International Journal of Engineering Research and General Science Volume 7, Issue 6, November-December, 2019
ISSN 2091-2730

Cloud Computing: Security Issues and Security Methods

Jiala Mafo Jules[1], Hongbing Cheng[2]

[1] College of Computer Science Zhejiang University of Technology Hangzhou-China

[2] College of Computer Science Zhejiang University of Technology Hangzhou-China

julemafo@outlook.com \ chenghb@zjut.edu.cn

Abstract— Cloud computing is becoming a priority for companies who want to improve the quality of their services. Unlike traditional solutions, where IT services are subject to appropriate physical, logical, and personnel controls, Cloud Computing moves application software and databases to large data Centers. However, data and service management may not be completely reliable. this data is the target of several network attacks, which aim to interrupt, intercept, modify and manufacture the information. therefore, it is critical to managing these attacks in the end to improve the use and adoption of the cloud. In this article, we present the different types of cloud services, deployment models, and architecture of Cloud computing with a special focus on security issues with Encryption and Decryption, and RSA algorithm. Also, the solutions for users to overcome some of the security issues are addressed in this paper..

Keywords— *Cloud computing, deployment models, services models, Cloud security, Encryption and Decryption, RSA algorithm.*

1. INTRODUCTION

Cloud computing aims to allow users to use technologies without the need for in-depth knowledge or expertise in the field. Several companies see cloud computing as an indispensable way to significantly manipulate all information technologies, how the data centers are built, how the software is deployed, and how to deal with updates. Virtualization is the main technology of cloud computing and virtualization software can be used for virtual computing devices, each of which can be easily used and managed to perform computing tasks **[1**], so it offers increased speed and flexibility**[2][3].** Despite all the benefits of the cloud, data security remains a major concern for some companies and slows the adoption of this technology. to facilitate this problem of cloud security and to reassure the companies, we will present through this paper some security technique that can help to understand why move to the cloud , how to use and the precautions to take. This paper is organized as follows: Section 2 describes the cloud service models and deployment models. Section 3 describes security issues, Section 4 describes the security methods, we will end this paper with a conclusion and perspectives

2. CLOUD SERVICES MODELS AND DEPLOYMENT MODELS

Every business has unique needs and meeting them all can be a tricky task. But the right cloud model and service model can transform the way we do business, It is also true that each business or organization has to go through its own unique requirements to decide on cloud deployment model.

2.1 CLOUD SERVICES MODELS AND DEPLOYMENT MODELS

Cloud service models are commonly divided into SaaS(software as , PaaS, and IaaS are exhibited by a given cloud infrastructure. It is helpful to add more cloud service models in SaaS, PaaS, and IaaS which are exhibited by a given cloud architecture (Figure1). DaaS (Data as a Service) and Naas (Network as a Service) are Cloud service models should be added to provide better service **[4]**.

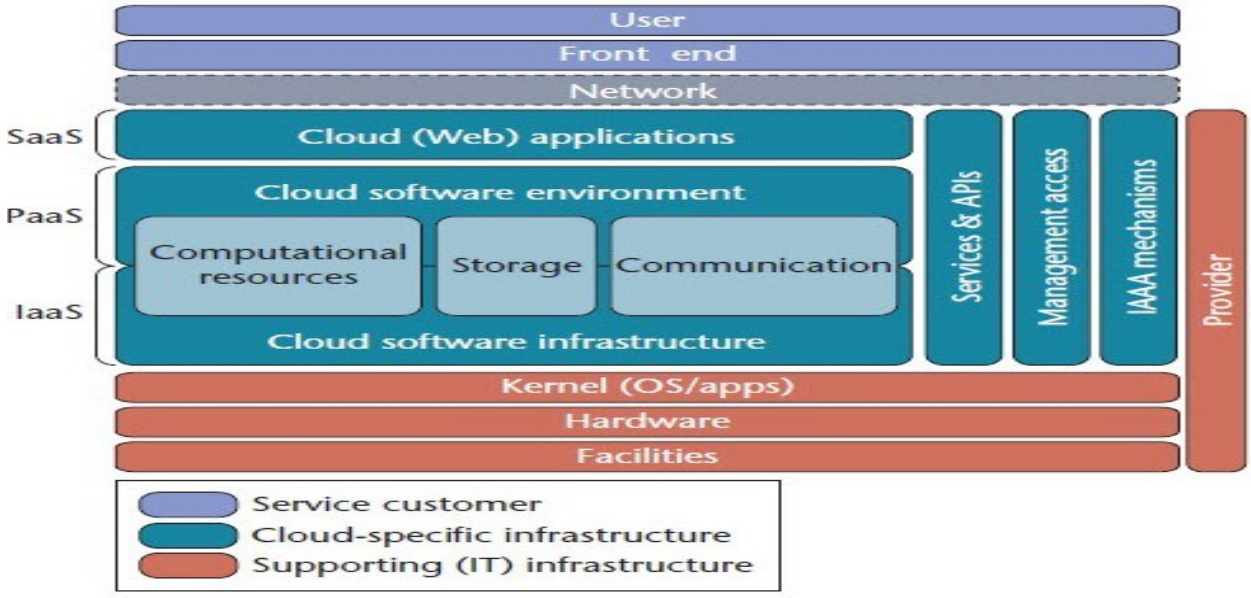

Figure 1: The cloud reference architecture.**[5]**

A. SaaS (Software as a Service)

It is the base layer which deals with virtual machines, storage (Hard Disks), Servers, Network and Load balancers. This reduces investment in computer hardware such as servers, networking devices and processing power**[6][7]**. The provider provides a ready-to-use, operational service capable of managing a large number of users. This service is accessible via the internet and is billed at use. The client has no installation task, maintenance or updates to perform. The user does not have to worry about the infrastructure underlying the application. The difference with a Classic software is paramount. It consumes the application in the same way that it consumes electricity. This is the most used cloud service level today. Figure 2 shows us the different players in the Cloud Market Computing. We note that there are many SaaS providers. For the most SaaS popular is Salesforce CRM, Google Apps or Exchange On Line.

Figure 2: Different players in the cloud market Computing

B. IAAS (INFRASTRUCTURE AS A SERVICE)

IaaS refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and uses Application Programming Interface (API) for interactions with hosts, switches, and routers, and is capable of adding new equipment in a simple and transparent manner [8]. In general, the user does not manage the underlying hardware in the cloud infrastructure, but controls the operating systems', storage and deploys applications. The service provider owns the equipment and is responsible for housing, running and maintaining it, the client typically pays on a per-use basis[7].

C. PAAS (PLATFORM AS A SERVICE)

This service is similar to SaaS in that the infrastructure is controlled by the cloud service provider but it is different in that the users can deploy their own software. In this model, the clients can install and deploy their customized applications by using the tools offered by the cloud service provider. Physical settings are controlled and restricted by the cloud service provider and application settings are given to each user to control them [9]. The PaaS offers the user, in addition to a software use service to distance, access to a real development platform, equipped with a programming language, development tools, and modules. The user benefits from a managed development environment, hosted, maintained by a cloud provider, based on an infrastructure that is external to his company. He will have the opportunity to develop unique tools for his business using a collective interconnection of several internal or external stakeholders.

The main PaaS offers are:
- Microsoft with Windows AZURE
- Google with Google App Engine
- Orange Business Services.

2.2 Cloud deployment Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand as depicted in figure 3. The Cloud Computing model has three main deployment models which are**[9].**

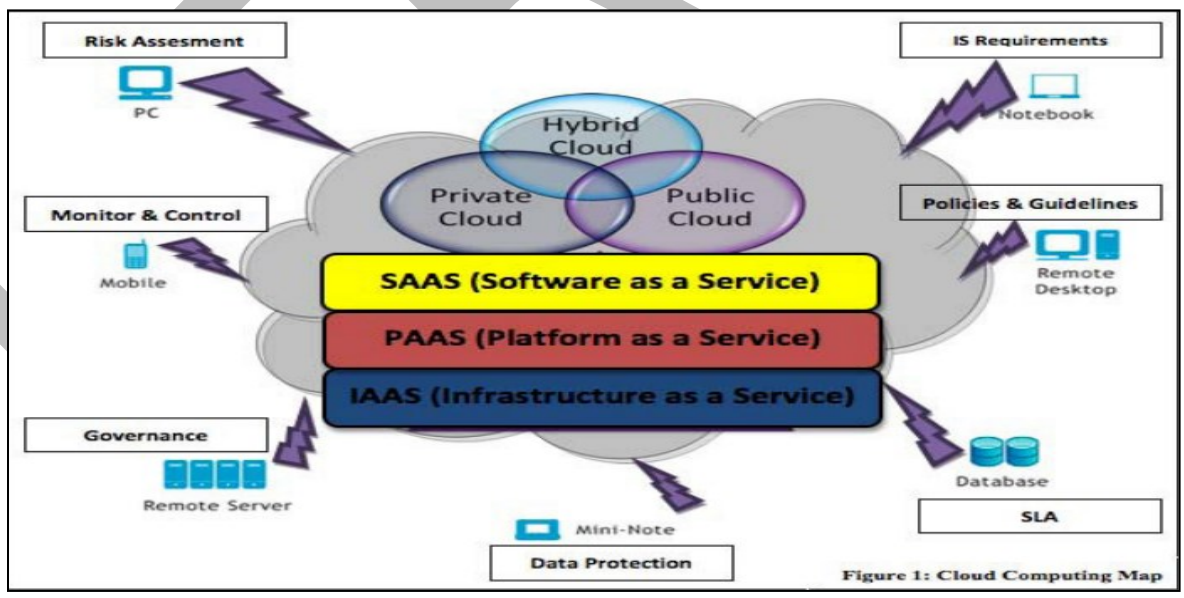

Figure 3. *Cloud Deployment Models*

A. Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination**[10][11]**. Public clouds are widely used in addressed offers to the general public, they are less likely to need infrastructure and security private clouds. However, businesses can still use the cloud to make their operations more efficient, for example for non-responsive content, collaboration with online documents and messaging web. It is important to note that all customers on public clouds share the same infrastructure pool with limited configuration, security protections and availability variances.

B. Private Cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising of multiple consumers (figure 1). It may be owned, managed, and operated by the organization, a third party, or some combination, and it may exist on or off premises **[12]**. The added security provided by the private cloud model is ideal for every type of organization or enterprise that needs to store and process data privaty, or to perform sensitive tasks. For example, a cloud service in the private sector can typically be used by a financial corporation obliged by law to store sensitive internal data, but who also wishes to use some of the benefits of cloud computing in its infrastructure, such as the allocation of resources on request.

C. Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination, and it may exist on or off premises**[13].** It is a model dedicated to a specific professional community including partners, subcontractors so that it can work collaboratively on the same project or it can be a governmental cloud dedicated to the institutions. state.

D. Hybrid Cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enable`s data and application portability (e.g., cloud bursting for load balancing between clouds) **[14].** The hybrid cloud therefore poses a significant problem for cloud computing: that of the integration. Hybrid Cloud models can be implemented in many ways:
- Cloud vendors join forces to provide integrated services in private and public clouds;
- Individual cloud providers offer a complete hybrid package;
- Organizations managing their own private cloud themselves subscribe to a public cloud service that they integrate into their infrastructure. Cloud Computing is a solution that provides a space in which it is possible to virtually place server or network infrastructures, development or execution, and all this can be deployed on different cloud typologies called cloud computing deployment models.

3. Cloud Security Issues

Due to the growth of the cloud in the industry, entrepreneurs have decided to adopt cloud services, in spite of being aware of its security issues. Thus, clouds attract attention from a potential dangerous community and other parties aiming to exploit security vulnerabilities. Numerous companies and people benefit significantly from the movement of their computing needs in the cloud**[15]**. Companies can reduce costs, improve the ease of use and increase the reliability by falling over for cloud services available on the public, but cloud computing is also attractive for cybercriminals. Here are examples of services of legitimate cloud computing, all of whom were taken advantage of by cybercriminals**[16][17]**:
-Blogs, Facebook and Twitter were used to pass on commands from Command and Control Servers, Google Docs, Dropbox and Pastebin served as zones of deposit for stolen data.
-Amazon EC2 was used to act as a hostile system of use general service providers succeed generally. Cloud does have certain security risks and it is important to understand them in order to avoid these problems. The most relevant threats are: Data loss/Data leakage, Insecure APIs, Malicious insiders, Account/Service & Traffic Hijacking, Abuse of Cloud Computing, Unknown Profile Risk, Shared Technology Vulnerabilities, Distributed Denial Of Service Attacks, Negligence of the users. these are the threats to cloud computing, plus the domains in which they are included and the service models they affects**[18]**.. A check √ mark means the threat affects the underlying model. A cross × means otherwise in table 1 .

Table 1: Top threats to cloud computing

Threat #	Name	IaaS	PaaS	SaaS
1	Abuse and Nefarious use of cloud computing	√	√	X
2	Insecure interfaces and APIs	√	√	√
3	Malicious insiders	√	√	√
4	Shared technology issues	√	X	X
5	Data loss or leakage	√	√	√
6	Account of service Hijacking	√	√	√
7	Unknown risk profile	√	√	√
8	Negligence of the users.	√	√	√

A. Data Loss / Data leakage

Data loss is any process or event that results in data being corrupted, deleted and/or made unreadable by a user and/or software or application. It occurs when one or more data elements can no longer be utilized by the data owner or requesting application and the problems that interrupt the activity are due to an internal malfunction of the software or hardware and human errors, which are also the problem of the Internal malfunction caused by either the users or the misconfiguration. We will give more details on how to avoid it in the last point of this paper. Figure 4 represents the graph of possible data loss reasons and their percentage is shown following the measures **[19][20]**.

Figure.4 errors percentages of the data loss

The Impacted Services Models are: IaaS, PaaS, SaaS, the threat of data compromise increases in the cloud due to the number of and interactions between risks and challenges, which are numbers unique to the Cloud , or more dangerous because of the architectural or operational characteristics of the cloud environment**[21][22]**; Due the establishment of a data protection system (DLP), it is the practice of detecting and preventing confidential data from being "leaked" out of an organization's boundaries for unauthorized use. Data may be physically or logically removed from the organization either intentionally or unintentionally. The solutions is based on centralized rules that identify, monitor and protect data that is stored, in use or in motion regardless of the medium**[23],** enforce powerful API security, secure data with SSL encryption, check for the integrity of the data running time duration as well as designing time duration, and explore the backup and collection plans of the provider.

B. Account or Service Hijacking

The cloud account hijacking occurs when the password for accessing data hosted in the cloud is stolen or hijacked by an attacker, regardless of whether it is a personal account or an organization. The cloud account hijacking is a tactic similar to identity theft**[13]**. The attacker uses the login information of an impersonated account to conduct malicious or unauthorized activity.
The Impacted Services Models are: IaaS, PaaS, SaaS. Although account or service hijacking is not new, cloud solutions add a new threat because a successful attacker can eavesdrop on the activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites as well as use your account or service instances as a new base for the attacker, which can possibly leverage the power of your reputation to launch subsequent attacks. Companies must take proactive steps in choosing cloud service providers. They need to look carefully at contracts to compare the security of data integrity systems**[24]**.

C. Malicious Insiders

ACcording to CERN(https://www.cert.org/insider-threat/), an insider threat is "A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems." The Impacted Services Models are :IaaS, PaaS, SaaS**[25]**; the system can have been damaged by an authorized employee, business partner, or administrator who has access to a network or resources. This dangerous threat affects the confidentiality, integrity or availability of business information.. A well-known malicious insider threat is amplified for customers under a single management domain, combined with a general lack of transparency into provider process and procedure as well as little or no visibility into the hiring standards and practices for cloud employees, creating an attractive opportunity for adversary**[26]**. Suggestions to mitigate this threat are plans to enforce authorized supply chain management, include human resource requirements in legal contracts, and absolute visibility in security mechanism and compliance.

D. Shared *Technology Vulnerabilities*

Cloud with its IaaS functionality provides high-end scalability by allowing users to access shared devices. A hypervisor allows a guest operating system to connect to other physical resources. This places the cloud at risk when the guest operating system gains access even to the unnecessary levels which influences other systems on the network. IaaS vendors deliver their services in a scalable manner by a multi-tenant architecture, so it should be used to ensure that the network is safe and secure. Suggestions to mitigate this threat are to achieve better security measures for the purpose of installation / configuration, auditing of non-authorized changes and activities, and scanning for vulnerabilities from time to time**[12]**.

E. Unknown Risk Profile

One of the best features or functionality of the Cloud is that it reduces costs and the costs of installing software. Although it may seem very helpful and extraordinary; it includes a few security risks beneath itself. Avoiding details like security mechanisms and policy compliance along with the details such as security and security infrastructure, and vulnerability assessments should also be considered. The Impacted Services Models are: IaaS, PaaS, SaaS . often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats. Suggestions to mitigate this threat are non-exposure of data and logs, non-revealing the details of infrastructure, and alerting on important issues.

4. Security Methods

The frequency and strength of cloud attacks are on the rise. With the exploitation of millions of non-secure Internet of Things devices, creating botnets that can launch highly distributed volumetric attacks is easier and more efficient than ever before. In addition to larger volumes, attacks forgo network and transport layers to target the application layer While the best way to protect user data in the cloud is by providing a layered security approach, cloud service providers should implement industry best practices to ensure the utmost level of cloud security on their side. Here are several tips on how cloud developers and users can ensure the security of their cloud-based solutions.

A. Encryption and Decryption Methods

The techniques used is encryption and decryption of data. These are also called encoding and decoding, or enciphering and deciphering. Encryption, encode or encipher is a method by which the original text, often called the plaintext, is changed, such that the meaning of the text is hidden, i.e. the plaintext is transformed into an unintelligible string of text, often called the ciphertext. In order to change the ciphertext to the plaintext, it has to be decrypted, decoded or deciphered. Figure 5 below shows an overview of encryption and decryption procedure.

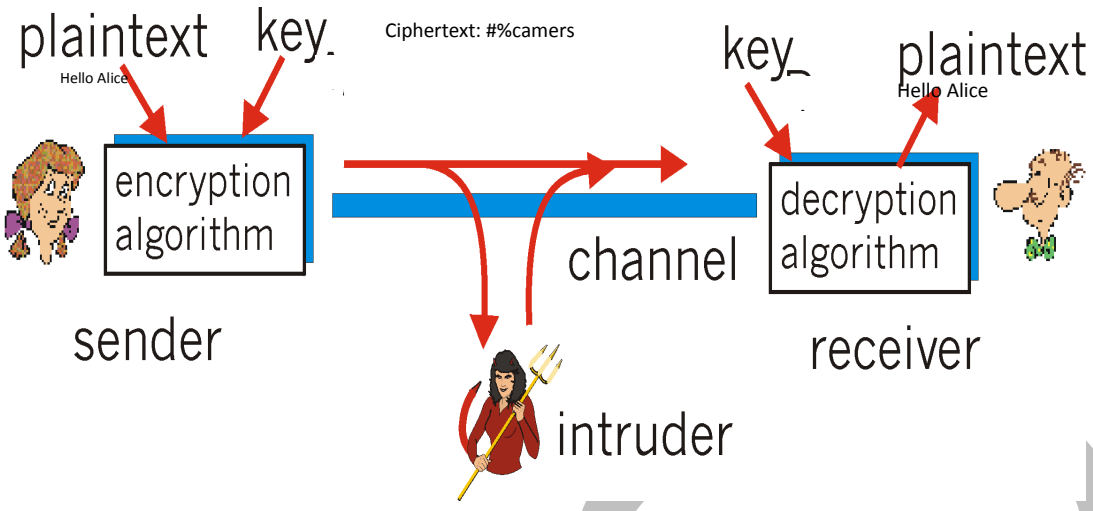

Figure 5: Shows an overview of the procedure of encryption and decryption.

Demonstration method: In the example shown in Figure 5, the plaintext P is considered a sequence of characters P =<H,e,l,l,o, ,A,l,i,c,e,!> and in the same way the ciphertext C = <#,%,c,a,m,e,r,s,,,{,:,?>. A system that encrypts and decrypts data is called a cryptosystem. If we denote the two processes in a cryptosystem formally, it would be C = E(P) and P = D(C), where C is the ciphertext, P is the plaintext and E and D are encryption and decryption algorithms respectively. The cryptosystem is denoted as P = D(E(P)), which means that the plaintext P is the decryption of encrypted P. In cryptosystems a key K is usually used with an algorithm in order to encrypt or decrypt data. If the same key is used for both encryption and decryption, then the process is called symmetric encryption, and the key is called a symmetric key. In this case the encryption and decryption algorithms are symmetric and they can be considered as reverse operations with look at each other. The formal notations would be C = E (K, P) and P = D (K, C), and the cryptosystem is denoted as P = D (K, E (K, P)). If the key is used for encryption, then the process is called asymmetric encryption. Here we use two keys, namely an encryption key (often called private key) KE for encryption and a decryption key (often called public key) KD for decryption. The formal notations in this case would be C = E (KE, P) and P = D (KD, C) and the cryptosystem is accordingly denoted as P = D (KD, E (KE, P)). This can be useful in the cloud when Platform-as-a-Service (PaaS) becomes mainstream to deliver enterprise applications through web technology to web users**[27]**.

B. **Homomorphic RSA Encryption**

The time is to outsource the data. It is cloud computing, which allows the sharing of the structures of conservation and data processing. One of the problems with this is the preservation of confidentiality between the customer and the provider. Certainly, the usual cryptography can partly answer this problem, since the customer can decide to store only encrypted data.

But this is not realistic. How do you do, for example, if you want to search your data? Impossible, normally, you would do it directly on the encrypted data! Unless your encryption system has the following property: Data processing algorithms pass through the encryption layer. In other words, if the customer wants to perform certain calculations on this data, it is sufficient that he asks the provider to perform these calculations on the encrypted data, the provider transmits the result (which is encrypted), the client decrypts it and he gets the desired result (in clear). These ciphers are called homomorphic encryption **[28][29].** The steps of the generation of encryption keys and decryption of the algorithm of RSA are as follows:

- **Key Generation:**

- we choose two primes x and y and one calculate the product n = xy;
- Then choose a random encryption key e, such that e and (x-1) (y-1) are first between them; Finally, the decryption key is calculated in such a way that:

$d = e^{-1} \mod ((x-1)(y-1))$

The public key is thus formed of the two numbers *e* and *n*, the private key is the number *b*.
Below the RSA algorithm in detail:

- **RSA Cryptosystem:**

√. **Generation of keys:**
- Choose x and y
- Calculate n = xy; *ø(n) = (x - 1) (y - 1)*
- Determine d such that*: e.d* ≡ 1 *ø(n)* mod *(n)*

Public key: xk = (e, n)
Private key: sk = d

√. **Encryption: Enc (m, pk)**
- Calculate $c = m^e \bmod n$

√. **Decryption: Dec (c, sk)**
- Calculate $m = c^d \bmod n$

human attacks from around the world means, by intercepting and replacing the public key, the attacker retrieves the public key of an interlocutor and provides the second with its own public key in place. Suppose we have c_1 and c_2 two ciphertext texts with the RSA algorithm and m1 and m2 the corresponding clear texts such as:

$$c_1 = m_1^e \bmod n$$
$$c_2 = m_2^e \bmod n$$
$$c_1.c_2 = m_1^e\, m_2^e \bmod n$$
$$= (m_1 m_2)^e$$

By deciphering the product of the figures, we obtain the product of the clears:

$$Dec_s(c_1 c_2) = \left((m_1 m_2)^e\right)^d \bmod n$$
$$= m_1 m_2$$

- **Experimental Results**

In this section, we are taking some sample data end implementing RSA algorithm over it.

√. **Key Generation:**
-We have chosen two distinct prime numbers x=17 and y=11.
-Compute n=xy, thus n=17*11 = 187.
-The Random encryption function, Ø(n)=(x-1) *(y-1),
Thus Ø(n)= (17-1) *(11-1) = 16*10 = 160.
-Chose any integer e, such that 1 < e < 160 that is coprime to 160.

-Here, we chose e=3.
Compute d, $d = e^{-1} (\text{mod } Ø(n))$,
thus $d=3^{-1} (\text{mod } 160) = 53$
Thus, the Public-Key is (e, n) = (3, 187) and the Private- Key is (d, n) = (53, 187). This Private-Key is kept secret and it is known only to the user.

√. **Encryption:**
The Public-Key (3, 187) is given by the Cloud service provider to the user who wish to store the data. √. Let us consider that the user mapped the data to an integer m=21.
Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user. $C = 21^3 (\text{mod } 187) = 98$.
This encrypted data i.e.; cipher text is now stored by the Cloud service provider.

√. **Decryption:**
When the user requests for the data, the Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid).
The cloud user then decrypts the data by computing, $m = 98^{53} (\text{mod } 187) = 98$.
Once the m value is obtained, user will get back the original.
RSA encryption realizes the Homomorphic multiplicative encryption. We can see that in the cloud, RSA encryption realizes the Homomorphic multiplicative encryption. A company is never safe from a malicious employee who is ready to steal unscrupulous data . To avoid this disaster, the best solution is to keep the encryption keys on a physical storage medium and not on the cloud. Companies that put their security back in the hands of a cloud computing provider are at increased risk.

C. Security Awareness

Some network administrator think that the only way to achieve a perfect level of security is without a user, but there are some ways around. Users, by their mistakes or because they are vulnerable to social engineering attempts, are often a prime target for attackers. Today, the vast majority of successful attacks begin by sending an email to someone trying to convince them to click on a link or open an attachment. Not trying to exploit a 0 day on a firewall. It is therefore necessary to always make users aware of the respect of a certain level of computer security and to do it themselves. Today with the exponential rise of cybercrime, if there is a universal message to remember about users, it would be: "*Think before clicking*". So, if we want to build security, we have to avoid straining users to respect complex security tasks, but teach them to be vigilant and how to long for convenient and safe solutions. The basic actions that users must perform to facilitate the work of engineers are:
-Do not open any questionable emails, and transfer them to the administrator for verification.
-Be careful with the passwords: do not memorize them in the browser on the workstation, do not share them with your friends or colleagues. Change your password immediately, when your co-worker leaves the company.
-Always inform your technician when you want to install new software on your computer because there is a lot of corrupted software.
-Be careful when using payments on the Internet. Always make sure the padlock is in the browser's address bar, if the address of the site starts with “HTTPS” (we are aware that not everyone has migrated from http to HTTPS). Privilege purchases with an order confirmation by SMS and never communicate your bank details by email or SMS.

CONCLUSION

Achieving a sufficient level of security in the cloud to prevent technological and informational risks is essential for individuals, organizations, or states that use or provide cloud services. It is important to be able to identify the values to be protected and the risks appropriately to determine the security requirements and the means to satisfy them. This implies a global, multidisciplinary and systemic approach to security. Cloud security must address the availability, integrity, and confidentiality needs of certain resources. Protecting information when it is transferred is not enough; it is just as vulnerable, maybe more, when it is processed, processed and stored. Cloud computing security in the context of the Internet and cyberspace is more commonly known as "cloud security”. The security of cloud computing will then be effective to the extent that we will be able to place homogeneous protection measures as cryptography, Homomorphic RSA encryption online solutions and complementary resources of the environment that also hosts them. However, in addition to proactive security measures to protect values, there is a need for reactive measures to mitigate unsolicited incidents, whether they are criminal or result from errors or natural disasters. The purely technical aspects of safety involve the effective implementation of operating and management procedures. In addition, the organization's staff must be trained in security measures and must commit to respecting them. Cloud computing security also relies on the integrity of people who design, manage, use cloud infrastructures and on the proper management of human resources.

REFERENCES:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, M. Zaharia, Above the Clouds: A Berkeley View of Cloud Computing, Technical Report No. UCB/EECS-2009-28, February, 2009.

[2] IBM Corporation , Create Operational Flexibility with Cost-Effective Cloud Computing, Produced in the United States of America January 2011.

[3] Ab Rashid Dar, Dr.D.Ravindran, Survey On Scalability In Cloud Environment, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5, Issue 7, July 2016.

[4] Colin Ting Si Xue and Felicia Tiong Wee Xin, Benefits and challenges of the adoption of Cloud Computing in Business. International journal on Cloud Computing: Services and Architecture, Vol. 6, No. 6, December, 2017.

[5] Santosh Kumar and R. H. Goudar, Cloud Computing-Research Issues, Challenges, Architecture, Platforms and Applications: A Survey, *International* December, 2012.

[6] Mukul Varshney, Anand Sharma and Shivani Garg, Cloud Computing: Architecture, Challenges and Application, *International Journal of Recent Trends in Engineering and Research*, Vol. 03, No. 06, pp. 1-7, June, 2017.

[7] Rabi Prasad Padhy, Manas Ranjan Patra Suresh Chandra Satapathy, Cloud Computing: Security Issues and Research Challenges, IRACST - *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, Vol. 1, No. 2, December 2011.

[8]Vijay Kumar, Brief Review on Cloud Computing, *International Journal of Computer Science and Mobile Computing*, Vol.5 Issue.9, September-2016, pg. 01-05.

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

[10] Intel, Cloud Solutions Meet Changing Needs with a Competitive Advantage, No. 335704-002US, September , 2017.

[11] Delvis Simmonds and Alli Wahab, Public Cloud Computing vs. Private Cloud Computing: How security Matters, Computing and Technology Department, Cameron University, Lawton, Ok, USA, pp 7-9 , April, 2012.

[12] Sumit Goyal, Public vs Private vs Community-Cloud Computing: A Critical Review, Computer Network and Information Security, Vol. 3, PP. 20-29, march, 2014.

[13] Tharam Dillon, Chen Wu and Elizabeth Chang, Cloud Computing and challenges, 2010 24th *IEEE International Conference on Avanced Information Networking and Applications,* Perth, Western Australia, pp. 2-7, April 2010.

[14] Gerad Briscoe and Alexandros Marinos, Digital Ecosystems in the Clouds: Towards Community Cloud Computing, LSE Research online, *international conference on Cloud Computing,* Beijing, China, PP.1-4 December, 2009.

[15] Tribikram Pardhan, Mukesh Patidar, Keerthi Reddy and Asha A, Understanding Shared Technology in Cloud Computing and Data Recovery Vulnerability, *International Journal of Computer Science And Technology (IJCST*) Vol. 3, Issue 4, Oct - Dec 2012.

[16] S. Venkata Krishna Kumar and S.Padmapriya, A Survey on Cloud Computing Security Threats and Vulnerabilities, *international journal of innovative research in Electrical, Electronics, Instrumentation and control Engineering* Vol. 2, Issue 1, January 2014.

[17] Peter Mell, The NIST Definition of Cloud , *Reports on Computer Systems Technology*, MD 20899-8930, p.1-7 sept, 2011.

[18] CSA, Top threats to cloud computing, Cloud Security Alliance, V1. 0, March, 2010.

[19] ALEX, Facts and Measures about Data Loss and Recovery Mechanism, Nextofwindows, May 8, 2018

[20] Somesh P. Badhel, Prof. Vikrant Chole, A Review on Data Back-up Techniques for Cloud Computing, *International Journal of Computer Science and Mobile Computing*, Vol. 3, Issue. 12, pp. 538-542, December, 2014.

[21] C. Linda Hepsiba and al, Security Issues in Service Models of Cloud Computing, , *International Journal of Computer Science and Mobile Computing, Vol.5*
Issue.3, pg. 610-615 , March- 2016.

[23] Data Leakage Detection and data prevention using algorithm, International Journal Of Computer Science And Applications Vol. 7, No.4, Apr 2017.
.
[24]Kashif Munir and Prof Dr. Sellapan Palaniappan,"Framework for Secure Cloud Computing", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.2, April 2013.

[25] Yasir Ahmed Hamza and Marwan Dahar Omar, Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing, International Journal of Computational Engineering Research||Vol, 03||Issue, 6||

[26] Microsoft, Microsoft Security Intelligence Report ,Volume 22 , January through March, 2017.

[27] Shuo Chen, Rui Wang, XiaoFeng Wang, and Kehuan Zhang. Side-channel leaks in web applications: A reality today, a challenge tomorrow. In IEEE Symposium on Security and Privacy, vol, 10, pp191–206, 2010.

[28] D.Chandravathiwr and Dr. P.V.Lakshmi Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 825-837.

[29] Iram Ahmad and Archana Khandekar, International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530.