International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# Up in the Air: Cloud Computing Security and RSA Algorithm

**Pooja Bharadwaj[1], Shivani Mankotia[2]**

[1, 2]GGSIPU, Bharati Vidyapeeth"s College of Engineering, Rohtak Road, Paschim Vihar, New Delhi, India

**Abstract:** ***Cloud computing has been the pillar of technology in the past few years, with some rare exceptions of organizations or businesses that have not accepted and/or embraced its power. The scope of this paper includes issues in Cloud Security, including major domains such as Confidentiality, Privacy, Data Integrity, Identity Management and other common aspects. One such focus in this disquisition is one of the possible solutions aiming to strengthen security, viz. Encryption and Decryption, using the RSA Algorithm. After covering various security aspects and issues in the initial segments, using brief and concise explanations, the challenges due to network concept are covered in the subsequent section. Further, the survey covers the recent works and developments or modifications in the RSA algorithm, in other words, its evolution over the recent years. RSA is one of the oldest algorithms for encryption and decryption and consists of basic three steps, Key Generation, Encryption, and Decryption. This is explained in the last section, where the algorithm itself is also presented.***

**Keywords:** security, Cloud Computing, security aspects, security issues, encryption, decryption, RSA Algorithm.

## 1. Introduction

The new phase of computing technology, Cloud Computing, is ubiquitous and convenient, it allows network access to storage, online applications etc., which are shared computing resources.

Amazon's „Amazon Web Service', Microsoft Corp.'s MSFT Azure and Office 365 and Google"s Google Drive are perfect examples of cloud computing services. Companies like Salesforce, Yahoo, Facebook, etc. are also switching many of their services to cloud for their users. The cloud providers or companies provide three different "services" to its users which are [5]:

(i) Infrastructure as a Service (IaaS): It is the most primary service, in this the companies provide "networking features", such as computers (virtual or on dedicated hardware), and space for storing data (e.g. Google Drive and DropBox).

(ii) Platform as a Service (PaaS): In Platforms as a service the company provides hardware and application tools for application development as a service. Hence, a user can develop or run new application. (e.g. Amazon web services Google App Engine and App Cloud of Salesforce.com).

(iii) Software as a Service (SaaS): The end user product or a completed product, is an application which is ready to be utilized by the user. This application is hosted and overseen by the service provider. (E.g. Mail services like Gmail and Hotmail, Google docs, sheets and slides).

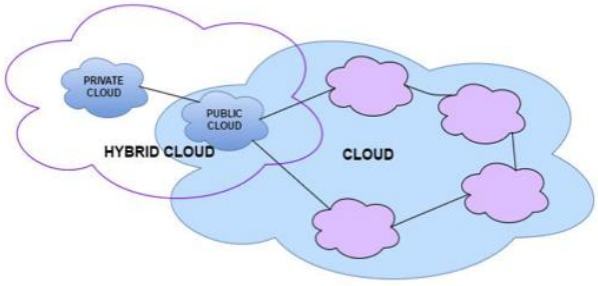


**Figure 1:** Types of Cloud

Clouds within an organization like a company or a university, which provides cloud computing services to its users only, are called Private or Internal clouds. [3].

Public Clouds, also known as external clouds, "in a more traditional sense, is basically the internet" [3]. Service providers use the internet to make resources, such as storage and applications which can include online games, music, picture editing softwares or online file conversion softwares etc., available to the general public.

Hybrid Clouds are the combination of multiple private and/or public clouds [3]. Having different service providers providing divergent private and public cloud services, security in hybrid clouds is weak. Therefore, it is easier to provide security to a public cloud or a private cloud than to a hybrid cloud because they have only one service provider.

### 1.1 Advantages of Could Computing

Popular platforms like Salesforce, Azure, AWS and others have succeeded in gaining an immense user base and wide popularity and acceptability due to the following reasons:

- Flexibility: businesses usually have fluctuating bandwidth demands which can be met efficiently using cloud;
- Disaster Recovery: cloud based backup and recovery is a colossal advantage for small and large companies alike, as

it saves time and is also a cost-effective solution rather than hiring third-party experts for the same;
- Increased Collaboration: Teams coordinating, access and resource sharing are possible easily in cloud, including real-time updates which are visible to everyone;
- No restriction on Location: to work in cloud, the only requirement is an internet connection. With the rapidly increasing development of applications for various platforms, hardware restrictions are also minimized.
- Environment-Friendly: Cloud computing has often been characterized as a form of green computing, moreover, there is a significant reduction in the carbon footprint as the server capacity scales up and down to fit the needs of the user/ organization [1].

Many companies and organizations are moving their database and user applications over to cloud, seeking the above benefits. This transition is accompanied with many security hazards like unauthorized access, malicious modification or denial of services etc. Hence, there is a need to provide security for the data, keeping in mind: Confidentiality, Availability, and Integrity of the data. [6].

In this paper, we'll give the steps of the RSA Algorithm, which is the most widely used Public-Key Algorithm. The rest of this paper is organized in the following manner: section 2, we introduce various security aspects; section 3, we give an overview of security issues. In Section 4, we give the challenges cloud computing faces from network concepts; section 5 discusses data encryption; section 6 discusses about the RSA Algorithm and recent works by various researchers and section 7 concludes the paper.

## 2. Security Aspects

### 2.1 Availability

Availability means that it should be ensured that Cloud Computing Systems can be used/accessed at any time, any place, whenever required by the user who has the correct privileges and authentication credentials. This, in turn, leads to some level of redundancy, but it is crucial to providing availability. For example, major Cloud Computing System providers like Google and Amazon offer the concept of geographic redundancy in their systems, thus hoping to enable higher availability on single providers [4].

### 2.2 Privacy and Confidentiality

Privacy is one of the most important issues in Cloud Computing security, both, in the context of legal compliance as well as user trust.

Confidentiality involves protecting and restricting access to user data in Cloud Systems. There are two basic approaches for achieving confidentiality, viz. physical isolation (storing unencrypted data in a physically isolated form, eg. using a virtual local area network) and cryptography [4].

Following things can be done by designers and developers to increase privacy and confidentiality [4].

a) Minimizing the personal information that is sent to and stored in cloud systems
b) Maximizing user control
c) Specifying and limiting the purpose of data usage to the user
d) Providing and acting on the received feedback

### 2.3 Data Integrity

Integrity, in simple terms, refers to the correctness of information. Ensuring data integrity involves ensuring that information is not lost or modified by unauthorized users. This is a very basic task because cloud computing systems usually provide very large data processing and manipulation capabilities, which make them prone to unauthorized and malicious manipulation, which compromises on integrity [4].

### 2.4 Identity and Access Management

Cloud providers also need to manage identities, which can be efficiently done through a strong and dependable federated identity management architecture and correct internal strategies in organizations [4].

### 2.5 Audit

It refers to being aware of or to watch exactly what is happening in the Cloud System. For instance, many factors like state changes that affect cloud system availability need to be audited and the “complete information about users' applications in the runtime environment should be audited as well” [4]. Also, the “monitoring should not be intrusive and must be limited to what the Cloud provider reasonably needs in order to run their facility” [4].

## 3. Overview of Security Issues

Due to shared resources and pay per use according to user demand, cloud computing faces many threats and problems related to security. Some of them are:

### 3.1 Abuse and Nefarious Use of Cloud Computing

Attackers are able to infiltrate a public cloud to upload spam and malware to a large number of connected client units (computers) and use the features and reach of the cloud infrastructure itself to launch an attack on many other machines.

### 3.2 Lack of Security in Application Programming Interfaces

Extremely secure authentication processes, data encryption, access control, and activity monitoring is required in APIs, as these are what the customers and end users use to interact with the cloud services.

### 3.3 Malicious Insiders

This threat is very important to consider because many cloud service providers don't reveal the process of hiring people

and how they are granted access to assets or the details of their monitoring process. Hence, transparency is an important factor in a secure cloud based organization, "along with compliance reporting and breach notification" [7].

### 3.4 Data Loss/Leakage

This can occur by deletion of data without creating backups, by loss of the key used for encoding and due to unauthorized access, the data stored on cloud is always vulnerable to being lost, manipulated and stolen. This is a major concern in organizations and businesses, as it is a compromise on their reputation and the fact that they are obligated by law to ensure the safety of the data, makes it essential for them to take this issue seriously.

### 3.5 Account and Service Hijacking

This includes phishing, denial-of-service (DoS) attacks, man-in-the-middle attacks, and spam campaigns.

## 4. Cloud Challenges in Network

These threats are listed below:

### 4.1 SQL injection Account and Service Hijacking

"In this type of attack, a malicious code is inserted into a standard SQL code. Thus, the attackers gain unauthorized access to database and are able to access sensitive information" [7].

### 4.2 Cross Site Scripting (XSS)

In this kind of attack, malicious scripts are injected into the Web. There are two methods for inserting the code into the webpage displayed to the user viz. Stored XSS and Reflected XSS.

In a Stored XSS, "the malicious code is permanently stored in a resource managed by the web application" [9]. Whereas, in Reflected XSS, "the attack script is not permanently stored; but is immediately reflected back to the user" [7].

### 4.3 Man in the Middle attacks (MITM)

Here, the intent of the attacker is to listen or snoop in an ongoing transaction between a server and a client and to inject wrong information with the intent of gaining knowledge of the confidential data that is transferred between them.

Examples of tools that implement strong encryption techniques are Ettercap, Airjack etc. which can be used to provide defense against MITM attacks.

### 4.4 Sniffer Attacks

These attacks can be implemented by applications which have the ability to capture the packets flowing in a network and if the transferred data in these packets is not encrypted, it can be read.

"A sniffer program, through the NIC (Network Interface Card), ensures that the data/traffic linked to other systems on the network also gets recorded" [7].

Fig 2 shows an illustration of the security and complexity aspects in Private and Public Clouds [22].

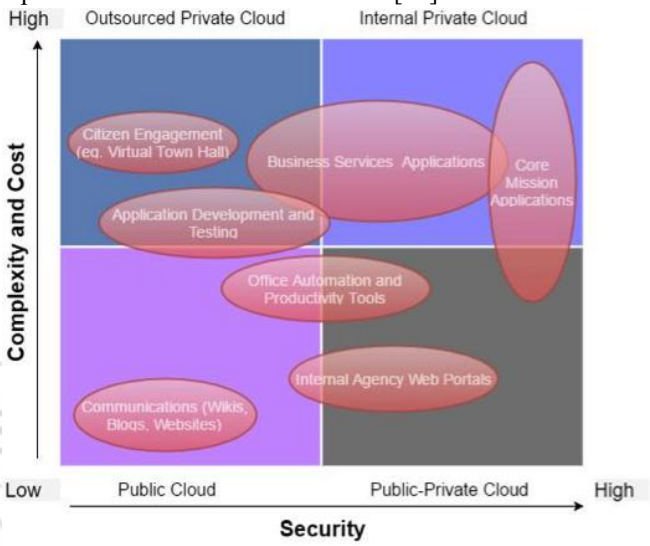


**Figure 2:** Security and Complexity in Private and Public Clouds

## 5. Data Encryption

Encryption and Decryption of data on the cloud, is a major requirement for both sides, the service providers and the cloud users. In other words, before outsourcing the data to a cloud server, encryption is done to convert it into cipher-text using a secret key following which, decryption is done by the user using the same shared private key [10]. The process of extracting the original information that was sent, from encrypted data that was received, is called Decryption.

In encryption algorithms, a stream of data is encrypted and an encryption key is generated. There are two broad classifications of encryption algorithms, viz. Symmetric and Asymmetric.

### 5.1 Symmetric Key Algorithms

When in an algorithms used the same key for both encryption and decryption, they are known as symmetric key algorithms. Hence, the key is kept a secret. An advantage of these algorithms is that they do not consume a large amount of computing power and high speed of encryption is an added bonus [6].

### 5.2 Asymmetric Key Algorithms

Algorithms that generate two different keys for encryption and decryption, are known as asymmetric key algorithms. The two types of keys are: Public and Private.

The sender for encryption generally uses the Public key and the receiver uses the Private Key for decryption of data.

Here, the sender is the cloud service provider and receiver is the user. In cloud computing, these keys i.e. public and private keys, are generated using asymmetric-key algorithms [6].

## 6. RSA Algorithm and Related Work

The recent works, developments and modifications in the RSA algorithm, in other words, its evolution over the recent years are compiled in TABLE I.

**Table 1:** Developments in RSA over the years

| *Author(s)* | *Modifications in RSA* | *Ref.* |
|---|---|---|
| Motasem A. Abu-Dawas, Abdulameer K. Hussain | Elimination of redundant messages occurred in some values of n, the product of two prime numbers, and this is considered as a weak point in the RSA method. The solution depends on appending extra agreement secure information. | [12] |
| Alok Kumar Shukla, V.Kapoor | By using two public keys and n prime number, this modified version will provide security over the network so that attacker cannot get keys and is unable to decrypt the message. | [13] |
| Harsh Chitrala, Dhananjay Pugila, Salpesh Lunawat, P.M.Durai Raj Vincent | "Introduced an algorithm, which is similar to RSA algorithm. With introduction to two values of N: N1 (for encryption) and N2 (for decryption), the value of N1 is determined using four variables, thus difficult to factorize N1. It will become very convoluted to determine the prime numbers from factors, if N1 is deciphered. The time taken for brute-force attack is more compared to RSA algorithm." | [14] |
| Alaa Hussein, Al-Hamami and Ibrahem Abdallah Aldariseh | Apart from private and public key, a third prime number is used in constitution with basic two keys, this resulted in an increase in the factoring complexity of variable (n). | [15] |
| Aayush Chhabra and Srushti Mathur | There is transfer of big prime numbers and the need of transfer of „n", that is, product of two random numbers is eliminated. | [16] |
| Wang Rui, Chen Ju, Duan Guangwen | "They combined the idea of RSA algorithm and the $k^{th}$ power residue theory to construct a k-RSA algorithm. Designed for improved security and achieve a balance between speed and space. Also realize following functions simultaneously: hierarchical system management, secret sharing etc." | [17] |
| Shilpi Gupta and Jaya Sharma | "They combined the two most important algorithms, RSA and Diffie-Hellman. Diffie Hallman algorithm is used for key exchange method that allows two parties that have no proper knowledge to each other to jointly share a secret key. RSA keys are taken as input for Diffie Hellman. The required keys are generated " | [18] |
| Vishal Garg and Rishu | "For better security to email services and to other web services." More secure codes added to current Diffie-Hellman encryption algorithm | [19] |
| Gaurav Shrivastava | RSA Algorithm combined with Triple DES, resulting in providing 504-bit key length. This results in enhancing the security level along with an increase in file size, which is the major drawback in this scheme. | [20] |
| Khushdeep Kaur, Er. Seema | Combination of DSA, RSA and MD5 algorithm for a hybrid link for wireless devices. It provides "better response time, less network delay and best throughput, efficient routing of packet with much less load on servers." | [21] |

## 7. The Algorithm

Ronald Rivest, Adi Shamir and Leonard Adleman, invented an asymmetric key algorithm and named it after themselves, called RSA Algorithm. This algorithm uses two exponents, a and b, where ‚a' acts as public key and ‚b' acts as private key. As the name suggests, the "Public Key" is known to all whereas the "Private Key" is known only to whom the data rightfully belongs. Therefore, the Cloud Service Provider does encryption through public key and decryption is done by the Cloud-User using its private key [11].

### 7.1 Key Generation

1. The first step involves selecting two distinct prime numbers randomly and of similar bit length. Let the prime numbers be „a" and „b".
2. Calculating the value of „n" by taking the product of „a" and „b" i.e. n = a * b.
3. Calculating value of „Ø(n)" function, by Ø(n)= (a-1) * (b-1).
4. The next step involves selecting an integer „e", which is the Public-key exponent, such that 1 < e < Ø(n) and greatest common divisor of „e", Ø(n) is 1.
5. Calculating value of „d", which is the multiplicative inverse of „e mod Ø(n)" by d = e-1(mod Ø(n)).
6. Private-Key component is „d", such that, d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent „e" i.e., (e, n).

The Private-Key consists of modulus n and the private exponent „d", and this must be kept a secret i.e., (d, n).

### 7.2 Encryption:

When public key is used for converting Plain Text into Cipher Text, it is called Encryption. Data is encrypted and the resultant cipher-text (data) C is

The Cloud service provider stores this converted text or encrypted data.

### 7.3 Decryption

The opposite of Encryption is called Decryption. The user makes a request to its cloud service provider for the data. The cloud service provider verifies the authenticity of the user. After verifying the authenticity it gives the encrypted data i.e. „C" to the user. The Cloud user then can decrypt the data through its private key,

$$m = C^d \pmod{n}.$$

## 8. Conclusion

Cloud Computing is relatively new but has made an impact, its versatility has gained it many followers, but its rampant growth has made it vulnerable to security threats. Once the data is shifted to cloud, the user loses the hold over the data. Hence, it is essential for users as well as service providers to stay alert wherever the security of sensitive data is concerned and there are many ways to do that. Cryptography plays an important role in cloud security. RSA is one of the cryptographic algorithms, which works on the principle of generation of Public and Private keys. In this paper, the existing works by different authors on RSA algorithm have been surveyed. All the techniques have been studied and analyzed that enhance the performance and security of algorithm.

## References

[1] Salesforce Uk. "Why Move To The Cloud? 10 Benefits Of Cloud Computing." Salesforce UK Blog. Web. 21 Mar. 016.
[2] Hashizume, G. Rosado, Fernández-Medina and B. Fernandez "An analysis of security issues for cloud computing." Journal of Internet Services and Applications 27 Feb. 2013 4:5.
[3] M.G. Jaatun, G. Zhao, and C. Rong "Strengthen Cloud Computing Security with Federal Identity Management U." CouldCom 2009, LNCS 5931, pp. 167-177 Springer-Verlag Berlin Heidelberg 2009.
[4] Jeng-Shyang Pan, Shyi-Ming Chen, Ngoc Thanh Nguyen, "Intelligent Information and Database Systems." 4th Asian Conference, ACIIDS 2012, Kaohsiung, Taiwan, March 19-21, 2012, Proceedings, Part I.
[5] Amazon Web Services, Inc. "Types of Cloud Computing." Amazon Web Services, Inc.
[6] Shakeeba S. Khan and R.R. Tuteja "Security in Cloud Computing Using Cryptographic Algorithms." IJIRCCE, Vol. 3(1), pp. 148-154 January 2015.
[7] Vahid Ashktorab and Seyed Reza Taghizadeh, "Security Threats and Countermeasures in Cloud Computing", IJAIEM, Volume 1(2), pp. 234-245, October 2012.
[8] Kevin Day, "Understanding Encryption and Password Protection" Attach Plus, LLC, pp. 1-3, 2009.
[9] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, "Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis", Proceedings of the Network and Distributed System.
[10] Prakash G L,Dr. Manish Prateek and Dr. Inder Singh "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", IJECS, vol. 3(4), pp. 5215-5223, April 2014.
[11] Parsi kalpana and Sudha Singaraju, " Data Security in Cloud Computing using RSA Algorithm", IJRCCT , vol. 1(4), 29 Sept. 2012.
[12] Motasem A. Abu-Dawas & Abdulameer K. Hussain, "Enhancement of RSA Scheme using Agreement Secure Information for Nearest Parameters" International Journal of Computer and Information Technology , vol. 4 ,pp. 194-196 ,March 2015.
[13] Alok Kumar Shukla & V.Kapoor, "Data Encryption and Decryption using Modified RSA Cryptography Based on Multiple Public Keys and „n" Prime Number ", International Journal of Engineering Sciences & Research Technology , vol. 3(6), pp. 713-720, June 2014.
[14] Pugila, Dhananjay, Harsh Chitrala, Salpesh Lunawat, and PM Durai Raj Vincent. "AN EFFICEIENT ENCRPYTION ALGORITHM BASED ON PUBLIC KEY CRYPTOGRAPHY." International Journal of Engineering and Technology, June-July 2013.
[15] Al-Hamami, A. H., & Aldariseh, I. A. (2012, November). Enhanced Method for RSA Cryptosystem Algorithm. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp. 402-408). IEEE.
[16] Chhabra, A., & Mathur, S. (2011, October). "Modified RSA Algorithm: A Secure Approach. In Computational Intelligence and Communication Networks (CICN), 2011 International Conference on (pp. 545-548). IEEE.
[17] Wang Rui; Chen Ju; Duan Guangwen, "A k-RSA algorithm," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, vol., no., pp.21,24, 27-29, May 2011.
[18] Gupta, S., & Sharma, J., "A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman".
[19] Garg, V., & Rishu, R.,"Improved Diffie-Hellman Algorithm for Network Security Enhancement.", International Journal of Computer Technology and Applications, vol. 3(4), pp. 1327-1331, July-August 2012.
[20] Garg, V., & Rishu, R. (2012). Improved Diffie-Hellman Algorithm for Network Security Enhancement. International Journal of Computer Technology and Applications, vol. 4(7), pp. 465-170, 2011.
[21] Kaur, Khushdeep, and Er Seema. "Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices." International Journal of Engineering Research and Applications (IJERA), vol. 2, pp. 914-917, October 2012.
[22] K.S.Suresh & K.V.Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2(10), pp. 110-114, October 2012.

## Author Profile

**Pooja Bharadwaj** is currently pursuing B. Tech in Information Technology from Guru Gobind Singh Indraprastha University, batch of 2013-17.

**Shivani Mankotia** is currently pursuing B. Tech in Information Technology from Guru Gobind Singh Indraprastha University, batch of 2013-17.