Cloud Security based on the Homomorphic Encryption

Waleed T. Al-Sit[1], Hani Al-Zoubi[3]
Department of Computer Engineering
Mu'tah University, Al-Karak, Jordan

Qussay Al-Jubouri[2]
Department of of Communication Engineering
University of Technology, Baghdad, Iraq

***Abstract*—Cloud computing provides services rather than products; where it offers many benefits to clients who pay to use hardware and software resources. There are many advantages of using cloud computing such as low cost, easy to maintain, and available resources. The main challenge in the Cloud system is how to obtain a highly secured system against attackers. For this reason, methods were developed to increase the security level in different techniques. This paper aims to review these techniques with their security challenges by presenting the most popular cloud techniques and applications. Homomorphic Encryption method in cloud computing is presented in this paper as a solution to increase the security of the data. By using this method, a client can perform an operation on encrypted data without being decrypted which is the same result as the computation applied to decrypted data. Finally, the reviewed security techniques are discussed with some recommendations that might be used to raise the required security level in such a system.**

Keywords*—*Cloud computing; homomorphic encryption; security

I. Introduction

Cloud computing represents the latest effort in delivering computing resources as a service. It enables any organization to obtain its computing resources and applications from any location via an internet connection. As reported in [1], the US National Institute of Standards and Technology (NIST) have defined cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources [2]. Networks, servers, storage, applications, and services can be rapidly provisioned and released with minimal management effort or service provider interaction".

In Cloud, computing Clients are permitted to store a vast amount of information on distributed storage, and it provides on-demand services over a network, by payment method. Different security issues like confidentiality, privacy, authentication, and integrity needed to address. The more significant part of the cloud administration supplier stores the information in plaintext and client need to utilize their encryption algorithm to secure their information. The information should be decrypted when t it is to be computed. As data is decrypted, it will be prone to attack. Therefore, finding a solution is essential to protect the data, and to perform any computation on it without decryption; this process is called Homomorphic Encryption. Several advantages of using cloud computing such as (i) low cost, (ii) easy to maintain, (iii) backup personalization and recovery, and (iv) remote access [5]. However, higher operational price, security, and privacy represent the main disadvantages. In this work, Homomorphic Encryption method is presented as a solution to increase the security of the data. By using this method, a client can perform an operation on encrypted data without being decrypted which is the same result as the computation applied to decrypted data. Organization of the remaining sections of this paper is as follows. Section II presents the definition of cloud computing. Next, security issues of cloud computing are described in Section III. The challenges that face security are then presented in Section IV. After that, several applications and vulnerabilities of the cloud computing are described in Section V. Recent related works are the presented in Section VI. Next, Homomorphic Encryption is described in Section VII. Finally; the work is concluded in Section VIII.

II. Cloud Computing Definition

Cloud computing system is split into two parts; the front end and the back end [3]. Front end represents the user, while the back edge represents the service provider and the network between them can be performed as shown in Fig. 1.

Cloud computing provides the following services:

- Platform as a Service PaaS, in which cloud computing provides a platform and also an application can be built, test, and deploy. This permits the clients to manage, run, and develop new applications or services. There is no need to buy any software but need to pay for the time that uses only [4].
- A service SaaS, Cloud-Computing Software supplies licensed application to clients, such as Google Apps, and web-based emails, CRM and ERP systems.
- Infrastructure as a service IaaS, Cloud Computing on this method, provides an entire virtual data center of resource such as servers, server space, processors.

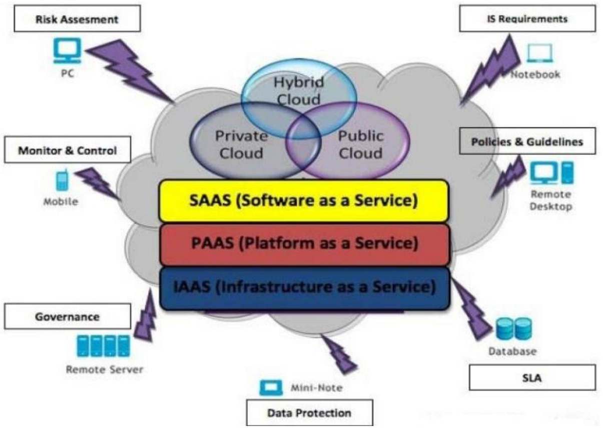

Fig. 1. Cloud Architecture [16].

IaaS hosts PaaS and SaaS, in this service, any breaking on IaaS will affect the security of both SaaS and PaaS services. If any cloud service is attacked, that will affect the other layer. The relationship between cloud models could be a source of risks. A SaaS provider could rent a development area from a PaaS provider, which may also rent infrastructure from an IaaS provider. Every provider is accountable for securing its services, which could result in an inconsistent combination of security models. It also makes confusion over which service provider is responsible if an attack happens. Utility Cloud computing is the using of computing resources by sharing it with several clients. There are a number of companies that support these services, such as Google, Amazon, and Microsoft, etc. Cloud computing is classified into four distributed models:

1) Private cloud, which is also named an internal Cloud, this type is used and modified only by the members of an individual organization. It represents a way to allow exclusive access for resources, facilities, applications, and services from everyone in a particular organization, and the organization or third-party provider owns the cloud infrastructure.

2) Public cloud, this type is made available to the industry or public where the cloud infrastructures, services, resources are available free to the public. Using this model, the services provider organization owns the Cloud (e.g., Amazon cloud service).

3) Community cloud, this type is shared among several organizations, and managed by them. By using this model, more than one organization is allowed to use and access cloud infrastructures, resources, facilities, and services. The main point of this model is that multiple organizations have the same policy and missions of work.

4) Hybrid cloud, this type combines between two or more of other computing cloud types where some services are allowed to public, where the other is granted only to an individual organization. The cloud infrastructure, services, applications, and data are a combination of private, public, and community cloud, on this module. The existence of a specific technology is necessary to allow portability (e.g., data stored in private manipulated by application in the community or public Cloud).

- Furthermore, three main components of cloud computing from the end-user perspective [7] are described as follows.
- *End-user*: Is a software or device that clients can use to access the services that are provided by the cloud service provider.
- *Cloud Network*: Represents a group of network devices that are used to connect the client with a cloud computing provider.
- *Cloud Application Programming Interface (APIs)*: A set of instructions that help programmer to develop different cloud services with various end-users.

The essential characteristics of cloud computing can be presented as five main keys below [3]:

- *On-demand self-service*: The services can be requested and managed from the cloud without the interaction with the service provider. The provision of the computing capabilities is accomplished when required automatically.
- *A broad network access*: The standard mechanism used to enable the user services and application to be accessible to the customers. The availability of the services should be heterogeneous using thin and thick clients.
- *Resource pooling*: The resources are shared to serve different costumers using multi-tenancy model. The mapping between the physical and the virtual resources provided to the end-user.
- *Rapid elasticity*: The resources are scaled-down and up as required. The current service matches the available resources.
- *Measured service*: Up-down scaling for the resources is automatically performed as well as controlling the resource usage by provisioning a metering ability for different kinds of services provided by the cloud.

Moreover, the data security of cloud computing mainly depends on the following requirements:

- *Data confidentiality*: It means that authorized people are only allowable to access data.
- *Data integrity*: It means that only authorized users perform modification on data.
- *Data availability*: It means that authorized users can access their data at any time and from anywhere. There are three main threats to availability; cloud service provider availability, network-based attack, and backup of saved data by the cloud service provider.
- *Data remanence*: This issue appears when data is removed it may be disclosed to an unauthorized part. Care must be considered when information is deleted. A simple schematic diagrams shown in Fig. 2 presents the life cycle of data.

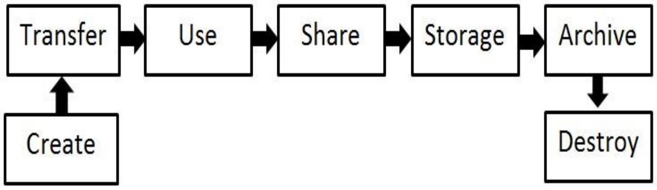

Fig. 2. Data Life Cycle [19].

III. Security Issues

Cloud-computing acceptance is affected by a low level of cloud security. It is a crucial factor to guarantee the success of any system, providing protection is a significant concern, cloud computing, which is also on this challenge.as shown in Fig. 3. However, security becomes more complicated when dealing with cloud environments and by multiple organizations that share resources.

In general, computer security focuses on these main objectives as reported in [4]. These objectives can be listed as follows:

1) Availability: It means clients can access services and resources that are provided by cloud computing providers from anywhere at any time.

2) Confidentiality: Data for the clients should be at a high level of security where it allows the authorized people to access only.

3) Data integrity: Keeps data safe, data shouldn't be lost or altered from unauthorized people or when it is stored or transport over the network.

4) Access Management (AM): Who can access the systems that have client's information? What can they access? Is the access appropriate? The answer is "provider has active identity management".

5) Audit: Everything in the system should be audited and checked, we can do that by adding a layer over the virtualized OS.

6) Control: Cloud computing provider sets strategies and regulations to organize the usage of the applications, services, resources, and so on.

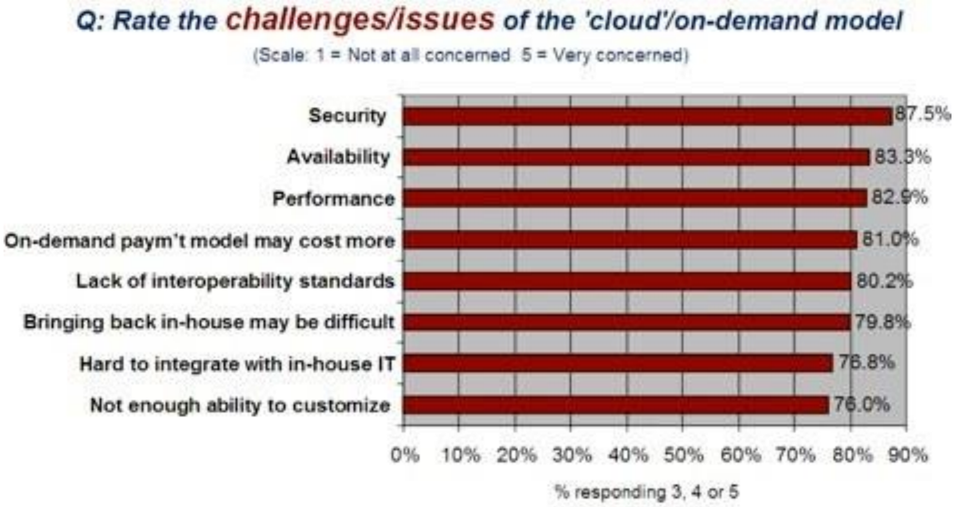

Fig. 3. Results of IDC Survey Ranking Security Challenges [8].

IV. Security Challenges

A. Delivery Model Security Challenges

The three service models are mentioned previously, and the relationship and dependency should be known between the delivery models and security challenges; to understand more about security concerns and security challenges. These layers are cumulated; which means an attack impacts on the Iaas layer, the attack will affect to the above two layers (SaaS-PaaS) [12]. The security challenge has a different level of each model and it can be summarized as follows.

In SaaS model, security challenge may raise according to the security responsibility which lies with the provider. Where, clients have less control over security when compared with two other models. So, it becomes difficult for the client to trust the security level and, also difficult to get confirmation of the services and application. In PaaS model, the clients have the ability to build their applications on the platform offered by the provider, so two security layers on this model the first one is the security of the client’s application implement on the platform that is powered by the clients while the second one is the security of the platform itself, the providers are responsible for this layer. Comparing this model with SaaS model, it seems more extensible, but any security under the application platform level will be powered by the provider. Some of the PaaS challenges related to data and other issues such as; Infrastructure security and third-party –services and tools. Best security level can be achieved with the IaaS model where the clients have full control over the security such as organization configures, control infrastructure, and policy security [6]. They should control the software running in VMM, but cloud providers still manage on the underlying infrastructure.

The security level of a network is also affected by network techniques which increase the probability to deal with certain attacks as follows [9][10]:

- *Hyper Visor Attack*: On virtualization hypervisor allows more than one operating systems use the same platform hardware. This may decrease the security on each such systems since it will be difficult to track and detect the security issues (e.g., any threats occur on the guest OS may be effective to the host OS).

- *Denial of Services*: Prevent the authorized clients to access their data and applications and also because the system to slow down by a huge number of requested by attacker this causes unavailable service for the authorized people.

- *Sniffer Attacks*: A sniffer is an application that can be used to catch the packets on the network. Sniffer attacks use this application by the hacker to read data on the packet if the data is being transferred through these packets are not encrypted. So the hacker can read clients passwords, sensitive data, and so on.

- *Reused IP addresses*: Each user on the network has an IP address assume that user moves out from the network then his IP address will give to another customer. From a provider's perspective, there is no problem; since it has a limited IP address. From a user's perspective, it will create a security risk to the new user since as there is a certain time delay between the change of an IP address in DNS and the clearing of that address in DNS caches, sometimes the old IP address still has a chance to access the data. This is violating the privacy of the earlier user.

- *Google Hacking Attack*: Search Engines, such as "Google" has been used by hackers to find system security vulnerability they decide to hake. There are two types of vulnerability found on the Internet, miss configurations and software vulnerability

The security is also affected by the location of the cloud systems [10] according to three main reasons:

1) Transfer data across countries borders.
2) Various location and services provider.
3) Data collection and Mixing.

V. Cloud Applications and Vulnerabilities

A. Netflix

Netflix is a global provider online video stream and now has over 75 million subscribers, In August 2008, the concept of the Cloud applied on this application, Netflix is considered one of the largest cloud services, and it gives services as SaaS module, but it was discovered that hackers tried to use Netflix according to the weakness in silver light Something like adobe flash. These attackers use fake advertisements to install virulent content on the users' system.

B. LinkedIn

It is a social networking site designed especially for the business community. To allow members to create their profiles and interconnect with trusted people, users create their profiles, and each account will have a user name and password. In 2012, this application lost a $5 million after hacker shared 6.5 million of its hashed passwords on password cracking forum.The company takes many procedures to increase security because they emailed the members to reset their passwords, Emailverfication, CAPTCHA (public Turing test), two-step verification(Two verification is needed in order to access an account).

C. iCloud

iCloud is a cloud sServices it allows apple client systems to store their information automatically, images up to date across. It was started 2011, by Apple Inc. Hackappcom shared a method that they can guess username and passwords for the clients using app API, DEFCON group it is also (Script Information), DEFCON group believes that the reason causing the cyber –an attack is iCloud. Response to this attacks iCloud now requested from the clients to enter passwords and anther such as SMS or email alternative verification.

D. Dropbox

It is a cloud service that offers the place for the clients to store their photos, file, videos, and allows safe back up and also many facilities. It was started in 2007. In 2011, hundreds of usernames and passwords of Dropbox clients were hacked. Also, there was a programming error that allowed access to the user accounts without passwords between 1:54 PM and 5:46 PM this error was detected immediately by Dropbox. To increase security, Dropbox uses two factors verification to allow clients to access their accounts.

VI. Related Works

Many methods and algorithms used to increase security in the cloud environment. Few of which are as follows:

A. Cloud Security Tools

Recently, there are many tools that are used by Cloud to prevent an attacker accessing the client's network; here are some of the most popular security tools [11]:

- *Silver Sky*: It is a Cloud-based on email and network security solutions. It provides email auditing and monitoring.

- *DocTracker*: Offers security Control for documents on the Cloud and services are working with file sharing (e.g. Microsoft SharePoint, Box, and API for integration). Without DocTracker when you send a document out of your system you cannot follow and track it, but DocTracker allows you to follow, control, and give each user you share a document with him a specific privilege.

- *Proof point*: Offers a high speed of response to block and detect spam's spread by email and insuring relevant data that come in and come out are secured.

- *Qualys*: Offers Web Application Security, Vulnerability Management, App Security Management, Web Access Management.

- *White Hat*: Offers a high level of protection website during the coding process.

- *Valuation:* Any data transferred from your network should be encrypted; this tool provides data encryption by AES Method.

B. *Using Mobile One-Time Password (OTP)*

Clients want to access their data at cloud computing storage on a remote server. Logging to the stored data using a static password will not provide a high-security level because of easiness hacking static password. In [13], the author recommends using a one-time password (OTP) method. It means when a user's logged to their account, they should enter the 4-digit pin on a login page which sent to their phone numbers have registered during upping sign account. Three most popular techniques to create the OTP password method are:

1) Time Synchronization: In this technique, both the server and client should be synchronized using synchronous time clocks; otherwise, OTP will not generate.

2) Event Synchronization: In this initial technique the counter assigned for both the client and the server, first when the client wants to login OTP will generate from the initial value of the counter then increment the counter to use for next login. On the server-side, the server will get the information that happened at the client-side, and then generate OTP from the initial value for the counter, then increment the counter value. After that, if two passwords from the client and server match, then the server will allow the client to access her/his data stored at cloud storage.

3) Asynchronous Challenge-Response Technique: In this technique, each time the server will provide a challenge to the client, which is dynamically unique every time. A hacking password will be complicated when used this technique.

C. *Software Security [14]*

A program composed by all kinds of people, and some are free that means open-source software allows both the developers and the hackers to edit the code; the hacker can exploit open-source code to find the failure points to install malicious on the cloud environment. So, security of the software can be enhanced as follows.

- *Virtualization:* Using virtualization technique provides security, this technique also allows isolation between hardware and lower-level functionality. Using this technique means the different process will run above the virtual isolation server when one of the VM is hacked, then the other VM will not be affected by this.

- *Host operating system:* This is one of the most important components of the cloud computing environment if hackers can access this OS, they can pierce all the guest operating systems on the computer. Therefor; host operating system should be secure, easy to update, and maintain.

- *Guest operating system*: Different types of operating systems can be used by clients to run their virtual private server (VPS). They can create, update, delete, and modify it. Since clients responsible for achieving security on their VMs; Awareness of customers will be very necessary, they should be informed about the importance of having the last updated version of OS and update of services and products; to avoid any security halls that can be exploited by the hackers.

- *Data encryption*: Using one of the encryption method keeping your data safe from hackers

D. *Physical Security*

A physical component in the cloud environment should be secure such as software; to avoid any vulnerability on the cloud environment can be exploited by the attackers. The enhancement of the security at the physical layer can be made by:

- *Backup*: For both customers and provider, it is essential to keep an offline backup of all their files.

- *Server location*: There are many factors that should be applied to the server location. At first server room should be isolated; it doesn't have windows and should be tight security to avoid any unauthorized access. Fire extinguishing system should be activated; also, cooling systems should be provided to prevent any overheating that may happen for machines.

- *Firewall:* Its a piece of hardware that helps screen out hackers, viruses, and worms that try to reach the computer over the Internet. Each client should be provided with the complete firewall solution by the cloud computing service provider. One of the most critical functions of the firewall is to protect against DDoS attacks.

E. *Algorithmic Approach for Securing Could*

- *Secure Data Division Algorithm*: The goal of this algorithm sharing data in a secure way, *(D)* is the whole data, where *(D1, D2, D3……, Dn)* are data pieces, *(S(D1), S(D2), …. S(Dk))* is the secure methods. This technique works as the following:

Algorithm [15]

```
S(D)
{If S(D) then return;
Else
{Divide D into smaller instanced D1, D2. ⋯. Dk, K⩾1
Apply Secure to each of these Data {D1, D2………… Dk}
Return Combine(S(D1), S(D2), …. S(Dk));
}}
```

- *Defense System for Advanced Persistent Threat*: It has been recommended that using a layered defense solution will be more secured compared to the single defense system. The basic idea of this system is to divide the cloud environment into several layers, and each layer will be responsible for a set of function to detect and protect the system from viruses and malicious. Using layered defense will provide a comprehensive approach for security to the entire component on the cloud environment [15].

VII. Homomorphic Encryption

In general, all the data that is stored in Cloud is encrypted, if the user needs to perform any computing on data, the cloud provider will decrypt the data, and then provides the decrypted data to the user. While the user process encrypted data on Cloud, it becomes prone to hacking; therefore, a new procedure technique was found to prevent data hacking and called Homomorphic Encryption. Homomorphic Encryption is a method that allows the user to perform an operation at ciphertext [18]. In addition, when the user decrypts the ciphertext, the process that is performed on it will appear in plain text. Homomorphic Encryption grants data security when storing, transmitting, and processing as shown in Fig. 4.

Let m be a plain text.

$$\text{Operation (m) = decrypt (operation (encrypt (m)))} \tag{1}$$

The Homomorphic operations are; the addition that performs on positive real numbers R+ and multiplication of set of logarithms R*as reported in [16].

Let x, y and z belong to R+

$$if\ x.y=z \tag{2}$$

Then

$$log\ (x) + log(y) = log\ (z) \tag{3}$$

Or

$$log\ (x) + log\ (y) = log\ (x * y) \tag{4}$$

The above two formulas help us to find the value of z directly, or through logarithms. In two cases, same result can be achieved, so it's more secure to perform computation on encrypted data than decrypting it. The basic concept in Homomorphic Encryption is shown in Fig. 5. Assume that a user wants to add two numbers 10 and 15, and the two numbers are encrypted into 100 and 150, then the encrypted two numbers will be added to each other on cloud servers. When the user wants to decrypt the result, he will gain 25.

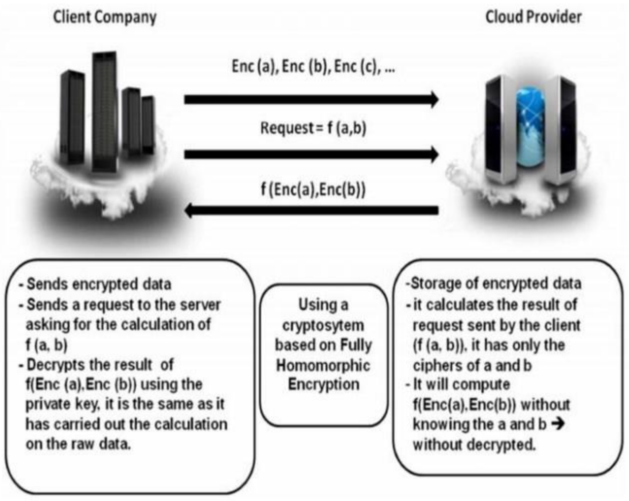
Client Company
Cloud Provider
Enc (a), Enc (b), Enc (c), ...
Request= f (a,b)
f (Enc(a),Enc(b))
- Sends encrypted data
- Sends a request to the server asking for the calculation of f (a, b)
- Decrypts the result of f(Enc (a).Enc (b)) using the private key, it is the same as it has carried out the calculation on the raw data.
Using a cryptosytem based on Fully Homomorphic Encryption
-Storage of encrypted data
- it calculates the result of request sent by the client (f (a, b)). it has only the ciphers of a and b
- It will compute f(Enc(a).Enc(b)) without knowing the a and b ➔ without decrypted.

Fig. 4. Homomorphic Encryption Applied to Cloud Computing [17].

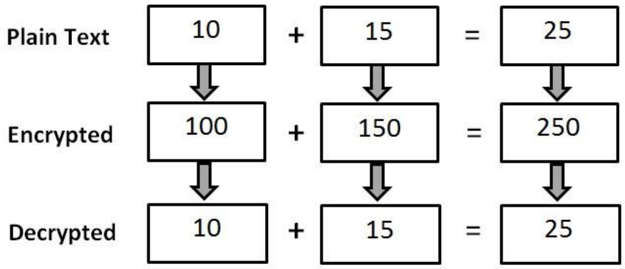

Fig. 5. Homomorphic Encryption Example [17].

There are three types of Homomorphic Encryption which can be presented as follows.

1) Fully Homomorphic Encryption (FHE), where an addition and multiplication are both performed on encrypted data with the full operation.

2) Partially Homomorphic Encryption (PHE), in this type of encryption, only one operation can be performed on encrypted data by either addition or multiplication. Pillars cryptosystem perform addition operation only while RSA cryptosystem performs multiplication operation on data.

3) Somewhat Homomorphic Encryption (SWHE), where the operation is performed on the limited number of multiplication or addition, and it is faster than FHE.

The two types (PHE and SWHE) are most widely used in cloud computing systems. Fig. 6 shows a schematic diagram of the HE system. To perform FHE on data stored in cloud servers, a secret key and a public key are needed. The following example will illustrate the FHE procedure, where J and K represent secret keys, P0, and P1 are public keys, N represents the user input. Fig. 7 describes FHE procedure. Craig Gentry from IBM has suggested the first "Full Homomorphic Encryption System" that calculates an arbitrary number of additions and multiplications, and thus computes any type of function on encrypted data. The interior working inserts another layer of encryption every step and uses an encrypted key to lock the inner layer of scrambled encrypted data. If the cipher text is decrypted, then the data will be refreshes without exposing it, allowing an infinite number of computations on it as shown in Fig. 6.

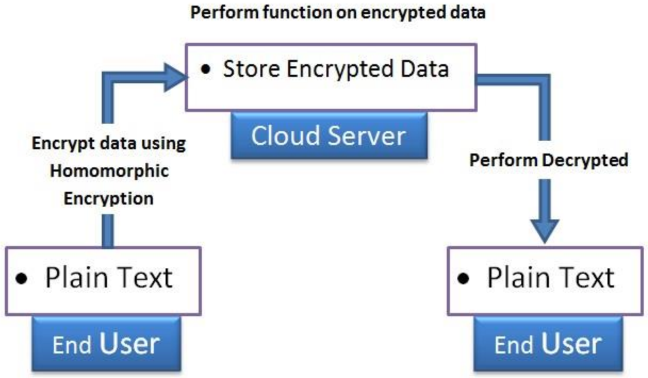

Fig. 6. FHE Proposed System [19].

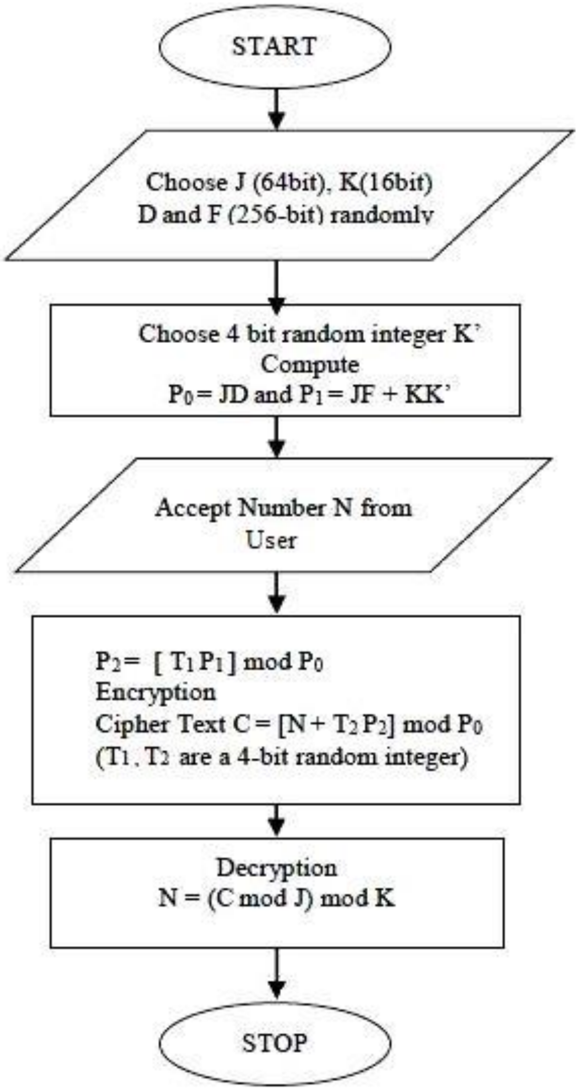
START
Choose J (64bit), K(16bit)
D and F (256-bit) randomly
Choose 4 bit random integer K'
Compute
$P_0 = JD$ and $P_1 = JF + KK'$
Accept Number N from User
$P_2 = [T_1 P_1] \bmod P_0$
Encryption
Cipher Text $C = [N + T_2 P_2] \bmod P_0$
(T_1, T_2 are a 4-bit random integer)
Decryption
$N = (C \bmod J) \bmod K$
STOP

Fig. 7. Flowchart of Fully Homomorphic Encryption Scheme [14].

The multi-layers of FHE cause the system to run too slowly. To solve this problem, many researchers have combined multiple schemes (see Fig. 8). The system starts with Homomorphic Encryption with a decryption algorithm embedded in a garbled circuit, which protects itself by Attribute-Based Encryption which ensures sustainable encryption [20].

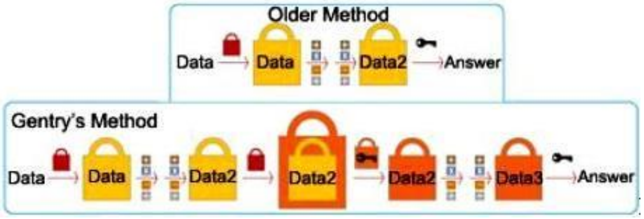

Fig. 8. Craig Gentry Implementation of FHE [20].

VIII. Conclusion

Although Cloud computing enhances the use of resources economically, there is a considerable amount of challenges it has to overcome. The main problems that arise due to the broad access nature of the networks are privacy, confidentially, and data security. Many encryption techniques are used to tackle these challenges such as Homomorphic encryption technique which is among the best encryption techniques to protect the data privacy in Cloud. It is known that all homomorphic techniques for Encryption, either partially or fully or somewhat, permit the processing of the encrypted data, which increases its security. In this review paper, some techniques and schemes for Homomorphic Encryption are discussed. In this paper, the approach of Homomorphic Encryption in cloud computing is presented and most security challenges at different levels of cloud computing with applications of vulnerabilities are explained. In addition, the most popular methods used to achieve the required level of security are presented as well. Cloud computing provides many facilities, flexibility, availability, but it faces security issues, so stringent security enforcement should be applied to ensure that the IT environments are more secure. However, it is essential to understand the security challenges and risks to avoid these challenges. On the cloud environment, all parties (customers, providers, network) should put further efforts than the traditional security solutions, because of the complex and dynamic nature of cloud computing.

Finally, several proposed solutions to migrate threats and attackers are suggested in this work as follows:

- Use more than one security layers on the application (e.g. factor authentication).
- Authentication and identity access management.
- Data encryption: when data transferred out of your network, it should be encrypted in cloud server.it is the best solution to secure information.
- Organizations should use Cloud-based security tools.
- Organizations should select an appropriate cloud model (e.g., group can use a hybrid model if they need to employ personal information on the private model, and they can use a public model to manage application).
- Do not use vendor-supplied default for any security parameters.
- Use high-security application interfaces.
- Isolation multi-tenant systems can be achieved by using isolation and segmentation techniques.
- The cloud user should have awareness of security; this creates a strong relationship between provider and customer.

References

[1] "United States : SOFTWARE ALLIANCE Hails Launch of US Framework for Improving Critical Infrastructure Cybersecurity." MENA Report, Albawaba (London) Ltd., Feb. 2014.

[2] P. Trenwith and H Venter,"A Model Aimed at Controlling the Flow of Information Across Jurisdictional Boundaries" International Conference on Cyber Warfare and Security, Academic Conferences International Limited, pp. 510, Jan. 2015,

[3] N. Dowlin, R. Gilad-Bachrach, and K. Laine,"Manual for using homomorphic encryption for bioinformatics," Proceedings of the IEEE , 2017.

[4] Top 10 Most Popular Code Review Tools for Developers https://www.softwaretestinghelp.com/code-review-tools/ (Accessed on 6th June 2019)

[5] Cloud Computing Security Benefits https://digitalguardian.com/blog/cloud-computing-security-benefits (Accessed on 1st July 2019)

[6] C. Prakash and S. Dasgupta, "Cloud computing security analysis: Challenges and possible solutions," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, pp. 54-57, 2016.

[7] K. Gupta,B. Rydhm, and B. Veerawali, "Cloud Computing: A Survey on Cloud Simulation Tools," International Journal for Innovative Research in Science and Technology, vol. 2, 2016.

[8] M. M. Alani,"Securing the Cloud: Threats, Attacks and Mitigation Techniques," Journal of Advanced Computer Science & Technology, vol. 3, 2014.

[9] V. Ashktorab, and R. T. Seyed, "Security threats and countermeasures in cloud computing," International Journal of Application or Innovation in Engineering & Management (IJAIEM) vol. 1, 2012.

[10] A. Murray, B. Geremew, N. Ebelechukwu, B. Jeremy, and P. Wayne, "Cloud Service Security & Application Vulnerabilit,." In Southeast Con, pp. 1-8. IEEE, 2015.

[11] S. Kuila, S. Shruthi, P. Chandan, and N. Ch SN Iyengar,"Cloud Computing Security by Using Mobile OTP and an Encryption Algorithm for Hospital Management," Journal of Computer and Mathematical Sciences vol. 7, 2016.

[12] E. Mathisen,"Security challenges and solutions in cloud computing," In 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011).

[13] Ch. Sasanapuri, H. Chilsi, Ch. Sudhakar, and Ch. Narasimham,"Classification of APT's and Methodological Approach to Secure Cloud Services," International Journal of Applied Engineering Research, vol 11, 2016.

[14] K. K. Chauhan, A. Sanger, and A. Verma, "Homomorphic Encryption for Data Security in Cloud ," IEEE, pp. 206-209, 2015.

[15] G. Rastogi and R. Sushil,"Cloud Computing Security and Homomorphic Encryption," IUP Journal of English Studies, pp. 47-59, 2015.

[16] K. Hashizume, D. G. Rosado, E. Fernández- Medina, and E. B Fernandez, "An analysis of security issues for cloud computing," Springer, pp. 1-13, 2013.

[17] M. M. Potey, C. A. Dhoteb, and D. Sharma, "Homomorphic Encryption for Security of Cloud Data," ScienceDirect, pp. 175 – 181, 2016.

[18] S. Bajpai and P. Srivastava, "A Fully Homomorphic Encryption Implementation on Cloud Computing," International Journal of Information and computation technology, vol.4, 2014.

[19] I. Ahmad and A. Khandekar, "Homomorphic Encryption Method Applied to Cloud computing," International Journal of Information and Computation Technology, vol. 4, pp. 1519-1530, 2014.

[20] R. M. Pir, Rumel M Pir, and I. U. Ahmed, "A Survey on Homomorphic Encryption in Cloud Computing," IJEDR, vol. 2, pp. 2173-2177, 2014.