Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques

Vinay kumar pant
M.Tech. (CSE)
Subharti Institute of Technology and Engineering Meerut, India
vnpant51@gmail.com

Jyoti Prakash
M.Tech. (CSE)
Subharti Institute of Technology and Engineering Meerut, India
jyotiprakashsrm@gmail.com

Amit Asthana
Assistant Professor (CSE)
Subharti Institute of Technology and Engineering Meerut, India
amitasthana80@gmail.com

ABSTRACT

Cloud computing is based on network and computer applications. In cloud data sharing is an important activity. Small, medium, and big organization are use cloud to store their data in minimum rental cost. In present cloud proof their importance in term of resource and network sharing, application sharing and data storage utility. Hence, most of customers want to use cloud facilities and services. So the security is most essential part of customer's point of view as well as vendors. There are several issues that need to be attention with respect to service of data, security or privacy of data and management of data. The security of stored data and information is one of the most crucial problem in cloud computing. Using good protection techniques of access control we can resolved many security problems. Accept that managing privacy and security of information in web highly challenging. This paper describes how to secure data and information in cloud environment in time of data sharing or storing by using our proposed cryptography and steganography technique.

Keywords: cloud computing, data security, RSA, Steganography, Decryption, Encryption.

I. INDRODUCTION

Cloud computing is the idea of moving the localized computer programs, data and processing to an Internet server for easier and more secure access. Cloud computing consider as a next generation technology that revolutionized the IT industry [4]. Cloud computing provides huge infrastructure to perform tasks and store data. The cloud customer does not want to work with single cloud provider due to compatibility issue, service availability issue and sometime insider problem. So they are use multiple cloud services according their need. User of cloud transfer their applications and data to the cloud environment, so it is necessary that the security method provided in the cloud are better than traditional methods. Unauthorized access of data, network and application by an unauthorized person (hacker) are cause lack of security and protection for cloud environment, which effects productivity and growth of the organization [1]. To determine the level of risk durability and concentrate on reducing the risks is the one of the most important part of cloud that cannot be neglected by the cloud service provider. Cloud computing have some important feature that overcome the feature of traditional services and prove the importance in growth of IT industry.

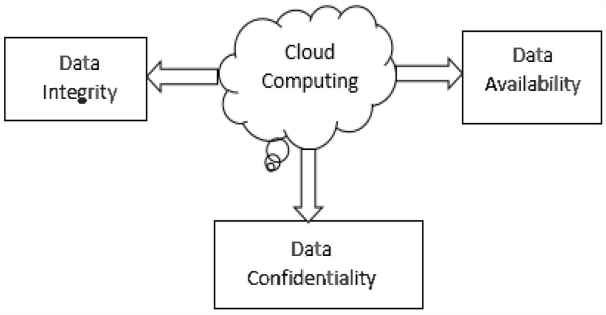

Fig.1. Three Main Feature of Cloud

A. Data Integrity

Data integrity assure that the information is absolute and valid. Integrity include controlling the network device and data from the unauthorized access or maintain them strictly. It also contains some feature like atomicity, durability, isolation and consistency [1]. Cloud service provider should ensure about data integrity and provide trust to the user for their data privacy or security.

B. Data Availability

Availability define as all the data and information are continually available at a required level that are requested by customer. So we can say that all machines have to stored data and application and deliver or process information when the user need them. Cloud venders are use authentic back up system to store and save the customer data, for security of data they use proxy server and according to the users need they deliver data over the network (web) [1, 2]. The storage area network (SAN) and network-attached storage (NAS) are two popular approaches to providing data availability. Data availability can be measured how often the data is available and how much data can flow at a time.

C. Data Confidentiality

Basically data confidentiality refers to a set of rules that limits access of information or data and keep confidential from outsider [2]. In cloud, the service provider that provide service

978-1-4673-7910-6/15/$31.00 ©2015 IEEE

and store data of customer are basically responsible for data confidentiality. Disclosure of data are cause of damage, loss and theft by unauthorized person. So provider and user both are follow different level of confidentiality like SLA (service level agreement), data portability, backup and traceability. At present we are using many data protection or confidentiality methods like data encryption, password protection and biometric verification.

II. CLOUD DATA SECURITY CONSIDERATIONS

Cloud computing face main problems today most popular is confidentiality and integrity of data. Cloud user store their data in multiple storage devices that are provided by cloud venders. But problem is that user doesn't know the location where the data are store and doesn't have the control on that. Some of the security issues are following:

1. Data Acquisition

Data acquisition is a method or technique that help to acquire data from different hardware. Cloud user and service provider should know about, how and where are we access the data for that they know the data stream and Peer to Peer operations [1].

2. Confidentiality

Data confidentiality is important for customers to gather their personal or confidential data in the cloud. On cloud it is one of the major issue. Data on cloud is stored at the remote locations and provider used cloud infrastructure for keeping the data, like VM machine (image), backups and monitoring logs or servers [1, 7]. Customer uses the shared storage to share the data and application. So sometime confidentiality problem arise due to attack, malicious activity and system failure. Therefore we need good security methods and technique to secure, unsecured storage or transmission of sensitive data.

3. Integrity and Authenticity

This is one another problem with cloud security. Data integrity means securing data from unauthorized deletion, fabrication or modification. Data integrity is easy in standalone system and database, but in case of cloud it is difficult because cloud services serve with multiple databases, applications, servers and networks [2, 4]. Authenticity indicate the process of controlling access of data and information. Only those user access the data that are authorized by the provider. Cloud is open source of information so some time many user face the problem of authorization and data access.

4. Multi-tenancy

Multi-tenancy define as where cloud systems shared computational resources, Storage, network and services. It is a cost saving and provide better utilization of resources. But harmful for the confidentiality of data due to shared resources. Many malicious activity destroy the servers and network resources so controlling the data or information flow (leakage) are difficult. Virtual machine attack is one of another problem with multi-tenancy.

5. Multi-tenancy

Enhancement of technology and use of internet provide a lot of facility to people. But it also increase many security problem, cyber-attack is one of them. Cyber-attacks use malicious code to change computer code or data, resulting in harmful effects that can compromise data and lead to cybercrimes, such as information and identity theft. Some major attack are Identity theft, malware, phishing, spoofing, Trojans and viruses, password sniffing, Denial-of-service (DOS) and distributed denial-of-service (DDOS) attacks [3].

III. METHODS USE FOR SECURITY OF DATA

Many security methods and technique are used to secure data and information. We describe some methods here are following-

1. Cryptography [11]

The Cryptography is a method of protecting information and transmitting data into an unreadable format. We use encryption to change readable text (called plain text) into an unreadable secret format (called cipher text). So we say that it is a technique of secrete writing. Only those people who encrypt the data and know the decrypt key are get the data or information in readable form (plan text). Cryptography play major role to secure ATM transmission, E-commerce, digital media privacy and web data transmission or storage. Modern cryptography work for four major concerns these are non-repudiation, integrity, authentication and confidentiality. Cryptography basically is the technique of encrypting and decrypting of data.

1.1. Encryption and Decryption [10]

Encryption is the process to converting data or information (plaintext) into another form, called cipher text, which cannot be easily understood by anyone except authorized parson. Decryption is the process to converting cipher text back into plaintext. The main purpose of encryption is to secure the confidentiality of digital data stored on computer systems or transmitted via other computer on network (internet). In process of encryption and decryption we generate a key to time of data encryption and use same or different key to decrypt the data.

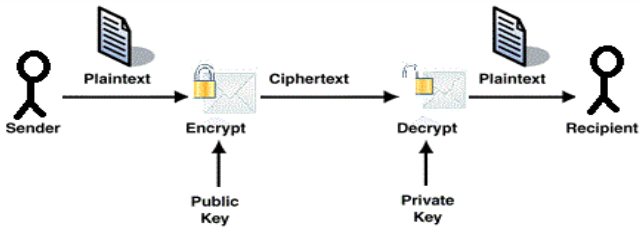

Fig.2. Simple Representation of Data Encryption and Decryption

2. Steganography

Steganography is the technique or art of hidden writing. In process of steganography we hiding a secret message within an ordinary message (Image, Video and Audio) and the extract message at its destination [11, 12]. We basically study three categories of steganography, secret key steganography, public key steganography and pure steganography. Its advantage over the cryptography is that the earmarked secret message does not attract attention of third party. So storing and sending data on web is very secure using this technique.

IV. Proposed Security Model for Cloud Data

In this paper we proposed three step data security model to secure cloud data. In first level we use cryptography using RSA algorithm, second level we use steganography technique where we hide our data within the image and third level we access the data from image and decrypted data using RSA algorithm. Here we use this method only for image data hiding but this also apply for video, text or audio.

1. First Step of Security

Here we using cryptography technique to secure our data to unauthorized access and the secure movement of data on the web. Before the using algorithm we need to understand, what is RSA? And why we are using RSA?

1.1. RSA Algorithm [5,7 9, 11]

RSA stands for 'Rivest-Shamir-Adleman' algorithm. RSA algorithm described firstly in 1977. It is an asymmetric cryptography algorithm that use to data encryption and decryption. In this algorithm user create two key, public key and private key. The public key can be shared with everyone, whereas the private key must be kept secret. RSA helps organizations solve their most complex and sensitive security challenges, preventing online fraud, defending against advanced threats or attack and safe access of mobile data. RSA is one of the ancient and widely used public key cryptographic systems. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography.

1.2. Algorithm for Generate RSA Key

In RSA algorithm we use two type of key public and private. Public key known by everyone and use to encrypt the massage (data) [6]. This encrypted massage decrypted by only using private key that is generated by user. Let n, e and d be integer number, then (e, n) and (d, n) respectively encryption key (exponent) and decryption key (exponent).

- Select two random prime numbers p and q.
- Compute modulus (n) = p*q. (multiplying to prime number p and q)
- Calculate totient of n, phi (n) = (p-1) (q-1).
- Select the integer e, such that 1< e < phi (n), where gcd (e, phi (n)) =1.
- Compute d, 1 < d < phi (n), such that de ≡ 1 (mod phi (n)) or $d = e^{-1}$ (mod phi (n)).
- Now we found encryption key (public key (e, n)) and decryption key (private key (d, n)).

1.3. Algorithm for Data Encryption [11]

After generating public key and private key we will encrypt our data in form of cipher text. Let we represent cipher text by C and plain text (Message) by M. So we use following step-

- Get the public key (e, n).
- Select the message as an integer M, such that 0< M< n.
- Calculate the cipher text C, such that $C = M^e \bmod n$.
- Get the C and send to receiver as a secrete message.

2. Second Step of Security

In the second step of security we are using image data hiding technique of steganography. In this technique we take an image of any format basically jpeg, bmp and gif. Here we perform some step to secure data (message) as following-

- First we get the cipher text which is an unreadable form of message (data) converted by using RSA algorithm encryption technique.
- Take an image. (here we taken an image(m.bmp) shown Fig.3.0)
- Now we use steganography tool (StegoTools (rRMS)) to hide data in image.
- Select the image and input your secrete data (ASCII Input box). (shown in Fig.3.1)
- Generate encryption key (e.g.-'12345') to read data from the image. (shown in Fig.3.1)
- Save the image. (shown in Fig.3.2)

Fig 3.0. Original Image (m.bmp)

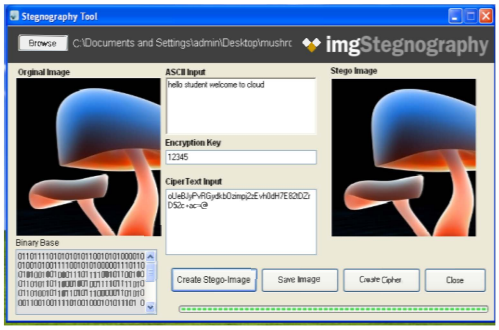

Fig 3.1. Gererating Encryption Key and Stegano Image

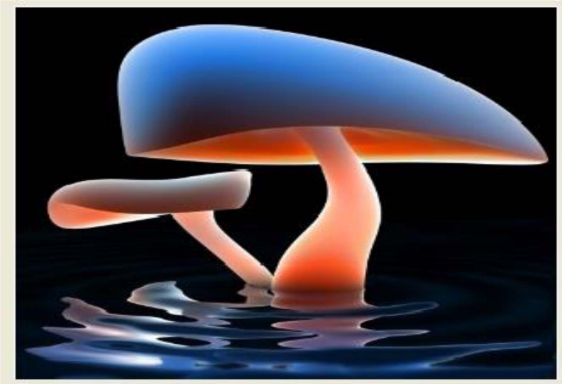

Fig 3.2. Encrypted Image (e.bmp)

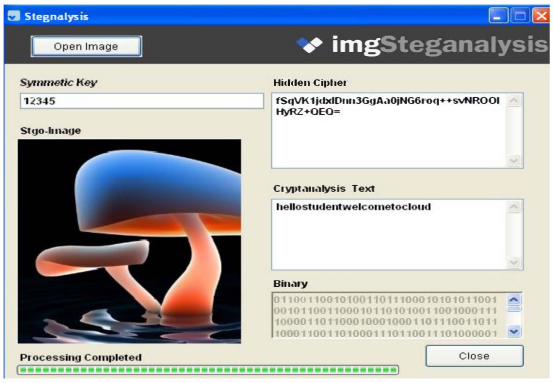

Fig 3.3. Extract data from image using Symmentic key

3. Third Step of Security

After generating stegano-image (encrypted image) we send this image to receiver. Only receiver know about the image containing the data or message. After that he read image and use symmentic key (encryption key) to get data from the image. To show this process we use steganography tool (StegoTools (rRMS)). This process is known as steganalysis. Some steps are follows-

- Get the encrypted image. (shown in Fig.3.2)
- Use steganography tool (StegoTools (rRMS)) to read the image. (shown in Fig.3.3)
- To get the encrypted message we need key (symmentic key (e.g.-'12345')) which we created at the time of image steganography.

3.1. Algorithm for data decryption [9,11]

Now we found the data or message which we hide in the image. This is a cipher text ('C') which we put on an image to secure from third party or hacker. Now we need to get actual text or plain text which is encrypted by RSA algorithm. To get actual message we use data decryption method. So follow the following step-

- Get the cipher text ('C').
- Use the decryption key 'd' which is generated at the time of key generation.
- Calculate the original message 'M' such that $M = C^d \bmod n$.

Now we get our actual message or original text. So these three step of security are very reliable to secure data from the outsider or hacker.

V. Future Work

Data security is a most important issue of cloud computing and IT industry. In this paper we use some technique to secure data in cloud or internet. I hope this work help to secure data form outsider or hacker, who destroy the important data. In future I want to work to improve the working of these algorithm in term of robustness or hiding capacity and use other secure algorithm or method to protect information (data) on cloud.

VI. Conclusion

Modern area of information technology are fully based on online service or web services. This paper discussed security problems in cloud computing systems and how they can be prevented, here we use cryptography and steganography method together to secure data. RSA algorithm is more secure than other algorithm. We integrate RSA algorithm with other algorithm to provide more security to data. In steganography process we get encrypted image, which looks exactly the same to original image by human eye. If we analysis the image binary codes then the differences would be seen. Otherwise we are unable to identify the original image. The approach we have use in this paper, will help to make a strong structure for security of data in cloud computing field or web.

References

[1] G. Dr. Mohammad V. Malakooti and Nilofar Mansourzadeh, "A Two Level-Security Model for Cloud Computing based on the Biometric Features and Multi-Level Encryption", The Proceedings of the International Conference on Digital Information Processing, Data Mining, and Wireless Communications, Dubai, UAE, 2015.

[2] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc.

[3] 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, Issue 10, 2012.

[4] Vinay Kumar Pant, Mr. Anshuman Saurabh, "Cloud Security Issues, Challenges And Their Optimal Solutions" International Journal of Engineering Research & Management Technology, ISSN: 2348-4039, Volume 2, Issue-3, May- 2015.

[5] M.Kaur, M.Mahajan," Implementing various encryption algorithms to enhance the data security of cloud in cloud computing", VSRD International Journal of Computer Science & Information Technology, Vol. 2 No. 10, October 2012.

[6] P.Kalpana, S.Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[7] M.Marwaha, R.Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, P. 367-370, January 2013.

[8] E.Gorelik, "Cloud Computing Models", Massachusetts Institute of Technology, January 2013.

[9] Amandeep Kaur, Sarpreet Singh, "An Efficient data storage security algorithm using RSA Algorithm", International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 – 4847, Volume 2, Issue 3, March 2013.

[10] Ms. Shubhra Saggar, Dr. R.K. Datta, "An improved RSA Encryption Algorithm for Cloud Computing Environments: Two key Generation Encryption (2KGEA)", International Journal of Software and Web Sciences 5(2), ISSN: 2279-0063, pp. 127-131, June-August, 2013.

[11] William Stalling, "Cryptography and Network Security-Principles and Practices", Third Edition, publication-Pearson.

[12] Rajeev Kumar, "DATA HIDING IMAGES USING SPREAD SPECTRUM IN CLOUD COMPUTING", International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 1, Issue 3, PP. 76-79, july-August 2013.

[13] Rashmi , Dr.G.Sahoo, Dr.S.Mehfuz, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, August 2013.