PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

Ministry of Higher Education and Scientific Research

ECHAHID HAMMA LAKHDAR UNIVERSITY - EL OUED

FACULTY OF EXACT SCIENCES

Computer Science department

End of Study Memory

Presented for the Diploma of

ACADEMIC MASTER

Domain : **Mathematics and Computer Science**

Spinneret: **Computer Science**

Speciality : **Artificial Intelligence and Distributed Systems**

Presented by :

- **Meriem AMIRAT**
- **Bassma ZEKAIRA**

Theme

Use of encryption algorithms for securing relational data in Cloud Databases

Supported in: 30 - 09 - 2020 In front of jury:

M.	Othmani Samir	MCA	President
M.	Soltani Khaled	MAA	Examiner
Dr.	Yagoub Mohammed Amine	MCB	Supervisor

University year: 2019/2020.

Thanks

First of all we thank the Almighty God, the Lord of the heavens and the earth, who guided us on the path and allowed us to carry out this work.

We would also like to extend our sincere thanks to the professors of Hama Lakhdar University in EL oued, especially Faculty of exact sciences, Department of Computer Science. And it is our pleasure to extend our deep thanks and gratitude to those who helped us in completing this memorandum, especially the honorable professor, supervisor, « **Yagoub Mohammed Amine** », for his Great credit for helping us complete this work and overcome the difficulties that we faced. He has all our thanks and appreciation, and we also especially thank the members of the jury for granting us the honor of accepting the evaluation of this work. Thank you very much to our families and friends for their eternal support.

Finally, we thank everyone who contributed directly or indirectly to the result from this humble work.

Dedicate

The search locomotive passed many obstacles, yet I tried to surmount them steadily, with the grace of and from God. The most trustworthy for everyone who had merit in my career, and helped me even with a little bit,

To my Mom,

To my Family,

To my Bestfriends,

To my Self,

I dedicate this humble work.

Meriem.

Dedicate

To my parents..

All my family..

Everyone who helped me..and all my classmates..

All my friends..

I dedicate this humble work..

Basma

Abstract

Cloud computing is an economic and technological revolution, in which resources are provided as a service over the Internet. These resources can be provisioned and dynamically released according to the service demand and with minimal effort of management. However, securing data while moving in the cloud remains a challenge for cloud service providers.

In fact, this data is the target of many network attacks aimed at interrupting and information interception, modification and manufacture. Therefore, it is imperative to counter these attacks and breaches to improve the use and adoption of the cloud. Through this paper we provide a detailed study on data security in the cloud by providing effective solutions that exist in this field based on encryption. Then we will introduce a more efficient security solution that also includes the adoption of encryption to protect our data.

Key_Words : Cloud computing, Security, Fully homomorphic encryption, SQL.

Résumé

Le cloud computing est une révolution économique et technologique, dans laquelle les ressources sont fournies en tant que service sur Internet. Ces ressources peuvent être provisionnées et libérées dynamiquement en fonction de la demande de service et avec un effort de gestion minimal. Cependant, la sécurisation des données lors du déplacement dans le cloud reste un défi pour les fournisseurs de services cloud.

En fait, ces données sont la cible de nombreuses attaques réseau visant à interrompre et intercepter, modifier et fabriquer des informations. Par conséquent, il est impératif de contrer ces attaques et violations pour améliorer l'utilisation et l'adoption du cloud. À travers cet article, nous fournissons une étude détaillée sur la sécurité des données dans le cloud en fournissant des solutions efficaces qui existent dans ce domaine basées sur le cryptage. Ensuite, nous présenterons une solution de sécurité plus efficace qui comprend également l'adoption du cryptage pour protéger nos données.

Mots clés : Cloud computing, Sécurité, Chiffrement complétement homomorphique, SQL.

ملخص

الحوسبة السحابية هي ثورة اقتصادية وتكنولوجية، يتم فيها توفير الموارد كخدمة عبر الإنترنت. يمكن أن تكون هذه الموارد موفرة وذات إصدار ديناميكي وفقا لطلب الخدمة وبأقل جهد ممكن للإدارة. ومع ذلك ، لا يزال تأمين البيانات أثناء النقل في السحابة يمثل تحديًا لموفري الخدمات السحابية. في الواقع ، هذه البيانات هي هدف العديد من هجمات الشبكات التي تهدف إلى مقاطعة و اعتراض المعلومات وتعديلها وتصنيعها. لذلك، من الضروري مواجهة هاته الهجمات والاختراقات لتحسين استخدام واعتماد السحابة. من خلال هذه الورقة نحن نقدم دراسة تفصيلية حول أمن البيانات في السحابة من خلال توفير حلول فعالة الموجودة في هذا المجال المعتمدة على التشفير. ثم سنقدم حل أمني أكثر نجاعة المتضمن أيضا اعتماد التشفير لحماية بياناتنا.

الكلمات المفتاحية: الحوسبة السحابية، الأمن، التشفير المتشاكل تماما ، قاعدة بيانات علائقية.

Contents

List of Figures

List of tables

Abreviations list

ACL Access Control Lists

AWS Amazon Web Services

API Application Programming Interface

CAD Computer Aided Design

CRM Customer Relationship Management

DoS Denial of Service

EC Elastic Compute

ENS Ecole Normale Sup´erieure

HRM Human Resource Management

IAM Identity (and) Access Management

IBM International Business Machines

IMEI International Mobile Equipment Identity

IMSI International Mobile Subscriber Identity

IP Internet Protocol

IPSEC Internet Protocol SECurity

IT Information Technology

MITM Man In The Middle

OS Operating System

OTP One Time Password

PIN Personal Identification Number

RSA Rivest Shamir (and)Adleman

SLA Service Level Agreement

SMEs Small (and) Medium-sized Enterprises

SQS Simple Queue Service

SSL Secure Sockets Layer

TLS Transport Layer Security

VM Virtual Machine

VMCO Virtual Machine Company

VMM Virtual Machine Monitor

XML XeXtensible Markup Language

General Introduction

Cloud computing is always evolving, with new technologies to respond to new demands. Information technology is centralizing with the emergence of data centers. Cloud computing consists of the interconnectedness and collaboration of information technology system resources, which exist in various internal, external, or hybrid structures and whose access depends on Internet protocols and standards. So, cloud computing has become the most discussed topic today in the IT sector.

In the face of the ever-increasing costs of creating and maintaining information systems, companies are increasingly outsourcing their IT services by assigning them to specialized companies such as cloud service providers.

The main advantage of this strategy for companies is that they do not only pay for services that are actually consumed. As for the cloud provider, the goal is to satisfy the customers' needs by spending the minimum possible resources.

With the development of IT services and resources for cloud computing, security problems arose that compromised data security, and this is what makes it one of the major challenges of the cloud, in fact data security outsourcing is a very desirable topic. Cloud computing security is all the technical, organizational, legal and human resources necessary in place to maintain, restore and ensure security.

Ensuring Cloud Security Computing is one of the activities of cloud management. For better data integrity in the cloud, it is important to protect it before storing it in the cloud to recover the necessary original data.

In this project, we are concerned with data security in cloud computing which is the number one obstacle to adopting the cloud. To remedy this problem, numerous research efforts have been made in recent years to secure and protect data in cloud computing, but protection is imperfect due to the variety of problems and potential attacks.

The main problem that we address with our proposal is untrusted cloud provider and data security issues and detects if the data is corrupt or not.

For this, we conducted our studies according to the following two Parts:

First Part: introduces some basic concepts and generalities about cloud computing, relational database , security in cloud, and the various potential problems and attacks and the proposed solutions for the required security services.

In the **Second Part**, then we present and implement our proposed technology to protect data in cloud computing then present discuss the results of our programming.

Part I: State of the Art

1 Introduction

The concept of cloud computing is constantly evolving, so the concepts and terminology used to define it often need clarification, perhaps press coverage cannot or does not understand the extent of the cloud computing, or explains how companies provide solutions in the cloud or how cloud computing is the way forward Sometimes.

Communications services in the cloud were also discussed, including cloud access methods such as web APIs and media control interface, and the importance of scalability and flexibility in a cloud-based environment.

Here we will see an introduction to the terms, features, and services associated with internet-based computing, referred to as cloud computing.

Basic business service models that are deployed (such as software, infrastructure as a service, and platform) and common deployment models used by service providers and users to use and maintain cloud services such as private , public , community, and hybrid clouds.

Benefits and challenges associated with cloud computing, cloud storage for data and a comparison between normal storage and cloud storage, advantages and disadvantages will be presented. Also, security in cloud computing (various attackers and attacks ...), data security, concepts about sql queries in the cloud.

To achieve this data security in the cloud, many encryption algorithms and techniques have been proposed.

In data encryption during transfer only data is visible when stored in the cloud, and this is completely unsafe. As for the encrypted data during the transfer and when stored in this case, there will be no possibility to perform operations on the data in the cloud, for example, research or mathematical operations on the encrypted data.

2 Cloud computing

2.1 A brief history

The first statement of the concept of cloud computing dates back to 1960 McCarthy claimed that computer resources would be available and consumed by the public in the same way that water and energy were distributed [3]. But by the mid-1970s the idea faded when it became clear that the IT-related technologies of the day were unable to support such a futuristic computing model however, since the turn of the millennium, the concept has been revitalized[45].

The concept of cloud computing was first adopted in 2002 by Amazon, the leader of e-business, who invested in a huge fleet of machines, to accommodate the heavy load of orders placed on their site at the time of Christmas holidays, but relatively untapped the rest of the year. The size of its fleet may cause their unavailability at prime time, which jeopardizes their business during the holidays (a large portion of its sales). Their idea was to unlock all of these unused resources for companies, so that they could rent them out. Since then, Amazon has invested heavily in this area and has continued to grow [3,44]. Today, cloud computing has brought about a devastating change in technology. This change was and will continue to revolutionize the way companies access and provide IT services.

Principale: Remonte service

Cloud computing is a general term for anything that includes the provision of various services hosted remotely via the Internet, these services include tools, applications, and others. The diagram illustrates the principle of remote work[10,13].

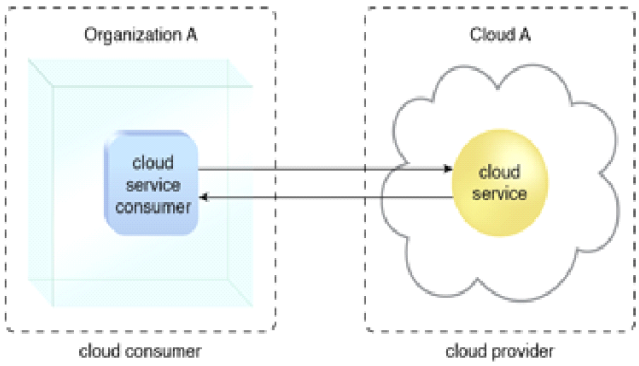

Figure 1: Remote service of cloud[9].

2.2 Cloud computing

The advent of cloud computing was not overnight. At the present time, cloud computing refers to many types of different applications and services that are provided in the Internet cloud. Cloud computing is the most important field of IT industry and the devices used to access it does not require any special applications often.

It is also a rapid model of development through new aspects and capabilities that have been announced.

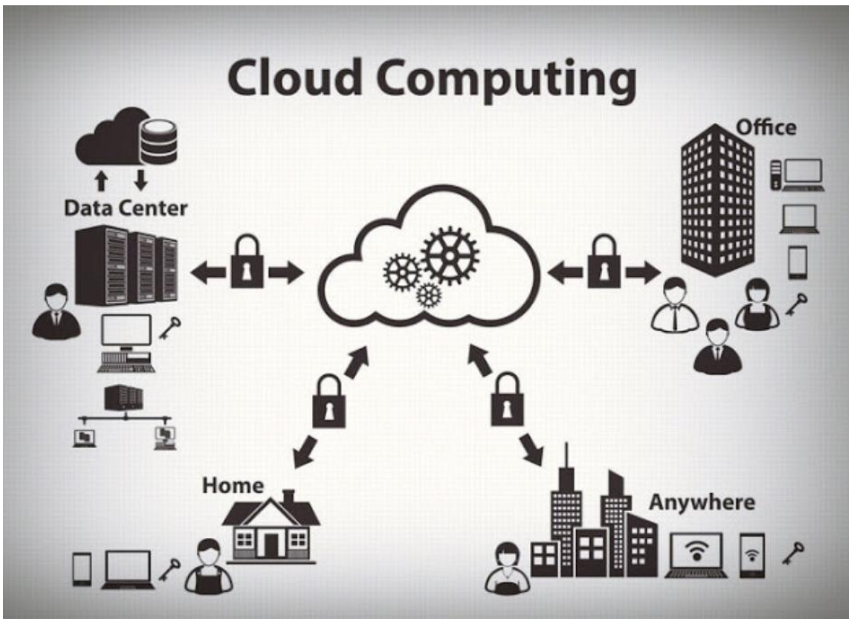

Figure 2: A simple diagram explaining the concept of cloud computing.

Many researchers in the industrial and academic fields have attempted to give a definition of "cloud computing" and to define the set of features that it provides.
- It is a technology that relies on transferring processing and storage space of a computer to the so-called cloud, which is a server device that is accessed through the Internet, and in this way the IT programs transform from products to services (Majid, 2014)[21].

- Cloud computing is internet-based computing through which we can access a large number of shared computing resources such as servers, software applications, and storage applications via Computers and other online devices (Mobaideen, 2015)[22].
- Cloud computing means that computing is used as a service that is subscribed online and not as a product it is purchased and installed on the user's machine. And because it is a subscription service, there are a large number of companies which provide this service for all its different conditions and different types (McCaw, 2013)[23].

- Cloud computing is a term that refers to computer resources and systems. Also, ordering over a network that can provide a number of integrated computer services without being restricted by resources also includes the capabilities of program handling, task scheduling and remote printing (Machey, 2014) [24].

The researcher believes that cloud computing is a group of connected technical servers together, which is centrally managed over a local area network or the Internet, in a so-called cloud, to deliver various computer services to the customer's audience. With the aim of shortening the time, speed of completion and exploitation capabilities and capabilities of a service provider without the need to purchase expensive devices. This cloud can be located in one place or distributed to several places, and also for a private company or centers for renting cloud services [25].

2.3 Objectives

The main goal of cloud computing is to create a community of practices on the concept of cloud computing: the specific goals that are sought to be achieved are :

- Providing objective data in this field by building a dynamic database.
- Generate interest and stimulate the reflection of stakeholders in this area.
- Motivating participation and cooperation and enhancing the information base.
- Ensuring the continuity and clarity of the practice community on cloud computing.

2.4 Main characteristics

Cloud computing is a new way to save it resources, characterized by[7,48]:

2.4.1 Access to self-service upon request

The customer can request his resources according to his needs through an interface that configures the configuration and manages it remotely.

2.4.2 Access the network

From everywhere Capacities are available on the network, can be accessed through standard mechanisms, which facilitate customer access to light or heavy service the heterogeneous platforms.

2.4.3 Pooling of resources

Resources: The resources available to customers are aggregated into a multi-tenant model, with dynamic physical and virtual resources customized according to demand. Usually the customer does not have any control or knowledge of the location of the resources, but is able to identify them with a higher level of abstraction (country, state, or data centre). This sharing of resources is the hallmark of managed cloud computing.

2.4.4 Accelerated flexibility

Accelerated flexibility: the capacities available to the customer (increase or decrease) can be set quickly (a few minutes or even a few seconds) according to the needs and / or loading and automatically in some cases. The user has an illusion of accessing

unlimited resources although the resource always sets a threshold (for example: 20 cases per region is the maximum possible (Amazon EC2).

2.4.5 Service measured permanently

Service measured permanently: the consumed resources are controlled and delivered to the customer and service provider transparently. It ensures a level of conditioning to suit the specific needs of clients. In conclusion, the sum of these five characteristics makes it possible today to determine whether or not the service provided is truly cloud computing.

2.5 Service models

Once cloud services are deployed, how cloud services can be deployed can differ in terms of business models according to requirements [4,5,43].

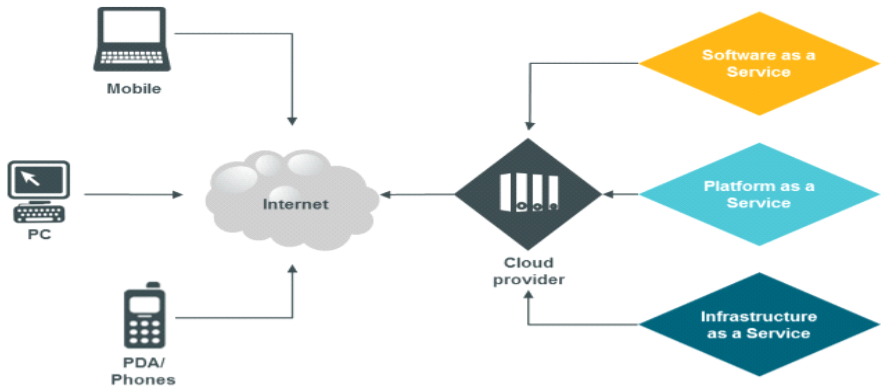

Figure 3: Cloud computing services delivered over the internet[2].

2.5.1 SaaS (Software as a Service)

SaaS application or what is called software as a service, which is software offered for use on the Internet and paid places and free places through advertisements or through selling lists of information for customers, which is known as internal cloud computing applications or what is known as on-demand software.

Consumers buy the ability to access and use an application or service hosted in the cloud, for example Salesforce.com, so that the information necessary for the interaction between the consumer and the service is hosted as part of the service in the cloud. Microsoft has made a significant investment in this area, and as part of the Microsoft® Office 365 cloud computing option, its Office suite is available subscription through its cloud-based services.

2.5.2 Paas (Platform as a Service)

Consumers are allowed to publish their software and applications in the cloud by purchasing access to platforms. The consumer cannot manage operating systems and access to the network, there may be restrictions regarding the applications that can be deployed, for example, Amazon Web Services (AWS) and Microsoft Azure.

2.5.3 Iaas (Infrastructure as a Service)

Consumers can control and manage systems in terms of operating systems, storage, applications and network connectivity, but they do not control themselves in the cloud infrastructure.

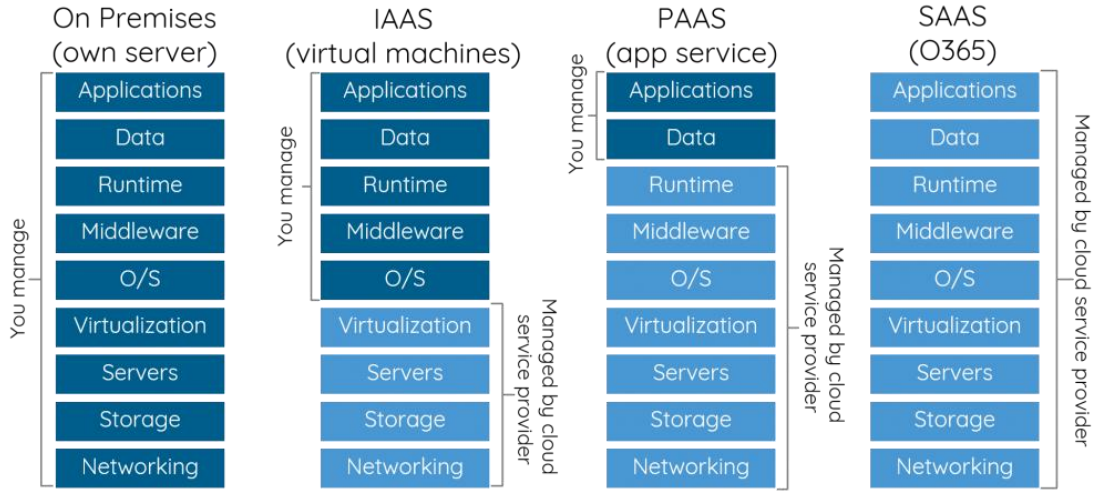

Figure 4: Cloud models[78].

It is also known that the different subgroups of these models may be related to a specific industry or market.

Communication as a Service (CaaS) is one of the subgroups used to describe hosted IP communication services. We can consider Caas a subgroup of SaaS.

2.6 Deployment models

Cloud computing deployment may differ according to requirements, and the following four deployment models have been identified, each with specific characteristics that support the needs of services and cloud users in certain ways see figure 5 [4].

2.6.1 Private cloud

Cloud infrastructure deployed, maintained, and operational for a specific organization. The process may be internal or with a third party in the building.

2.6.2 Community cloud

Cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help reduce the costs of capital expenditures for their establishment as costs are shared between organizations. The process may be internal or with a third party in the building.

2.6.3 Public cloud

Cloud infrastructure is publicly available on a commercial basis by the cloud service provider. This allows the consumer to develop and deploy a service in the cloud with very little financial cost compared to the capital spending requirements usually associated with other deployment options.

2.6.4 Hybrid cloud

Cloud infrastructure consists of a number of clouds of any kind, but clouds have the ability through their interfaces to allow the transfer of data and / or applications from one cloud to another.

This can be a combination of private and public clouds that support the requirements for keeping some data in the organization as well as the need to provide services in the cloud.

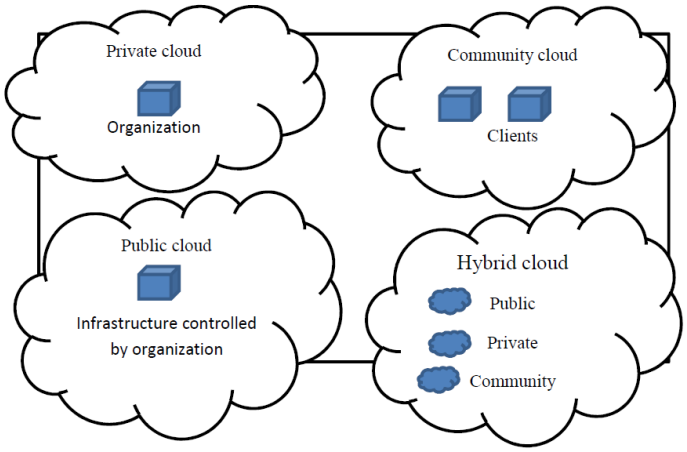

Figure 5: The cloud computing deployment models[26].

2.7 Benefits

Here are some of the potential benefits for those providing cloud computing-based services and applications[64]:

2.7.1 Cost savings

Companies can reduce their capital expenditures to increase their computer capabilities and use operating expenses. This is as a minimum entry barrier and also requires fewer resources to provide system support.

2.7.2 Flexibility

Companies can start with a small publishing process and grow to a large publishing process fairly quickly, and then downsize if necessary. The flexibility of cloud computing also allows companies to use additional resources at peak times, allowing them to meet consumer demands.

2.7.3 Reliability

Reliability Services that use multiple redundant sites can support business continuity and restore ability to work after disasters.

2.7.4 Maintenance works

Cloud service providers maintain the system, and access is done through APIs that do not require application installations on computers, thus reducing maintenance requirements.

2.8 Challenges

The following are some of the noticeable challenges associated with cloud computing. These challenges have a major impact on data security and the performance of cloud systems. Although some of them may cause slowdowns when more services are introduced in the cloud, most of them can provide opportunities if they are resolved carefully and carefully in the planning stages.

Here are the main challenges we saw [27,79]:

2.8.1 Security

Security risks have become more likely to organizations since the emergence of the public cloud. Cybersecurity experts care more about the security of the cloud than

other IT personnel. Whereas, after a 2018 survey by Crowd Research Partners, 90% of security professionals are concerned about cloud security. More specifically, they have concerns about data loss, leakage, data privacy, and breaches of confidentiality.

2.8.2 Managing cloud spending

The RightScale Report found that for some organizations that manage spending on the cloud, it has enduring security as the biggest challenge to cloud computing. According to their own estimates, companies waste about 30 percent of the money they spend on the cloud. Organizations make a large number of mistakes that can help increase their costs. Most of the time, developers or IT professionals spin a cloud instance that's supposed to be used for a short period of time and forget to turn it off again. Many organizations find themselves at bay with vague cloud pricing schemes that provide multiple opportunities for discounts that organizations may not use.

2.8.3 Resource / Experience lack

Lack of resources and expertise that instantly manages security and cost ranked among the top cloud implementation challenges in the RightScale survey. Nearly three-quarters of the respondents said this was a challenge while the rest said it was a huge challenge. While many IT workers are taking steps to enhance their cloud computing expertise, employers are still struggling to find workers with the skills they need. This trend appears to be continuing. Robert Half Technology's 2018 salary guide noted that, "Tech Workers with knowledge of the latest developments in cloud, open source, mobile, big data, security, and other technologies will become more valuable companies in the coming years.

2.8.4 Governance

In this situation, one of the greatest benefits of failed computing - the speed and ease of deploying new computing resources - can become a potential flaw. Experts say organizations can mitigate some of their cloud computing management problems by following best practices, including setting and enforcing standards and policies. Several vendors offer cloud management software to simplify and automate the process. In the RightScale survey, 71% of respondents described it as a challenge, including 25% who saw it as a great challenge.

2.8.5 Managing a multi-cloud environment

Most organizations don't use just one cloud. According to RightScale's findings, 81 percent of organizations follow a multi-cloud strategy, and 51 percent have a hybrid strategy (merging public and private clouds together). Multi-cloud environments add to the complexity that an IT team faces. To overcome this challenge, experts recommend best practices such as conducting research, training employees, actively managing vendor relationships, and rethinking processes and tools.

2.8.6 Migration

which is when cloud service providers or users transfer their data to another cloud service provider and the exchanged data does not have a standard architecture. Most of them use non-interoperable cloud applications. Second, migration of virtual machines which aims to balance the workload between data centers, to avoid hot spots, but it is not easy to achieve.

2.8.7 Vendor lock-in

At present, a small number of vendors, namely Amazon Web Services, Microsoft Azure, Google Cloud Platform and IBM Cloud, dominate the public cloud market. For both analysts and corporate IT leaders, this raises the specter of a seller lock.

2.8.8 Immature technology

Many cloud computing services are at the forefront of technologies such as artificial intelligence, machine learning, augmented reality, virtual reality, and advanced big data analytics. A potential aspect of reaching this exciting new technology is that services do not always live up to the organization's expectations for performance, usability, and reliability.

2.8.9 Integration

Lastly, many organizations, particularly those with hybrid cloud environments report challenges related to getting their public cloud and on-premise tools and applications to work together.

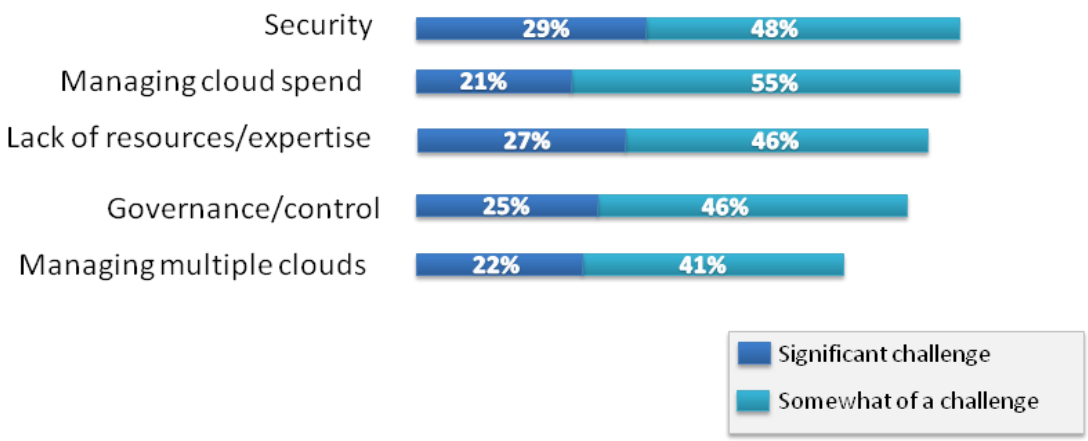

Figure 6: Some of the key challenges facing cloud computing by RightScale 2018 report on state of the cloud[79].

3 Data storage in cloud computing

3.1 Definition

Cloud storage is a service in which data is maintained, managed remotely, and backing up. This service is available to users over a network, which is usually the Internet.

Cloud computing is a hot topic in recent research and applications. So far, Google, Microsoft, IBM, Amazon and some other famous companies have proposed the application of cloud computing, and made cloud computing one of the most important strategies in the future. Cloud storage is the bottom layer of a cloud computing system that supports serving other layers above it. Plus, it is an effective way to store and manage heavy data. So I focused on more attention from some researchers [5]. (Zhang 2008).

Many of these services are available free of charge for a certain number of gigabytes, with additional storage available for a monthly fee. All cloud storage services provide drag-and-sync access to folders and files between your desktop computers and mobile devices with drag-and-drop. It also allows all account users to collaborate with one another on documents.

3.2 Cloud storage types

Many people provide cloud storage resources to cloud service providers because of ease of use and cost savings, as well as making accounting, administration, and

payroll employees simpler. People use cloud services to protect their important data and share it with others. We just need to select the type of cloud storage that best suits the needs of the user. There are three basic types: private, general, and hybrid[11].

3.2.1 Private cloud storage

This system is designed for a company specific to the needs of the customer or one person as the name indicates, for this type of storage two formats are inside the company and hosted abroad. Both work well, but for companies primarily and not for individuals. Also, you have more administrative control and you can design the system according to what you want to achieve according to business needs.

3.2.2 Public cloud storage

This service does not require a lot of administrative controls and can be accessed via the Internet by anyone who hires it. The same security can be obtained as on the private and do not require strict integration with your business needs or private storage concerns.

3.2.3 Hybrid cloud storage

A mixed cloud is a mixture of private and public clouds. The client can customize its features and include applications that meet his needs, in addition to the resources that suit him. Maintaining the most important data can be on the private cloud, while the less important data can be stored in the public. The customer can store data in an efficient storage environment which saves money and time.

3.3 Cloud storage models

There are three forms of cloud data storage: object storage, file storage and block storage. Each one offers its own advantages and has its own use cases [12]:

3.3.1 Object Storage

Applications developed in the cloud often benefit from the enormous scalability and metadata characteristics. Object storage solutions are ideal for building modem applications from scratch that require flexibility and size, and can also be used to import existing data stores for backup, analytics or archiving, such as Amazon Simple Storage Service (S3).

3.3.1.1 Relational database

A relational database is a set of data elements organized as a set of officially described tables through which data can be accessed or regrouped in several different ways, without the need to reorganize the database tables [71].

In other words, a relational database is a group of tables that contain data that is structured into pre-defined classes. Each table (sometimes called a relationship) contains one or more data categories in columns and each row contains a unique instance of data for the categories defined by the columns. When creating a relational database, you can define the range of possible values in the data column and additional restrictions that might apply to that data value. Speaking of the individual elements in the database, It could be a species, a geographic object, or the like. The entity is used a lot. Entities may have attributes and relationships with each other [74].

Here we show a list of the major RDBMS Vendors in the world:

- **MySQL:** One of the most popular open source relational database management systems, developed, distributed and supported by Oracle Corporation. It offers both the proprietary and community version of MySQL.
- **PostgreSQL :** is a robust, open source, and feature rich system - Relational Database Management System (ORDBMS) is known for its excellent support of the ANSI standard. Besides MySQL and SQLite, it is one of the three leading open source implementations for RDBMS.
- **Oracle Database:** Often referred to as the first commercially available RDBMS, it was developed in 1979 by Relational Software, Inc. (Later changed to Oracle Corporation). It is the most popular database management system in the world and the leading supplier of relational database by revenue [77]at the time of writing.
- **Microsoft SQL Server:** Developed by Microsoft Inc. , And it was first released in 1998. It works exclusively on the Windows platform. It is one of the largest commercial database management systems, along with Oracle and DB2.

- **IBM DB2:** traces its root back to System R, in 1974, and is the first relational DBMS based on the original concept of relational database by Edgar Codd [71]. From IBM [74].

I. Structured Query Language

The standard user interface and implementation for a relational database is the Structured Query Language - in short: SQL commands, also called SQL statements, are used for interactive queries about information from a relational database and for gathering data for reports. SQL is a standard interactive programming language for getting and updating information from a database. Although SQL is an ANSI standard and an ISO standard, many database products support SQL with special extensions for the standard language. Queries take the form of a command language that allows you to select, insert, update, locate data, etc. There is also a programming interface [73].

1 SQL data type

Every column in the relational table is declared a data type [73].

The SQL standard and every database resource has a set of data types that it supports. Generally speaking, there are the basics like number, boolean, character, date and time, etc. New data types are included as the technical demand grows, such as XML, JSON, network address, etc [73].

2 SQL Statement

The main part of the SQL language is the statement. Each SQL statement performs a specific action (command) on the database, such as data definition, data modification, query, access control, etc. People often classify or classify SQL statements that modify and query the database as a data processing language (DML: this includes SELECT, INSERT, UPDATE, and DELETE from records within tables.) And those that define data structure as a data definition language (DDL: This includes creating (Tables, Views, Objects, etc.), ALTER and DROP (delete)) [74].

3 Sql in Cloud

Cloud is a fully managed database service that helps you set up, maintain, manage, and manage your relational databases on the cloud. Cloud SQL can be used with MYSQL, PostgreSQL or SQL Server.

3.3.2 File storage

Some applications need access to shared files. This type is often supported by a network attached storage (NAS) server. File storage solutions are ideal for use cases such as large content repositories, warehouses, media, development environments, or home user guides. Like Amazon Elastic File System (EFS).

3.3.3 Block storage

Other enterprise applications often require dedicated low-latency storage for each host, such as databases or enterprise resource planning (ERP) systems. This is similar to Directly Attached Storage (DAS) or Storage Area Network (SAN).

Block-based failover storage solutions are provided with every virtual server and provide the extremely low latency required for high-performance workloads, such as Amazon Elastic Block Store (EBS).

3.4 Compare cloud storage with traditional storage

Since cloud storage is a new product in storage, it will definitely compare to traditional storage. There are many differences between them. Compare cloud storage and traditional storage in Table 1.

Item	Cloud Storage	Traditionnel Storage
Architecture	Not only a structure, but also a service. The underlying use of distributed architecture and virtualization technology, Easy to expand, single point of failure does not affect the overall service.	The architecture is a dedicated, specific hardware component that is used for a particular application.
Service mode	On-demand use, according to the use of billing, service providers can quickly deliver and respond.	The user through the machine to buy or rent the storage capacity.
Capacity	Support for infinite expansion .	For a particular application storage, by the application requirements to define capacity, difficult to expand.
Data management	Not only to provide the traditional way of access, but also to provide massive data management and external public service support, Using the strategy to protect data in the same time.	The user data manager can see the information and is not safe enough. Users can not flexibly configure personalized storage policies and protection policies.

Table 1: The comparison of cloud storage and traditional storage [5] (Loomis 2010).

3.5 The impact of cloud storage on the internet

Enterprise dependence on search engine becomes weaker. At this point, many people try to use Google when they encounter problems. With the development of cloud storage, especially city cloud services, the industry cloud and the corporate cloud. People will prefer direct access to the cloud, and continue searching for information in the cloud. Cloud growth will also increase with instant communication tools, not just with search engines. (Boss 2012).

With the establishment of enterprise cloud, industry cloud, city cloud, more systematic and structured information, people will be more suitable to access information.

3.6 Advantages of storage in cloud

Data cloud storage has many advantages, here are the most important [27] :

Advantages	Description
Usability	All cloud storage services reviewed in this topic contain desktop folders for Mac computers and computers. This allows users to drag and drop files between cloud storage and their files into local storage.
Bandwidth	You can avoid sending files via email to individuals and sending a web link to recipients via your email.
Accessibility	Stored files can be accessed from anywhere via internet connection.
Disaster Recovery	It is highly recommended that companies have a contingency backup plan ready in case of an emergency. Cloud storage can be used as a backup plan by companies by providing a second copy of important files. These files are stored in a remote location and can be accessed through an internet connection.
Cost Savings	Companies and organizations can often reduce annual operating costs with cloud storage; the cost of cloud storage is around 3 cents per gigabyte for internal data storage.

Table 2: Advantages of Storage in Cloud.

3.7 Disadvantages of storage in cloud

Cloud storage has disadvantages, which are as follows (limits)[5]:

Disadvantages	Description
Usability	Be careful when using drag / drop to move a document to the cloud storage folder. This will permanently move your document from its original folder to the cloud storage location. Copy and paste instead of drag / drop if you want to keep the original location of the document as well as move a copy to the cloud storage folder.
Bandwidth	Many cloud storage services have a certain bandwidth allowance. If the organization exceeds the allowance, the additional fees may be significant. However, some providers allow unlimited bandwidth. This is a factor companies consider when looking at a cloud storage provider.
Accessibility	If you do not have an internet connection, you cannot access your data.
Data Security	There are concerns about the safety and privacy of important data stored remotely. The possibility of mixing private data with other organizations makes some companies uncomfortable
Software	If you want to be able to process your files locally with multiple devices, you will need to download the service on all devices.

Table 3: Limits of Storage in cloud.

4 Data security in cloud computing

Cloud computing security is a subdomain associated with cloud computing. Includes concepts such as network security, control strategies, deployed devices to protect data, applications, and cloud-related infrastructure. An important aspect of the cloud is the concept of bonding with different materials which makes it difficult and necessary to secure these environments.

Here we will discuss the types of data in the cloud, including the SQL data and its security in the cloud.

4.1 Data Security Requirements

Data security has consistently been a major issue in information technology. In the cloud computing environment. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. In this section, we make a

comparative analysis of the existing regarding the data security and privacy protection techniques used in the cloud computing.

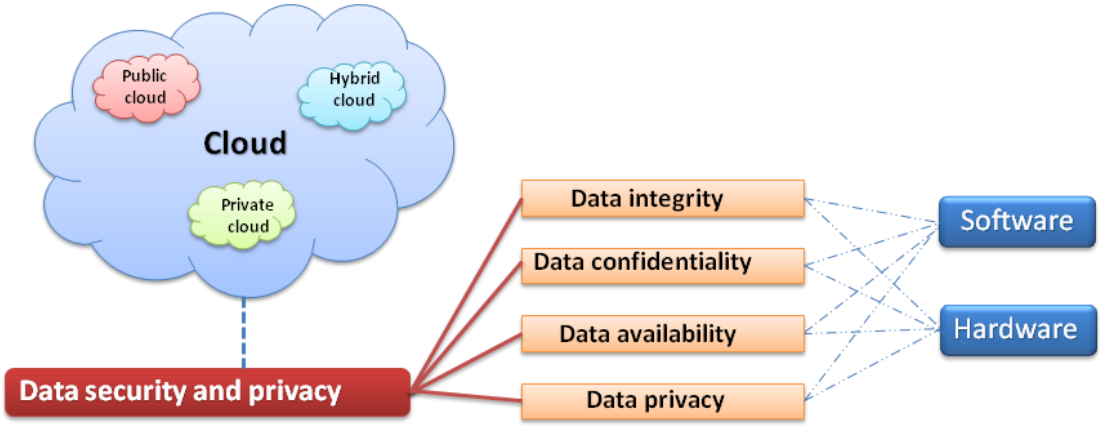

Figure 6: Organization of data security and privacy in cloud computing.

4.1.1 Data integrity

Data integrity is the overall accuracy, completeness, and consistency of data. Data integrity also refers in regards to regulatory compliance (GDPR :General Data Protection Regulation) compliance — and security. It is maintained by a collection of processes, rules, and standards implemented during the design phase. When the integrity of data is secure, the information stored in a database to the cloud will remain complete, accurate, and reliable no matter how long it's stored or how often it's accessed. Data integrity also ensures that your data is safe from any outside forces. [75][76].

4.1.2 Data Confidentiality

Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing cloud reliability and trustworthiness. Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization[76].

4.1.3 Data Availability Data availability means that information must be available when authorized persons need it. Data availability is one of the biggest concerns of service providers. If, for some reason, Cloud service is interrupted, many clients will be affected. Service providers contractually Undertake to ensure an availability level of 99.9%. In addition, the duplication of data and physical resources and their distribution in different locations increases the level of availability. There are many risks that could affect the availability of data in the Cloud such as storage reliability, dependence on internet connection and technical failures [76]

4.1.4 Data Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively. Privacy has the following elements.

(i) **When**: a subject may be more concerned about the current or future information being revealed than information from the past.

(ii) **How**: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.

(iii) **Extent**: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

In the cloud, the privacy means when users visit the sensitive data, the cloud services can prevent potential adversary from inferring the user's behaviour by the user's visit model (not direct data leakage).

The privacy issues differ according to different cloud scenarios and can be divided into four subcategories as follows:

- how to enable users to have control over their data when the data are stored and processed in cloud and avoid theft, nefarious use, and unauthorized resale,
- how to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is an usual choice, and avoid data loss, leakage, and unauthorized modification or fabrication,

- which party is responsible for ensuring legal requirements for personal information,
- To what extent cloud subcontractors are involved in processing which can be properly identified, checked, and ascertained[76].

4.1.5 Non-Repudiation

It means proving that the data has been sent and received, and it also means the ability to verify that the sender and receiver are the two parties who claim to have sent or received the message, respectively[45].

4.1.6 Authentication

consists of ensuring the identity of the user. Access control (for example by password that must be encrypted) can only allow access to resources for authorized people. Without authentication, an attacker could impersonate another user to carry out their attack on the network[45].

4.2 The data life cycle in cloud computing

The life cycle of data in the cloud can be divided into five (5) main steps (data transfer, data storage, use, retrieval, and data destruction)[41]:

4.2.1 Data transit stage:

These are the stages related to sending data from the company's internal systems to the cloud or returning it, where companies can encrypt data internally before transferring and then send it or use the standard protocols in the encryption function which is IPSEC (Internet Protocol Security) and SSL (Secure Sockets Layer (Widespread). These protocols make it possible to transfer data to and from the cloud safely, so that the systems become reliable and easy to use.

4.2.2 The data storage stage:

Once data reaches the cloud it is stored, if there are no recognized standards, implementation of cryptographic functions of the service provider depends. Some of them offer systems whose work is often not clear.

If the cloud stores data to ensure its availability, it is best to encrypt the data before it is sent by the cloud client. It is also clear that in the case of the service type (SaaS), encryption can only be performed by the resource, as there is no role for the final customer in this coding step.

4.2.3 Using data in the cloud:

VM is a virtual machine, deployed to the IaaS cloud (Infrastructure as a Service). VM uses a file system to store the, applications, and application data and operating system. Even if we encrypt this file system, the decryption of the key must be present in the VM for it to work. An attacker could gain access to the data on the VM if he could recover these keys. In this particular case, the security of the data will depend on the access control metrics that are set up to access the data, either for external access only to those responsible for the cloud or the access of operators.

4.2.4 Data recovery:

It is necessary to obtain a guarantee that you have the means to recover data in the event of problems other than the lack of it. The refund must be viable for implementation in accordance with the terms of the final criteria that respect and take into account authorized restrictions and business needs. However, the data must be published in a transparent manner to the cloud user.

4.2.5 Destroying data:

Once the data has been recovered from the cloud, it is important to ensure that it is destroyed. But what are the means, procedures and obligations that are implemented by the supplier to do this (erase all traces of your data). In this case, encryption can be used. But in reality, without a decryption key, the previously encrypted data is completely unfit for use. To destroy data, just destroy the encryption key. This is the solution or concept that makes it possible to ensure that the data is inaccessible even in the extreme case where the cloud service provider destroyed the key without his prior knowledge.

4.3 Attackers classification

With the advent of the Internet, cybercrime has become widespread; the perpetrators are ordinary teenagers or real professionals[4].

4.3. 1 Kiddie Scripts:

The most common hacker category included teenagers. This is often used when playing with scripts and other software that is downloaded randomly from the Internet. These scripts are used against random targets. Fortunately, discovering the scenario is easy, despite the low or no qualification level, children's scripts sometimes pose a real threat to system security. On the one hand, the kiddie texts are very many, and on the other hand, they are often stubborn to the point that sometimes several

days pass in an attempt to all possible combinations of the password, which leads to the risk of success a lot though.

4.3.2 Real pirates:

Real pirates, besides children's scripts, are people who are enthusiastic about networks and seek to understand the work of computer systems and test the capabilities of the tools and their knowledge.

Generally they have a high level of creativity, real hackers love to explore and exploit vulnerabilities in any kind of database systems, server applications, web servers, etc. Most intruders claim to break into systems out of passion for computers and not to destroy or steal data.

4.3.3 The internal threat:

it represents a third category by the pirates in enclosed places. Usually they are employees or former employees of a company who work out of personal revenge or as part of economic espionage. Many companies condone such threats.

4.3.4 Organized structures:

This last fourth category relates to piracy of governments, terrorist and criminal organizations, their economic or ideological motives.

4.4 Attacks classification

The trends of the world are increasing more and more towards cloud computing, to become more complex and this is what attracts the attention of attackers to find and detect new weaknesses. Computing faces a specific type of attack. An attack represents any action that harms the security of the information held by an organization or individual, so we will see the various attacks that face cloud computing here (the core)[4]:

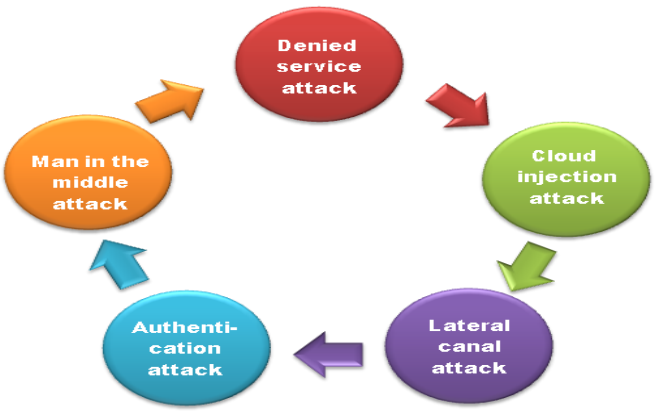

Figure 7: Types of attacks in cloud computing[4].

4.4.1 Denied service attack (DoS Attacks)

Principle

Denial of service attacks is a scourge that can affect any company server or any other person connected to the Internet. The purpose of this attack is to harm corporate reputation not to recover or change data, and it may adversely affect their performance if their activity depends on the information system. Technically, these attacks are not complicated but they are no less effective against any type of device with an operating system (Windows, Linux, or Unix commercial) or any other system. The cloud is more vulnerable to attack by denying the service as defined by the Cloud Security Alliance because it is used by many users which makes it the most harmful.

The principle of denial or denial of service is the transmission of unusual size IP packets or data in order to cause saturation or an unstable state of victim devices, thus preventing them from ensuring the network services they provide.

4.4.2 Cloud injection attack

Principle

In a malware attack, an attacker attempts to inject a malicious service or device virtual in the cloud. In this type of attack the attacker creates his own unit implement malicious services (SaaS or PaaS) or an instance of the virtual machine (IaaS), and is trying to add it to the Cloud. The main scenario behind Cloud injection attack is that the attacker conveys an instance of service Malware in the cloud so that service requests can be accessed through victim. To do this, the attacker must control the victim's data in the cloud. According to the classification, this attack is the main representative of exploitation cloud attacks. The purpose of this attack may be something, things where the attacker is interested; data modifications can include, changes to full functionality or back obstacles.

4.4.3 Lateral canal attack

Principle

An attacker tries to hack the Cloud system by placing a virtual machine, the attack is near the target cloud server system, and then launch side channel attack. Side channel attack appeared as a kind of effective threat security targets the implementation of a cryptographic algorithm system. Therefore it is important to evaluate cryptographic systems that are side-attack attack to design a secure system. Side channel attacks use two steps:

VM CO-Residence and Placement : An attacker can often place his position on the same physical machine as the target instance.

VM Extraction: The ability of a malicious example to use side channels to find out information about common cases.

It can be very easy to get confidential information from a device, so security should be provided against side channel attacks in the cloud.

4.4.4 Authentication attack

Principle

This type of attack can be easily produced in cloud environments. whereas attackers easily target servers with these types of authentication attacks. Attackers target the user's mechanism. The mechanism used to be capture authentication and attackers attempt to access confidential information. They use different decryption mechanisms to transfer the most confidential data.

4.4.5 Man in the middle attack (Cryptographic Attacks)

Principle

In this attack, the attacker intercepts messages when exchanging public keys, then it resends it, replacing its public key so that both parties can they are still in contact with each other. The sender of the message not realizing that the receiver is an unknown attacker when trying to access or modify the message before resending it to the recipient. So the attacker controls the whole communication process.

In MITM Attack, see Figure 8, message between two computers (here a PC on the left and a server on the right) the message was intercepted by a third party, here MITM. Looks like chatting between the computer and the server. But all messages actually pass through MITM, which they can read and pretend to be returning or one of the two ends (computer or server).

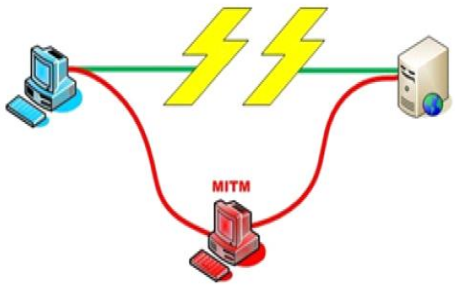

Figure 8:Main in the middle attack[4].

4.5 Data security algorithms and techniques in the cloud

Several algorithms and technologies and solutions for securing data in the cloud have been proposed. These solutions can be classified according to several criteria, whereby the classification of security technologies or solutions depends on the security strategy and the principle of the coding inspired [29].

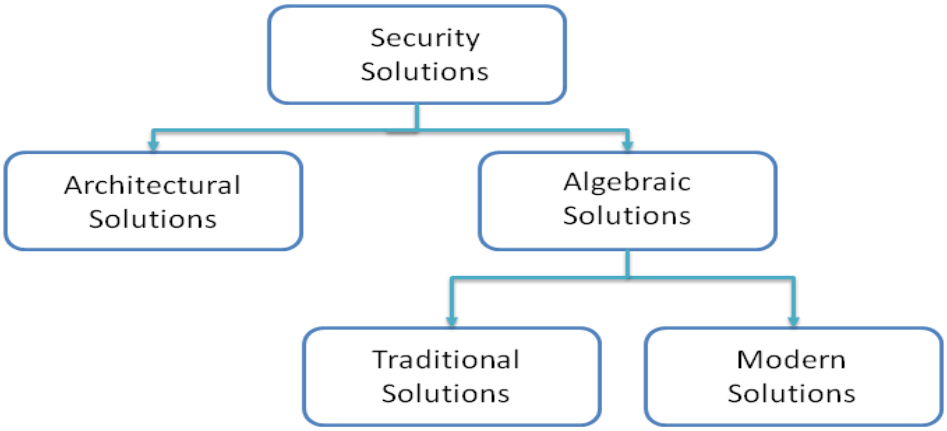

Figure 9: Taxonomy on cloud data security solutions[29].

4.5.1 Architectural solutions

In the work of several researchers, multi-cloud structures have been identified which makes it possible to maintain safety in the cloud. These structures or structures are suitable for cloud platforms, and these structures generally do not provide a server or intermediary agent between the cloud provider and the client. Using the multiple cloud mechanism can reveal different theories to target different aspects of security of confidentiality, integrity, and consistency in data stored in different clouds. This architecture uses the principle of regular distribution of user data across multiple cloud service providers [30,31,32,33].

Work in [34] , provides two cloud buildings with a series of communication protocols for external database service. The proposed technology guarantees data protection, confidentiality, statistical characteristics, and application design. The proposed system includes a database administrator and two unplanned clouds. In this form, the database administrator can execute on the client side. Both Clouds (referred to as Cloud A and Cloud B) provide storage and computing service. The two Clouds work together to respond to each Client / Certified user.

Working with a secure database requires encryption and data storage, data storage is external(cloud A) and keys for encryption in the second cloud (cloud B).

Experimental results of this structuring or approach show that confidentiality requirements can be met and that they are an effective method in established databases, but the effectiveness of the approach is reduced.

With the increase in the size of databases. In this case, the complexity of the approach is higher, the increase in the required memory space is greatly increased, and thus it is not possible to cover the processing of requests for certain operations such as operation SUM.

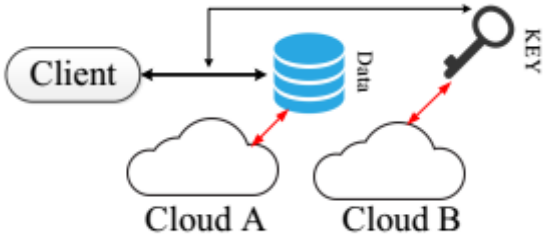

Figure 10: Architecture with two clouds[29].

4.5.2 Algebraic solutions

In recent years, a lot of internet based applications have appeared such as online shopping, stock trading, paying electronic bills etc. These transactions over public wired and wireless networks require secure communications from both parties, and are confidential to ensure data authentication and also to ensure availability and integrity.

Computer Security Guide NIST defines the term computer security as "the protection afforded to an information system in order to achieve applicable goals for maintaining the integrity, availability, and confidentiality of information system resources (including hardware, software, and firmware) and information / data and communications". Security is a mechanism by which services and information are protected from unintended access, change, or destruction. Security in networks is based on encryption and message transfer science to make it safe against any attack. Encryption is a key way to ensure the security of sensitive information.

We have here two types of encryption techniques and algorithms, traditional and modern.

4.5.2.1 Traditional solutions

Cryptographic algorithms traditional perform different transformations and replacements over plain text, many cipher algorithms traditional are available and widely used in data security. Encryption algorithms traditional are classified into two groups: symmetric encryption (also called a secret key) and asymmetric encryption (also called a public key).

Symmetric key encryption is a form of encryption system in which encryption and decryption are performed using the same key. Also known as traditional cryptography.

Asymmetric encryption is a form of encryption system in which encryption and decryption are performed using different keys. One is a public key and the other is a private key. Also known as public key encryption. The key is alphanumeric, numeric, or special code[49].

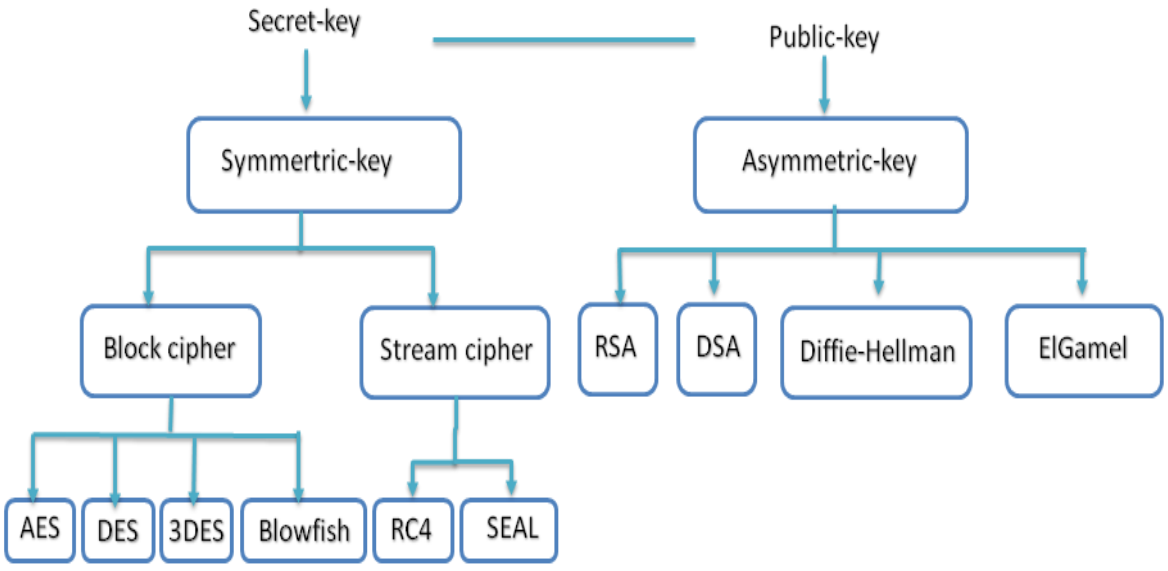

Figure 11: Classification of encryption methods[49].

I. Symmetric encryption algorithms

Symmetric encryption is widely used to protect information in many modern computer systems for its high speed. Here we will list some of the famous symmetric encryption algorithms.

DES algorithm

DES algorithm is the most common symmetric security algorithm. This means that the same keys are used to encrypt and decrypt sensitive data. It uses 8 bytes for encryption and decryption of data, which means that the key length is 8 bytes (64 bits). But you use 1 byte(8 bits) to check parity. It is a block cipher algorithm, which is why the data block size for the DES algorithm is 64 bits. For encryption and decryption of data the DES algorithm uses the structure of Feistel therefore, some uses round to encrypt / decrypt data. Although the block size is 64 bits, the number of rounds will be 16 rounds. Therefore, you will use different keys for each round. So the number of surveys will be 16 subkeys[53].

General Structure of DES is depicted in the following illustration:

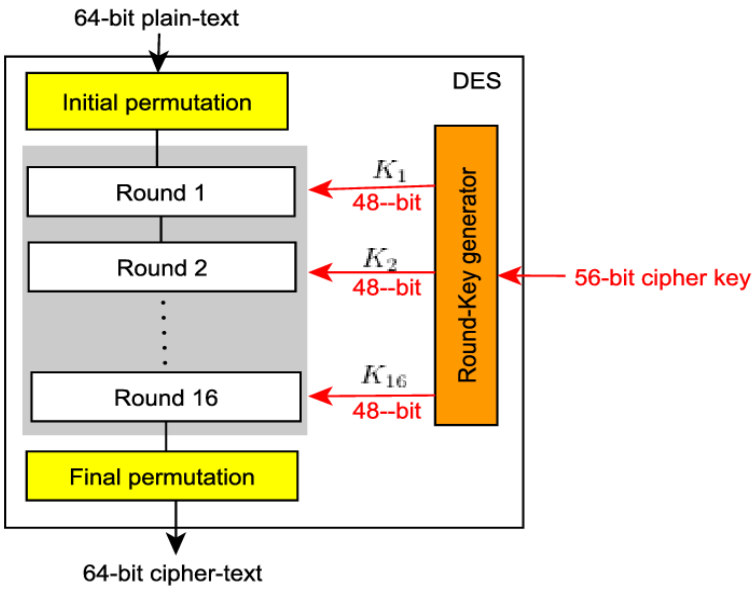

Figure 11: General structure of DES[42].

Modes of Operation

There are different modes of operation when using the DES algorithm. If each 64 bit is encrypted or decrypted independently, then this mode is ECB.

If each 64-bit data is dependent on the previous one, then this mode is called CBC or CFB mode.

Triple DES algorithm

3DES it is one of the types of encryption algorithms and it is considered one of the types of block encryption algorithms (BLOCK) and it is considered an improved alternative to the DES algorithm that was known to be safe, but after it was penetrated and revealed how it was broken it became the need for a very important alternative. Perhaps the main defect in the DES is that the length of the encryption key is very short As it was 168 bits long, "one of the suggestions to fill this gap is to lengthen the key, but the original algorithm may not be of use with a long key, so the proposal also included that the message be encoded three times by different keys, this of course bridged one of the holes, but other holes remained unchanged. These vulnerabilities have weakened 3DES, though it is still safe[54].

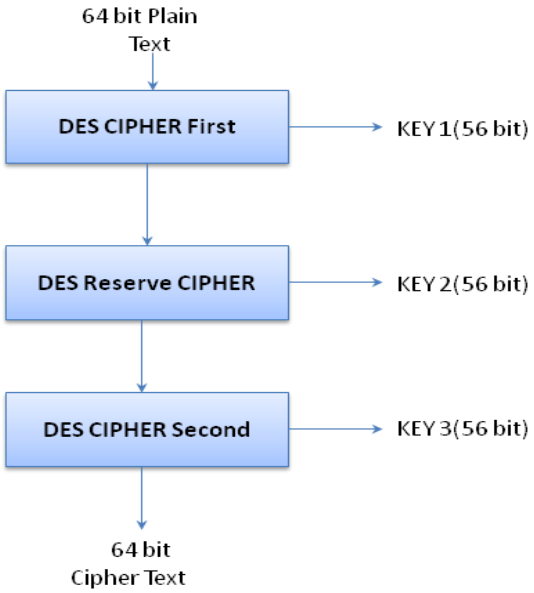

Figure 12: 3DES algorithm[56].

How to encrypt clear text in Triple Des:

1- Clear Text blocks using (Single Des Block With key 56 bit (k1))

2- Output encoding the first process again using (Single Des Block With key 56 bit (k2)).

3- Encode the second process output again using (Single Des Block With key 56 bit (k3)).

4- The final output is Ciphertext.

How to decrypt ciphertext in Triple Des:

The decryption process takes place just as the encryption process is done and the only difference is that the decryption process will take place unlike the encryption process where the user begins to decode K3 and then decode K2 and then K1 and the end result is clear text.

Blowfish algorithm

The blowfish algorithm is a type of symmetric encryption algorithm developed by (Bruce Schneier). This algorithm can be used to be a data encryption standard, a data encryption standard (DES) because of its advantages. This algorithm for its key takes different lengths (from 32 bits to 448 bits) as the key length between these two numbers is mentioned. This makes it ideal and very fast-paced compared to the Des algorithm[49].

How it works:

In terms of work, this algorithm is divided into two parts

Part One: Key Expansion (Key Expansion)

Part Two: Data Encryption (Data Encryption)

The 448-bit key expands to subkeys totaling 4168 bytes. These keys are generated just before the encryption and decryption process. Where P has 18 arrays, each one has 32 bits. P1, P2, ……. P18.

There are four (S-boxes 32 bit) consisting of 256 bits for each of them.

Example:

S1,0, S1,1, ……. S1,255

S2,0, S2,1, ... S2,255

S3,0, S3,1, ... S3,255

S4,0, S4,1, …… ..S4,255

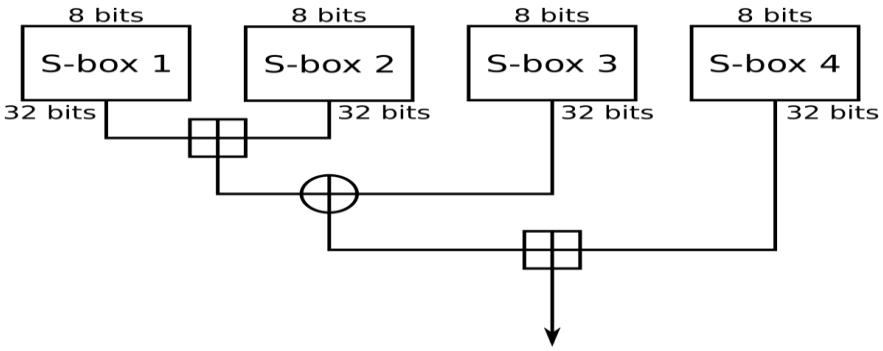

Figure 13: The Feistel structure of Blowfish[55].

AES algorithm

AES (Advanced Encryption Standard), is one of the most popular ways to encrypt important data, and it is used before organizations from Apple to Microsoft to the National Security Agency.

AES is a unique advanced encryption standard algorithm thanks to the following advantages: protection, cost, implementation.

Terminal encryption algorithm, this encryption method stores information using a terminal encryption algorithm. It works on entering plain text and outputting encoded text, measured by bit. For example, when using 128-bit AES, there are 128 bits of ciphertext that produce every 128 bits of plaintext.

Generally, there are three advanced encryption standard terminal codes AES-128, AES-192 and AES-256. Each advanced encryption standard code encrypts and decrypts 128-bit data sets using 128, 192 and 256-bit encryption keys, where 256-bit is safer. For 128-bit keys, there are 10 cycles of the encryption process, 12 cycles of 192-bit keys and 14 cycles of 256-bit keys. The AES algorithm is the same, which means that the same key is used for the encryption and decryption process, so the sender and recipient know that they are using the same key.

With continuous technical progress, cyber attacks are ever increasing. Currently, there is no known way to hack AES encryption, which makes it a strong protection force and essential to protect your information and reduce the risk of any attacks. AES encryption already integrates with many software and hardware systems, and if fully reliable, its capabilities seem limitless[52].

II. Asymmetric encryption algorithms

We can apply asymmetric encryption to systems where many users need to encrypt and decode a message or a group of private data when speed and computing power are not required. We can use a public key for encryption and another private key for decryption. Here we have an explanation of some of these types of algorithms.

RSA algorithm

A method has been suggested for implementing a public key cryptography system whose security depends on the difficulty of manipulating large prime numbers[50].

It was so successful that the public key algorithm RSA is used today in the world. Through this technology, it is possible to create signatures and encrypt digital data.

The encryption scheme uses RSA and signature of the fact that:

$$m^{ed} \equiv \text{m(mod n)} \qquad (1)$$

For an integer m. encryption and decryption schemes are displayed in formulas 1 and 2. Decryption works for it:

$$c^d \equiv (m^e)^d \equiv \text{m(mod n)} \qquad (2)$$

The safety lies in the difficulty of computing a clear text m from a ciphertext

$\text{c} = m^e \, mod \, n$ and the public parameters n (e)[51].

Diffie-Hellman algorithm

It is an encryption protocol that allows two people who do not already know each other to create a shared secret key on an insecure channel. This key can then be used to encrypt subsequent conversations using the symmetric key encryption algorithm. One of the first protocols that appeared in the field of public key cryptography has appeared for the first time in 1976, in which Diffie and Hellman offer a specific way to carry out the task of exchanging keys, and this is by a mathematical issue called the problem of intermittent logarithm.

Here we will explain what is used in this encryption, and how it works on a step-by-step basis. Let the users be named Alice and Bob.

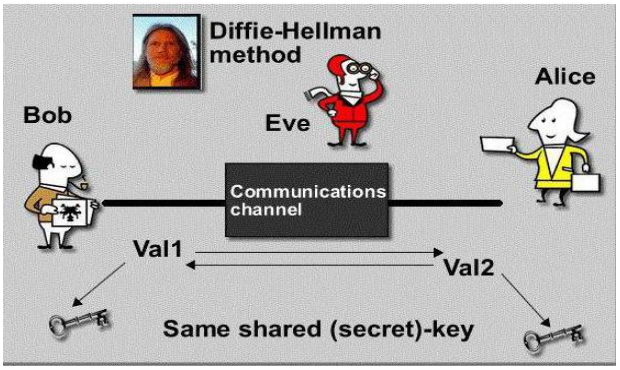

Figure 14: A simplified explanation of Diffie-Hellman algorithm.

Initially they agreed on two prime numbers, Alice now chooses a large random number as her private key, and Bob also chooses a large number. Then they calculate the key that they will send to the other.

Now both Alice and Bob count their common key, which Alice calculates as Bob does.

$$K=B^a \ (mod\ p) = (g^b)^a \ (mod\ p)$$

and Bob computes as

$$K=A^b \ (mod\ p) = (g^a)^b \ (mod\ p).$$

This can be done by computing α from $A= g^a \ (mod\ p)$ or b from $B=g^b (mod\ p)$. This is the discrete logarithm problem, which is computationally infeasible for large p . The security of the RSA encryption system depends on the time it takes to calculate the separate logarithm of a module approximately the same amount as it takes to analyze the product of two major devices of the same size as p, so Diffie-Hellman is almost safe. [57].

ElGamel algorithm

It is an encryption algorithm devised by Taher El-Gamel in 1985, which is used for encryption of open keys to the public. It relies on the Diffie-Hellmann principle to exchange cryptographic keys.

El-Gamel has the disadvantage that encoding text is twice the length of plain text. It has a feature that gives it the same plain text as a different encoding text every time it is encrypted.

Here we will explain what is used in this encryption[58,59]. Let the users be named Alice and Bob.

Alice chooses

i) A large prime ρ_A (say 200 to 300 digits),

ii) A primitive element α_A modulo ρ_A,

iii) A (possibly random) integer d_A with $2 \leq d_A \leq \rho_A - 2$.

Alice computes

iv) $\beta_A \equiv \alpha_A{}^{d_A} \pmod{\rho_A}$.

Alice's public key is $(\rho_A, \alpha_A, \beta_A)$. Her private key is d_A.

Bob encrypts a short message M ($M < \rho_A$) and sends it to Alice like this:

i) Bob chooses a random integer k (which he keeps secret).

ii) Bob computes $r \equiv \alpha_A{}^{k} \pmod{\rho_A}$ and $t \equiv \beta_A{}^{k} M \pmod{\rho_A}$, and then discards k.

Bob sends his encrypted message (r, t) to Alice.

When Alice receives the encrypted message (r, t), she decrypts (using her private key d_A) by computing tr^{-d_A} .

Note

$$tr^{-d_A} \equiv \beta_A{}^{k} M (\alpha_A{}^{k})^{-d_A}$$

$$\pmod{\rho_A} \equiv (\alpha_A{}^{d_A})^{k} M (\alpha_A{}^{k})^{-d_A}$$

$$\pmod{\rho_A} \equiv M \pmod{\rho_A}$$

Even if Eve intercepts the ciphertext (r, t), she cannot perform the calculation above because she doesn't know d_A.

$$\beta_A \equiv \alpha_A{}^{d_A} \pmod{\rho_A}, \text{ so } d_A \equiv L_{\alpha A}(\beta_A)$$

Eve can find d_A if she can compute a discrete log in the large prime modulus ρ_A, presumably a computation that is too difficult to be practical.

Caution: Bob should choose a different random integer k for each message he sends to Alice.

If M is a longer message, so it is divided into blocks, he should choose a different k for each block.

DSA algorithm

The digital signature algorithm (DSA) is one of the federal information processing standards for making digital signatures dependent on the mathematical concept or we can say standard exponential formulas and the separate logarithm problem of digitally signing encoding in this algorithm. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in the Digital Signature Standard (DSS).

A digital signature is a value that is computed from the data and a secret key that only the signer or the person whose signature is that knows. In fact, in the real world, the recipient of the message needs to ensure that the message belongs to the sender and should not be able to penetrate the origin of this message due to misuse or anything[60,61].

The first part of the DSA algorithm is the public key and private key generation, which can be described as[62]:

- Choose a prime number q, which is called the prime divisor then choose another primer number p, such that p-1 mod q = 0. p is called the prime modulus.
- Choose an integer g, such that 1 < g < p, g^q mod p = 1 and g = $h^{(p-1)/q)}$ mod p. q is also called g's multiplicative order modulo p.
- Choose an integer, such that 0 < x < q, compute y as g^x mod p, package the public key as {p,q,g,y}, package the private key as {p,q,g,x}.

The second part of the DSA algorithm is the signature generation and signature verification, which can be described as[62]:

- Generate the message digest h, using a hash algorithm like SHA1.

- Generate a random number k, such that 0 < k < q.
- Compute r as (g^k mod p) mod q. If r = 0, select a different k.
- Compute i, such that k*i mod q = 1. i is called the modular multiplicative inverse of k modulo q.
- Compute s = i*(h+r*x) mod q. If s = 0, select a different k.
- Package the digital signature as {r,s}.

To verify a message signature, the receiver of the message and the digital signature can follow these steps[62]:

- Generate the message digest h, using the same hash algorithm.
- Compute w, such that s*w mod q = 1. w is called the modular multiplicative inverse of s modulo q(compute u1 = h*w mod q , compute u2 = r*w mod q and compute v = (((g^{u1})*(y^{u2})) mod p) mod q).

If v == r, the digital signature is valid.

4.5.2.2 Modern solutions

The restrictions, primarily confidentiality, obligate researchers to provide other data protection technologies. Some businesses take advantage of one or more encryption technology in the cloud and thus the best known concept is "Homomorphic". Homomorphic It is a feature that allows calculations to be assigned to the cloud, without data or results being available to the cloud provider. Symmetric encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the customer is the only owner of the secret key. When we decode the result of any process, it is as if we had calculated the raw data. In the proposed modern techniques, we can study coding systems for Partially Homomorphic Encryption, Somewhat Homomorphic Encryption and Fully Homomorphic Encryption [37].

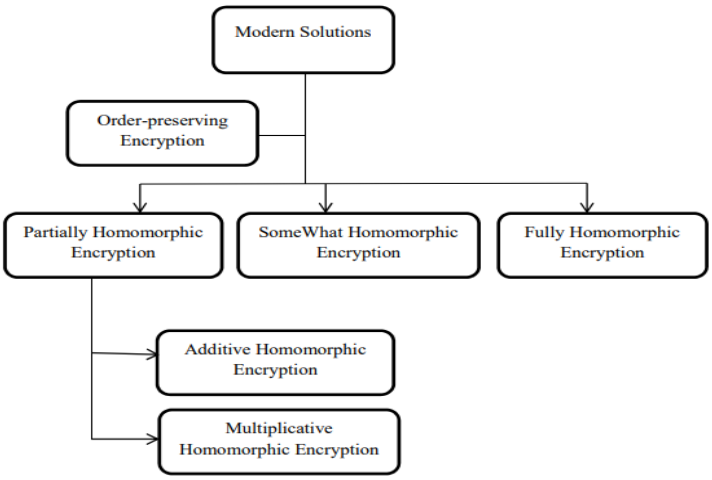

Figure 15: Techniques modern of data security[29].

4.5.2.2.1 Partially homomorphic encryption

We talk about a system that is partially homogeneous when its own subject area of assessable functions is limited by the area of accountable functions. Partially symmetric encryption PHE allows us to perform only some operations on encrypted data such as addition or multiplication, but not the two.

This coding process or two systems can be named or divided into two categories, the first category being in homogeneous coding schemes added that allow limited or unlimited additions to encrypted data [38,39]. The second category of duplicate homogeneous coding schemes allows for limited or unlimited multiples of encoded data [40].

However, with all this, the PHE systems are not effective because the actual requests are mostly or all of them include multiple processes that exceed what can be controlled by these systems (PHE).

Symmetric encryption increases the computational burden on the data owner of mobile devices restricted by mobile phone resources and increases the high communication burden due to the connection between the cloud server and the authorized user to recover files.

4.5.2.2.2 Somewhat homomorphic encryption

In Sometimes Homomorphic Encryption (SWHE), multiple unlimited multiples and additions can be made to encrypted data, but the mode and number of operations are

limited in certain terms. This coding system was the first algorithm to be computed using schemas on encrypted texts [29].

Somewhat Homomorphic Encryption (SHE): In SHE, both addition and multiplication operation is allowed but with only a limited number of times[35].

4.5.2.2.3 Fully homomorphic encryption

Fully Homomorphic Encryption (FHE), new security concept on cloud computing. This system can calculate any type of job on encrypted data. Most of the works in FHE have been designed to compute with noise during coding to obtain completely homogeneous properties[29].

Fully Homomorphic Encryption allows a large number of different types of evaluation operations on the encrypted message with unlimited number of times[35].

Also, it basically allows FHE to do random computations on encrypted data. Computing on encrypted data means if the user has an f function and wants to get f (m1, ... , mn) for some input m1,... Mn, it is possible to alternatively compute to encode these inputs, c1,... , Cn, to get a result that decodes to f (m1, ... , mn)[36].

4.5.2.2.4 Ordre-preserving encryption

This property ensures the arrangement between data elements based on their encoded values, without disclosing the data. This enables us to create an index of encrypted data that can be used on request queries. [46,47].

Therefore, technologies for homogeneous security can be provided through encryption mechanisms. To choose the appropriate technology or mechanism, the mechanism must meet the user's specified restrictions - key size, data, processing time, and data properties.

Here we propose a completely homogeneous coding of the arrangement in a scheme created by simple standard and linear expressions of the formula $(a * x + b) \bmod p$.

The expressions used are clear, but the(a, b, p) transactions are kept confidential. An attacker could not obtain sufficient information to solve these linear equations from the input values that were created, so the proposed coding and indexing system was theoretically safe. In the next part we will review the details of this proposal.

5 Conclusion

Cloud computing is a promising technology for the next generation of IT applications. The barriers and obstacles to the rapid growth of cloud computing are issues of privacy and data security. Reducing the cost of storing and processing data is a mandatory requirement of any organization while analyzing data and information is always the most important task in all organizations for decision making. Therefore organizations do not transfer their data or information to the cloud until trust is built between the cloud service providers and consumers. Several techniques have been proposed by researchers to protect data and to achieve the highest level of data security in the cloud. However, there are still many gaps that need to be filled by making these technologies more effective. More work is required in the field of cloud computing to make it acceptable to cloud service consumers. This section surveyed the concepts of cloud computing and data storage and use in the cloud ,focusing on the different attacks and attackers, different solutions and techniques about data security and privacy, for data protection in the cloud computing environments to build trust between cloud service providers and consumers. In the next part we will present our proposed solution as well as the implementation.

Part II: Proposal and Modeling

1 Introduction

The goal of cloud computing is to provide resources transparently Information technology for its customers. The cloud should be reliable, safe and effective the cloud age forces companies of all types and sizes to protect the assets of important information more interactive way. Provide Security information is actionable.

To achieve this data security in the cloud, many encryption algorithms and techniques have been proposed.

In data encryption, during transfer, only data is visible when stored in the cloud, and this is completely unsafe. As for the encrypted data during the transfer and when stored in this case, there will be no possibility to perform operations on the data in the cloud, for example, research or mathematical operations on the encrypted data.

In this part, we show our solution which is mainly based on coding, depending on the idea that underlies it as well as the process shown in the diagram. Finally, we will end with the validation phase of the submitted solution.

This part aims to mention the most relevant ideas exploited in the implementation of the system, conceived before. for this we will give the IT environment supporting our system.

After the presentation of this environment and its motivations, we then move on to the next section which is devoted to the presentation of the realization of our application as well as certain results obtained.

2 The proposed solution

The use of encryption technology that ensures the uniformity of form and structure between encrypted data. The basic requirements are binding on it. This commitment is very important when resolving confidential issues or when there is a lack of trust between users and cloud service providers. For this purpose, we offer a successful process that can be accomplished in a database that exists at the level of cloud environments that we do not trust.

Accordingly, in this section the goal is to find a method for calculating the quantitative data, the proposed FHE technique allows random operations to be performed on the quantitative data. Here we will explain the details of the proposal.

2.1 Preliminary and formal model

The definition of a homomorphism is given by the following explanation:

Let there be two groups (M, ◊) and (C, □). We denote by e_M (respectively e_C) the neutral element of M (respectively of C). A map $f : M \rightarrow C$ is a group homomorphism if:

- If x and y are two elements of M, then $f(x \lozenge y) = f(x) \square f(y)$.
- $f(e_M) = e_C$

Property: Let $f : M \rightarrow C$ be a group homomorphism. So:

1) $f(1_M) = 1_C$

2) For any element x of M, $f(x^{-1}) = f(x)^{-1}$

3) For any non-zero integer n, $f(x^n) = f(x)^n$

4) For any non-zero integer n, $f(x^{-n}) = f(x)^{-n}$

Formally, if c_1 and c_2 are two elements of a group noted C and which are the cyphers of m_1 and m_2 respectively, where m_1 and m_2 two elements of a group noted M. A cypher function $f: M \rightarrow C$ is a homomorphism if there are two operations ◊ and □ such that:

$$f^{-1}(c_1 \lozenge c_2) = f^{-1}(c_1) \square f^{-1}(c_2) = m_1 \square m_2$$

Typically, ◊ will be modular addition or multiplication, but this is not always the case.

In addition, the following axioms must be satisfied:

Closure: For each $m_1, m_2 \in M$ the result of the operation $m_1 \square m_2 \in M$.

Identity element: There exists an element $e \in M$, such that for any element $m \in M$, the equality $m \square e = e \square m = m$ is true. Such an e is a single element, so we call e the element identity.

Inverse element: For each $m_1 \in M$, there exists an element $m_2 \in M$ such that:

$m_1 \square m_2 = m_2 \square m_1 = e$ where e is the neutral element.

With

- $A \equiv M$, $A' \equiv C$
- $(a,b,c) \equiv (m_1, m_2, m)$
- $(a',b',c') \equiv (c_1, c_2, c)$

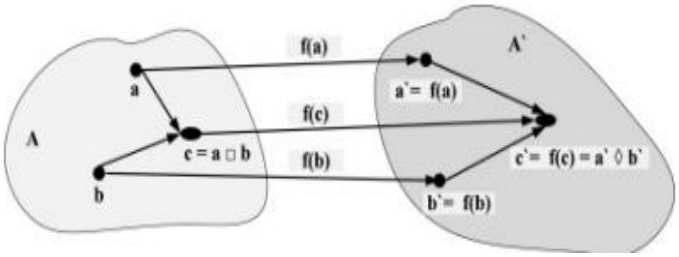

Figure 16: A homomorphism encryption.

A homomorphism $f : A \rightarrow A'$ is a structure-preserving map between sets A and A' with the composition operations □ and ◊, respectively. Let a,b,c ∈ A with c = a □ b and a',b',c' ∈ A' with c' = a'◊b'. Let a' = *f* (a), b' = *f* (b), c' = *f* (c) be the results of the mapping *f* (·). If *f* is a homomorphism, then the composition operation □ target domain A produces the same result as mapping the result of the operation □ applied to the two elements in the original domain A: *f* (a) ◊ *f* (b)= *f* (a □ b) [35].

2.2 Encryption and Decryption scheme

We present mathematical definitions and important concepts required in the proposed technology. This coding is dependent on the standard factor. So we define our FHE function as shown in equation (1).

$$f: c_i = (m_i + r_i * p) \bmod p^2 + m_i * k^2 \quad (1)$$

Where

$$r_i: (m_i * k) \bmod p^2 \quad (2)$$

And we use the notation k, the encryption key used because in our use case, the same entity that encrypted the data will decrypt it later. However, the decryption process follows equation (3).

$$f^{-1}: m_i = (c_i \bmod k^2) \bmod p \quad (3)$$

Composition and conditions: The conditions for this coding system are as follows:

1) The chosen values of k and p must be kept secret and of large prime numbers and p ≤ k, where the user only makes known the value of (k, p);

2) For any given m_i and m_j, the condition below should be satisfied:

$$\forall m_i \forall m_j, m_i + m_j < p \text{ and } m_i * m_j < p$$

3) Key generation: Let k and p have two distinct key types randomly chosen with $p \in [2^{\lambda-1}, 2^{\lambda}]$ and $k \in [2^{\eta-1}, 2^{\eta}]$. Here, it should be large enough to override the direct treatment of k ∗ p.

4) Encryption: To encode a specific message m ∈ M, the cloud user applies the function *f* of equation (1) to get c.

5) Decoding: To decrypt an encrypted message c ∈ C, the cloud user applies the function f^{-1} from equation (3) to get m, where k is confidential.

Algorithme 1 ***Our schema***

KeyGen key Generation ***(k,p)***
Entred: k,p
Calculate: static k ∈ a large prime number;
Calculate: static p ∈ a large prime number;
Output: (k, p)
Encryption ***Crypt (m, k, p)***
Entred: m, k, p
Calculate: r_i***: (m*** $_i$ ***∗ k) mod p2***
Calculate: ***(m*** $_i$ ***+ r*** $_i$ ***∗ p)) mod p*** ^{2} ***+m*** $_i$ ***∗ k*** ^{2}
Output: c
Decryption ***Decrypt (c, k, p)***
Entred: c, k, p
Calculate: ***m =(c mod k*** ^{2} ***) mod p***
Output: m

2.3 Fully homomorphic encryption

Here we explain the concept of symmetry of shape for the proposed encryption technology, which will immediately lead us to convey its characteristics and its advantages towards the requirements of cloud computing. Assume a cloud user has it I calculated the k and p keys. Suppose f is a function of M in C, and m_1, m_2 is a pair of elements of M, if it is the sum of $m_1 + m_2$ belongs to M, we can apply f to get the f ($m_1 + m_2$) element of C.

On the other hand, we can first apply f to obtain the two elements $f(m_1)$ and $f(m_2)$; Sum of these. The new elements in C are $f(m_1) + f(m_2)$[29].

We convert the encrypted relation from: [29]

$$C_i=(m_i + r_i * p) \bmod (p^2) + m_i * k^2$$

To

$$C=m_i + £ * p + m_i * k^2$$

Which

$$m_i + £ * p < p^2$$

And from it the evidence will be as follows [29] :

Evidence:

$$f(m_1) + f(m_2) = m_1 + £_1 * p + m_1 * k^2 + m_2 + £_2 * p + m_2 * k^2 =$$

$$(m_1 + m_2) + (£_1 + £_2)p + (m_1 + m_2) * k^2$$

So

$$f^{-1}\ (f(m_1) + f(m_2)) = m_1 + m_2$$

Evidence:

$$f(m_1) * f(m_2) = (m_1 + £_1 * p + m_1 * k^2) * (m_2 + £_2 * p + m_2 * k^2) =$$

$$(m_1 * m_2) + (m_1 * £_2 * p) + (m_1 * (m_2 * k^2)) + (£_1 * p * m_2)$$

$$+ (£_1 * p * £_2 * p) + (£_1 * p * (m_2 * k^2)) + ((m_1 * k^2) * m_2) + ((m_1 * k^2) * £_2 * p) + (m_1 * k^2) * (m2 * k^2)$$

$$=(m_1 * m_2) + ((m_1 * £_2) + (£_1 * m_2) + (£_1 * £_2))\ p + (m_1 * m_2 + £_1 * p * m_2 + m_1 * m_2)$$

$$+ (m_1 * £_2 * p + m_1 * m_2 * k^2)\ k^2$$

So

$$f^{-1}\ (f(m_1) * f(m_2)) = m_1 * m_2$$

2.4 Preservation of order

One of the techniques for maintaining the arrangement of data is the technology for indexing encrypted data. With it, the arrangement requests are guaranteed to be fulfilled. The goal of maintaining order is to maintain the full sequences of the original elements of the data and to find any index within a given time interval, without revealing the original elements of the indexes [29].

This technology manages the arrangement of data on encrypted cloud databases by including a system improved coding to preserve order. Here we will suggest an effective indexing scheme to maintain order. A simple linear expression is used for the form ($a * x * b^2$) To hide the correct values used, the parameter b is kept secret.

Linear expressions must respect the indexing order, which leads us to define the system preservation function. By its definition, $\mathbf{r_i}$ is bounded by $\mathbf{0 \leq r_i < p^2 < k^2}$, which guarantees that the linear expression strictly increases.

Therefore, $\forall\ \mathbf{m_1, m_2}$ **if** $\mathbf{m_1 < m_2}$**, then** $\boldsymbol{k^2} * \mathbf{m_1} + \mathbf{r_{i1}} < \boldsymbol{k^2} * \mathbf{m_2} + \mathbf{r_{i2}}$.

Thus, the basic linear expression respects the order of **m** used in **M**. This mechanism

indexing prevents attackers from breaking the clues if they don't know the $\mathbf{r_i}$ of everything $\mathbf{m_i}$ given [29].

3 Architecture adapted to the proposed approach

In this work, we describe a high-level security architecture for cloud database storage and communication services. Figure 17 shows a schematic representation of the proposed architecture. The frame was built using two levels.

- The first is the database service provider tier, which is in a non-trusting public cloud. And which contains an encrypted database.
- The second is the client tier that deploys into the client's environment through a client proxy.

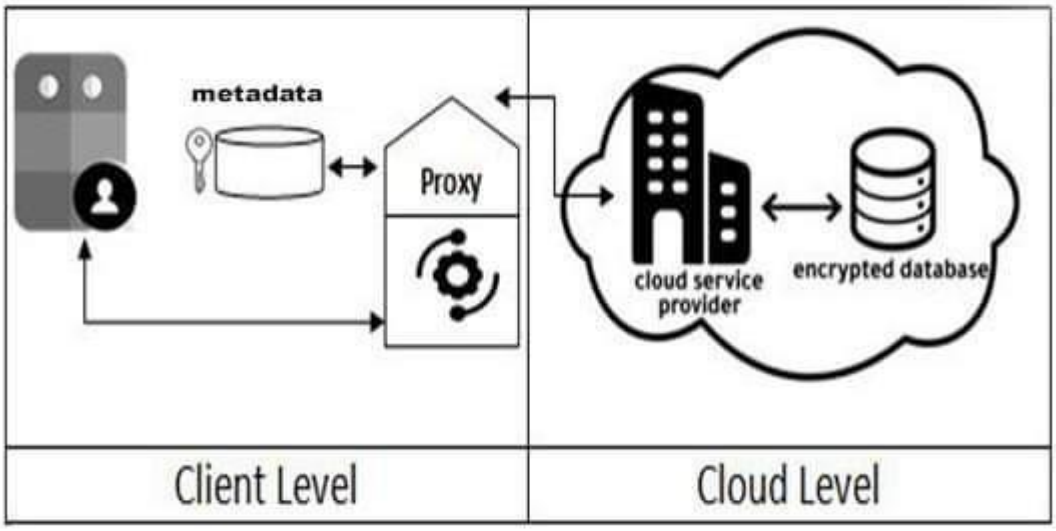

Figure 17: The proposed architecture.

- **Client**: has a proxy that manages communication between the encrypted database and client applications.
- **Proxy:** When the client executes a request, the proxy converts it into an encrypted request that runs directly in the cloud. When a request result is taken from the cloud, the proxy decrypts it before transmitting it to the client. The proxy depends on a metadata module, which contains the database schemas and the encryption and decryption keys.

Specifically, before a tuple is inserted into the database, the proxy uses the FHE encryption and indexing mechanism offered above. The tuple is then stored in the encrypted database. When a request is received from the client, the proxy parses its syntax. the proxy calculates its encryption. Then the proxy sends the forwarded request to the cloud to be executed in the encrypted database. Once the result is returned from the Cloud, the proxy decrypts it.

3.1 Data structures

During this phase, the proxy interroge the client to create its database as an administrator of the database management system (DBMS). The result of this operation is metadata, where the metadata structure is designed by the proxy encryption process. The schema created (encrypted) is different from that used in the client level. The metadata contains all of the client database schemas, and for each

database schema, another encrypted database schema is generated. The operations of the described transformation architecture are presented in Algorithm 2.

Algorithm 2 Encrypted Database Schema Generation

Input: sql query
Sql parsed = Jsqlparser(sql query)
Output: Sql parsed
Input: Sql parsed, k , p
1 Create new database schema
2 NewSchema.name = Database.CryptName (InputSchema.name, k, p);
3 For any T_i Structure in InputSchema
4 Create Structure ET_i such as
5 ET_i.name=" T_" + Structure.CryptName (T_i.name, k, p);
6 For any Data R_j in T_i
7 Add ERV_j data in ET_i such that
8 ER_j.name="RW_" + Data.CryptName(R_j.name, k, p) and
9 EV_j.val= Data.CryptVal(R_j.val, k, q);
10 End For
11 End For
Output: new database schema

To create a Data D in a T structure in the Cloud database, the proxy encrypts the name of the T structure by the T_ET, so that the result of the structure name is meaningless to non-trusting Cloud administrators. T_ is a prefix added by the proxy and ET is calculated by the Crypt Structure name operation. For data D in T, the proxy creates data RW_ER so that RW_ are prefixes added by the proxy, and ER is calculated by the operation Crypt Name. The notation ER represents the encryption of the name D. Figure 20 shows an example of a data structure, in which the structure is generated by the proxy.

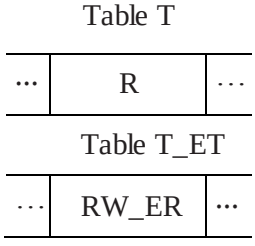

Figure 18: Original data and encryption data.

3.2 Case study

We describe the encrypted employer management system CRYPTEMSYS. In CRYPTEMSYS we considered a simple scenario in which we assume that the Cloud database is accessible only by a customer.

- The client connects to the cloud-level database through the Proxy.
- The client creates, inserts, and interrogates his data.
- The proxy encrypts/decrypts the data and sends it to the cloud.

To apply it, we have used Employee table. It has many columns of which we consider three: ID, Name and Salary. ID represents the employee's identification number, Name represents the employee's name and Salary is their salary. Since the queries below are executed, the proxy creates the encrypted table which is shown in Table 4 using Algorithm 2 such that Structure, in this case is a table and Data is a column. This table represents the database of the new CRYPTEMSYS system.

Create table Employee (ID int, Name varchar, Salary float, ...);
Insert into Employee (ID, Name, Salary) values (1, "ahmad", 100000);
Insert into Employee (ID, Name, Salary) values (2, "Salim", 50000);
Insert into Employee (ID, Name, Salary) values (3, "Lina", 40000);

In Table 4 below, we take the basic queries according to the SQL standard which can be used in EMSYS and CRYPTEMSYS.

Original *Table : Employee*			**Encrypted table*: T_2417…***		
ID	***Name***	***Salary***	***RW_37...***	***RW_68…***	***RW_54…***
1	*Ahmad*	*100000*	*112…*	*532…*	*424…*
2	*Salim*	*50000*	*159…*	*337…*	*424…*
3	*Lina*	*40000*	*207…*	*142…*	*577…*

Table 4: Original table and numbered table.

3.2.1 Generation of Query's

The proxy receives the original request sent by the EMSYS client and modifies it according to the desired functionality and structure to obtain a new encrypted request

to execute in CRYPTEMSYS. The encryption of the calculated column are performed at the client level. The transformation operations of any instruction are carried out in a flexible manner using the algorithms 3, 4, 5, 6 ,7 proposed. In the following we deal with the basic queries in the database management process.

3.2.1.1 Insertion Query

When an insert request arrives at the proxy, it processes it using Algorithm 3 to transform it into another insert request executable in the CRYPTEMSYS system. In this case the proxy encrypts the names of the table and the columns of the table then encrypts the values.

Algorithm 3 ***Insert query Generation***

Input: sql query
Sql parsed = Jsqlparser(sql query)
Output: Sql parsed
Input: Sql parsed, k , p
Add table ET.name = "T _" + Table.CryptName (T.name, k, p)
For any R_i column in query
Add column ER_i.name="RW_"+ Column.CryptName(R_i.name, k, p);
Add value EV_i= Column.CryptVal(V_i, k, p);
End For
Exit : **new query**

3.2.1.2 Update Query

When an update request arrives at the proxy, it processes it using Algorithm 4 to transform it into another update request executable in the CRYPTEMSYS system. In this case the proxy encrypts the names of the table and the columns of the table then encrypts the values.

Update T_i Set R_1= V_1 ,....., R_n=V_n where R_c = V_c;

Update employee Set Name="Salim", Salary=25000 WHERE id=2;

Algorithm 4 ***Update query Generation***

Input: sql query
Sql parsed = Jsqlparser(sql query)
Output: Sql parsed
Input: Sql parsed, k , p
Add Table ET.name =" T _" + Table.CryptName (T.name, k, p)
For Any R_i column in query
For Any Condition C_i in query
If C_i in {=} then

Add column ER_i.name="RW_" + Column.CryptName(R_i.name, k, p);
Add value EV_i= Column.CryptVal(V_i, k, p);
End If
End For
End For
Exit : **new query**

3.2.1.3 Delete Query

When a delete request arrives at the proxy, it processes it using Algorithm 5 to transform it into another delete request executable in the CRYPTEMSYS system. In this case the proxy encrypts the names of the table and of the columns the table then encrypts the values.

Delete from T_i where $R_c = V_c$;

Delete from employee where Name="Ali";

Algorithm 5 ***Delete query generation***

Input: sql query
Sql parsed = Jsqlparser(sql query)
Output: Sql parsed
Input: Sql parsed, k , p
Add table ET.name =" T _" + Table.CryptName (T.name, k, p)
For any R_i column in query
For Any Condition C_i in query
If C_i in {=} then
Add column ER_i.name="RW_" + Column. Crypt Name (R_i.name, k, p);
Add value EV_i= Column. Crypt Val (V_i, k, p);
End If
End For
End For
Exit : **new query**

3.2.1.4 Select Query

3.2.1.4.1 Simple Select

Any query that does not contain a condition, as shown below, will be considered a simple query. In these types of queries, there is usually no parsing of the query statement. An example for this type of query is the following statement:

Select $R_1, \ldots, R_n$ *from* T

Select id, Name, Salary from employee;

Algorithm 6 ***Simple query generation***

Input: sql query
Sql parsed = Jsqlparser(sql query)
Output: Sql parsed
Input: Sql parsed , k , p
Add table name ET.name="T_"+Table.CryptName(T.name, k, p);
For Any column R_i in query
Add column. Name ER_i.name="RW_"+ Column.CryptName(R_i.name, k, p);
End For
End If
Exit: new query

3.2.1.4.2 Conditional Select Query

The condition of queries is defined by a composition of logical formulas like $R_i < V_i$ or $R_i > V_i$, where V_i is a value of the domain of column R_i, using logical connectors (i.e., AND , OR).

select	$R_1, ..., R_n$	
from	T_i	
where	R_{c1} [> | <] V_1	{ C_1}
[AND | OR]	.....	
[AND | OR]	R_{cm} [> | <] V_m	{ C_m}

Select id, Name, Salary from employee where Salary >26500;

When translating the condition C_i, it suffices to replace each logical expression with the translated one. The R_{ci} condition [> | <] V_i is translated to:

"RW" + Column.CryptName(R_i.name, k, p) [>|<]column.CrypteVal(Vi, k, p);.

3.2.1.4.3 Select with Order

Select id, Name, Salary from employee Order by id;

the "Order by R_i" constraint is frequently used in queries. It is translated into:

"order by" RW" + Column.CryptNom(R_i.name, k, p).

3.2.1.5 Sum Query

In this query class, the homomorphic property is used. The query usually contains arithmetic operations or aggregations like SUM or AVG. Generally, a query must contain a condition such that Ri op Rj = V (op represents arithmetic operations). The client request can take the following basic form:

$$select\ R_1, \dots, R_n, SUM(R_i), \dots\ from\ T\ where\ R_c = V_c;$$

Select id, Name,SUM (Salary) From employee where Name = "Ahmad";

The proxy encrypts the values and names of the columns for creating a new request for and sending it to the cloud. The operation of creating homomorphic and order property queries is translated into:

$$Add\ "RW\_"+ column.\ CrypteName(R_{i1}.name, k, p)\ op\ "RW\_"+column.$$
$$CrypteName(R_{i2}.name, k, p)\ [\ =\ ]\ column.\ CrypteValue(V_i, k, p);$$

The main processes and transformations of the proxy are described in Table 5.

Original Query	**Encrypted Query**
Create table Employee (ID int, Name varchar, Salary float, . . .);	*Create table T_163... (RW_37… varchar, RW_68... varchar, RW_54... DECIMAL);*
Insert into Employee (ID, Name, Salary) values (1,"Amine",100000);	*Insert into T_163... (RW_37… RW_37…, RW_68...) VALUES ("11...", "53...", "42...");*
Select Name from Employee where ID = 1; (Select with equal)	*Select RW_68... from T_163… WHERE RW_37…="532…";*
Select SUM (Salary) FROM Employee; (Select with Hom)	*Select SUM (RW_54…) from T_163…;*
Update Employee set Name ="Lina" where id < 3;	*Update T_163… set RW_68... = "577…", RW_68…= "104…" where RW_37...< "207…";*
Select ID, Name from Employee order by ID; (Select with order);	*Select RW_37…, RW_68… from T_163… order by RW_37…;*
Delete from Employee where ID = 1;	*Delete from T_163… where RW_37…= "53…";*

Table 5: Original query and encrypted query.

4 Implementation

The aim of this part is to mention the most relevant ideas exploited in the implementation of the system, conceived before. for this we start by presenting the IT environment supporting our system.
after the presentation of this environment and its motivations, we then move on to the second part which is devoted to the presentation of the realization of our application as well as certain results obtained.

4.1 Objectifs

Given the data security issues in Cloud Computing, our work revolves around the following objectives:

- Protect data from loss.
- Recover data securely.

Our goal is to develop an application that can solve data security issues and detect whether the data has been corrupted or not.

4.2 Implementation of solution

In the process of implementing a solution comes after a sequence of several steps and its main goal is to achieve a system capable of solving the problems posed by using tools and algorithms. In order to realize and validate the ideas proposed in this chapter, the following shows the tools and the configuration used to develop this system.

4.2.1 Tools and Platforms Used

In order to facilitate the development of our system, we used a Core I3 processor computer with 8 GB RAM under Windows 7, but we can implement this system on any operating system thanks to the Java virtual machine. we used the NetBeans integrated development environment (IDE) for developing with Java.We also hired javacc is a parser generator for use with Java applications.

4.2.1.1 Java

Java is a high-level programming language developed by Sun Microsystems. It was originally designed for developing programs for set-top boxes and handheld devices, but later became a popular choice for creating web applications.

The Java syntax is similar to C++, but is strictly an object-oriented programming language. Java programs are not run directly by the operating system. Instead, Java programs are interpreted by the Java Virtual Machine, or JVM, which runs on multiple platforms. This means all Java programs are multiplatform and can run on different platforms, including Macintosh, Windows, and Unix computers. However, the JVM must be installed for Java applications or applets to run at all. Fortunately, the JVM is included as part of the Java Runtime Environment (JRE), which is which is available as a free download .

4.2.1.2 Java CC

Java Compiler Compiler (JavaCC) is the most popular parser generator for use with Java applications. A parser generator is a tool that reads a grammar specification and converts it to a Java program that can recognize matches to the grammar.

In addition to the parser generator itself, JavaCC provides other standard capabilities related to parser generation such as tree building (via a tool called JJTree included with JavaCC), actions and debugging. All you need to run a JavaCC parser, once generated, is a Java Runtime Environment (JRE)[65].

4.2.1.3 NetBeans

NetBeans is an open-source integrated development environment (IDE) for developing with Java, PHP, C++, and other programming languages. NetBeans is also referred to as a platform of modular components used for developing Java desktop applications.

NetBeans is coded in Java and runs on most operating systems with a Java Virtual Machine (JVM), including Solaris, Mac OS, and Linux. NetBeans manages the following platform features and components: User settings, Windows (placement, appearance, etc.), NetBeans Visual Library, Storage, Integrated development tools, Framework wizard.

- NetBeans uses components, also known as modules, to enable software development.
- NetBeans dynamically installs modules and allows users to download updated features and digitally authenticated upgrades.
- NetBeans IDE modules include NetBeans Profiler, a Graphical User Interface (GUI) design tool, and NetBeans JavaScript Editor.
- NetBeans framework reusability simplifies Java Swing desktop application development, which provides platform extension capabilities to third-party developers[69].

4.2.1.4The Parser Implementation

The role of the parser is to ensure that the SQL query, which needs to be parsed, is correctly formulated. By doing this any language parser executes three important phases:

1. **Lexical**, which is a tokenisation process of the query. This is mostly achieved by checking common patterns combinations of allowed characters by using regular expressions or grammars

rules. In this phase there is a distinction between keywords, numeric constants, strings and all the language component in a model.

2. **Syntactic**, which is an analysis that checks if the sequence of a sentence tokens have right shape and form compare to the grammar language.

3. **Semantic**, where it is possible to evaluate, check the consistency and in some cases optimise the parsing result by using a rewriting process.

4.2.1.4.1 JSqlParser:

In our case, the first two and part of the third phase are done by JSqlParser[66]. JSqlParser has been used in order to ensure a correct SQL parsing process. This open source Java library, parses an SQL statement and translates it into an hierarchy of Java classes which can be navigated using common Visitor Pattern software techniques. JSqlParser also, partially analyses and ensures the lexical, syntax and semantic integrity of the SQL query q to be parse. The problem in using JSqlParser is that it parses all kind of SQL used from many DBMS (Oracle, MySql, MS-SQL,

DB2, Postgres) which imply to distinguish each different database grammar in order to check if the parsed SQL query is semantically correct. For this reason the parser allows SQL queries which are written in a standard SQL.

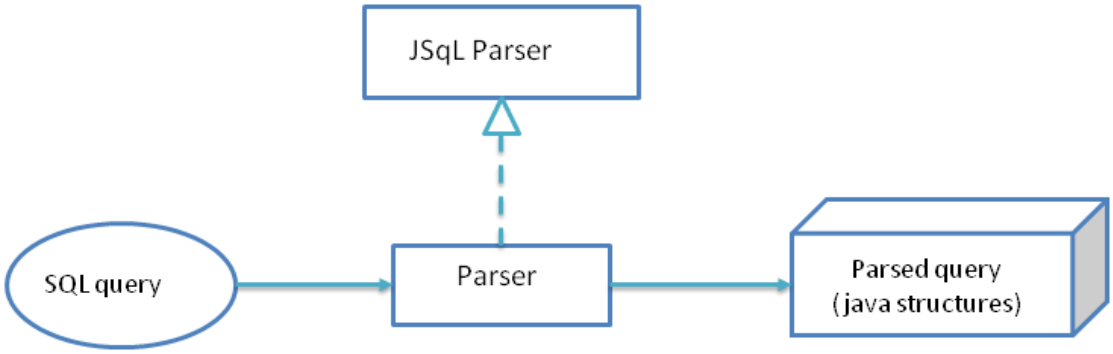

Figure 19: Parsing process.

In this section, we introduce an overview of the Java structures into which the parsed query is stored. This object represents a recursive structure and is implemented as a Java Arraylist. To avoid a technical description of the Java structures, we decided to design a model describing the Java object (see Figure 20).

Our customized parser and its Java structures have mainly been thought and designed by Nesrine Noughi[68], teaching assistant and PhD student at University of Namur .

Parsed query: It represents the parsed query. There exist three main types of query: an Invalid query, an Insert query and a Where clause query.

Invalid query: It represents an invalid query. An invalid query can appear in two cases:

1. Unparsed query: the parser cannot parse the query either if there is a syntax error or if the query is not a CRUD operation.

2. No relevant information: an invalid query may be a query without relevant information. For instance, if the query contains only columns and tables that are not present in the logical schema.

Insert query: It represents an inserting query. An inserting query consists in putting new values *(Inserted values)* in a table *(table name)*. It inserts a new value *(new value)* for each column *(column)*.

Where clause query: Deleting query *(Delete query)*, updating query *(Update query)* and selecting query *(Selecting query)* belong to this category, namely every query type that might have a where clause *(Where clause)*.

Delete query: It consists in removing some lines of a table *(table name)*, and a where-clause *(Where clause)* as obtained for the where clause of the SELECT query .

Update query: It consists in updating some columns (*Updated values*) of a table (*table name*). Each updated column (*column*) receives a new value (*new value*).

Select query: This query type consists in extracting some columns (*Selected column*). A selecting query also has a from clause with tables (*From table*).

Where clause: A where clause may contain several expressions with unary/binary operators (*Expression*) and may have several sub-request.

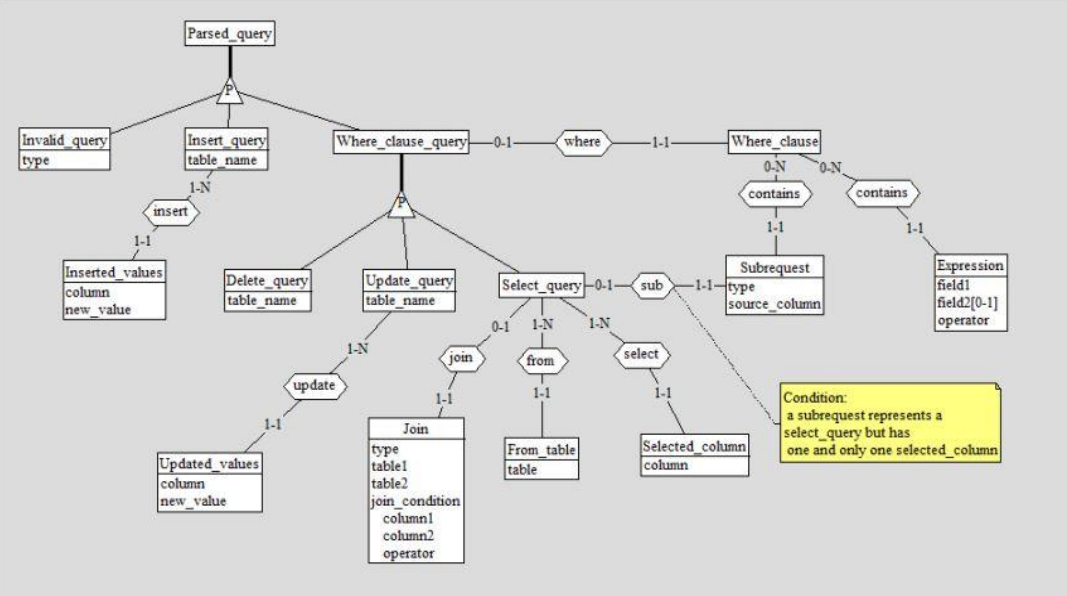

Figure 20: Java structures of a parsed query-modeling.

In this case, lists the parsing (in terms of clauses) of five examples of queries extracted from sql query (Table 6). For instance, the first query depicts the parsing of a select query, where we obtained three clauses (SelectClause, FromClause and WhereClause), each of them containing a specific item of information [67].

Query	Clauses
Create table Employee (ID int, Name varchar, Salary float, . . .);	Create Clause={ *Employee* } Column Clause ={*ID, Name,Salary*}
Insert into Employee (ID, Name, Salary) values (1,"Amine",100000);	Insert Clause={ *Employee* } Values Clause={*(=, ID,1), (=, Name,"Amine"), (=, Salary,100000)}*
Select Name from Employee where ID = 1; (Select with equal)	Select Clause={ *Name*} From Clause={*Employee*} Where Clause={(=, *ID, 1*)}
Select SUM (Salary) FROM Employee;	Select Clause={ *Salary* } From Clause={*Employee*}
Delete from Employee where ID = 1;	Delete Clause={ *Employee* } Where Clause={(=, *ID,1*)}

Table 6: Exemple of the parser structure.

4.3 Comparison and analysis

Table 7 shows the comparison of these three algorithms with our hybrid algorithm which are implemented under the same hardware and software conditions. Our experiments assess the encryption overhead and compare the response times of operations performed on the encrypted database. The experimental results show the performance of the Blowfish, AES and RSA encryption algorithms which are used in the communication module. The comparison shows that the proposed algorithm has the same response as the other algorithms. The best time is obtained because the Blowfish key is very small, and the RSA key, which is more powerful, provides an optimal level of security.

Algorithm	Packet Size Bit	Encryption time (ms)	Decryption time (ms)
Blowfish	128	19.27	0.85
AES		36.11	0.31
RSA		3.73	58.78
Proposed Method		2.40	3.91
Blowfish	512	30.69	1.18
AES		54.65	0.41
RSA		3.70	60.14
Proposed Method		3.75	8.77
Blowfish	1024	21.89	0.84
AES		36.28	0.40
RSA		3.61	56.14
Proposed Method		4.05	12.83
Blowfish	2048	24.69	1.84
AES		56.90	0.62
RSA		3.59	54.64
Proposed Method		10.71	15.74

Table 7: Comparisons of encryption algoritms.

4.4 Description of how the proposal works

In order to protect the data shared in the Cloud Computing environment against unauthorized access attempts and the risks of loss, modification and alteration, we offer a solution (application) based on encryption and recovery (decryption) Data.

We validate the applicability of our approach in different cloud solutions by implementing and managing encrypted database operations on emulated cloud infrastructures. The current version of our prototype supports MySql relational databases. This type of database offers SQL interface standards that simplify the scalability and availability of the cloud database. On the plus side, our proposal only uses standard SQL commands to encrypt user data on any cloud-based database service.

First, the user creates a data center instance after choosing the type of database, in our case it is a MySQL database. when it gets the creation code, it generates another cloud diagram according to algorithm 4 and metadata to send it to the user. In this state the cloud database becomes ready to operate.

This step represents the entire life of the database after creation. Each time a user connects to the database. This package includes a query analyzer (parser) , An encryption , query rewrite, which encrypts the data or fields of the query with all the encrypt and decryption algorithms.

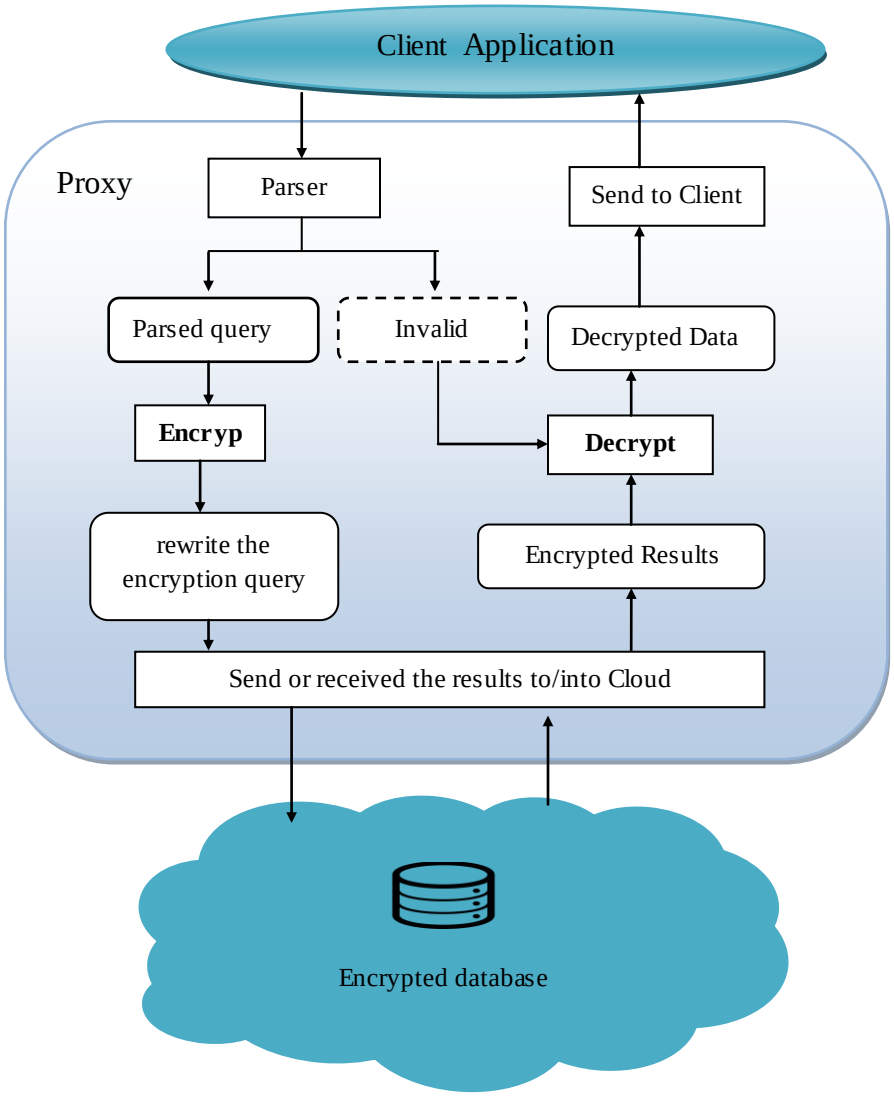

Figure 21: The simulation of the implementation.

4.5 Application interfaces

In this part, we will present the interfaces of our realization.

4.5.1 Client interface for data reception

The following figure (figure 22) represents the Client interface after receiving the data.

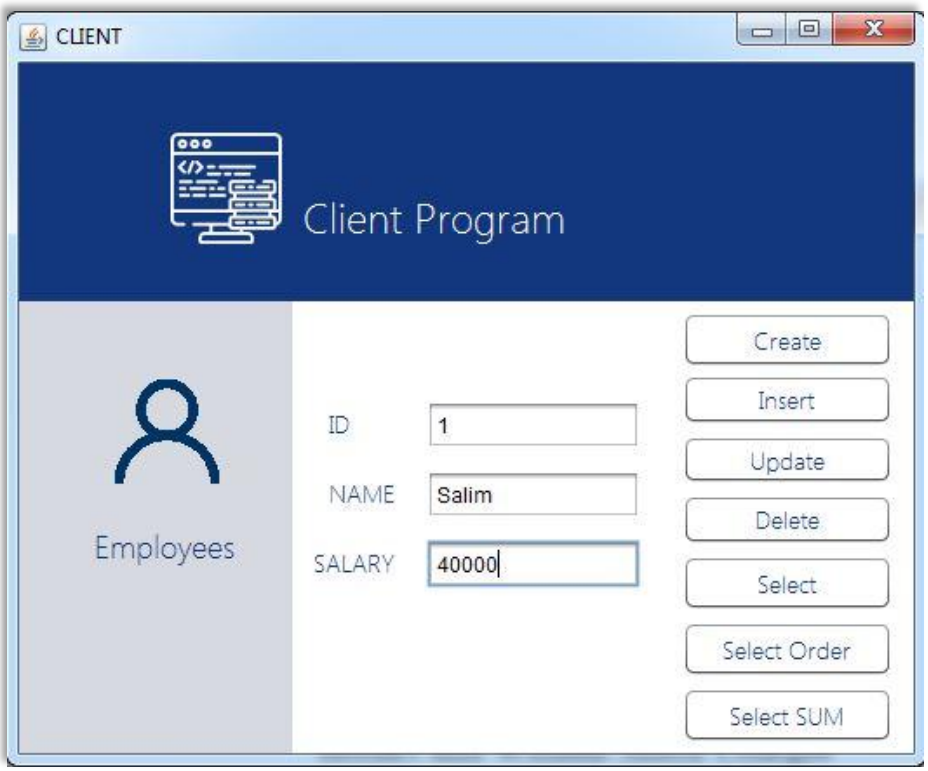

Figure 22: The Client interface-Data reception.

4.5.2 Proxy interface sends data

The following figure (figure 23) shows the interface for sending and receiving data into the Cloud server provider.

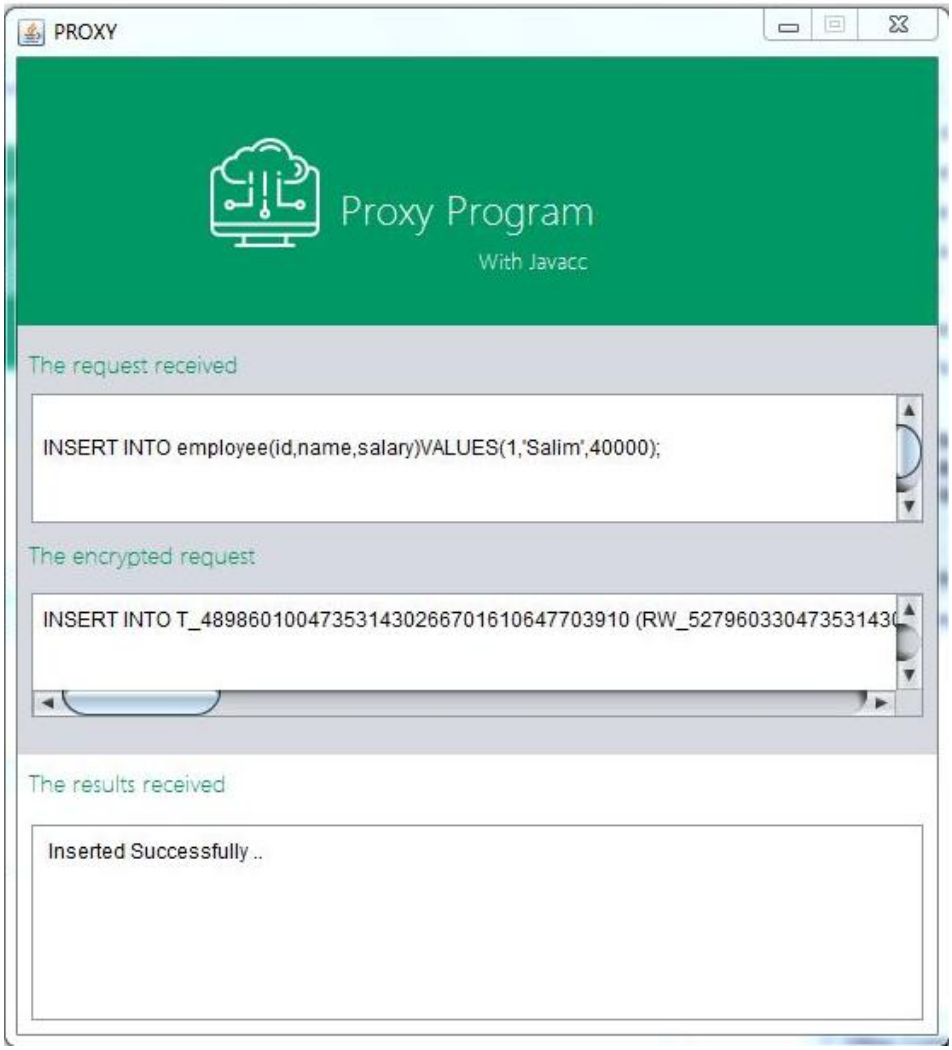

Figure 23: The interface of proxy sends data.

5 Conclusion

In this part, we have proposed a method to generate a fully homomorphic encryption by ensuring the preservation of the order between the encrypted data which is stored in the Cloud, in order to allow the execution of the different operations on this protected data. This technique is easy to use because it is based on linear and modular expressions. We assessed the complexity of modifying an application to make it work according to our approach. The types of queries and applications can support a predefined level of security and the performance impact obtained using linear computation.

We have also described SQL CRYPTEMSYS by taking a simple scenario in which we have assumed that the cloud database is with an untrusted vendor. In the implementation section, we analyzed the proposed technique and validated its applicability for different cloud solutions. Important tests are oriented to verify its functionality in the cloud database environment. Then we have provided our solution and validation of it in order to remedy the problem of data security in Cloud Computing. We have also illustrated a diagram representing the steps of the proposed solution as well as the implementation of it.

General Conclusion

Cloud Computing is a new concept in the deployment of computer systems, it offers many advantages in terms of computing power, response time and cost reduction. Users can take full advantage of cloud services that meet their needs on demand. However, like every technological advance, outsourcing its IT resources also brings its share of risks, particularly in terms of data security, because if the user cannot have his own resources in a secure manner, at all times and from n any geographic location, then the effectiveness, benefits, and even definition of cloud computing will be at risk. We will then observe a decline in cloud adoption and even a loss of customers.

Our main objective was to propose an approach for data security in Cloud Computing. The ultimate goal is to meet the needs of Cloud users, while providing the most trusted and trusted data security solution. The proposed solution must first guarantee confidentiality and integrity.

In the first part, we focused on the concept of cloud computing and data storage , we have defined relational databases relational SQL database. Also we discussed security issues, privacy and security threats .

In the second part, we proposed a technique to generate a fully homomorphic encryption by ensuring the preservation of the order between the encrypted data stored in the Cloud. The objective is to allow the execution of the various operations on this protected data. This technique is easy to use because it is based on linear and modular expressions .

We presented our contribution. It emphasizes the issue of confidentiality of data stored in the Cloud. We have implemented a model that guarantees data confidentiality. We validated this solution by a simple scenario described by relational SQL.

In conclusion, this message allowed us to examine a wide range of concepts, models and technologies in the fields of data security and cloud. Our goal was to investigate data security issues stored in the cloud, while focusing on data privacy and remote

data integrity. We have provided new architectures based on encryption techniques to meet our objectives. We have also shown that the proposed work joins a rich and encouraging research theme.

Bibliography

[1] Introduction to Cloud Computing: (October/2017) Available at <https://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf>(Accessed 25-11-2019).

[2] Cloud Computing Guidelines: Available at< https://www.motc.gov.qa/sites/default/files/cloud_computing_ebook.pdf>>(Accessed 25-11-2019 / 10: 00 am).

[3] J. McCarthy, Informatique utilitaire : http ://computing in the cloud. wordpress.com/2008/09/25/ utility-cloud computingflashback-to-1961-profjohn-mccarthy / (Accessed 02/2020).

[4] Berkani, Nassima, and Salima Moussaoui. *La sécurité des données dans le Cloud Computing*. Diss. université Abderrahmane Mira, 2016.

[5] Neelima, M. Lakshmi, and M. Padma. "A study on cloud storage." *International Journal of Computer Science and Mobile Computing* 3.5 (2014): 966-971.

[6] Spoorthy, V., M. Mamatha, and B. Santhosh Kumar. "A survey on data storage and security in cloud computing." *International Journal of Computer Science and Mobile Computing* 3.6 (2014): 306-313.

[7] Ikram, Adli, and Hachem Slimani. *Monitoring des "applications scientifiques" dans un environnement combiné "Cloud-Grid"*. Diss. Université Abderrahmane Mira-Bejaia, 2016.

[8] Laribi, I. "La mise en place de la solution Openstack." *Mémoire master, Université Abou Bekr Belkaid-Tlemcen* (2014).

[9] Giovanna Di Marzo Serugendo.Cloud computing Architectures, services et risques.Institute of Information Service Science-University of Geneva.(2012).

[10] Margeret Rouse.Cloud Computing.WhatIS.com : https://searchcloudcomputing-techtarget-com.cdn.ampproject.org/v/s/searchcloudcomputing.techtarget.com/definition/cloud-computing. June,2020. .

[11] Different Cloud Storage Types : https://www.cloudstoragebest.com/cloud-storage-types/January 22,2013/(Accessed 06/2020).

[12] Margaret Rouse , Information Technology: https://whatis.techtarget.com/13 Feb 2019/(Accessed 06/2020).

[13] Eric Griffith.What is cloud computing ?. https://www-pcmag-com.cdn.ampproject.org/v/s/www.pcmag.com/news/what-is-cloud-computing?.June,2020.

[14] Afzalpulkar, Nitin, et al., eds. *Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing: ICRCWIP-2014*. Springer, 2016.

S. Maninder, S. Sarabjeet. Design and implementation of multi -tier authentication scheme in cloud, International Journal of Computer Science Issues. vol. 9, no. 2.

[15] Kumar, Satish, and Anita Ganpati. "Multi-authentication for cloud security: A framework." *International Journal of Computer Science & Engineering Technology* 5.4 (2014): 295-303.

[16] Arasu, S. Ezhil, B. Gowri, and S. Ananthi. "Privacy-preserving public auditing in cloud using HMAC algorithm." *International Journal of Recent Technology and Engineering (IJRTE) ISSN* 2277.3878 (2013): 149-152.

[17] Kalpana, Parsi, and Sudha Singaraju. "Data security in cloud computing using RSA algorithm." *International Journal of research in computer and communication technology, IJRCCT, ISSN* (2012): 2278-5841.

[18] Pateriya, Pankaj, and Inderveer Guide Chana. *A Secure Data Transfer Technique for Cloud Computing*. Diss. 2014.

[19] Somani, Uma, Kanika Lakhani, and Manish Mundra. "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing." *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*. IEEE, 2010.

[20] Balasaraswathi, V. R., and S. Manikandan. "Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach." *2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies*. IEEE, 2014.

[21] Majed, Hassan Mohamed. Cloud computing, Sohag University, Egypt. (2014).

[22] Mobaideen, Ibrahim. Cloud computing, Jordanian company specialized in systems solutions Information and Information Technology. (2015).

[23] McCawy, Maram. Cloud computing ... Do magic features overcome security concerns? Caravan Magazine, issue 60. (2013).

[24] Machey, Musa Ali. Cloud computing, Jazan University, Saudi Arabia. (2014).

[25] Dr.Tayssir Andrews Slim, Cloud Computing, Theory and Practice, No. 42, June 2016.

[26] Diaby, Tinankoria, and Babak Bashari Rad. "Cloud computing: a review of the concepts and deployment models." *International Journal of Information Technology and Computer Science* 9.6 (2017): 50-58.

[27] Sajid, Mohammad, and Zahid Raza. "Cloud computing: Issues & challenges." *International Conference on Cloud, Big Data and Trust*. Vol. 20. No. 13. 2013.

[28] Yan, Cheng. "Cloud Storage Services." Thesis CENTRIA UNIVERSITY OF APPLIED SCIENCES Information Technology June 2017.

[29] Yagoub, Mohamed Amine. Une approche basée agent pour la sécurité dans le Cloud Computing. Diss. Université Mohamed Khider de Biskra, 2019.

[30] Z. O., D. A. et D. H., «Cloud computing security through parallelizing fully homomorphic encryption applied to multi-cloud approach,» Journal of Theoretical & Applied Information Technology, vol. 87, n° %12, 2016.

[31] B. A., C. M., Q. B., A. F. et S. P., «Depsky: dependable and secure storage in a cloud-of-clouds,» ACM Transactions on Storage (TOS), vol. 9, n° %14, p. 12, 2013.

[32] A. M. A., P. E., S. B. et T. J. A., «Cloud computing security: from single to multi-clouds,» System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE, p. 5490–5499, 2012.

[33] D. B. J., J. A. et O. A., «Hail: A high-availability and integrity layer for cloud storage,» Proceedings of the 16th ACM Conference on Computer and communications Security. ACM, p. 187–198, 2009.

[34] X. K., L. S., H. J., X. Y., Y. N. et H. P., «Two-cloud secure database for numeric-related sql range queries with privacy preserving,» IEEE Transactions on Information Forensics and Security, vol. 12, n° %17, p. 1596–1608, 2017.

[35] Will, Mark A., and Ryan KL Ko. "A guide to homomorphic encryption." (2015): 101-127.

[36] Armknecht, Frederik, et al. "A Guide to Fully Homomorphic Encryption." IACR Cryptol. ePrint Arch. 2015 (2015): 1192.

[37**]** Tebaa, Maha, Saïd El Hajji, and Abdellatif El Ghazi. "Homomorphic encryption applied to the cloud computing security." *Proceedings of the World Congress on Engineering*. Vol. 1. No. 2012. 2012.

[38] G. S. et M. S., «Probabilistic encryption,» Journal of Computer and System Sciences, n° %12, p. 270– 299, 1984.

[39] N. D. et S. J., «A new public-key cryptosystem,» International Conference on the Theory and Applications of Cryptographic Techniques. Springe, p. 27–36, 1997.

[40] L. R. R., S. A. et A. L., «A method for obtaining digital signatures and public-key cryptosystems,» Communications of the ACM, vol. 21, n° %12, p. 120–126, 1978.

[41] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." 2012 International Conference on Computer Science and Electronics Engineering. Vol. 1. IEEE, 2012.

[42]DataEncryptionStandard.Available .at[https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm].(Accessed 07/2020).

[43]ReportofSaaS.https://shaweweb-wordpress-com.cdn.ampproject.org/v/s/shaweweb.wordpress.com.07/03/2017.(Accessed 07/2020).

[44] Messeguem, Abdel Djalil. *Analyse des données avec apache spark*. Diss. 2019.

[45] Fellah Hadjer.CLOUD COMPUTING ET SECURITE : Une architecture organique pour la sûreté de fonctionnement des processus métiers. UNIVERSITE LARBI BEN M'HIDI-OUM EL BOUAGHI,2013.

[46] B. A., C. N., L. Y. et O. A., «Orderpreserving symmetric encryption,» Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, p. 224–241, 2009.

[47] L. D. et W. S., «Programmable order-preserving secure index for encrypted database query," in,» Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, p. 502–509, 2012.

[48] Merizig, Abdelhak. Approche de composition de services web dans le Cloud Computing basée sur la coopération des agents. Diss. Université Mohamed Khider-Biskra, 2018.

[49] Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." *International Journal of Computer Applications* 67.19 (2013).

[50] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[51] da Silva Quirino, Gustavo, and Edward David Moreno. "Architectural evaluation of algorithms RSA, ECC and MQQ in arm processors." International journal of Computer Networks & Communications 5.2 (2013): 153.

[52] Final Guide to Advanced Encryption Standard (AES). https://ar.wizcase.com/(07-2020).

[53] Cryptography With the DES Algorithm. https://dzone.com/articles/security-algorithms-des-algorithm(07-2020).

[54] The largest gathering of computer students in Iraq. ComnuterScience

http://fkraaaa.blogspot.com/2017/07/encrypt-and-decrypt-algorithms.html?m=1.

(07-2020).

[55] Introduction to Blowfish.
https://www.splashdata.com/splashid/blowfish.htm.(07-2020).

[56] Double DES and Triple DES.https://www.geeksforgeeks.org/double-des-and-triple-des/.(07-2020).

[57] Diffie-Hellman Protocol. https://mathworld.wolfram.com/.(07-2020).

[58] CRYPTOSYSTEM, A. PUBLIC KEY, A. SIGNATURE, and SCHEME BASED ON DISCRETE LOGARITHMS. "1501 Page Mill Rd Palo Alto CA 94301." *Advances in Cryptology: Proceedings of CRYPTO'84*. Vol. 196. Springer, 2003.

[59] Ustimenko, Vasyl. "On desynchronised multivariate El Gamal algorithm." (2017).

[60] What is DSA(Digital Signature Algorithm). http://www.herongyang.com/Cryptography/DSA-Introduction-What-Is-DSA-Digital-Signature-Algorithm/.(07-2020).

[61] Monika Sharma.Digital Signature Algorithm (DSA) in Cryptography.February 29, 2020.

[62] Michael Pace. DSS: Digital Signature Standard and DSA Algorithm. http://www.iup.edu/.(07-2020).

[63] Yunchuan Sun,1 Junsheng Zhang,2 Yongping Xiong,3 and Guangyu Zhu4:" Data Security and Privacy in Cloud Computing". International Journal of Distributed Sensor Networks (2014)

[64] BENDIAB GUELTOUM. Sécurité des applications métiers au niveau du Cloud

Computing :" Contrôle d'accès au niveau des APIs du Cloud Computing". Mémoire de Magister en Informatique. - Université Abdelhamid Mehri – Constantine 2.(14 / 05 / 2015).

[65] Javacc parser. <http://web.cs.wpi.edu/~kal/courses/compilers/JAVACC/JavaccPaser.htm////>. [Online; accessed 2020].

[66] JSqlParser. http://jsqlparser.sourceforge.net/.

[67] Noughi, Nesrine, «Understanding Data-Intensive Systems Through The Analysis of SQL Execution Traces[En ligne]. Available: https://researchportal.unamur.be/en/studentTheses/understanding-data-intensive-systems-through-the-analysis-of-sql-, [University of Namur, Accès 19 Jun 2020].

[68] Nesrine Noughi. https://researchportal.unamur.be/en/persons/nesrine-noughi.

[69] The apache software foundation announces apache ^{R} netbeans^{TM} as a top-level project. <https://www.globenewswire.com/news-release/2019/04/24/1808620/0/en/The-Apache-Software-Foundation-Announces-Apache-NetBeans-as-a-Top-Level-Project.html////>. [Online; accessed 2020].

[70] D. D. Chamberlin, M. M. Astrahan, M. W. Blasgen, J. N. Gray, W. F. King, B. G. Lindsay, R. Lorie, J. W. Mehl, T. G. Price, F. Putzolu, P. G. Selinger, M. Schkolnick, D. R. Slutz, I. L. Traiger, B. W. Wade, and R. A. Yost. A History and Evaluation of System R. Commun. ACM, 24(10):632–646, October 1981.

[71] E. F. Codd. A Relational Model of Data for Large Shared Data Banks. Commun. ACM, 13(6):377–387, June 1970.

[72] K. E. Kline, D. Kline, and B. Hunt. SQL in a Nutshell. O'Reilly, third edition, 2008.

[73] J. R. Groff and P. N. Weinberg. SQL: The Complete Reference. McGraw-Hill/Osborne, second edition, 2002.

[74] J. Bowman, S. Emerson, and M. Darnovsky. The Practical SQL Handbook: Using SQL Variants. Addison-Wesley, 4th edition, 2001

[75] Dr. NEDHAL A. AL-SAIYD, NADA SAIL "DATA INTEGRITY IN CLOUD COMPUTING SECURITY." Journal of Theoretical and Applied Information Technology Vol. 58 No.3 (31st December 2013).

[76] M Sulochana ,Ojaswani Dubey. "Preserving Data Confidentiality using Multi-Cloud Architecture " Procedia Computer Science 50 (2015) 357 – 362.

[77] DB-Engines Ranking. http://db-engines.com/en/ranking.

[78]CLOUD on move. Available at[http://cloudonmove.com/iaas-paas-saas-what-do-they-mean/01-08-2017].(Accessed 07/2020).

[79] Cynthia Harvey. challenges of cloud computing — and how to address them . August 2, 2018.