How to Cite:
Alkhaldi, S., AlZain, M. A., & Masud, M. (2022). Data protection in cloud educational system in Saudi Arabia. *International Journal of Health Sciences*, *6*(S1), 8879–8902.
https://doi.org/10.53730/ijhs.v6nS1.7031

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 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 this 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 [i]. 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” [ii]. 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 [iii]. Cloud computing has many characteristics, based on NIST's description, there are five main cloud computing characteristics: Rapid Elasticity, Measured service, On-Demand Self-Service, Ubiquitous networks Access, Resource pooling. A first step in order to better understand the security issues related to cloud computing and its services, we must understand the configuration of cloud computing. Cloud configuration according to NITS consists of a number of actors: cloud consumer, cloud provider, cloud auditor, cloud broker, cloud carrier. There are three cloud service models based on the NIST classification [iv], these models are : Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) which provide a set of services in several layers of business models. NIST divides the cloud into four models based on the main purpose of consumer and depending on suitability [v]. They are: Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud. Cloud Security includes methods that help ensure that data is protected from potential threats [v, 48,49, 50, 51] ."In fact, the security services implemented by security mechanisms execute security policies" [vi].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 [v]. Computer and information security is achieved by providing confidentiality, integrity, availability, authentication and non-repudiation services [vi].

The remainder of this paper is organized as follows:
Section two presents a review of cloud computing including: definition, characteristics, configuration, service models, deployment models, and cloud computing applications. Section three discusses cloud security from aspect of: security service and data security issues. Section four shows access control as a security mechanism for cloud computing. Fifth section shows data protection techniques, security practices of data protection, and protect data by cryptography.

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 [i].
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 [vii], The following figure (Figure 2.1) shows how different entities are connected to cloud computing.

Figure 2. 1 Cloud computing [vii] .

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 viii.

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” [ii].
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 [ix].

Cloud computing Characteristics

Based on NIST's description, five main cloud computing characteristics have been identified as follows:

1- Rapid Elasticity: Cloud computing is characterized by reducing or increasing resources according on-demand of users.
2- Measured service: This characteristic measurement is highly important for service improvement, access control, billing, capacity setting, and other services. Cloud service providers are responsible for managing their service resources.
3- On-Demand Self-Service: This characteristic makes it easy for users to access cloud services and infrastructure when they need them with minimal interaction or contact with the service provider.
4- Ubiquitous networks Access: This characteristic makes it easy for thin and dense users to access service resources across networks, regardless of their usage.
5- Resource pooling: Cloud computing enables the distribution and allocation of technological and physical services and provides the user with a multicenter platform, from which the user chooses what suits him, without knowing nothing about the details of the resources provided, but he can locate the resource with a high level of abstraction x.

Cloud configuration

Cloud configuration, which will be presented in the following lines, is important as a first step in order to better understand the security issues related to cloud computing and its services. Cloud computing companies consist of resources that are dedicated to user requests
Cloud configuration according to NITS consists of a number of actors as will be explained in the Table 2.1. [xi, xii].

Table 2. 1 Different actors in cloud computing [xi, xii].

Actor	Definition
Cloud consumer	A person or organization that maintains a business relationship with, and uses service from, cloud providers
Cloud provider	A person, organization, or entity responsible for making a service available to interested parties
Cloud auditor	A party that can conduct an independent assessment of cloud services, information system operations, performance and security of the cloud implementation
Cloud broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers
Cloud carrier	An intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers

This classification highlights the security threats to cloud service providers as well as their customers and risk-awareness associated with them. The actors shown in the Table2.1 are those that play a role, share and exchange services through the cloud [vi] .
Cloud consumer:
This term refers to an organization or person that obtains services from cloud providers .The cloud consumer chooses the most popular service by looking at the range of services provided by the providers and then entering into a contract, and

the cloud consumer must agree to the service-level agreement (SLA) provided by the service provider.

SLA is an agreement covering aspects of the service provided by the provider to the consumer, such as security, consistency of service quality, performance failure, and prevention. Cloud consumers tend to choose the most suitable and affordable providers [vi] .

Cloud provider:

This term refers to the organization or person that provides services to consumers of the cloud.

The role of service providers lies in arranging and organizing cloud computing programs by preparing and controlling the infrastructure

For example, In SaaS, cloud providers provide predictable levels of services by deploying, configuring, updating, and fixing vulnerabilities of application and software.

Due to the limitations of cloud management applications, the SaaS provider has to take on the responsibilities of controlling and managing the infrastructure,

In PaaS, by using cloud software, a service provider manages the basic cloud computing infrastructures of his platform and provides the components of that system (such as databases, runtime programs, and any other supporting software)

In IaaS, service providers own the physical resources of the cloud, including storages, servers, networks, and infrastructure to host consumers [vi].

Cloud auditor:

Responsible for the independent examination of cloud services, verifies that services conformance with standards that are defined in several objective evidence, and assesses a cloud provider's service from multiple aspects including: security controls, privacy impacts, performance and other areas important to the consumer [vi].

Cloud broker:

The cloud computing service cannot be controlled by its consumers because of the complexity of its services integration, so there must be a cloud broker between the service provider and the consumers of the cloud instead of direct communication between them, so consumers get the service through this cloud broker.

The role of a cloud broker is to manage the usage, delivery and performance of the cloud service, and to regulate the relationship between the cloud consumer and the service provider

The services provided by the cloud broker can be divided into three services:

1- Service intermediation:

Provides a value-added service to the cloud consumer, and improve services by improving certain capabilities. This improvement includes performance reporting, security improvement, identity management, access management for services etc [vi] .

2- Service aggregation: It means a set of process taken by the cloud broker to merge or combine several services of cloud into one service or more services.

For example, works on data integration and acts as a bridge among service providers and consumers.

3- Service arbitrage: Its work is similar to the aggregation Service, but the services aren't collected to remain fixed, but the cloud broker is given flexibility in choosing the desired service from the appropriate agency by arbitrage the

services. For example, a cloud broker selects and evaluates the best agencies using credit services [vi].
Cloud carrier:
It plays an important role in providing a secure connection to the service provider and the consumer as it mediates between them to provide services
As cloud carriers can reach consumers through networks or other devices of access based on the service level agreements of the cloud carrier, also the service provider provides its services to consumers in compliance with these agreements [vi]
Figure 2. 2 indicates an overview of the NIST cloud computing configuration [xii] .

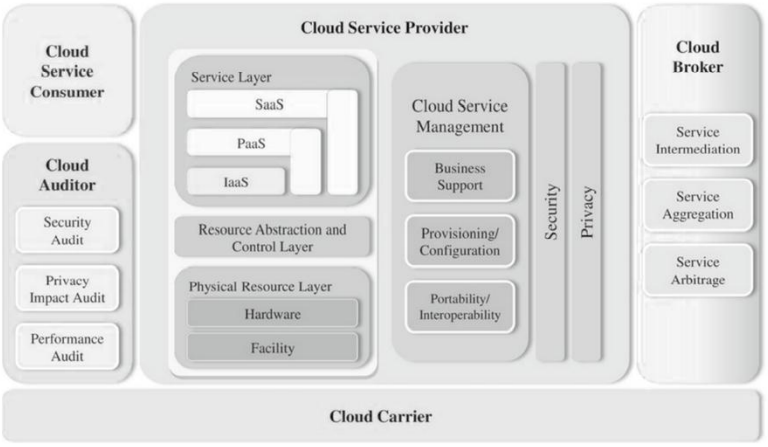

Figure 2. 2 NIST cloud computing configuration [xii].

This diagram shows the main actors and their functions and activity in cloud computing ,and based on the data shown, it also shows the characteristics, standards and requirements of cloud computing [vi] .

Cloud Service Models

There are three cloud service models based on the NIST classification iv, these models provide a set of services in several layers of business models
Software as a Service (SaaS): This service model provides consumers with software applications via the Internet. These applications depend on the basic infrastructure of the service provider. This service takes care of the basic setup costs and infrastructure maintenance costs. It also takes over the automation of updates, and it makes the basic infrastructure and implementation platforms under its control in terms of security and not under the Consumer control Consumer.

Platform as a Service (PaaS): This service provides an integrated and abstract cloud environment which supports the creation, development, management and operation of applications. In the sense of offering an online platform.
Cloud service providers control the basic infrastructure, including servers, networks, storage, and operating systems. Consumers can get possibility for application deployment and configure settings of configuration for their

application hosting environment, giving consumers greater scalability and control over security more than SaaS and less than IaaS.
Infrastructure as a Service (IaaS): In this service, cloud computing resources are delivered virtuality, including its networks, storage services, and devices**,** and the control is by the consumer in the aspects of operating systems and certain sections of network and deployed services, while the role of the service provider is to manage the infrastructure completely, this model provides a greater of control over security aspects when compared to SaaS and PaaS v.

Cloud Deployment Models

NIST divides the cloud into four models based on the main purpose of consumer and depending on suitability [v].

Public Cloud:
A public cloud provides cloud computing services to general consumers or large famous business organizations, with the cloud located at the provider's end. The public cloud offers its consumers reliability and scalability, but it puts them in front of several problems, including: consumers are not aware of the physical geographical location in which their data is located and are not aware of the types of storage approved by the provider and any organization that stores their data with them (specifically in: multi-tenancy), which means that an organization that decides to move to a public cloud may compromise on certain security considerations [v].

Private Cloud:
The private cloud provides cloud computing services to one organization exclusively. The cloud is owned by the organization itself or a third party. The cloud may be located inside or outside the building. Thus, it avoids the problems of security aspects found in the public cloud, but it costs the organization many overhead expenses such as provisioning, capacity control, and storage of management etc v.
Community Cloud:
A community cloud provides cloud computing services exclusively to communities of organizations that have common interests (for example: compliance considerations, policy **,**security requirements, or emission. the cloud is owned by the organization itself or by a third party. It may be located inside or outside the buildings **.**Among its shortcomings are the open questions about the aspects related to the data published by various domains and organizations, such as: service interruptions, the effects of contracts and security [xiii] .

Hybrid Cloud:
In this model, the infrastructure is the composition of more than one infrastructure from the previous service models (private, public or community), each infrastructure remains independent, but it is interconnected with each other with a special or standard technology that allows the exchange of applications and data. Hybrid cloud combines the advantages of a public cloud in terms of cost and scalability, and the advantages of a private cloud in terms of its concern for security issues and control. Because privacy controls in a public cloud are very different from those in a private cloud, there are issues that pose threats to a

hybrid cloud that include data integrity and privacy while data moves between the private and the public cloud xiii .

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 Storagexiv, 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. [iii]

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 [xv].

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 xv, 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. 3 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 v."In fact, the security services implemented by security mechanisms execute security policies" [vi] .

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 [v].

Computer and information security is achieved by providing confidentiality, integrity, availability, authentication and non-repudiation services [vi] .

Confidentiality, Integrity, and Availability are the three aspects that have been examined in this study v of Cloud computing security. Since the CIA is a commonly used standard for identifying system problems in traditional computing, the requirements of security for a cloud system will be defined within this standard. Accordingly, in many studies, fine-grained and sub-categories are provided that help mapping, understand and evaluate attacks that threaten cloud computing and possible solutions [v].

1-Confidentiality means protecting corporate assets and individual data from disclosure through unauthorized access. This may be illegal access through clients in that Cloud computing system who seek to illegally access someone else's data, Stored at the same database as this intruder with the service provider. It's also possible that the Cloud service provider (CSP) has some malicious or curious members who might see or tamper by the client's sensitive and important information. Regardless of the data stored, the VMimage, VM network, and so on all have to adhere to strict confidentiality standards [v] .

2- integrity:

Integrity means ensuring that the data is not modified by unauthorized parties with this modification, whether by addition, deletion or editing. This feature ensures the authenticity and accuracy of the assets for the data owner. This

modification may occur in files stored in the cloud because consumers access these services via the web, and web-based attacks are widespread and threaten data integrity, as these attacks target the modification of the files contents, database, or even metadata of the virtual machine [v].

3- Availability

Availability means ensuring the services availability to cloud computing customers at any time they need them, and it is an important issue that the service provider must maintain, and this obliges organizations that provide services to customers through the cloud to ensure their availability at all times, as few downtimes may lead to losses cannot be compensated. The service level agreement (SLA) must state that the service provider agrees to ensure that the service is available on demand request [v].

Hamed Tabrizchi's [vi] discussed two additional factors to the previous three: Authentication and non-repudiation.

Authentication: One of the services that help verify and confirm the identity of recipients and senders accurately, which maintains the confidentiality and integrity of information [vi] .

non-repudiation: repudiations can be from the source or destination by deny the message delivery or transmission, and the non-repudiation service provides procedures that cannot be rejected by any party [vi] .

Data security issues

Based on the requirements of each aspect of the CIA standard, this study v 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 3.1:

Table 3. 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 attack 4- Metadata Spoofing 5-Wrapping attack

When security issues and problems are discussed, solutions must also be discussed. Many researches have presented wonderful and useful designed methodologies for solving the diverse security problems of the three aforementioned CIA aspects. The Srijita Basu study compared multiple methodologies for data confidentiality, virtualization confidentiality, data integrity and virtualization integrity. Data confidentiality means, as we mentioned, protecting data from intruders and not being informed by the service provider. Data confidentiality problems have been resolved using multiple encryption

methodologies. There are a number of solutions proposed for data confidentiality, including restrict access by using access control models like : Attribute-based encryption for fine grained access control (ABE), which will be discussed in this thesis. Another important aspect for cloud computing customers is the data confidentiality, so methodologies to ensure data confidentiality are also proposed [v].

Study xvi dealt with data security in cloud computing, Cloud security has been classified into several categories, as shown in the following figure (Figure 3.1):

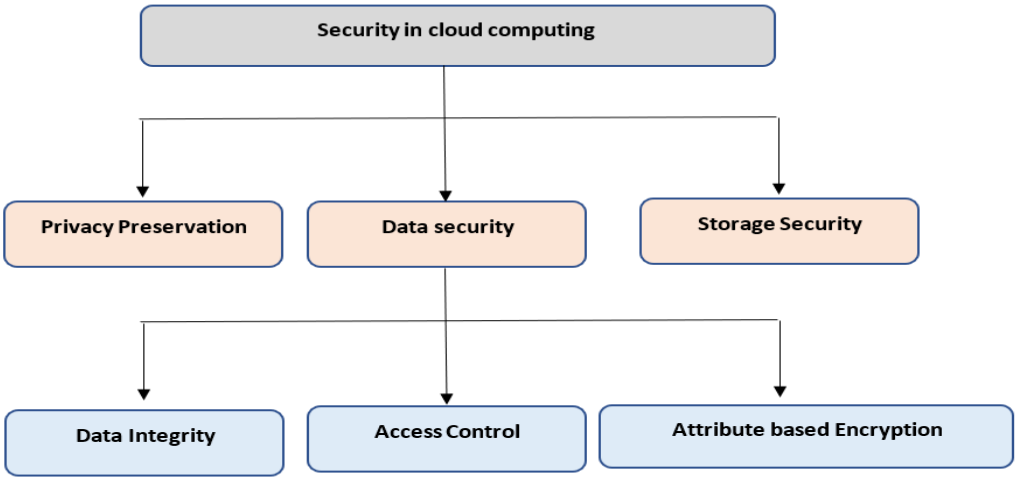

Figure 3.1 Security Classification in cloud.

Since our research focuses on data in terms of its confidentiality a and security, we will address the two sections concerned with Privacy Preservation and data security.

Privacy Preservation: The privacy of user data is very important in cloud computing, because of the absolute lack of trust in cloud servers, authorization and confidentiality are requirements to maintain privacy in the cloud [xvi] .

Data security ensures that data is not modified and protected from unauthorized access, especially sensitive information for users. For data security we must ensure: authentication, authorization, confidentiality and integrity. As shown in the Figure 3.1, Data security include three important features Data integrity, access control and attribute-based encryption. Access control and attribute-based encryption we will discuss it in the following sections [xvi].Also we can protect data of users on cloud side by using many techniques will discussed in other section.

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 xvii:

1- Access Control Systems
2- Identity and Authentication.
3- Privacy
4- Protocol and Network Security
5- Intrusion Detection Systems
6- Trust Management

Benefits provided by the access control mechanisms:

- It Enables the users of system security
- It Enables authentication for devices and users
- It Enable to monitor network security
- It Processes all previous items at the same time

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 [xviii].

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 [xix].
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 4.1): shows the main components and the decision-making method for authorization through access control [xx].

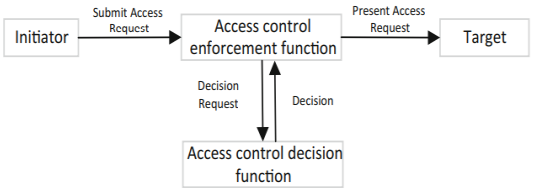

Figure 4.1 The process of access control.

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

Table 4.1 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 [xx].
Lampson summarized the access control problem and proposed a graphic representation using the access control matrix, subject and object [xxii].

Access Control models

The following table (Table 4.2) presents some studies that discussed access control methods used in cloud computing:
Table 4.2 Access control models

Access Control models	xxiii 2021	xxiv 2020	xxv 2020	xx 2019	xxvi 2018	xxvii 2018	xviii 2018	xxviii 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 [xxv] . Attribute-based encryption attracted researchers and was the first to introduce the term ABE Sahai and Waters [xxix] 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 [xxviii] . the next figure shows Architecture of ABE model:

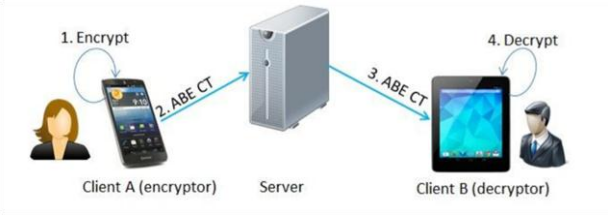

Figure 4.2 Architecture of ABE model [xxx] .

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 [xxxi].

At CP-ABE : The following figure (Figure 4.3) shows an example of using CP-ABE. Each user has a set of attributes associated with it. User 3 decrypt data because it's set of attributes satisfy to the access policies defined by the ciphertext [xxxii].

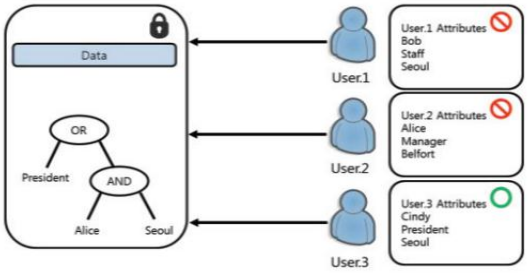

Figure 4.3 CP-ABE (Ciphertext Policy Attribute Based Encryption) [xxxii].

At KP-ABE: In this type, attributes are defined for the data, and users are given keys that contain an access policy that can to distinguish between attributes. Through these policies, the user decrypts data when the access policies specified in his key satisfy with the set of attributes assigned to the data xxxii. as shown in the next figure (Figure 4.4):

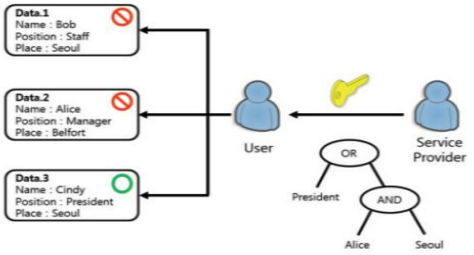

Figure 4.4 KP-ABE (Key Policy Attribute Based Encryption) xxxii.

The following table (Table 4.3) provides a comparison between these two types through a number of criteria:

Table 4.3 Compression between CP-ABE and KP-ABE

	CP-ABE	KP-ABE
access policy	The access policy is defined in the ciphertext xxv.	The access policy is known by encoding it in a user's attribute secret key (user's private key) xxv .
user's attribute secret key	user's attribute secret key (user's private key) is associated with user's attributes sets xxxiii .	the ciphertext contains user's attributes sets xxxiii .
access tree structure	The private keys for decryption must meet the policies defined by the encoder using the access tree structure xxxi .	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 xxxi.
decrypt	The user can use a given key to decrypt the ciphertext if and only if the access structure matches the attributes	The user can use a given key to decrypt the ciphertext if and only if the access structure matches the attributes associated with the

	associated with the private key of the tree nodes xxv .	ciphertext xxv.

The procedure of KP-ABE and CP-ABE encryption and decryption is shown in the following figure (Figure 4.5):

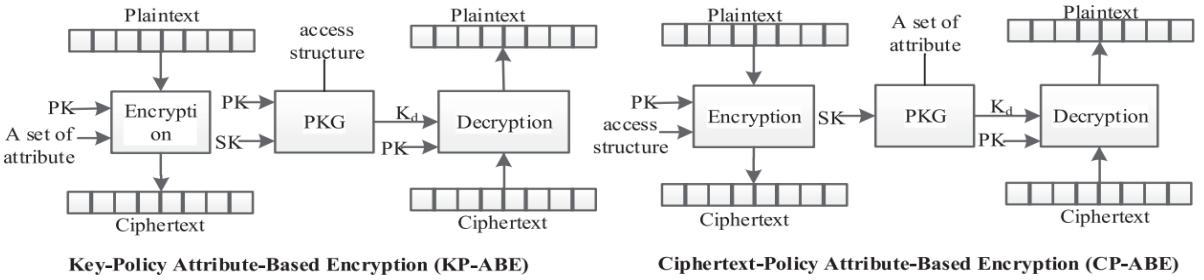

Figure 4.5 The comparison between KP-ABE and CP-ABE methods xxxi.

In general, attribute-based encryption is the appropriate technology for access control issues in cloud computing in terms of protecting data privacy and enabling the data owner to directly define access policies. The user can access the data when the attributes comply with the access policy specified by the data owner [xxvi].CP-ABE is more suitable for controlling access in the cloud than KP-ABE, because the access policy can be set by the data owner by defining the access method based on the attributes and encrypting the data based on them [xxxiv] , [xxxv]. Its mean "access policy determination in CP-ABE is put on the data owner's hand" [xxv].

As shown in the following figure (Figure 4.6), the access policy is set by the data owner, and the data is encrypted based on these policies. Each user is given his own private key according to his attributes. When decrypting, the user decrypts the data only if his attributes included in his private key match the access policy specified in the ciphertext. Long operating time and difficulty in managing are a downside to this mechanism [xxxvi] .

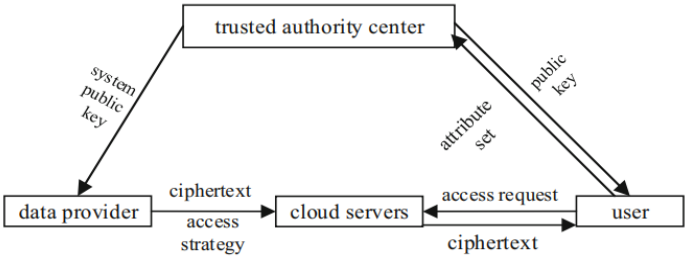

Figure 4.6 The ABE model for cloud computing environment [xx] .

The following table (Table 4.4) shows the steps of the attribute-based encryption algorithm [xx] :

Table 4.4 The steps of ABE algorithm xx.

Setup	Authorization center executes to generate the master key and the system public key
Encrypt	CT = Encrypt(PK, M, T), sender executes with attribute set T and plain text M, cipher text is CT
KeyGen	SK = KeyGen(MK, A), authorization center executes by to generate the user's private key SK
Decrypt	M = Decrypt(CT, SK), receiver executes using private key SK to get back message M

Encryption based access control

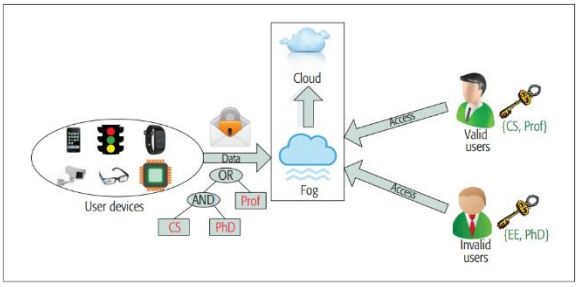

Figure 4.7 ABE-based access control [xxvi] .

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 [xx] 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 [xxxvii].

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.
- ntrusion 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 [xxxviii].

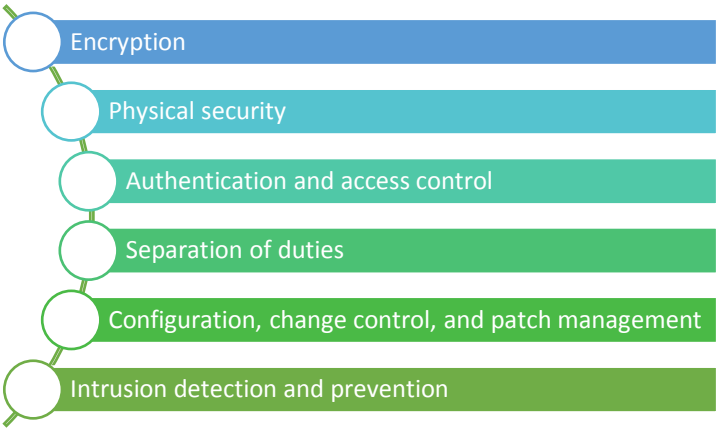

Figure 5.1 Security practices of data protection.

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 [xxxvii].
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 [xxxix], As shown in the following figure (Figure 5.2):

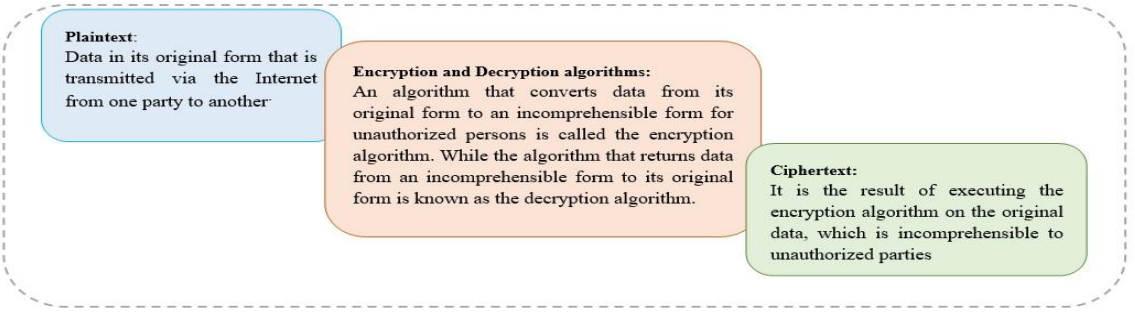

Figure 5.2 Cryptography basic components.

Cryptographic algorithms are classified into two main types:

- Symmetric Key Encryption Algorithms [xl].
- Asymmetric Key Encryption Algorithms [xli].

The following table produce comparison between these two categories [xxxix] :

Table 5.1 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 [xxxix], 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 [xxxvii] ,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 [xlii] .

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 [xxxvii].

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 [xliii]. 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 healthcare data security [52-57] and the use of 5G technologies with other cutting-edge technologies for the data transfer and data security including the blockchain, ransomware protection, etc. can enable further data security, and the same can be implemented for the educational data protection and security as well.

The following table (Table 5.2) 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 5.2 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 [i]		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 the key Size and block size.	168,112 or 56	Not scalable	Scalable	Not scalable	Scalable	Scalable
	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 [ii]		Not structure, Enough, Already Broken [iii]	Adequate security	Excellent security	Excellent security			
	Flexible	No	Yes	Yes	Yes	-	-	-
A survey on cryptography algorithms [iv]			-			No	Yes	Yes
		-	-	-	Fast Cipher in SSL	Low Speed	fast Speed	Low Speed
Security of Low Computing Power Devices: A Survey of Requirements, Challenges & Possible Solutions [46]	Speed	Slow	Slowest [44]	Fast	Fastest [44]	-	-	-
	Block Size	64bits	64 bits	128 bits	64 bits	128 bits	Variable	-

The following figure (Figure 5.3) summarizes the most important cloud topics discussed in this thesis:

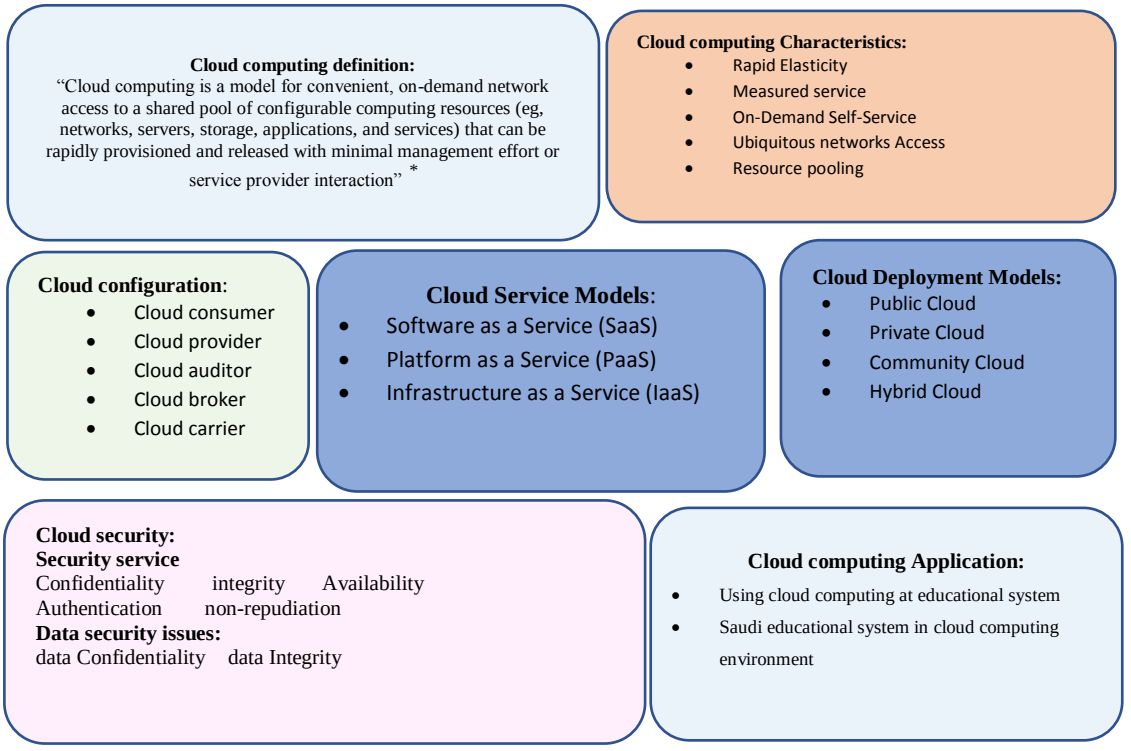

Figure 5.3 Cloud Computing Summary.

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 them.

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, characteristics, configuration, service models, deployment models, 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.

REFRENCES

[i] 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.

[ii] 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.

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

[iv] Mell P.M. and Grance.T. 2011. "The NIST Definition of Cloud Computing." In Computer Security Publications from the National Institute of Standards and Technology (NIST) SP 800145.Gaithersburg: National Institute of Standards & Technology.

[v] 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.

[vi] 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.

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

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

[ix] 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.

[x] Singh, Jaswinder & Dhiman, Gaurav. (2021). A survey on cloud computing approaches. Materials Today: Proceedings. 10.1016/j.matpr.2021.05.334.

[xi] Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, 465-472.

[xii] Csrc.nist.gov (2018) SP 500-299 (DRAFT), NIST Cloud Computing Security Reference Architecture | CSRC (online). https://csrc.nist.gov/publications/detail/sp/500-299/draft. Accessed 11 Sept 2018

[xiii] Goyal, S. (2014). Public vs private vs hybrid vs community-cloud computing: a critical review. International Journal of Computer Network and Information Security, 6(3), 20.

[xiv] 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.

[xv] 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.

[xvi] 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.

[xvii] 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.

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

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

[xx] 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.

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

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

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

[xxiv] 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.

[xxv] 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.

[xxvi] 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.

[xxvii] 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.

[xxviii] 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.

[xxix] Sahai, A., & Waters, B. (2005, May). Fuzzy identity-based encryption. In Annual international conference on the theory and applications of cryptographic techniques (pp. 457-473). Springer, Berlin, Heidelberg.

[xxx] Asim, M., Petkovic, M., & Ignatenko, T. (2014). Attribute-based encryption with encryption and decryption outsourcing.

[xxxi] Sookhak, M., Yu, F. R., Khan, M. K., Xiang, Y., & Buyya, R. (2017). Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. Future Generation Computer Systems, 72, 273-287.

[xxxii] Lee, J., Oh, S., & Jang, J. W. (2015). A Work in Progress: Context based encryption scheme for Internet of Things. Procedia Computer Science, 56, 271-275.
[xxxiii] Goyal, V., & Pandey, O. a. Sahai andB. Waters, IattributeY Based Encryption for fineYgraind access control of encrypted data. In Proceedings of the 13th aCM conference on Computer and communications security.
[xxxiv] Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P., & Jonker, W. (2009, August). Mediated ciphertext-policy attribute-based encryption and its application. In International Workshop on Information Security Applications (pp. 309-323). Springer, Berlin, Heidelberg.
[xxxv] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, April). Attribute based data sharing with attribute revocation. In Proceedings of the 5th ACM symposium on information, computer and communications security (pp. 261-270).
[xxxvi] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.
[xxxvii] Khan, S. S., & Tuteja, R. R. (2015). Security in cloud computing using cryptographic algorithms. International Journal of Innovative Research in Computer and Communication Engineering, 3(1), 148-155.
[xxxviii] Gampala, V., Inuganti, S., & Muppidi, S. (2012). Data security in cloud computing with elliptic curve cryptography. International Journal of Soft Computing and Engineering (IJSCE), 2(3), 138-141.
[xxxix] Semwal, P., & Sharma, M. K. (2017, September). Comparative study of different cryptographic algorithms for data security in cloud computing. In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) (pp. 1-7). IEEE.
[xl] Ebrahim, M., Khan, S., & Khalid, U. B. (2014). Symmetric algorithm survey: a comparative analysis. arXiv preprint arXiv:1405.0398.
[xli] Bala, T., & Kumar, Y. (2015). Asymmetric Algorithms and Symmetric Algorithms: A Review. International Journal of Computer Applications (ICAET), 1-4.
[xlii] Hardjono, T., & Dondeti, L. R. (2005). Security in Wireless LANS and MANS (Artech House Computer Security). Artech House, Inc..
[xliii] Mahalle, V. S., & Shahade, A. K. (2014, October). Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In 2014 International Conference on Power, Automation and Communication (INPAC) (pp. 146-149). IEEE.