interest in this research as shown in Table 1:

Table 1
Data issues classification

	issues
data Confidentiality	1-client data segregation 2- The actual geographical location of the user's data 3- Improper or incomplete data deletion by the CSP 4- third-party assistance for data-backup services 5- CSP does not allow consumers to encrypt their data. 6-Service providers' curiosity to know the contents of users' files
data Integrity	1- Data outsourcing 2- SQL injection attack 3- Cross scripting attacks 4- Metadata Spoofing

	attack 5-Wrapping attack

Study dealt with data security in cloud computing, Cloud security has been classified into several categories, as shown in the following figure (Figure 3):

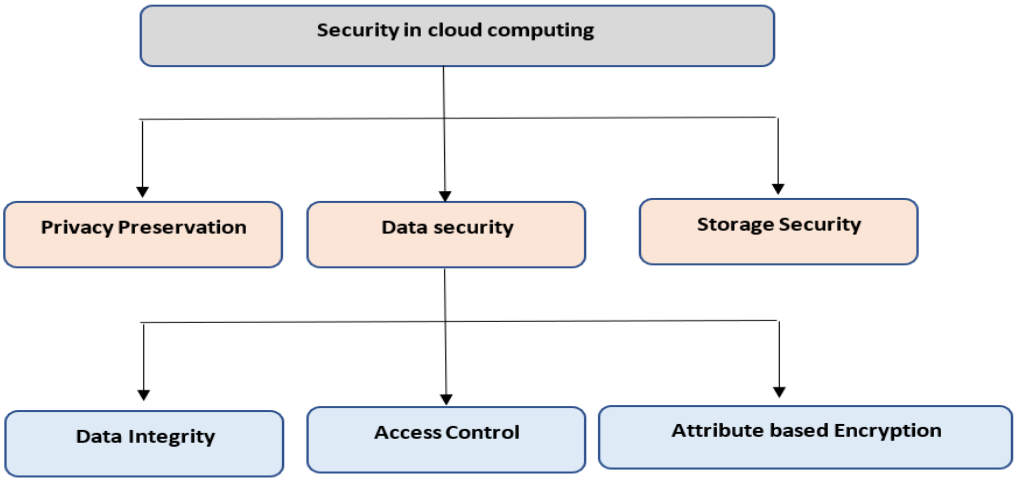


Figure 3. Security Classification in cloud

Access control as a security mechanism for cloud computing

Security mechanisms play an effective and important role in defending against potential threats, so it is important to use multiple kinds of security mechanisms and services. These mechanisms must take into account a number of common limitations and requirements, such as support for mobile devices or any other entity such as virtual machines, and reduce latency, and other considerations, and security mechanisms that can be used include the following:

- Access Control Systems
- Identity and Authentication.
- Privacy
- Protocol and Network Security
- Intrusion Detection Systems
- Trust Management

Access control policies must be defined in order to be applied in a correct manner, through a set of appropriate and correct control rules, also priorities must be set, and they are an essential component of policies.

Basic elements of access control

The main objective of access control technique is to restrict a subject's access to objects, by allowing a subject to access an object where it allows access to resources in a legal rules. The access control model consists of three main components: access control policy, object and subject. Subject: It is the active party requesting access, in other words it is the access attempt initiator. Object: It is the passive party that receive access attempt from other parties, in other words, it is the access attempt recipient. Access control: it is group of rules that control the subject's access to the object the following figure (Figure 4): shows the main components and the decision-making method for authorization through access control.

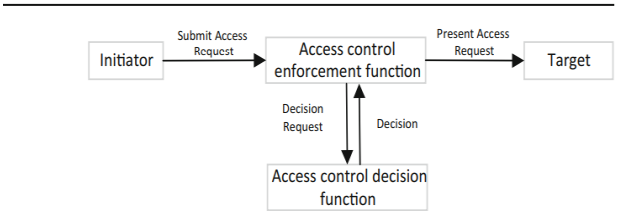


Figure 4. The process of access control

To describe the system's access control policies The following access control matrix can be used.

Table 2
Access control matrix

	$Object_1$	$Object_2$	,,,,,,	$Object_n$
$Subject_1$	Own, read, write	Write	,,,,,,	Own, read, write
$Subject_2$	Read	Read,	,,,,,,	Write
,,,,,,	,,,,,,	,,,,,,	,,,,,,	,,,,,,
$Subject_n$	Read, write	Read	,,,,,,	Own, read, write

This model demonstrates the method of accessing a subject to an object, using a reference observer that controls access based on this matrix, as shown in Table 4.1. Lampson summarized the access control problem and proposed a graphic representation using the access control matrix, subject and object.

Access Control models

The following table (Table 3) presents some studies that discussed access control methods used in cloud computing.

Table 3
Access control models

Access Control models	2021	2020	2020	**Error! Bookmark not defined.** 2019	2018	2018	**Error! Bookmark not defined.** 2018	2017
Discretionary Access Control (DAC) model	✓	✓			✓		✓	✓
Mandatory Access Control (MAC) model	✓	✓			✓		✓	✓
Role-based Access Control (RBAC) model	✓	✓			✓		✓	✓
Attribute-based Access Control (ABAC) model	✓	✓		✓	✓		✓	✓
Usage-control-based Access Control (UCON) model				✓	✓			
Reference monitoring Access Control (RMAC) model					✓			
Proxy re-encryption (PRE) model					✓			
Task based access control	✓			✓				
Action based access control				✓				
Organization Based Access Control (OrBAC)								✓
Attribute-Based Encryption Access Control (ABE Access Control model)		✓	✓	✓	✓	✓		✓
Hierarchical Attribute-Based Access Control (HABE)							✓	
Attribute-Based Encryption Fine Grained Access Control (ABE FGAC)							✓	
Identity-Based Encryption (IBE)		✓						
Towards Temporal Access Control (TTAC)		✓						
Capability-Based Access Control (CBAC)		✓						
Purpose Based Usage Access Control (PBAC)		✓						
Novel Data Access Control		✓						

Model (NDAC)								
Gateway Based Access Control Model (GBAC)		✓						

Attribute-Based encryption

Studies have shown that access control mechanisms that use symmetric encryption techniques or traditional public key encryption techniques lack scalability and flexibility**.** In symmetric encryption, every time a new user enters the system, the owner of the data must share a shared secret key with him, which is used to encrypt the owner's data again. As well as traditional public key encryption when a new user enters ,the data owner must encrypt his data with the new user's public key, which may differ from the public keys of previous users, which means that the shared secret keys and public keys are required from the data owner in order to outsource his data to the cloud. Scalability and flexibility play an important role in access control policies and their impact on the accession of new users to the access control system**.**Attribute-based encryption technology came to help implement access mechanisms accurately and scalability, where a set of attributes are placed in ciphertext, and the data owner does not need to know the identity of the user before encryption, and when a new user joins the system ,this does not affect the data owner and does not require him to act anything, this ensures the scalability and flexibility of attribute-based access control systems **Error! Bookmark not defined. .** Attribute-based encryption attracted researchers and was the first to introduce the term ABE Sahai and Waters * as a promising field in cryptography.

ABE model components

Authority: Its role is to provide users and data owners with the keys, data owner: uses the attribute set and the public key to encrypt the data, data users: they use their private key to decrypt the ciphertext and get the data **Error! Bookmark not defined.** . the next figure shows Architecture of ABE model:

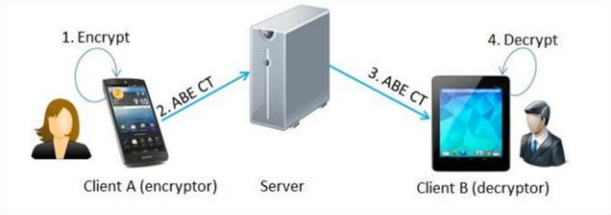


Figure 5. Architecture of ABE model

ABE categories

Attribute-based encryption comes in two main categories: ciphertext-policy ABE which is referred to by the acronym CP-ABE and key-policy ABE which is referred to by the acronym KP-ABE. The following table (Table 4.3) provides a comparison between these two types through a number of criteria:

Table 4
Compression between CP-ABE and KP-ABE

	CP-ABE	KP-ABE
access policy	The access policy is defined in the ciphertext.	The access policy is known by encoding it in a user's attribute secret key (user's private key).
user's attribute secret key	user's attribute secret key (user's private key) is associated with user's attributes sets.	The ciphertext contains user's attributes sets.
access tree structure	The private keys for decryption must meet the policies defined by the encoder using the access tree structure **Error! Bookmark not defined.** .	The KP-ABE model defines the user's private key by means of the access tree structure, and the attributes of user are contained in the leaves **Error! Bookmark not defined.**.
decrypt	The user can use a given key to decrypt the ciphertext if and only if the access structure matches the attributes associated with the private key of the tree nodes **Error! Bookmark not defined.** .	The user can use a given key to decrypt the ciphertext if and only if the access structure matches the attributes associated with the ciphertext **Error! Bookmark not defined.**.

Encryption based access control

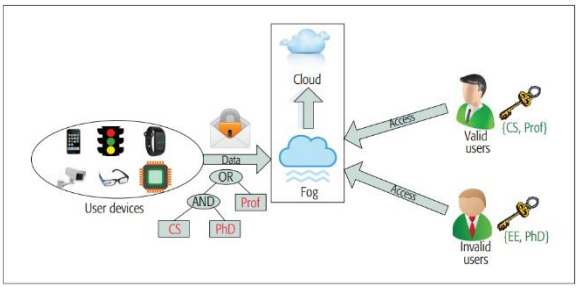


Figure 6. ABE-based access control

Cryptographic-based access mechanisms achieve integration by combining access control based on policies and an encryption algorithm. There are several models of encryption-based access mechanisms, including the attribute-based encryption **Error! Bookmark not defined.** discussed in this thesis Specifically, CP-ABE type.

Data protection techniques

The problems of data privacy, anonymity, security and reliability are among the prevailing problems associated with the transition from traditional computing to cloud computing services, the most important of which is security, which the service provider should ensure to its users.

Security practices of data protection

The service provider must ensure many security practices and choose the best and most appropriate in traditional information technology or in cloud services, so that the service provider ensures maintaining the security of infrastructures in a manner that preserves authentication, availability, integrity and confidentiality of data. These practices include the following:

- •Encryption: The host operating system software uses encryption mechanisms that preserve sensitive data, by encrypting this data, and encrypting network traffic.
- Physical security: Environmental security and physical protection such as doors, an important element for maintaining data stored in virtual systems and cloud service hosts.
- Authentication and access control: Authentication can be provided in virtual systems through authentication methods in physical systems such as face recognition and fingerprint recognition, and additional capabilities must be included in these systems that help authentication and access control, such as: passwords.
- Sending data from one cloud to another also requires authentication, a digital signature can be used to authenticate the message when it is sent from one party to another.
- Separation of duties: There must be accountability and verification of the enforce of the least privilege, in order to reduce the occurrence of configuration errors resulting from insufficient communication or inexperience, which may result from increasing the complexity of the system.
- Configuration, change control, and patch management: One of the mistakes small organizations sometimes make is ignoring change control, configuration, and patch management, so configuration, operations, and patch management must be kept up-to-date in the physical or virtual world.
- Intrusion detection and prevention: These mechanisms enable to know what is going out from or coming into the network, by monitoring network traffic with hypervisor-based solutions, as well as intrusion prevention and detection systems.

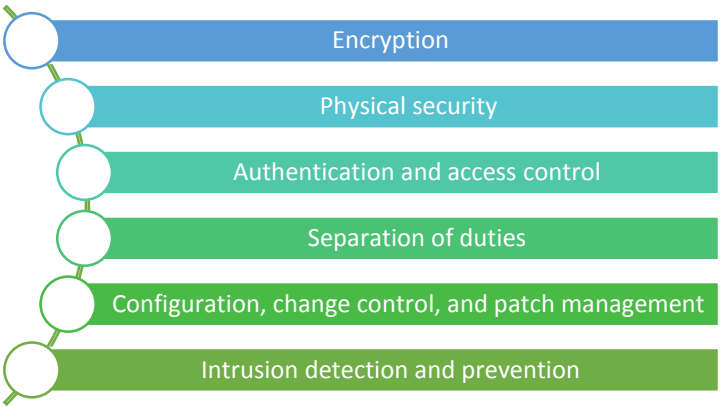


Figure 7. Security practices of data protection

Protect data by cryptography

Cloud security is concerned with securing processing operations (computations) and storage capabilities (service provider databases). The data confidentiality in cloud computing can be maintained using cryptography. Cryptography is the science of designing and analyzing algorithms that transform data from its original form into an incomprehensible form, so that it becomes incomprehensible to anyone else who is not authorized to access it, and that makes it accessible and understood by authorized persons only. Cryptography consists of three basic components: the plaintext, the encryption and decryption algorithms, and the ciphertext, As shown in the following figure (Figure 8):

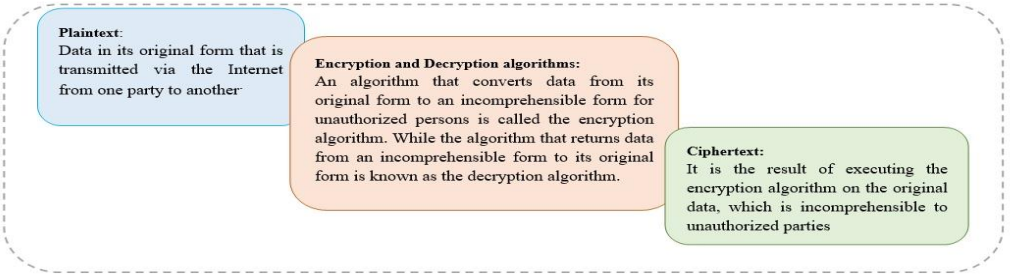


Figure 8. Cryptography basic components.

Cryptographic algorithms are classified into two main types:

- Symmetric Key Encryption Algorithms.
- Asymmetric Key Encryption Algorithms.

The following table produce comparison between these two categories:

Table 5
General comparison of the main types of cryptographic algorithms

SYMMETRIC KEY ALGORITHMS	ASYMMETRIC KEY ALGORITHMS
Referred to as the Secret Key (SK) Encryption Algorithm.	Referred to as the Public Key (PK) Encryption Algorithm.
A same one key used for encryption by the sender and decryption by the receiver.	Two keys are used, one called the public key used by the sender for encryption, and the other called the private key used by the receiver for decryption.
Most popular symmetric encryption algorithms: • Data Encryption Standard (DES). • Triple Data Encryption Standard(3DES). • Advanced Encryption Standard (AES). • Blowfish.	Most popular asymmetric algorithms: • RSA (Rivest-Shamir-Adleman). • ECC (Elliptic-curve cryptography). • Deffie Hellman (DH).

Semwal and Sharma, mentioned Key exchange is the biggest challenge in symmetric key encryption, so it must be kept confidential and protected from

intruders, and they concluded that when message integrity and privacy are paramount, the AES algorithm is preferred. Based on Khan & Tuteja's research, Cloud computing contains a huge number of databases, so the use of asymmetric encryption algorithms is slower than the use of symmetric encryption algorithms, asymmetric encryption algorithms can be used to create encryption keys. Asymmetric encryption algorithms are commonly used in cloud computing are: RSA, DH, IKE, and symmetric encryption algorithms are commonly used: DES and AES. Symmetric key encryption algorithms require less power to process computations, so they are almost a thousand times faster than asymmetric key encryption algorithms that require higher power.

To ensure the security of cloud computing, symmetric encryption algorithms such as DES, 3DES ,AES, and Blowfish can be used. The DES algorithm is easier to implement than the AES algorithm. Asymmetric encryption algorithms such as RSA and (DH) Diffie-Hellman can also be used, however there is still a need to develop improved algorithms aimed at increasing the level of cloud computing security. According to Mahalle & Shahade research, using more than one encryption algorithm provides higher security than using one algorithm alone, which makes intruders access to data a difficult task. Therefore, we proposed in this thesis the use of a complex encryption technique, which combines the symmetric encryption algorithm AES and the RSA encryption algorithm. Using the secure health related data [39-44] and the use of 5G technologies with other cutting edge technologies for the data transfer including the blockchain, ransomware protection, etc. can enable more data security. The following table (Table 6) presents a comparison between the most famous symmetric and asymmetric encryption algorithms used in cloud computing based on a set of factors that were addressed by a group of some previous studies:

Table 6
Comparison between symmetric and asymmetric encryption algorithms used in cloud computing

Researches	Factors	Symmetric-key algorithms				Asymmetric-key algorithms		
Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms †		DES	3DES	AES	Blowfish	RSA	ECC	Diffie Helman
	Developer	IBM in 1975	IBM in 1978	Joan Daemen and Vincent Rijmen in 1997	Bruce Schneier in 1993	Ron Rivest, Adi Shamir, and Leonard Adleman in 1977	Koblitz and Miller in 1985	Witfield Diffie and Martin Hellman in 1976
	Key length	56 bits	K1, k2, k 3 168 bits	128,192, 256	32-448 bits (128 by default)	1024 bits	112 bit to 512 bit	2013,224 bits for q and 2048 bits for p
	Scalability	It is scalable algorithm Due to varying	168,112 or 56	Not scalable	Scalable	Not scalable	Scalable	Scalable

		the key Size and block size.						
	security	Security applied to both providers and user		Secure for both provider and user	Secure for both providers and user/client side	Secure for user only	Based on difficulty of generating key	Vulnerable and secure against eavesdropping
A comparison of symmetric key algorithms DES, AES, BLOWFISH, RC4, RC6: a survey ‡		Not structure, Enough, Already Broken §	Adequate security	Excellent security	Excellent security			
	Flexible	No	Yes	Yes	Yes	-	-	-
A survey on cryptography algorithms **			-			No	Yes	Yes
	Speed	-	-	-	Fast Cipher in SSL	Low Speed	fast Speed	Low Speed
Security of Low Computing Power Devices: A Survey of Requirements, Challenges & Possible Solutions §		Slow	Slowest †	Fast	Fastest †	-	-	-
	Block Size	64bits	64 bits	128 bits	64 bits	128 bits	Variable	-

The proposed model

This section proposes Secure Cloud Education System (SCES) model which ensures different aspect such as access control management, data protection, and time performance. This chapter focuses on the concerns associated to the data protection aspect, in cloud computing such as, confidentiality and integrity. It's called a Secure Cloud Education System (SCES) which ensures different aspect such as access control management, data protection, and time performance. Moreover, it presents and describes the architecture of the proposed SCES model. Then it will define the components and layers of SCES model. The outcome and execution of the new proposed model will be examined to present the security elements in the proposed model, for example access control management, data protection and time performance. SCES model control the access to the educational system with ABE-Access control model, and helps protect data after authorization with appropriate combined encryption techniques (AES+RSA). The main aim of the proposed new model is to increase security, avoiding the risks of hackers and intruder in the cloud educational system.

Overview of cloud model

Figure 9 presents an overview of the educational system in the Kingdom of Saudi Arabia in the cloud computing environment, it shows the users of the educational system with different attributes, whether they are students, teachers, parents, and administrators. Users can login to their accounts in the education system with the username and password provided by the educational system, it means they send requests to access and request some files from the cloud system, which must be secure and keep data confidential Stored in cloud databases.

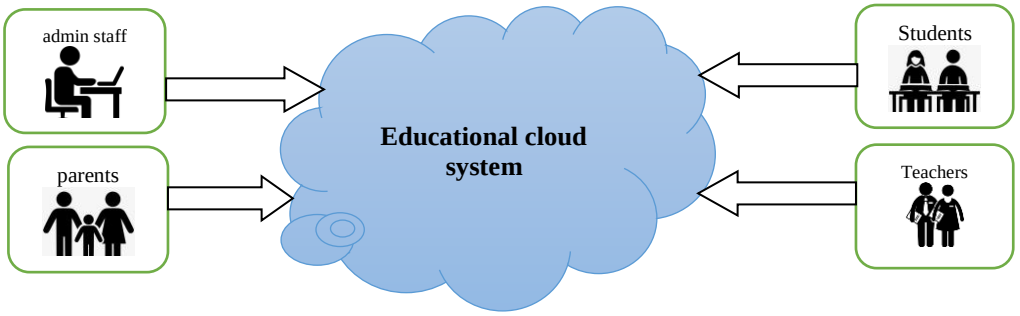


Figure 9. Overview in educational cloud system

The Proposed SCES Model

SCES model provides a secure educational system in cloud computing environment by restricting access by using Attribute-Based encryption Access Control model, which is one of the cryptographic-based access mechanisms, that combines access control based on defining access policies and applying cryptographic algorithms, and this reduces the access of intruders and hackers to the system. SCES model also maintains on the security, confidentiality and integrity of data through the use of appropriate combined encryption techniques (AES+RSA), instead of using one technology, it increases the security of the data and protects it from intruder access. Figure 10 shows the SCES proposed model architecture.

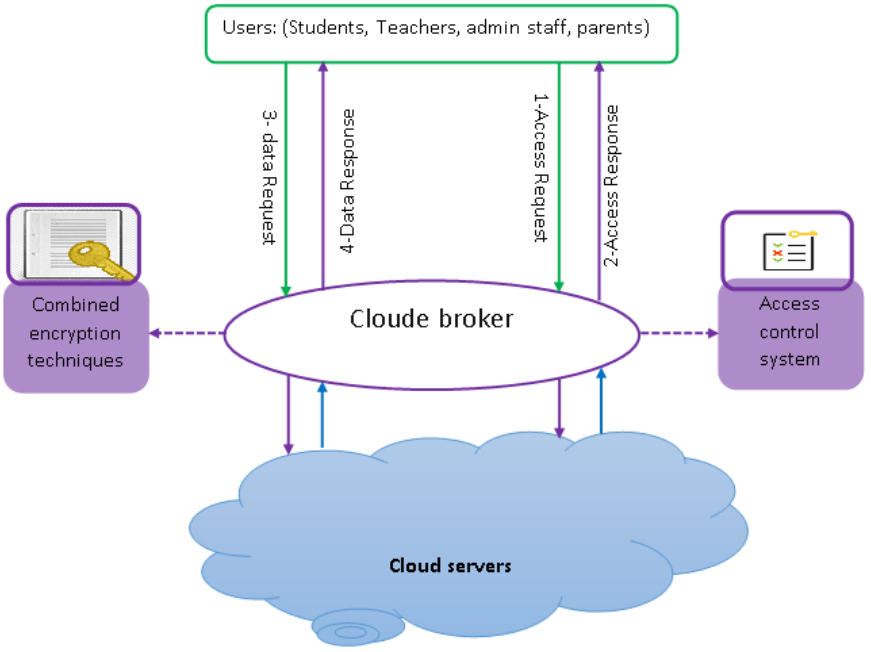


Figure 10. SCES proposed model architecture.

SCES Components

As is clear from the Table 6.1, that SCES model consists of several components: users, access control system, combined encryption techniques, cloud broker, and cloud servers (Data center). First of all, users of the educational system, whether they are students, teachers, admin staff or parents, they login to the educational system through user interface using Internet browser. User interface asks him to enter the login data: the user's name and the password that he was previously provided with from the educational system. After the user's login data is entered, the browser sends it as an access request through the cloud broker, which in turn passes it to the cloud service provider and then back to the data owner. Through the use of the access control system provided by the cloud broker, the data owner allows the user to access the system through Attribute-Based encryption access control. This is done by generation the encryption and decryption keys by the attributes authority server (Key distribution), The data owner uses the encryption key to encrypt the data, and the cloud broker uses the decryption key to decrypt the data and return it to the user, the response is returned to the user and he arrives at the site.

Here lies a security risk in the event that an unauthorized person accesses the user's data illegally, and thus may be able to request and view users' data and violate their privacy, so we proposed a combined encryption techniques that uses the AES algorithm to encrypt user data and to increase security this system encrypts the secret key of the AES algorithm using the RSA algorithm. The AES algorithm provides high security for user data, and is characterized by its speed of encryption as it is one of the symmetric encryption algorithms that use a one secret key, where the encryption speed factor is an important factor when dealing

with a huge amount of data as in cloud computing. The RSA algorithm is also more secure because it uses more than one key, so it is used to encrypt the secret key of the AES algorithm, where the volume of data in this case is suitable for its use.

Through the cloud broker, the key distribution center provides the data owner with the data encryption key for AES algorithm (secret key) and the public key for RSA algorithm, and provides the decryption system with the private key for the RSA algorithm, the data owner encrypts the users' data with the AES secret key and then encrypts the secret key with the RSA public key. After that, the encrypted user data file is sent with the encrypted AES secret key. When the encrypted data reaches the decryption system, it decrypts the AES secret key using his RSA private key, then decrypts the data using this AES secret key resulting from the decryption.

Table 7
SCES Model's components

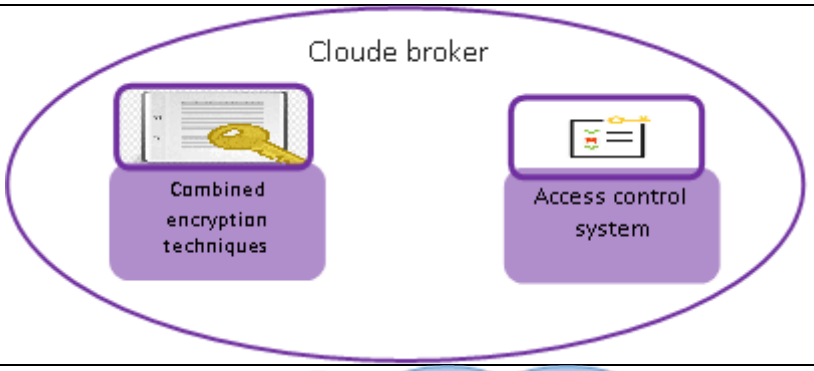
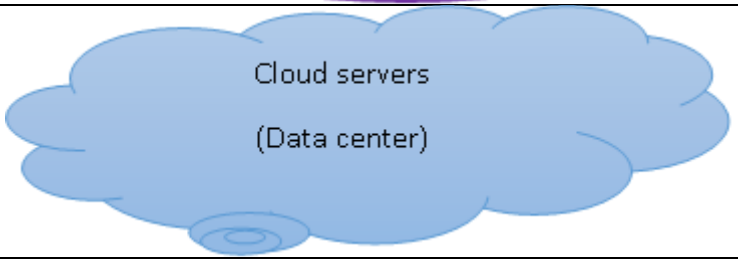
SCES Component	Description
Users	This component represents the users of the educational system, including students, teachers, administrative staff, and parents
Cloud broker	It is the broker between the users of the educational system and the cloud servers, it provides the following services: Access control system: It represents the proposed method of access control which restricts the access of unauthorized persons to enter the system, it is a method that uses Attribute-Based encryption access control Combined encryption techniques: It represents the proposed method to protect data in the event of unauthorized access to this data, which is a method that protects data using a combination of AES encryption and RSA encryption
Cloud servers (Data center)	It contains data of all educational system (users – data owner)

SCES Layers

SCES model contains three layers. Table 8 shows the three layers which are application layer, administrative layer, and cloud servers layer. In the application layer, it includes the browser of users. Administrative layer it includes cloud broker that responsible for implementing access control system and combined data encryption techniques. The last layer is cloud servers layer that contains cloud servers (Data center) which contains data of all educational system (users – data owner)

Table 8
SCES Layers

Layers	SCES Component
Application layer	Browser of users

Administrative layer	
Cloud servers layer	

SCES Model Data Flow

This section explains the data flow in the SCES model, starting with the user entering the educational site, and entering his login data, which is sent to the cloud servers by cloud broker. That sends the request and returns the response in a way that ensures that access is restricted to authorized persons only, then the user requests his data and the broker again sends it to the cloud servers and returns the data in a way that is protected by combined encryption techniques. As shown at Figure 6.3.

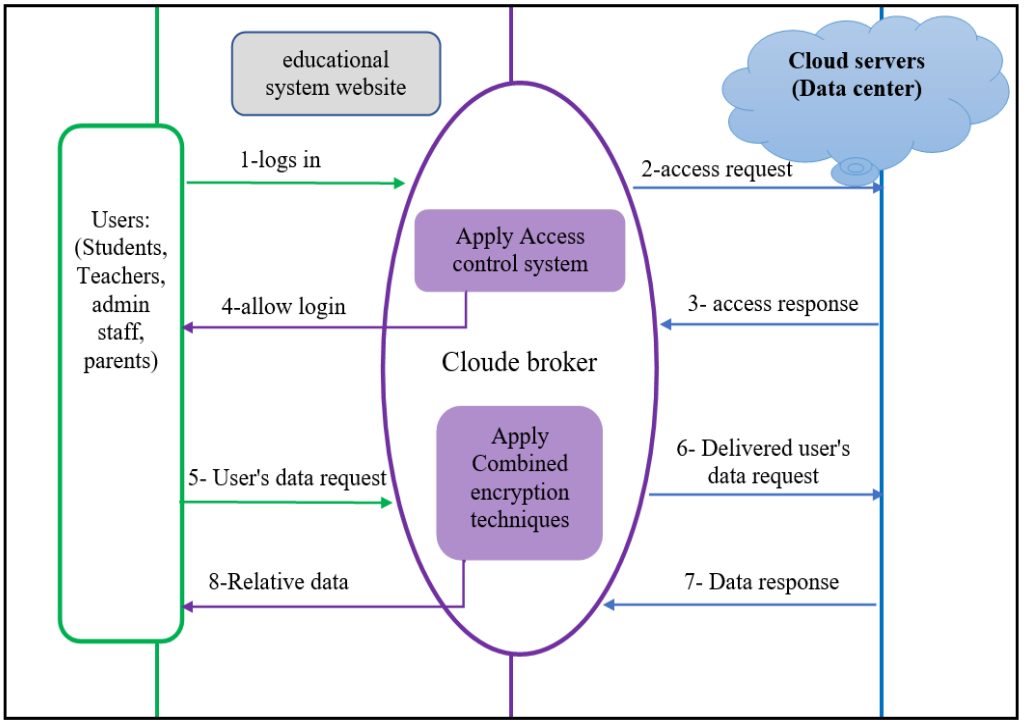


Figure 11. SCES data flow

Access control system

The use of educational systems in cloud computing environment is beneficial and provides a pleasant and attractive environment for users. Where they can benefit from traditional services, but electronically, such as virtual classrooms, virtual laboratories, e-mail services, as well as office programs. This moves to educational services in an electronic form put its users in front of challenges related to the security of their data and the preservation of its privacy from intruders. Therefore, it is necessary to provide security mechanisms to defend potential threats, and the diversity of mechanisms gives an increase in the level of protection, taking into account the support of these mechanisms for different devices. Users can access the educational system's website using the data given to them by the educational system (username and password). The login is considered as an access request, which is sent to the cloud server through the cloud broker who, in turn, implements the access policy proposed in the SCES model. After the user's access to the system is verified, he is allowed to enter the system by replying to the request.

Implementation of access control mechanisms helps authenticate users and allows only authorized persons to enter after verifying their identity, and also helps in monitoring network security, by defining and properly implementing access control policies that are an essential component of any access control model. The authentication process goes through multiple stages through which the attribute-based encryption access control mechanism is implemented. Users log in to the education system site and then the login attempt is sent as a request

to access services from the user to the cloud servers. This is done by the cloud broker that plays an important role between the users and the cloud servers where it manages the use of cloud services and organizes the operations between users and cloud servers, the cloud broker should be flexible in choosing the appropriate services for users, and it can combine several services into one service. This process shown in Figure 12.

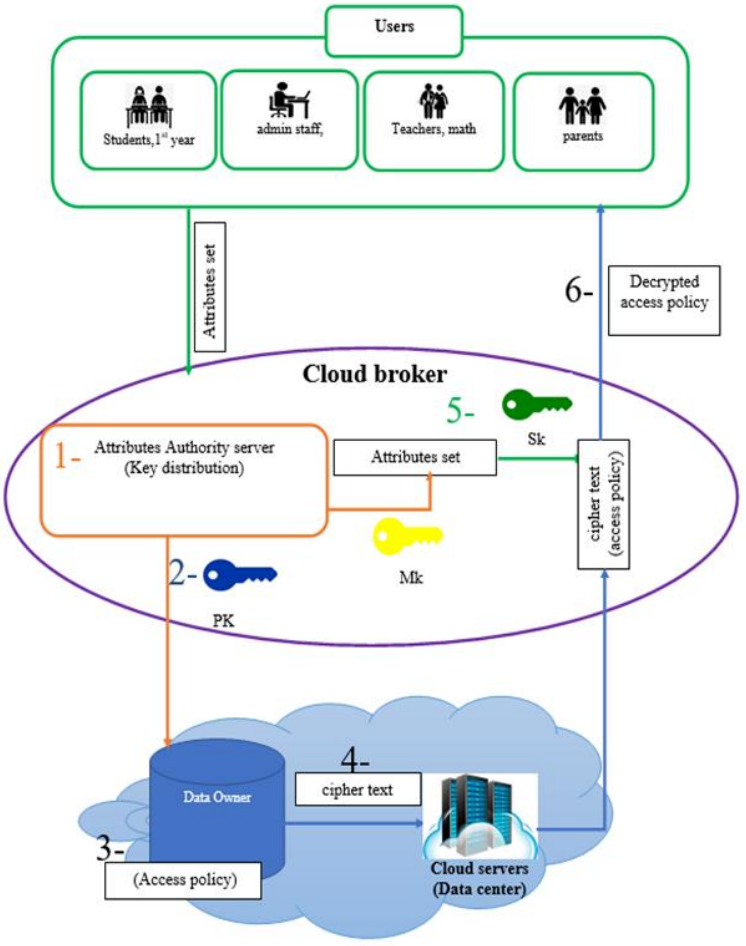


Figure 12. Access control system based on attributes sets (Access policy)

In the proposed model, the cloud broker helps improve security by authenticating users and controlling their access to services through the use of an access control system that uses the attribute-based encryption access control model, which is one of the types of access control mechanisms that rely on encryption and achieves integration through combine policy-based access control with implementing encryption algorithms. The use of attribute -based encryption in access control mechanisms is more flexible and scalable than symmetric and asymmetric encryption. This flexibility is important when new users join. The type CP-ABE in which access policies are defined in ciphertext is more suitable for use

in a cloud environment, because access policies are defined by the owner. Cloud broker provides access control system by providing the following:

- The Attribute Authority (key generation): generate system keys, Public key (PK) and Master key (MK).
- Public key (the encryption key) sends to the data owner.
- The data owner defines access policies that define who can access the system based on their attributes, and encrypts these policies with a public key that results in a ciphertext.

Ciphertext= Encrypt (PK, Access policy)

- This ciphertext sent to the cloud server that sends it to the cloud broker.
- (SK) Secret key (the decryption key) generated by Attribute Authority based on their attribute set provided by cloud broker from users, using MK provided by Attribute Authority.
  SK= generation (MK, attribute set)
- Ciphertext that contains the access policy will decrypt with secret key (SK) if user attributes set included in his secret key match the access policy specified in the ciphertext, then he can access the system.
  Access policy = Decrypt (SK, Ciphertext)

Combined encryption techniques

As mentioned previously, the goal of the proposed SCES model is to provide security for educational system, which can be achieved by enforcing access policies that prevent unauthorized persons from accessing the systems, but we may face a new challenge in the event of unauthorized persons accessing the system and tampering with users' information of these systems. Therefore, a solution to this challenge was presented, which is the use of combined encryption techniques. Encryption contributes to maintaining the privacy of data, and protecting it from tampering from intruders on the system from unauthorized persons, who access these data in an illegal and illegitimate manner, with the aim of penetrating its privacy for any purpose.

The use of encryption algorithms in the educational system helps to convert data from its original form to a form incomprehensible to unauthorized persons. Only authorized persons must be provided with keys to decrypt this data and return it to the original form. Each common type of encryption has several advantages, whether it is symmetric or asymmetric encryption, since previous studies showed that symmetric encryption algorithms are faster in encryption than asymmetric encryption algorithms when dealing with large databases such as the one in the cloud-based educational system, it was proposed to use the AES algorithm as one of the ways to protect user data in the educational system which may consume a shorter time compared to the rest of the algorithms. Since the use of combined encryption increases the security of data and makes it more difficult for intruders to access it, the RSA algorithm has been proposed to encrypt the AES algorithm key previously used to encrypt user data. When the user again requests access to his data stored in the educational system, this request is passed to the cloud servers through the cloud broker also, which in turn applies combined encryption

techniques that uses the AES algorithm to encrypt user data and to increase security this system encrypts the secret key of the AES algorithm using the RSA algorithm. This process shown in Figure 13:

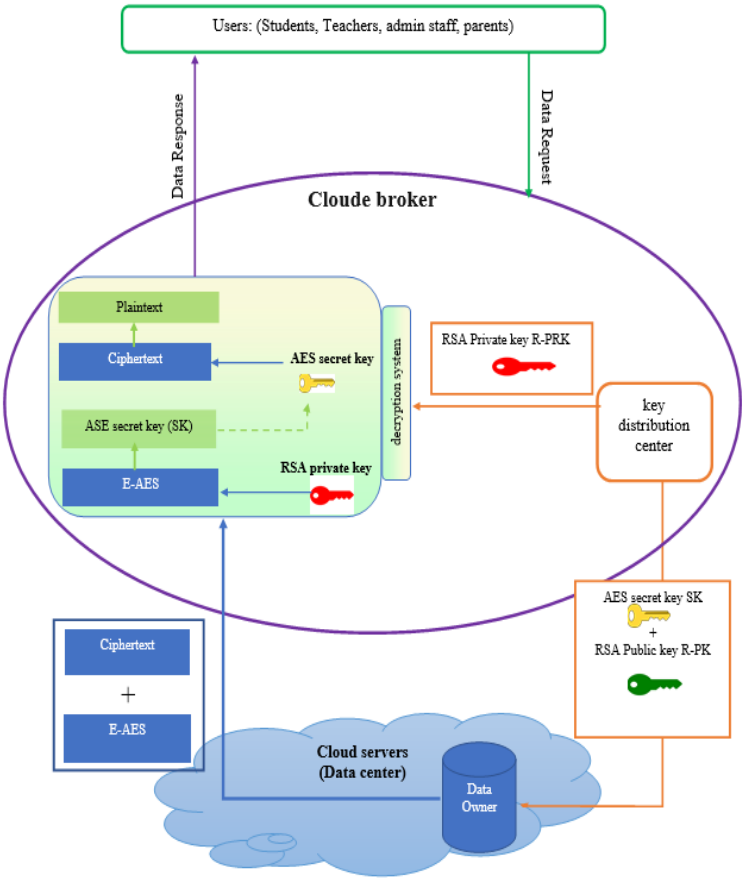
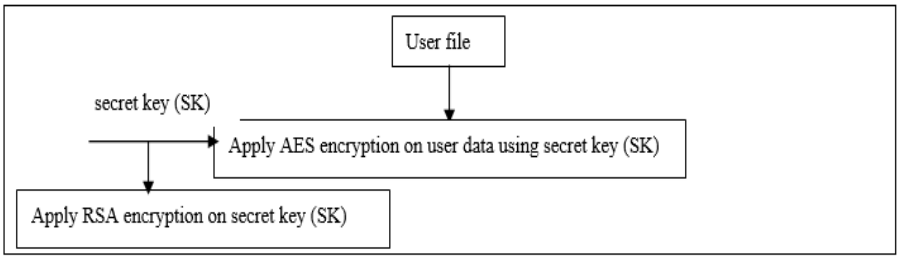


Figure 13. Combined encryption techniques using AES and RSA encryption algorithms.

Cloud broker provides combined encryption techniques by providing the following:

- The key distribution center: generate system keys, AES secret key (SK), RSA Public key(R-PK), and RSA Private key(R-PRK).
- Data owner receive two keys from key distribution center, they are:
- AES secret key (SK): the data encryption key to encrypt user data (Plaintext) and produce cipher text.
- RSA Public key (R-PK) to encrypt AES secret key.



- The data owner encrypts user data using AES secret key, to produce encrypted data as Ciphertext:
  Ciphertext= Encrypt (SK, Plaintext)
  And encrypt AES secret key using RSA Public key, to produce encrypted AES secret key (E-AES):
  E-AES = Encrypt (R-PK, SK)
  And send all to cloud broker.
- Cloud broker apply decryption operation via decryption system as follows:
  using RSA private key (R-PRK) to decrypt E-AES and extract AES secret key.
  SK=decrypt (E-AES, R-PRK)
  Using SK to decrypt Ciphertext and extract user data as a Plaintext:

  - Plaintext= decrypt (Ciphertext, SK)

The data will be sent back to the user upon his request.

Requirements analysis

This section presents different types of analysis, theoretical analysis and practical analysis of our SCES proposed model which aimed to addressing cloud security issues in educational cloud system such as access control management, data protection, and time performance. First of all, in the theoretical analysis, we will summarize what we discussed in literature review with regard to access control models, which were presented in the Table 4.2, as some of these models based on cryptographic and others non-cryptographic models. The cryptographic-based models are characterized by that they combine the possibility of defining the access policy and applying encryption algorithms, which gives the access control model a higher level of security. One method of them is Attribute-Based Encryption Access Control which we proposed in our SCES model. Attribute-based encryption is divided into two parts as shown in the Table 4.3, CP-ABE was chosen as the most suitable for use in cloud systems, as the access policy is in the hand of the data owner.

Also, a practical analysis of SCES model will be presented through the experiment of the proposed encryption system to protect the data of users in the educational system when it is stored on data centers in cloud servers. Firstly, this section explains SCES scenarios with its components. Secondly, in relation to cloud security, this section examines data encryption and decryption procedures. Thirdly, in relation to cloud performance, this section summaries the experimentation of our proposed model. The experiment for studying efficiency

and time performance of the SCES model and to show the procedures of data encryption and data decryption works.

SCES Scenarios

As it is clear in section 6 of our proposed SCES model, SCES model uses Attribute-Based encryption Access Control model to provide a secure educational system in cloud computing environment by restricting access to the system, which is one of the cryptographic-based access mechanisms, that restricts access based on defining access policies and applying cryptographic algorithms, and this increase security and reduces the access of intruders to the system. And we aimed to protect users' data stored in cloud servers. When the user requests access to his data stored in the educational system, this request is passed to the cloud servers through the cloud broker, which in turn applies combined encryption techniques that uses the AES algorithm to encrypt user data and to increase security of SCES model, the cloud broker system encrypts the secret key of the AES algorithm using the RSA algorithm.

Data storing (Data encryption from the user to the cloud)

When the data is stored by the user, it is sent to the cloud service provider through the cloud broker, which applies the encryption techniques to this data in preparation first for storing it on the cloud server. The key distribution center in the encryption system generates the system keys, which include the secret key of the AES algorithm, and sends it to data owner, who uses it to encrypt the data, also provides him with the public key of the RSA algorithm, which he uses to encrypt the secret key used to encrypt the data.

Data retrieval (Data decryption from the cloud to the user)

When the data is requested by the user, it is retrieved from the cloud service provider through the cloud broker, which keeps the RSA private key that was previously generated with the public key of the RSA algorithm and used by the data owner to encrypt the secret key of the AES algorithm. The data is retrieved in its encrypted form from the cloud server data center. The decryption system in the cloud broker decrypts the AES secret key using the RSA private key, then this key is used to decrypt the data and return it back to the user in its original form.

Data Security Analysis

This section presents data security analysis in our SCES proposed model.

Access control system

The security of the data in the SCES proposed model can be ensured through the implementation of an access control system, which restricts people’s access to the educational system, by enforcing access policies through ABE access control model, thus increasing the level of security by combining the identification of access policies and the application of cryptographic algorithms. The type CP-ABE

in which access policies are defined in ciphertext is more suitable for use in a cloud environment, because access policies are defined by the owner.
Enforcing the access control system enables the system to authenticate users, and thus helps protect the privacy and confidentiality of their data stored in these systems.

Data protection techniques

To protect the data in the SCES model and ensure its privacy and confidentiality, we used combined encryption techniques, which use symmetric encryption algorithms and asymmetric encryption algorithms. Because symmetric encryption algorithms are faster in implementation than asymmetric encryption algorithms, they were used to encrypt user data on the system, and to increase security we used the RSA algorithm to encrypt the key of the AES algorithm, this combined encryption makes it difficult for intruders to access the data in its original form.

Time performance

The use of encryption techniques leads to better performance, through the use of encryption technology appropriate to the data size. Due to the speed of symmetric encryption techniques in encryption compared to the asymmetric encryption techniques, the AES algorithm was used as a faster encryption process with large data such as usually stored in cloud systems, on the other hand, encryption will take longer if we use asymmetric encryption techniques to encrypt the same data size. We conduct time performance evaluation in term of: encryption time and decryption time on files of different sizes.

- Encryption time: The time it consumes for an encryption algorithm to convert data from its original form (plaintext) to the encrypted form (ciphertext).
- Decryption time: The time it consumes for the decryption algorithm to return the data from its encrypted form (ciphertext) to its original form (plaintext).

Experiment and Evaluation

This part clarifies the experimentation to study the SCES model. The experiment done by Python programming language, we conduct our experiment by using computer with 1.99 GHz CPU and 8 GB RAM to show data encryption and decryption procedure. The experiment provides a comparison between the time spent in the process of encryption and decryption procedure with different sizes of data.

Performance of data encryption procedure

The data is encrypted in our SCES proposed model with the symmetric encryption key AES algorithm with key size 256 and CBC mode, to encrypt data. We implement experimentation for data encryption procedure in SCES model using constant data size 1MB, 5MB, and 10MB in five cycles. The following figures (Figure 7.1 , Figure 7.2 , and Figure 7.3) show the time it takes to encrypt

different sizes of files, and Figure 7.4 shows a comparison of the time taken to encrypt data in the three sizes.

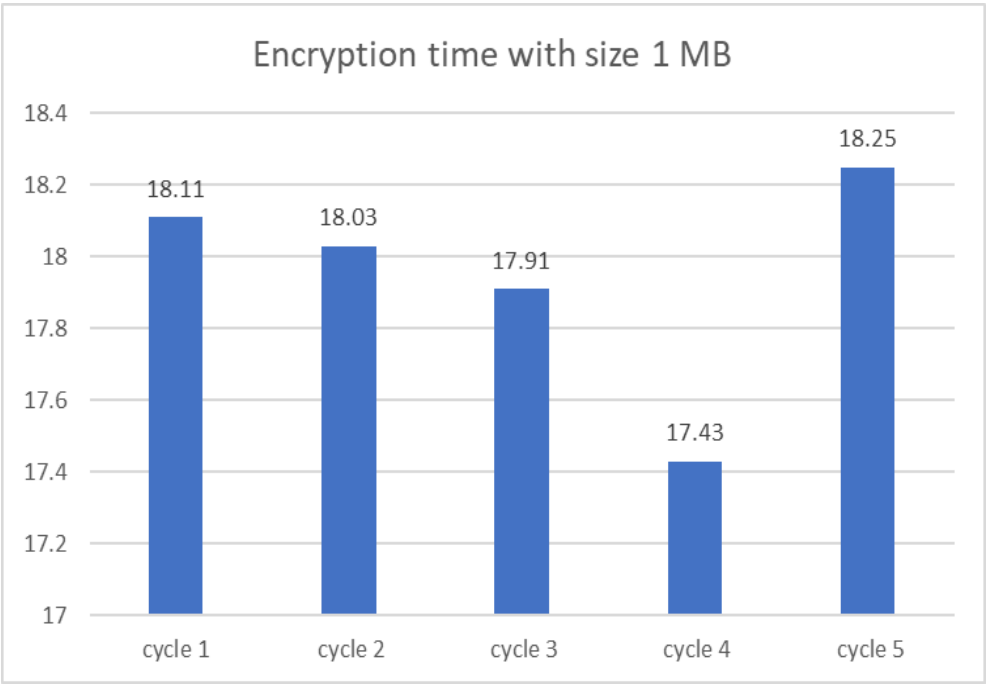


Figure 14. Evaluation of encryption time performance using 1MB size.

It is clear from Figure 14 that time performance using 1 MB is nearly constant in the five cycles in SCES model, the time consumed to encrypt for this size of files ranges from 17.43 milliseconds to 18.25 milliseconds. That is, the average time is: 17.946 milliseconds. Table 8, shows the values of experimentation for 1 MB.

Table 8
Encryption time with average for 1 MB

Cycles	Encryption time
Cycle 1	18.11
Cycle 2	18.03
Cycle 3	17.91
Cycle 4	17.43
Cycle 5	18.25
Average Time	17.946

Encryption time increases as file size increases in multiples of data size in SCES model as it is shown in Figure 15 and Figure 16:

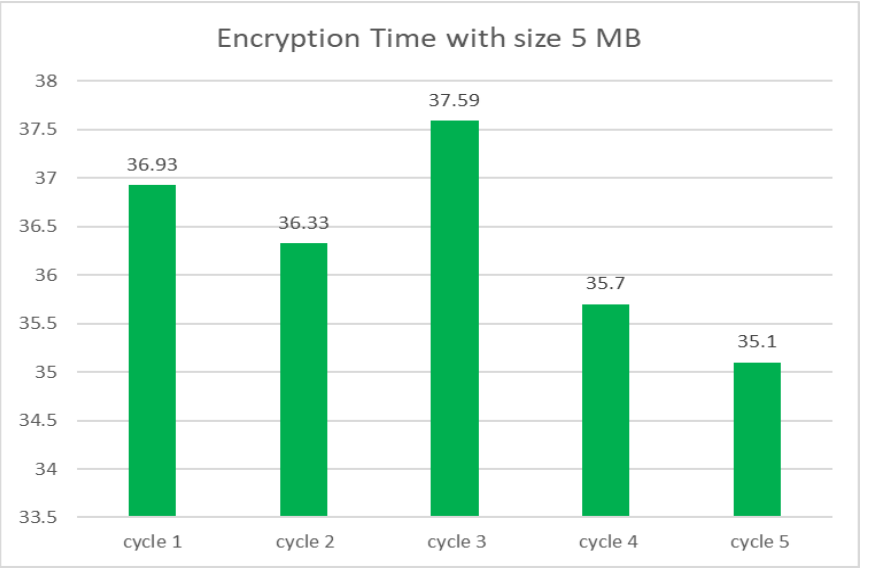


Figure 15. Evaluation of encryption time performance using 5MB size.

We noticed that the encryption time for a 5MB file size of exceeds the time of encryption of a 1MB file size, as shown in Figure 7.2, where in the five cycles of encryption the least time consumed is: 35.1 milliseconds, while the highest time is: 37.59 milliseconds, that is, the average time to encrypt a 5MB file size is: 36.33 milliseconds. Table 7.2, shows these values of experimentation.

Table 9
Encryption time with average for 5 MB

Cycles	Encryption Time
Cycle 1	36.93
Cycle 2	36.33
Cycle 3	37.59
Cycle 4	35.7
Cycle 5	35.1
Average Time	36.33

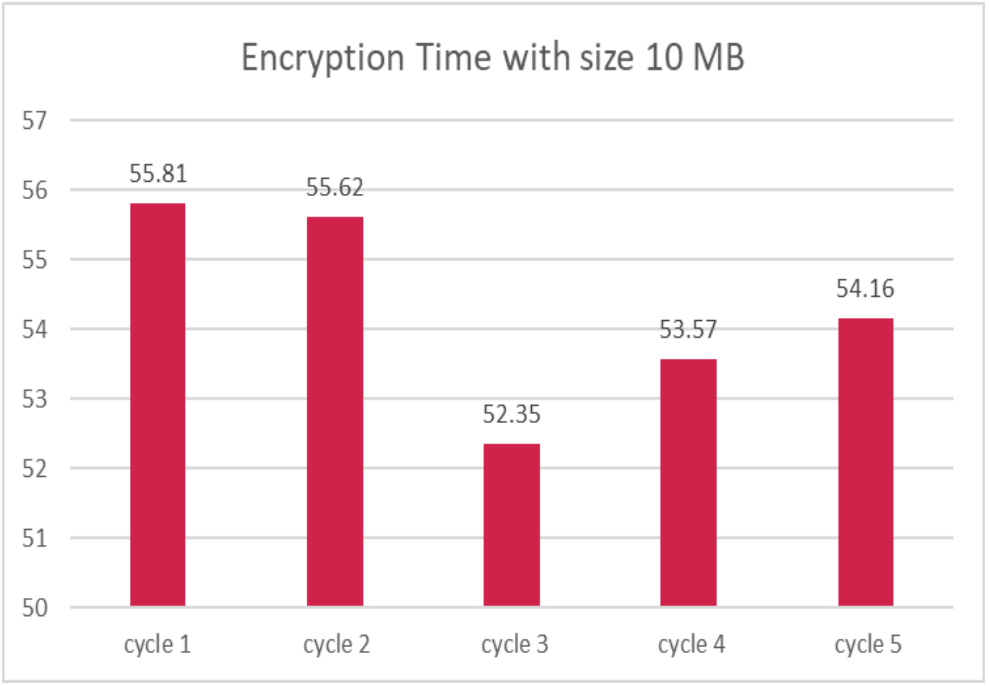


Figure 16. Evaluation of encryption time performance using 10MB size.

Figure 17, also shows that when conducting the encryption experiment in five cycles for 10MB size, the encryption took longer than the time taken to encrypt the previous two sizes: 1MB and 5MB, where the lowest time for encryption is: 52.35 milliseconds, while the highest time is: 55.81 milliseconds, meaning that the average time is: 54.302 milliseconds. These values shown at Table 7.3.

Table 10
Encryption time with average for 10 MB

Cycles	Encryption Time
Cycle 1	55.81
Cycle 2	55.62
Cycle 3	52.35
Cycle 4	53.57
Cycle 5	54.16
Average Time	54.302

The following Figure 17, shows a comparison between the encryption time of the three files in the five cycles, which confirms that encryption takes longer with data of a larger size.

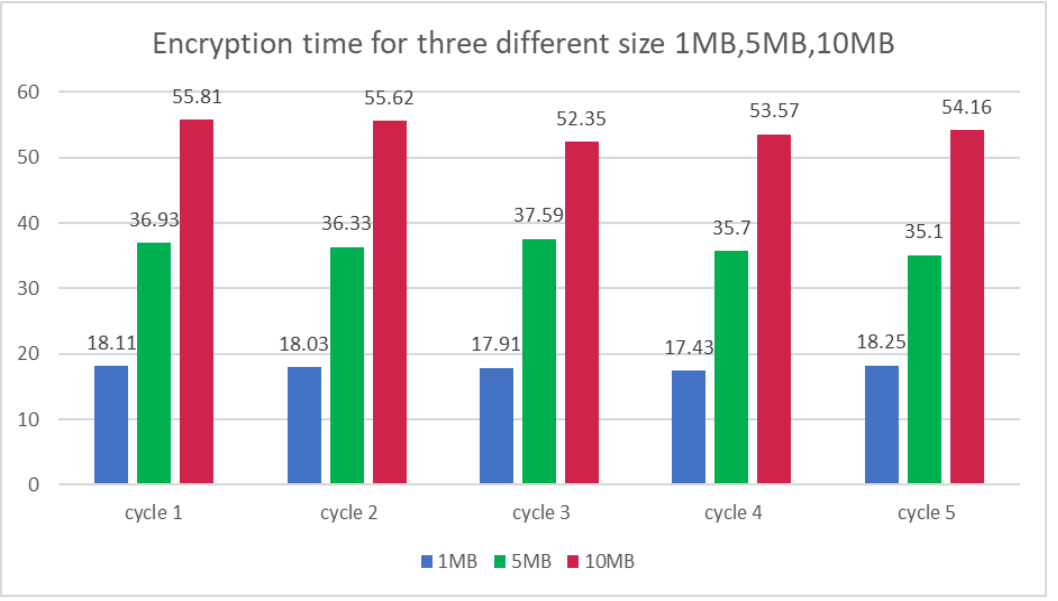


Figure 17. Encryption time performance for three different size 1MB, 5MB, 10MB

Performance of data decryption procedure

Since the encryption used to protect the data is a symmetric encryption, the decryption is done using the same key to restore the data to its original form. The following figures: Figure 7.5, Figure 7.6, and Figure 7.7 show the time they take to decrypt same previous files.

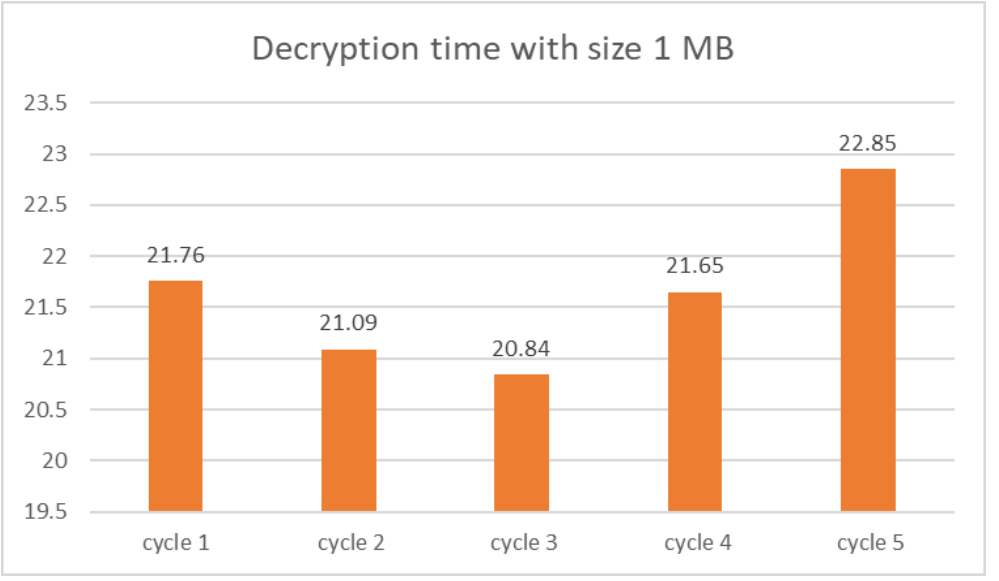


Figure 18. Evaluation of decryption time performance using 1 MB

From Figure 18, we observed that decryption time with size 1 MB is nearly constant in the five cycles in SCES model, the least time it takes to decrypt a file

of 1 MB is: 20.84 milliseconds, and the highest time is: 22.85 milliseconds, and the average is: 21.638 milliseconds. Table 7.4, shows the values of experimentation for 1 MB.

Table 11
Decryption time with average for 1 MB

Cycles	Decryption time
Cycle 1	21.76
Cycle 2	21.09
Cycle 3	20.84
Cycle 4	21.65
Cycle 5	22.85
Average Time	21.638

Moreover, we noticed that the decryption time increases as file size increases in multiples of data size in SCES model as it is shown in Figure 19 and Figure 20.

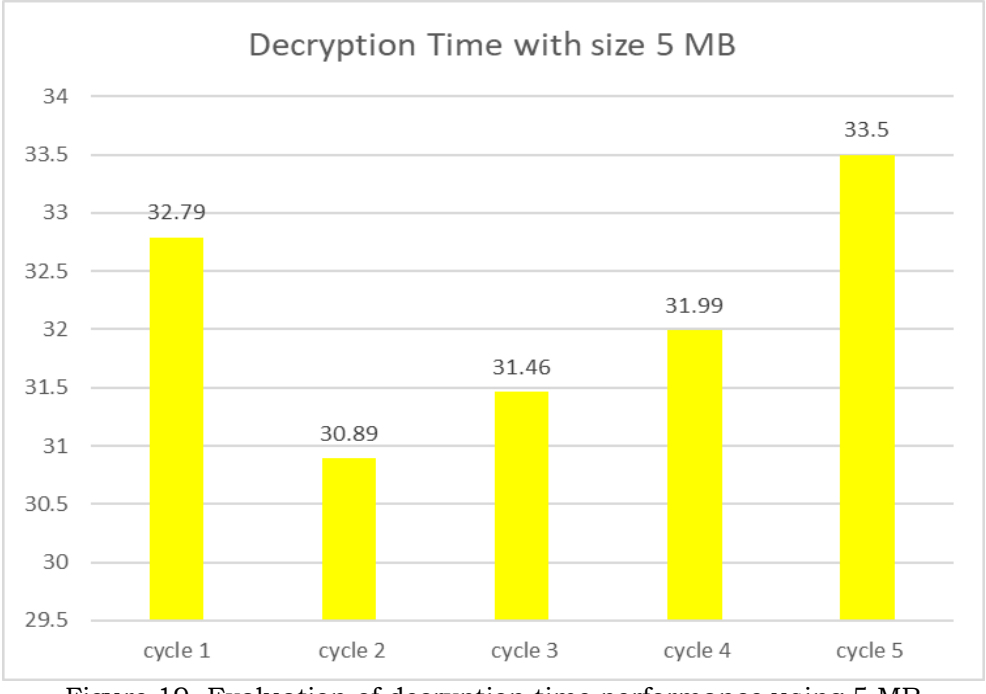


Figure 19. Evaluation of decryption time performance using 5 MB

As shown in Figure 19, the decryption time of size 5 MB is more than the decryption time of size 1 MB, since in the five cycles of decryption, the least time consumed is: 30.89 milliseconds, while the highest time is: 33.5 milliseconds, the average time for decryption: 32.126 milliseconds. Table 7.5, shows the value of experimentation for 5 MB.

Table 12
Decryption time with average for 5 MB

Cycles	Decryption Time
Cycle 1	32.79
Cycle 2	30.89
Cycle 3	31.46
Cycle 4	31.99
Cycle 5	33.5
Average Time	32.126

When performing the decryption experiment in five cycles for size 10 MB, we notice from Figure 20, that decryption took a longer time when compared to the time taken to decrypt the previous two files 1MB and 5MB.

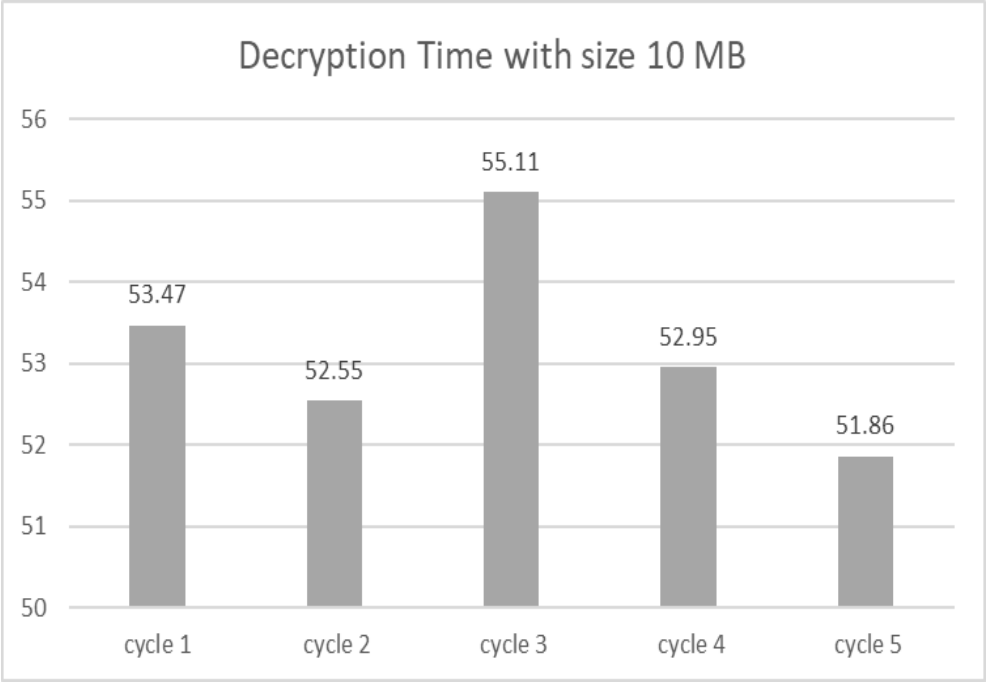


Figure 20. Evaluation of decryption time performance using 10 MB

The average decryption time is: 53.188 milliseconds, considering the highest time is: 55.11 milliseconds, and the lowest is: 51.86 milliseconds, as shown in Table 13.

Table 13
Decryption time with average for 10 MB

Cycles	Decryption Time
Cycle 1	53.47

Cycle 2	52.55
Cycle 3	55.11
Cycle 4	52.95
Cycle 5	51.86
Average Time	53.188

By comparing the decryption times of the three files in the five cycles, as in the Figure 21, it is clear to us that decryption takes longer with data of a larger size.

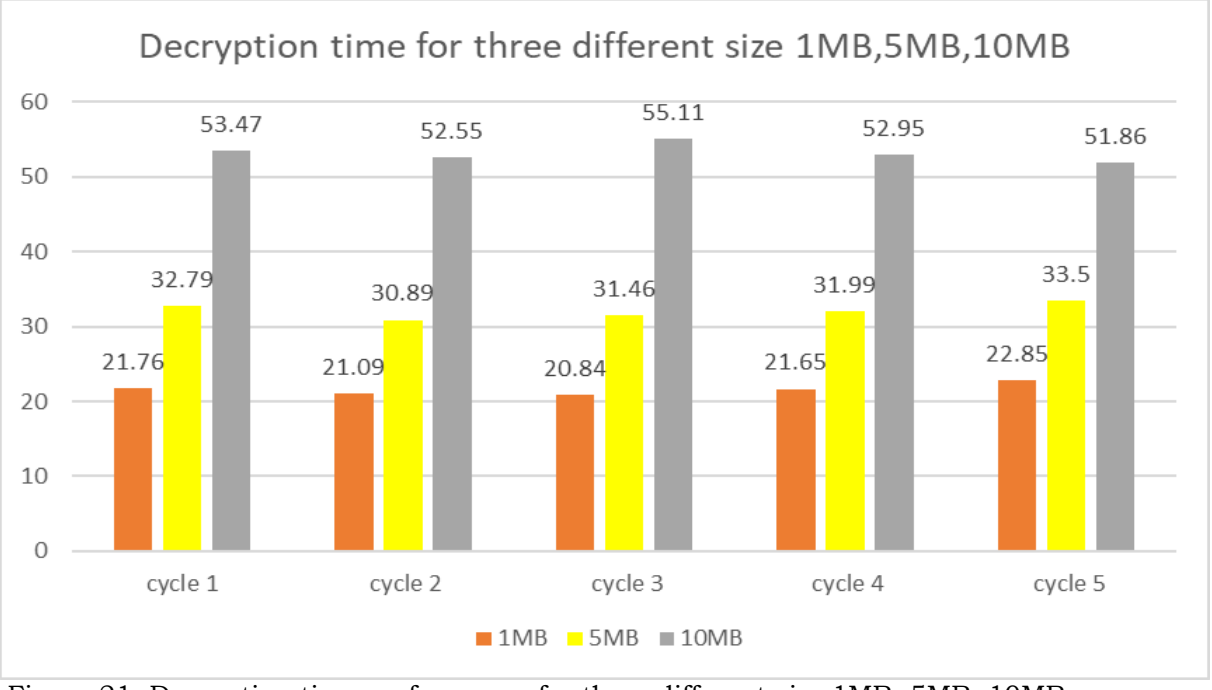


Figure 21. Decryption time performance for three different size 1MB, 5MB, 10MB

Comparison between encryption and decryption time for same file size

In this section we will show a comparison between the encryption and decryption time of the same file in five cycles, to show the performance of encryption and decryption time for the same file, as shown in Figure 22, Figure 23, and Figure 24.

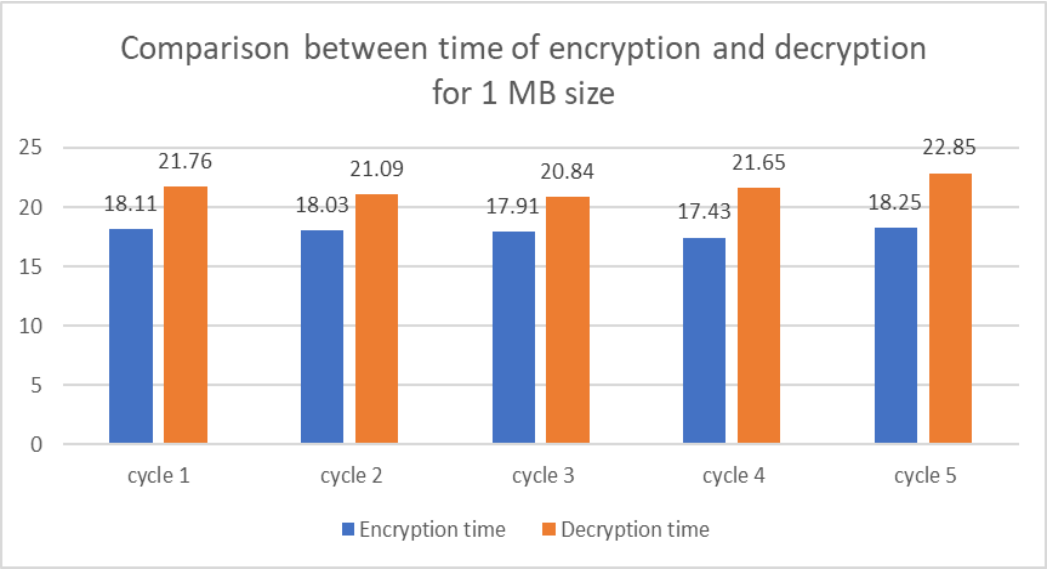


Figure 22. Comparison between time performance of encryption and decryption for 1 MB size

As we can note from Figure 22, decryption took longer than encryption on a data size as small as 1 MB. Where the average encryption time is: 17.946 milliseconds, and the average decryption time is: 21.638 milliseconds.

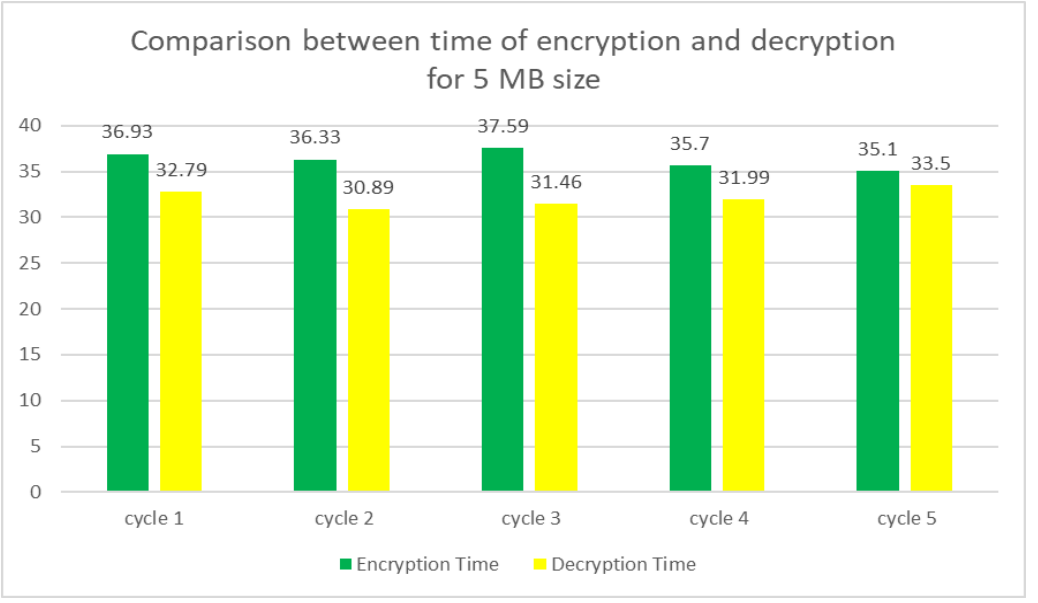


Figure 23. Comparison between time performance of encryption and decryption for 5 MB size

When we move to the experiment with a larger file size, 5 MB, for example, as in the Figure 23, the encryption takes longer time than decryption, with an average

time for encryption 36.33 milliseconds, and the average time for decryption 32.126 milliseconds.

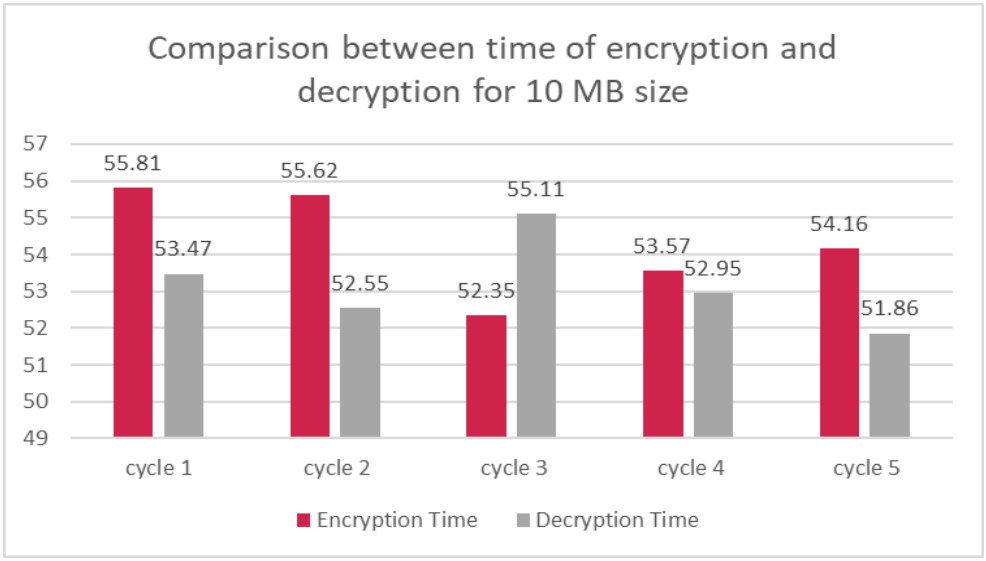


Figure 24. Comparison between time performance of encryption and decryption for 10 MB size

We observed when we encrypt and decrypt a file with a size larger than the previous two sizes, 10 MB, as in the Figure 24, that the time taken for encryption is also more than the time taken for decryption in most cycles, with an average encryption time: 54.302 milliseconds, and an average decryption time : 53.188 milliseconds.

Conclusions

Cloud computing is considered a great development in the field of information technology, and it has become possible to apply it in many fields. And what helped in its spread and development, is its characteristics and the services it provides. With the development of these technical areas, they are facing many security risks with the increase in the number of hackers and the development of their technical skills. Therefore, it is necessary to research and study the risks that threaten the security of these systems, and find solutions and measures to reduce them45-51. The goal of this paper is to is to discuss solutions related to protect the user's data of the educational system, by restricting people's access to the cloud-based educational system, so that the solutions help authenticate users and allow only authorized people to access data within the system, and using encryption that help on protecting the user's data, so that is difficult to violate its privacy in the event that intruders access it in an illegal manner.

Section 2 reviewed literature on cloud computing definition,also reviewed using of cloud computing at Saudi educational system. Cloud security were also reviewed at section 3 including: security service, data security issues, access control as a security mechanism for cloud computing reviewed at section four. Section 5 presented data protection techniques that are used to protect data. The aim of section 6 is to proposed secure model, called SCES model, which control the access to the educational system with ABE-Access control model, and helps protect data after authorization with appropriate combined encryption techniques (AES+RSA), and described the SCES model architecture, its components, layers and model data flow. Finally, section 7 tested the proposed encryption system and compared its time performance on different size of data.

Future works

In future work, we will seek to develop our SCES model by experimenting with other methods and mechanisms for access control and data encryption, so that we reach a method that achieves a high level of security, which increases the confidence of users in relying on these systems. We will search for the most dangerous threats to these systems, and search for the possibility of finding appropriate solutions to them.

References

Jouini, M., & Rabai, L. B. A. (2019). A security framework for secure cloud computing environments. In Cloud security: Concepts, methodologies, tools, and applications (pp. 249-263). IGI Global.

Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., & Fu, C. (2010). Cloud computing: a perspective study. New generation computing, 28(2), 137-146.

Rashid, A., & Chaturvedi, A. (2019). Cloud computing characteristics and services: a brief review. International Journal of Computer Sciences and Engineering, 7(2), 421-426.

Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., ... & Sarkar, P. (2018, January). Cloud computing security challenges & solutions-A survey. In

2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 347-356). IEEE.

Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

Alam, T. (2021). Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1, 108-115.

Sriram, I., & Khajeh-Hosseini, A. (2010). Research agenda in cloud technologies. arXiv preprint arXiv:1001.3259.

Taghipour, M., Soofi, M. E., Mahboobi, M., & Abdi, J. (2020). Application of cloud computing in system management in order to control the process. Management, 3(3), 34-55.

Bhad, P., Hande, J. Y., & Tiwari, S. J. INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY APPROACH TO THE OVERVIEW OF CLOUD COMPUTING, APPLICATION AND FUTURE SCOPE.

Aljabri, M., Chrouf, S. M., Alzahrani, N. A., Alghamdi, L., Alfehaid, R., Alqarawi, R., ... & Alduhailan, N. (2021). Sentiment Analysis of Arabic Tweets Regarding Distance Learning in Saudi Arabia during the COVID-19 Pandemic. Sensors, 21(16), 5431.

Rajeswari, S., & Kalaiselvi, R. (2017, December). Survey of data and storage security in cloud computing. In 2017 IEEE International Conference on Circuits and Systems (ICCS) (pp. 76-81). IEEE.

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698.

Karatas, G., & Akbulut, A. (2018). Survey on access control mechanisms in cloud computing. Journal of Cyber Security and Mobility, 1-36.

Shen, H. B., & Hong, F. (2005). Review of access control model. Appl. Res. Comput, 22(6), 9-11.

Cai, F., Zhu, N., He, J., Mu, P., Li, W., & Yu, Y. (2019). Survey of access control models and technologies for cloud computing. Cluster Computing, 22(3), 6111-6122.

Han, D. J., Gao, J., & Zhai, H. L. (2010). Research progress of access control model. Computer Science, (11), 29-33.

Lampson, B. W. (1968). A scheduling philosophy for multiprocessing systems. Communications of the ACM, 11(5), 347-360.

Dubey, S., & Rai, P. K. (2021). A Review of Cloud Service Security with Various Access Control Methods.

Albulayhi, K., Abuhussein, A., Alsubaei, F., & Sheldon, F. T. (2020, January). Fine-Grained Access Control in the Era of Cloud Computing: An Analytical Review. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0748-0755). IEEE.

Zhang, Y., Deng, R. H., Xu, S., Sun, J., Li, Q., & Zheng, D. (2020). Attribute-based encryption for cloud computing access control: A survey. ACM Computing Surveys (CSUR), 53(4), 1-41.

Zhang, P., Liu, J. K., Yu, F. R., Sookhak, M., Au, M. H., & Luo, X. (2018). A survey on access control in fog computing. IEEE Communications Magazine, 56(2), 144-149.

Zhong, H., Zhu, W., Xu, Y., & Cui, J. (2018). Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. Soft Computing, 22(1), 243-251.

Sifou, F., Hammouch, A., & Kartit, A. (2017, October). Ensuring security in cloud computing using access control: A survey. In Proceedings of the Mediterranean Symposium on Smart City Applications (pp. 255-264). Springer, Cham.