IJCSE International Journal of Computer- Science and Engineering Open Access
Research Paper Volume-2, Issue-3 E-ISSN: 2347-2693

Enhance Security Issues Using Data Cipher Algorithm In Cloud

Jaswinder Singh[1] and Runa Rana[2*]

[1]*Departmen of Computer Science & Engineering, SRM University, India, waliajaswin@gmail.com*
[2*]*Department of Computer Science & Engineering, SRM University, India,runach91@gmail.com*

www.ijcseonline.org

Received; 9 March 2014 Revised: 14 March 2014 Accepted: 26 March 2014 Published: 31 March 2014

Abstract— Cloud Computing is a internet based computing that facilities hardware, network and software resources and provide flexible infrastructure on demand as pay per usage. The benefits of cloud computing is due to its reduced cost, resource sharing and performance. Cloud is based on the difficulty of securing storage data and maintain privacy. The security is the only problem in the cloud .Security is not provided in the cloud ,many companies have their own unique security structure Though , Amazon has its own security structures. The data placed in the cloud is accessible to everyone . To overcome this difficulty ,we have proposed RSA algorithm between cloud service provider and the user. The aim of our proposed work is to enhance security issues and maintain privacy.

Key Words— RSA Algorithm, Cloud Computing, Encryption , Decryption, Public Key, Private key ,Security Attributes

I. INTRODUCTION

Cloud computing is the hottest topic for both research and industry.It is basically a virtual pool of resources and it provides these resources to users through internet.Cloud computing is the key driving force in many small, medium and large size companies and as many cloud users seek the services of cloud computing the major concern is the security of their data in the cloud[5].

Cloud computing can deploy,allocate or reallocate computing resources dynamically and monitor the usage of resources at all times [3][6].The problem associated with cloud computing is data privacy ,security , anonymity and reliability. But the most important between them is security and how cloud providers assures it[6].According to IEEE cloud computing define as "A large scale distributed computing paradigm that is driven by economies of scale , in which a pool of abstracted , virtualized , dynamically-scalable, managed computing power ,storage, platforms , and services are delivered on demand to external customers over the Internet.[4]"

CHARACTERISTICS OF CLOUD COMPUTING

- On demand self service - Cloud computing obtain computing capabilities like usage of various servers , network and data storage[1][6].
- Broad network access - The services are delivered across the network and allow customer to access through the hetrogenous system(PC, mobile phones and PDA)[1].
- Resource Pooling - The resources are pooled together and shared by multiple consumers. Example. Storage, processing, memory, network,bandwidth and virtual machine[1] .
- Rapid elasticity – Whenever we need resources then we scale up and released them into scale down[6].
- Measured service – It measure the usage of resources to each individual metering capability is provided.

CLOUD SERVICE MODELS

- Infrastructure as a Service(IaaS) - This is the lowest layer in the service model .It is used to access essential IT resources such as data storage, hardware resources , and network access etc[6].
  Example. AmazonEC2, Rackspace
- Platform as a Service(PaaS) - It provide environment for developing and deploying cloud applications .The user of this layer are developer seeking to develop and run a cloud application for a particular platform[6].
  Example. GoogleApps Engine, Saleforce.com
- Software as a Service(SaaS) - SaaS provide complete applications to a cloud's end user.It is mainly accessed through a web portal and service oriented architecture based on web service technologies[6].
  Example. Google Apps , MS Office 365

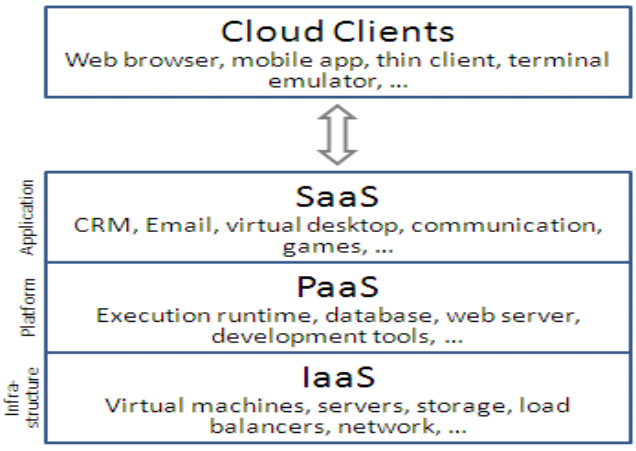

Figure.1.1 Cloud Service Models [10]

Corresponding Author: *Runa Rana*

CLOUD DEPLOYMENT MODELS

- Public Cloud - The cloud infrastructure is open for general public or a large industry group and can be owned by an organization by acquiring cloud services.
- Private Cloud - The cloud is open for a specific organization .It may be managed by the organization itself or by third party.
- Community Cloud – The cloud infrastructure is managed by several organization .It may be managed by third party or the organization itself.
- Hybrid Cloud – The cloud infrastructure is a combination of more than one cloud (private, public or community) which always remain single entity.

II. SECURITY ISSUES

1) Confidentiality:-

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network[4]. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored[1]. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Confidentiality is necessary for maintaining the privacy of the people whose personal information is held in the system.

2) Integrity:-

Data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.This means that data cannot be modified in an unauthorized or undetected manner[1].

3) Availability:-

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly[1][6].

4) Authenticity:-

In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by some one possessing the proper signing key[1].

5) Non-repudiation:-

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction[4][1].

III. RSA ALGORITHM

RSA stands for Ron Rivest, Adi Shamir and Len Adleman was described in 1977. RSA is most widely used public –key cryptography for security and privacy.Our proposed work plan is based on RSA algorithm for encryption and decryption[2].

The RSA algorithm is used to encrypt the data that provides security, so that only the concerned user can access it . By security the data , we are not allowing unauthorized parties to access data. Initially the user encrypt the data and stores in the cloud . When required , user places a request then cloud provider for the data , cloud provider authenticates the user , if it is valid then delivers the data to the user.Thus encryption is done by the cloud service provider and decryption done by the user. Once the data is encrypted with the public key then it can be decrypted with the corresponding private key. In Cloud sender act as a cloud service provider and receiver act as a user.

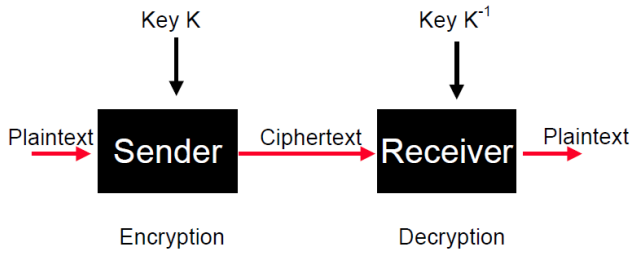

Figure.1.2 shows RSA algorithm process[10]

IV. PROPOSED METHODLOGY

The aim of RSA algorithm for securing storage data and maintain privacy. Every message in block cipher is mapped to an integer with the help of digital signature technique[9]. RSA consists of both public and private key.In cloud environment public key is known to everyone where private key is known only to the user who originally owns the data[3].

RSA algorithms has three main steps-

1. Key Generation
2. Encryption
3. Decryption

Key Generation – It is the initial step of the algorithm.Key generation is done between the cloud service provider and the user[8][3].

STEPS-

1) Choose two distinct non- composite prime integer numbers p and q.
2) Compute n = p *q
3) Compute Euler's totient function Q(n)=(p-1)*(q-1)
4) Choose an integer e such that 1<e<Q(n) and greatest common divisor of e , Q(n) is 1.
   Gcd(e,Q(n)) = 1.
5) Compute d , d*e = 1modQ(n).
   d= e^{-1}(mod Q(n)).
6) The public key consists (e, n).
7) The private key consists (d, n).

Encryption -
It converts plaintext (m)into ciphertext(c).
$c = m^e \pmod n$.

Decryption -
It converts ciphertext (c)into plaintext(m).
$m = c^d \pmod n$.

V. RESULTS

Key Generation:
The original message m = 25.
1.We have choosen two distinct integers p = 11and q = 3.
2.Compute n = p *q thus , n = 11*3 = 33.
3. Compute Q(n) =(p-1)*(q-1) thus ,Q(n)=(11-1)*(3-1)= 20.
4.Choose integer e is 3 such that 1<e<Q(n) and gcd(3,20)=1.
5.Compute d*e = 1(modQ(n)).
Thus , d*e (mod Q(n)) = 1.
7*3(mod 20) = 1 => 21 (mod20)= 1.
6.The public key (e,n) = (3,33).
7. The private key (d,n) = (7,33).

Encryption:
$c = m^e \pmod n$
$c = (25)^3 \pmod{33}$
= 16.

Decryption:
$m = c^d \pmod n$
$m = (16)^7 \pmod{33}$
= 25.

Message(m)	Integer p and q	N	Q(n)	E	d	c	M
25	11,13	33	20	3	7	16	25
10	17,3	51	32	11	3	37	10
5	17,11	187	160	7	23	146	5
20	19,13	247	216	7	31	58	20

Table1.1 shows result of RSA algorithm

VI. CONCLUSION AND FUTURE WORK

In this research , we focus on the security and privacy issues of the cloud computing.The cloud computing is an internet based computing that share resources such as hardware , software and network and provide flexible infrastructure on demand of the user.Throughout this paper, we focus on the security attributes(such as confidentiality,integrity and availablity) that is responsible for maintain privacy between cloud service provider and the user [9].The RSA algorithm provides more security and reliability for data encryption and decryption on the cloud.Though ,RSA is an efficient algorithm for internet based computing[7][3].

The future work of our research based on security algorithms that enhance security issues.Some other powerful algorithms that work for same security issues (such as AES ,DSA algorithm).These algorithms may also increase the performance and security in cloud computing environment[6].

VII. REFERENCES

[1] Shaheen Ayyub and Devshree Roy,"Cloud Computing Characteristics and Security Issues ", International Journal Of Computer Sciences and Engineering,Volume-1,Issue-4,Page no- 18-22, Dec 2013.
[2] Manpreet Kaur and Rajbir Singh,"Implementing Encryption Algorithm to Enhance data Security of Cloud in Cloud Computing ", International Journal of Computer Applications,Volume-17,Issue-18, ISSN-0975-8887, May 2013.
[3] Parsi Kalpana,"Data Security in Cloud Computing Using RSA Algorithm" , International Journal of Research in Computer and Communication Technology ,ISSN 2278-5841,Volume-1, Issue- 4,Page no-143-146, September 2012.
[4] Zhifeng Xiao and Yang Xiao, "Security And Privacy in Cloud Computing " ,IEEE, Volume-15, Issue-2, Page no – 843-858. Second Quarter 2013.
[5] Mandeep Kaur and Manish Mahajan, " Using Encryption Algorithms to Enhance the Data Security in Cloud Computing", International Journal of Communication and Computer Technologies,Volume-1, Issue- 12, Page no-56-59,January 2013.
[6] Rajesh Piplode and Umesh Kumar Singh ,"An Overview and Study of Security Issues & Challenges in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering , Volume-2, Issue-9 , Page no- 115-120, September 2012.
[7] Mamta Devi ,"Security and Privacy Concerns in Cloud Computing", International Journal of Research Review in Engineering Science and Technology, Volume-1, Issue-2, Page no -109-117 , September 2012.
[8] William Stallings, "Network Security Essentials Applications and Standards", Pearson Education , Third Edition ,2007.

[9] Atul Kahate "Cryptography and Network Security " , Tata MC Graw-Hill Education , Second Edition Page no -320-321 ,2010.
[10] www.google.com.

AUTHORS PROFILE

Ms. Runa Rana has completed her M.Tech Degree in Computer Science & Engineering from SRM University Delhi NCR Campus Modinagar , Ghaziabad.

Mr. Jaswinder Singh has completed his M.Tech degree in Computer Science & Engineering from Punjab Technical University, Punjab. He is working as Assistant Professor in SRM University Delhi NCR Campus Modinagar, Ghaziabad.

