A SURVEY ON ENHANCING CLOUD DATA SECURITY USING RSA ALGORITHM

RAJENDRA H.RATHOD[#1], MS.R.R.TUTEJA[*2]

[#]*M.E. (Pursuing), Computer Science and Engineering,*
Prof.Ram Meghe Institute of Technology & Research,
Badnera-Amravati, Maharashtra, India
[1]rh_rathod@yahoo.com

[*]*Professer, Prof.Ram Meghe Institute of Technology & Research,*
Badnera-Amravati, Maharashtra, India
[2]ranu.tuteja@gmail.com

ABSTRACT: **Cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Cloud computing is so flexible with the fact that services are accessible anywhere any time lead to several potential risks. But the problem associated with Cloud Computing is the Cloud security and the proper implementation of Cloud over the Network. Data security is a critical issue in the cloud computing environments. In cloud, the data can be physically located anywhere in any data centre across the distributed network. The cloud nature issues more with user authentication, data integrity and confidentiality. The data hosted in the cloud is completely under the third party control to ensure the data usage in the cloud. The main aim of this paper is to survey security issues and some cryptographic concepts in cloud computing communications already presented in the papers by various authors to increase the security of encrypted data in cloud servers. In this paper is attempt to secure data from unauthorized access, the method of data security is RSA algorithm for providing data security by encrypting the given data based on the KEY combinations.**

Keywords: Data Integrity, Data Confidentiality, Cloud Computing, RSA, NIST, cipher text, plain text.

I. INTRODUCTION

The definitions of Cloud Computing considered by the National Institute of Standards and Technology (NIST): "Cloud Computing is 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", [1]. In the cloud environment, resources are shared among all of the servers, users and individuals. As a result files or data stored in the cloud become open to all. Therefore, data or files of an individual can be handled by all other users of the cloud.[13,14] Cloud computing can be expressed as a combination of Software-as-a-Service which refers to a service delivery model to enabling used for business services of software interface and can be combined creating new business services delivered via flexible networks and Platform as a Service in which Cloud systems offering an additional abstraction level which supplying a virtualized infrastructure that can provide the software platform where systems should be run on and Infrastructure as a Service which Providers manage a large set of computing resources which is used for storing and processing capacity. [12].

II. THEORY

Characteristics of Cloud Computing

According to NIST, the Cloud model is composed of five essential characteristics:

On-demand self-service:

On-demand self-service means that consumer (usually organizations) can request and manage their own computing resources. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider [1].

Broad network access: Cloud capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations) [1].

Resource pooling:

Resources pooling means that customers draw from a pool of computing resources, usually in remote data centers. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacentre). Examples of resources include storage, processing, memory, and network bandwidth [1].

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time [1].

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability (pay-per-use basis) at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service [1].

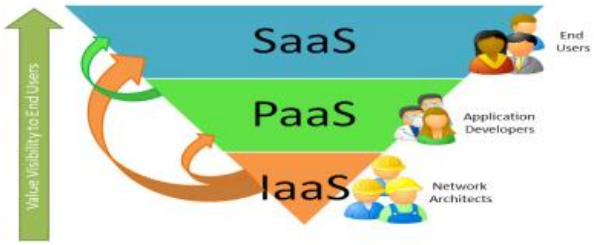
III. SERVICE MODELS OF CLOUD COMPUTING:

According to NIST, the cloud model is composed of three service models:

Software as a Service (SaaS): In this model the providers that maintaining the cloud will install the software and the clients that belong to that particular cloud provide access to the users of that cloud. So, this type of service provides more comfort because the users of cloud can access the software application without installing in their own computer because a cloud client provides access to the cloud use. So there will be a less concern on maintaining it [1],[17].

Platform as a Service (PaaS): In this cloud providers provide a computing platform for accessing their applications so, user develop their programs and execute in the execution environment provided by the cloud providers. In this the resources that are existing with cloud users such as computers storage resources are automatically match with the application of particular computing platform. [1],[17].

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) [1].



There are four main type of cloud: [4],[6]

Public Cloud : The cloud computing resource is shared outside, anyone can use it and some payment maybe need. It is also known as external cloud, the services are provided by a third party via Internet, and they are available and are for commercial purposes.

Private Cloud : This cloud consists on the hosting of private applications and services for private use (private networks) only, it's resource is limit to a group of people, like a staff of a company etc.

Hybrid Cloud : This is a mixture of previous two clouds, some cloud computing resource is shared outside but some don't.

Community Cloud: It is a combination of public and private cloud. This is a better option when someone don't want to invest too much in infrastructure and on the other side wants the data to be secured by using private cloud deployment. More than one community shares a cloud to share and reduce the cost of computing system.

IV. IMPORTANT SECURITY ISSUES IN THE CLOUD COMPUTING

Even though, the virtualization and Cloud Computing delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud which makes the users to resist themselves in adopting the technology of Cloud Computing. Some of the security issues in the Cloud are discussed below:

Integrity: Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a regular basis which will then be stored in an off-site location [2].

Availability: Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that

companies have business continuity plans (BCP‟s) in order for their systems to have redundancy [2].

Confidentiality: Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren't encrypting their communications [2].

There are complex data security challenges in the cloud: [3]

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management

A new type of insider who does not even work for your company, but may have control and visibility into your data

V. LITERATURE REVIEW

Multiple research activities were introduced to address the issue of intrusion detection within cloud computing environments. Many authors have proposed a method by implementing various algorithms and IDS. In this paper we are focussing on using of RSA algorithm to ensure the security of data in cloud computing. RSA algorithm encrypts the data to provide security so that only the concerned user can access it. The purpose of securing data, unauthorized access does not allow. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public -Key and Private-Key, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.[5],[7],[8]

ENCRYPTION ALGORITHMS

Various encryption algorithms are available to protect the data and information. These are categorised as symmetric key and asymmetric key algorithms

Symmetric key: Symmetric-key algorithms are those algorithms which use the same key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption [7],[8]. Examples are:

- **Data Encryption Standard (DES) :** At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit ciphertext, at the decryption site, it takes a 64-bit ciphertext and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm.
- **Advanced Encryption Standard (AES):** AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits as shown in figure 3. AES operates on a 4×4 column-major order matrix of bytes, known as the state.
- **Blowfish Algorithm:** The block size for Blowfish is 64 bits; messages that aren't a multiple of 64-bits in size have to be padded. It uses a variable –length key, from 32 bits to 448 bits. It is appropriate for applications where the key is not changed frequently. It is considerably faster than most encryption algorithms when executed in 32-bit microprocessors with huge data caches.

Asymmetric key: Asymmetric-key algorithms are those algorithms that use different keys for encryption and decryption. The two keys are: Private Key and Public Key. The Public key is used by the sender for encryption and the private key is used for decryption of data by the receiver. In cloud computing asymmetric-key algorithms are used to generate keys for encryption. [7],[8]. Examples are:

- **Homomorphic encryption:** Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. [25]
- **Diffie-Hellman Key Exchange :** In 1976, Whitfield Diffie and Martin Hellman introduced a key exchange protocol with the use of the discrete logarithm problem. In this protocol sender and receiver will set up a secret key to their symmetric key system, using an insecure channel.[8]
- **RAS Algorithm:** Ronald Rivest, Adi Shamir and Leonard Adleman have invented the RSA algorithm and named after its inventors. RSA uses modular exponential for encryption and decryption. RSA uses two exponents, a and b, where a is public and b is private. The detail is given in the next section.[8]

VI. DATA SECURITY IN CLOUD COMPUTING USING RSA ALGORITHM

RSA Definition: Public key encryption algorithm has been developed by Rivest, Shamir, and Adleman in MIT as Pioneers work. By taking their initial name, this algorithm is called RSA-encryption system. [7],[8]

The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. [5],[7],[8],[20].

The algorithm involves multiplying two large prime numbers and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key.. [5],[7],[8],[20].

The basic steps of RSA algorithm are:
- Key Generation
- Encryption and
- Decryption

RSA Encryption Algorithm:

Let us define some integer parameters 'P' as a plain text, 'C' as an encrypted text, '*e*' as the encryption key, '*d*' as the decryption key, and '*n*' as modulo number. The encryption can be made by following equation. [8], [10]

$$C = P^e \bmod n$$

The following equation is used for decryption

$$P = C^d \bmod n$$

We randomly choose quite large number of two prime factors *p* and q ($p \neq q$). Then modulo '*n*' is defined as $n = p \times q$.

Key generation

The encryption key consists of the pair of integers (*e*, *n*) and the decryption key is (*d*, *n*). Pick two large prime numbers *p* and *q*, *p*. The value of *n* should be quite large, a product of two primes *p* & *q*. Both *p* and *q* should be large.
Next, a relatively large integer *e* is chosen so that *e* is relatively prime to $(p - 1) * (q - 1)$.
Finally, select *d* such that

$$e * d = 1 \bmod (p - 1) * (q - 1)$$

Using *Euler totient function* $\phi(n)$ is the number of positive integers less than n that are relatively prime to *n*. If *p* is prime, then

$$\phi(p) = p - 1$$

If $n = p * q$, where *p* and *q* are both prime, then

$$\phi(n) = \phi(p) * \phi(q) = (p - 1) * (q - 1)$$

The value *e* is selected so that we can easily find its inverse *d*. Because *e* and *d* are inverses mod $\phi(n)$,

$$e * d \equiv 1 \bmod \phi(n)$$

Encryption

For encryption, calculate the cipher text C from plain text P as

$$C = P^e \bmod n$$

Decryption

For decryption, calculate the plain text P from cipher text C as

$$P = C^e \bmod n$$

[20]

Example:

Let's say that your WEB Browser has a piece of data, say number 14 (we'll call it a Plain message and label it as P=14) and it wants to encrypt this Plain message first and then send it to the Server. Upon receipt of this encrypted message, the Server wants to decrypt it to its original value.

Key generation

Before any communication happens, the Server had calculated, in advance, its public (n =33 and k=7) and private (j=3) keys as below:

1. Pick two prime numbers, we'll pick p = 3 and q = 11
2. Calculate $n = p * q = 3 * 11 = 33$
3. Calculate $\phi(n) = (p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 20$
4. Choose a prime number *e*, such that *e* is co-prime to $\phi(n)$, i.e, $\phi(n)$ is not divisible by *e*. We have several choices for *e*: 7, 11, 13, 17, 19 (we cannot use 5, because 20 is divisible by 5). Let's pick $e = 7$
5. So, the numbers $n = 33$ and $e = 7$ become the Server's public key.
6. Now, still done in advance of any transmission, the Server has to calculate it's secret key.
   $(e * d) \bmod \phi(n) = 1$ or $e * d = 1 \pmod{\phi(n)}$
7. $7 * d = 1 \pmod{20}$
8. $(7 * d) / 20 = ?$ with the remainder of 1, So, $7 * d = 21$, and $d = 3$

Encrypting the message

Here is the encryption math that Browser executes:

$C = P^e \bmod n$ After plugging in the values
$C = 14^7 \bmod 33$
105413504 / 33 = 3194348.606
3194348 * 33 = 10541348
C = 105413504 – 10541348 = 20

This is now the value that the Browser is going to send to the Server. When the Server receives this message, it then proceeds to decrypt it.

Decrypting the message

Here is the decryption math the Server executes to recover the original Plain text message which the Browser started with.:

$P = C^d \bmod n$ After plugging in the values
$P = 20^3 \bmod 33$
8000 / 33 = ? with the remainder of P
8000 / 33 = 242.424242
242 * 33 = 7986
P = 8000 – 7986 = 14, which is exactly the Plain text message that the Browser started with.

RSA algorithm uses modular exponentiation operation. For $n = p \times q$, e which is relatively prime to ϕ (n), has exponential inverse in mod *n*. Its exponential inverse *d* can be calculated as the multiplicative inverse of *e* in mod ϕ (*n*).

The premise behind RSA's security is the assumption that factoring a big number (*n* into *p*, and *q*) is hard. And thus it is difficult to determine ϕ (*n*). Without the knowledge of $\phi(n)$, it would be hard to derive *d* based on the knowledge of *e*.

VII. CONCLUSION

In this survey paper, we gave the overview of data storage in cloud computing and the security in cloud system. Here the main idea is to give integrity to the cloud storage area with different data models and security algorithm. We first present the cloud data storage architecture along with the cloud data models. Then we suggest the algorithm for cloud security using RSA algorithm. In this method some important security services including key generation, encryption and decryption are provided in Cloud Computing system. The main goal is to securely store and manage data that is not controlled by the owner of the data. Because the RSA method's security rests on the fact that it is extremely difficult to factor very large numbers. Many values of n have over 200 digits, making the RSA algorithm nearly unbreakable. So it almost solves the problem of security arises in cloud computing.

REFERENCES

[1] Peter Mell. (2011) Timothy Grance 'The NIST Definition of Cloud ', Reports on Computer Systems Technology, sept 2011

[2] Wood K, Pereira E. (Nov.2010) 'An Investigation into CLoud Configuration and Security', 2010 International Conference for Internet Technology and Secured Transactions, 1-6.

[3] http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud.pdf

[4] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security ", VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.

[5] Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA

[6] Leena Khanna, Prof. Anant Jaiswal "Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To overcome Them", International Journal of Advanced Research in Computer Science and Software Engineering 3(3), March - 2013, pp. 279-283.

[7] Atul, Kahate, Cryptography and Network Security, (Second Edition 2008)

[8] William Stallings, ―Cryptography and Network Security Principles and Practices, Prentice Hall, New Delhi.

[9] Rashmi Nigoti, Manoj Jhuria, Dr.Shailendra Singh "A Survey of Cryptographic Algorithms for Cloud Computing "

[10] R.L.Rivest, A.Shamir, and L.Adleman. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems", Communications of the ACM, 21(2), 120- 126, February 1978.

[11] Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. (2009, Feb. 10). Above the clouds: A Berkeley view of cloud computing. EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009-28[Online]

[12] Vikas Goyal, Dr. Chander Kant, International Journal ofEngineering Sciences, ISSN : 2229-6913, September 2011,4, pp. 274-282. "Security Issues for Cloud Computing".

[13] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011

[14] Mladen A. Vouk, "Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[15] Gurpreet Kaur, Manish Mahajan Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms. ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.782-786

[16] Sanjoli Singla & Jasmeet Singh :Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm"

[17] Sandeepraja Batchu, J.N. Chaitanya, Sai sagar.N, Eswar Patnala "A study on Security Issues Associated with Public Clouds in Cloud Computing"

[18] Priyanka Arora, Arun Singh and Himanshu Tiyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, pp. 179-183, 2012.

[19] Behrouz A Forouzan, "Data Communications and etworking", cGraw-Hill, 4th Edition

[20] Charles P. Pfleegger, Shari Lawrence Plfeeger "Security in Computing" Pearson, 4th Edition

[21] Aruna A, Kiruthika P, Suganya N "Reliable Data Uploading and Distribution in the Cyber Space"

[22] Subashini S, Kavitha V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011), vol. 34 Issue 1, January 2011

[23] Sonal Guleria, Dr. Sonia Vatta "TO ENHANCE MULTIMEDIA SECURITY IN CLOUD COMPUTING ENVIRONMENT USING CROSSBREED ALGORITHM"

[24] RSA Data Security, Inc.The RSA Factoring Challenge. http://www.rsa.com/rsalabs/node.asp?id=2092.

[25] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering Volume I, July 4 - 6, 2012, London, U.K. ISBN: 978-988-19251-3-8, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online).