Karary University

Computer science

Information security

Master’s thesis

Cryptography-based Approach for preserving Privacy in Cloud Computing

By: Fatimah al-basher

Supervisor: Dr. yasir abdalgadir

**Abstract**

Cloud computing is a term referred to storing, processing and accessing data over the internet. It reduces the burden of storing data on the local storages.

In cloud computing, you can access data from a remote server.

### Cost saving is the biggest benefit of cloud computing. It helps you to save capital cost as it does not need any physical hardware investments, and also offer Mobility Employees who are working on the at the remote locations can easily access all the could services. All they need is an Internet connectivity.

ButCloud has a lot of security issues that are gaining great attention nowadays, including the data protection, network security, application integrity, and identity management.

Data protection is one of the most important security issues,

There many techniques are suggested for data protection in cloud computing, but there are still a lot of challenges in this field.

In this thesis, we propose protect and secure data stored in cloud using authentications and encryptions /decryptions algorithm to make protection of data form unauthorized access.

**Introduction**

In today’s highly competitive business environments, businesses are finding ways and means to operate efficiently so as to cut cost and maximize profit. A new paradigm of computing, cloud computing has emerged to change the old ways of computing.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or

service provider interaction. (NIST 2009a)

Cloud is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software.

Rather than keeping files on a proprietary hard drive or local storage device, [cloud-based storage](https://www.investopedia.com/terms/c/cloud-storage.asp) makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. [1]

One of the key benefits of cloud is reduced time and costs. Cloud computing is providing companies and organizations to use shared storage and computing resources. It is better than to develop and operate with the own infrastructure.

Cloud provide many important serves like: email Storage, backup, and data retrieval, Creating and testing apps, analyzing data, Audio and video streaming and delivering software on demand.

In as much as much as this is important and attractive for the enterprise, the necessary precautions must be taken to ensure that confidentiality, integrity and available of information and information systems are not compromised in the cloud environment.

.

1.1 **Cloud computing:**

Cloud computing is a model for enabling ubiquitous, convenient,on-demand network access to a shared pool

of configurable computing resources

(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"

[11].

1.2 **Service Levels**

Cloud computing is offered in three different service models which each satisfy a unique set of business requirements. These three models are known as Software as a Service

(SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

**SaaS**:

Software as a Service offers applications that are accessed over the web and are not managed by your company, but by the software provider. This relieves your organization from the constant pressure of software maintenance, infrastructure management, network security, data availability, and all the other operational issues involved with keeping applications up and running. SaaS billing is typically

based on factors such as number of users, usage time, amount of data stored, and number of transactions processed. This service model has the largest

market share in cloud computing; according to Gartner, its sales will reach 117 billion USD by the year 2021

[12].

Current applications for SaaS include Field Service solutions, system monitoring solutions, schedulers and more.

**IaaS**

infrastructure as a service offers a standardized way of acquiring computing capabilities on demand and over the web. Such resources include storage facilities,

networks, processing power, and virtual private servers. These are charged under a “pay as you go” model where you are billed by factors such as how much storage

you use or the amount of processing power you consume over a certain timespan. In this service model, customers do not need to manage infrastructure, it is up to the provider to guarantee the contracted amount of resources and availability.

According to Gartner, this service model is forecasted to grow by 35.9% in 2018[12]. IaaS services offered today, include Google Cloud Platform and Amazon EC2.

**PaaS**:

Platform-as-a-service (PaaS) is a complete, scalable development and deployment environment that is sold as a subscription service. PaaS includes all elements that a

developer needs to create and run cloud applications—

operating system, programming languages, execution environment, database, and web server—all

residing on the cloud service provider's infrastructure. an organization can develop and deploy custom cloud applications without needing to invest in hardware or

development tools. Likewise, an organization can use PaaS to extend or rearchitect their existing applications in the cloud Examples of platform-as-a-service are AWS Lambda, Microsoft Azure PaaS, Google App Engine, Apache Stratos.

Globally, more than one-half (52%) of all organization use some type of cloud platform services, according to

the 2019 McAfee Cloud Adoption and Risk Report.

That percentage is expected to increase as organizations build more of their applications in the cloud

**2.3 Type of cloud computing**

**Public**

Constituting publicly accessible services that are accessed over the Internet and are

often described using the term”The Cloud".

**Private**

These are private services deployed on private networks. Such clouds may also be managed by third parties.

**Hybrid**

A combination of services offered both privately and publicly. For example, core-services

may be offered on a private cloud; other services originate from public clouds.

**1.3 Cloud Security Issues:**

Cloud computing as a novel technology for processing and transferring data electronically is nowadays used in almost every computer system. however, as you and your customers begin to expand their adoption of software as a service, platform as a service and infrastructure as a service model, organizations need to understand the risk that is introduced as data and resources are moved outside of the enterprise firewall. When implementing any (or all) of these three models, one

needs to pay close attention to the security tradeoffs for not only data, but also organizational compliance when organizations separate application and information resources form the underlying physical infrastructure. [13]

Cloud computing runs on a network infrastructure that is opened for different

types of Security Issues like:

**Misconfiguration,** **Unauthorized Access,** **Hijacking of Accounts,** **Malicious Insiders**

**Denial of Service Attacks.**

**1.4 Security Requirements**

Cloud computing is very promising for the IT applications; however, there are still some problems to be solved for personal users and enterprises to store data

and deploy applications in the cloud computing environment. One of the most

significant barriers to adoption is data security, which is accompanied by issues including compliance, confidentiality, availability, and integrity

[6,7].

The meaning of security requirements.is the combination

of Integrity, confidentiality, availability.

**Integrity**:

means protecting data from unauthorized deletion, modification.

Managing entity's admittance and rights to specific enterprise resources ensures

that valuable data and services are not abused, misappropriated, or stolen.

**Confidentiality**:

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality.

**Availability**:

when accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can

be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.

**1.5 Motivation:**

Cloud computing is become more important to people to store their information and data; these data may be sensitive, so security is very important in cloud environment, but, the use of cloud computing comes along with a variety of issues of its own like loss of control over data, security, privacy and confidentiality. Hence, there is a need to secure data not only from unauthorized users but also from malicious authorized users try to access and tamper

the data,

They need to make sure that data stored on the cloud is accessed

only by authorized members to reduce the risk of losing

control over data.

**1.6Research objectives:**

Cloud computing users work with data and applications that are located

off-premise However,

many user and organizations are inconvenient with the idea of having their data and applications on systems they do not control.

Some cloud user want to control on data privacy in cloud and make sure no unauthorize assess to their data.

The idea is how to make user able to control of data privacy in cloud? and how to impose strong authentication access to make sure no unauthorize access to data in cloud?

The goal of this thesis is to create a framework that provide control of privacy preserving on data in cloud computing by providing encryption to data before uploaded to cloud and build strong authentication access depending on Mobil number authentication.

**Related Work**

**Related Work**

There has been a growing interest in the study of cloud storage and ways to secure the data.

inthis chapter, we will list some the existing work in the areas of secure data storage and authentication Systems in a cloud environment.

Some methods use authenticationto manage which users have the rights to access to data stored on cloud, and some use other method like data encryption.

**2.1 authentication Systems in Cloud**

Since cloud environment has to offer services to various customers. Number of authentication Systems has been developed for the cloud.

The authors in. [14] They suggested model contains an authentication agent for validating user legal identities and acquiring their access control privileges for the resources according to the role information.

User Authentication Agent (UAA) has been introduced and applied in the suggested model to evaluate user authentication for validating user legal identities and acquiring their access control privileges for the resources according to

the role information.

They used two types of authentication for cloud-based environments (VDA) and (PAP). The first type is related to the belonging devices of users and the second one considers provisional accesses from un-registered devices.

They show their model enhances the rate of security and reliability in cloud environments without affecting the rate of energy and time consumption, and scalability.

Sudha and S.S in. [15] proposed system presents the authentication process at different levels.

The main aim of this multi-level authentication is to eradicate the possessing of fingerprint devices or smart cards and other equipment. The authentication process in four stages gives different scope, and distinctive security parameters enhance the security measure.

During the first stage, the user has to submit the Username and Password to move on to the second stage. The user’s correct answer to the security question allows the user to move on to the third stage.

At this stage, an OTP (One Time Password). request will be given to Cloud Server,

and the same will be sent to the user’s registered mobile number. The distinctive approach here is that the user has to enter the new password, which can be formed by combining the Old Password and OTP Thus the user can have a new

password for every session, and the hackers cannot predict the OTP as well as the Password methodology. If the password is wrong, the user is stopped from

accessing the Cloud services and again the user has to give a request for OTP.

M.Meena et al. [16] introduced authentication mechanism .

This mechanism proposes a three-level authentication.

During the first level, the user has to provide their personal details a username and password, at the second level, identification of images from the 4 x 4 matrix which is already set by the user during the registration phase, and in the third level, if the above steps go correctly then the user will receive the OTP on the registered number. User can enter the OTP and complete the verification process

This technique will provide strong resistance against Shoulder Surfing and Spy Ware attack.

The disadvantage of this algorithm is password change option is not given and forgot password

.

**2.2 Secure Stored Data in Cloud:**

Securing data in a cloud storage becomes critical requirement, while amount of sensitive data stored in a cloud increases, the encryption is solution to keep data private, data is encrypted by the owner before uploaded it to the cloud, this secures data from both cloud service provider as well as unauthorized users.

the authors in [17], proposed a mediated certificate less encryption scheme. The data is encrypted using the users’ keys generated by the cloud based on the access control policies. When a user requests this data, the cloud decrypts the encrypted data partially which can be decrypted to the original data using the user’s own private key. Since, the cloud handles partial decryption and key management, user revocation is easier to handle. But, this might prove to be a risk from security point of view. In addition to this, as decryption is performed twice, it increases the computation cost of decryption.

The authors in. [18], they address security issue in cloud computing and proposed solution to manage security issue by encryption,

They suggested to encrypt the encryption key at the time when it is generated or periodically change the key in order to avoid theft of key by unauthorized person,

And same time encrypt data using symmetric encryption algorithms.

Arockiam and Monikandan in. [19] they proposed technique to achieve confidentiality of data .

This technique uses both encryption and obfuscation to preserve the confidentiality as it considers encryption alone cannot provide security.

Same with the case of obfuscation as reverse engineering attacks or brute force techniques can break this.

Here obfuscation is integrated with encryption. Obfuscation uses a mathematical function or employs programming techniques to disguise illegal users. This approach depends on the type of data. Encryption can be applied to alphabets and

Alphanumeric type of data and obfuscation to numeric data.

The data that needs to be stored should be encrypted and obfuscated

Encryption and obfuscation is done at the user side and the key required for encryption is produced at user environment. Obfuscation does not use any key and uses any mathematical function or programming Technique.

## **Reference**:

1. Frankenfield .Jake from Investopedia

2. Timothy Grance Peter Mell.NIST Special Publication 800-145.NIST, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

3 .Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special

Publication 800-145, Sep. 2011.

4 .Iliana Iankoulova and Maya Daneva. Cloud computing security requirements: A systematic review. InResearch Challenges in Information Science(RCIS), 2012 Sixth International

5. By (Mohammed. Fursan, Thabit. Ahmed) ,New Enhanced Techniques for Security in Cloud Computing

6. Shah, M. A., Swaminathan, R., Baker, M. Privacy-preserving audit and extraction of digital contents IACR Cryptology EPrint Archive 2008 186

Google Scholar

7. Xiao, Z., Xiao, Y. Security and privacy in cloud computing IEEE Communications Surveys & Tutorials 2013 15 2 843 859 10.1109/SURV.2012.060912.00182 2-s2.0-84877272118

Google Scholar | Crossref | ISI

8.Cong Wang, Qian Wang and Kui Ren,”Ensuring Data StorageSecurity in Cloud computing”978-1-4244 -3876-1/2009 IEEE

9.http://en.wikipedia.org/wiki/AES\_implementations

10.LIU, Qin, WANG, Guojun, et WU, Jie. Secure and privacy preservingkeyword searching for cloud storage services.Journal of network andcomputer applications, 2012, vol. 35, no 3, p. 927-933.

11. Peter Mell and Tim Grance. The NIST de nition of cloud computing.National Institute of Standards and Technology, 53(6):50, 2009. 7, 9

12.  <https://www.gartner.com/newsroom/id/3871416>

13. <https://www.arrow.com/ecs/na/channeladvisor/channel-advisor-articles/saas-paas-and-iaas-what-are-all-the-risks/>

14 . Faraz Fatemi Moghaddam ,Nasrin Khanezaei ,Sina Manavi ,Mohammad Eslami,Alireza Samar ,"UAA: User Authentication Agent for Managing User

Identities in Cloud Computing Environments ",2014,researchgate

15 . S.Sudha ,S.S.Manikandasaran,"Asynchronous Password-Based Authentication and Service\_Provider\_ID Module for Secured Cloud

Environment",researchgate 2020

16 . M. Meena, H. S. Lamba, D. Taterwal, and M. Shaikh, “System for 3 level security verification using image-based authentication & OTP,”

researchgate, 2018.

17 . Seo, , Nabeel, Ding, & Bertino, E. (2014). An Efficient Certificateless

Encryption for Secure Data Sharing in Public Clouds. IEEE Transactions on

Knowledge and Data Engineering.

18 . Thomas,Jose V, P.Afsar ,"Cloud computing security using encryption technique"

19 . L. Arockiam, S. Monikandan,”Efficient Cloud Storage Confidentiality to Ensure Data Security”, 2014 International Conference on Computer Communication and Informatics

,academia.edu,2014.