International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Review Paper on Cloud Security using Stegnography and Cryptography

Sukhjeet Kaur[1] ,Dr. Deepak kumar[2]

[1][M.Phil Scholar],[2] [Professor in Computer Application]

Guru Kashi University, Talwandi Sabo, (India)

ABSTRACT

Cloud computing is potential technology in the world. It used to store huge quantity of data and capable to access these data anywhere on demand. There are many cloud service providers that provide the cloud service to users. Cloud service providers like Google, Amazon, IBM, Microsoft, etc. security is the biggest alarm about cloud computing. There is also an option for the attacker to take the information in cloud from legal user. Security issues such as confidentiality, integrity, control and so on. To solve the problem of security in cloud computing, we are going to arrange these two combined techniques for preventing security breaches on cloud computing. Two combined techniques are cryptography and steganography. Cryptography changes the data in coded format. Steganography complete hide its existence from the users, not including the proposed receiver. In this paper, a technique is used combined approach cryptography and steganography because it will provide two way security to the data being transmitted. First, changes the data in coded form through the use of encryption algorithm (AES, DES) then coded form convert into images through the use of steganography. The encryption for the data is performed to provide the extra security layer for the client for data migration. An Enhanced LSB Approach is used to hide the text data into the image which is then finally migrate to the cloud. Each technique have different parameters like quality, payload and time. This paper present study the existing techniques like AES, DES and evaluate ELSB technique based performance metrics like payload and time with existing system.

Keywords—Cloud Security, Cloud Computing, Stegnography, Cryptography.

I. INTRODUCTION

Cloud computing usually refers to a utility-based provisioning of computational resources over the Internet. Widely used analogies to explain cloud computing are electricity and water supply systems. Like the Cloud, they provide centralized resources that are accessible for everyone. Also, in the Cloud you only pay for what you have used. And finally, it is usually consumed by those who have difficulties to produce necessary resources by themselves or just do not want to do that. Despite the description by analogy, it is difficult to give a unique and precise definition. One of the main ambiguities to define cloud computing is the fact that it is still evolving and taking its shape.

Computing and communication have continued to impact on the way we run business, the way we learn, and the way we live. The rapid technology evolution of computing has also expedited the growth of digital data, the workload of services, and the complexity of applications. Today, the cost of managing storage hardware ranges from two to ten times the acquisition cost of the storage hardware. We see an increasing demand on

technologies for transferring management burden from humans to software. Data migration and application migration are one of popular technologies that enable computing and data storage management to be autonomic and self-managing.

"Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs."

II. CLOUD DEPLOYMENT MODELS

A. Private Clouds

Also known as internal clouds, private clouds are designed for exclusive use (storage, computing...) by a single organization on a private network. A private cloud offers the highest degree of control over performance, reliability and security. However, they are purchased and completely managed by the organization, so private clouds don't benefit from lower costs due to shared environments unlike other models and requires internal IT expertise or delegate the management to third parties.

B. Public Clouds

Public clouds provide on-demand services to the general public over a common infrastructure hosted, operated and managed by a third-party vendor. Security management and day-to-day operations are relegated to the vendor. Public clouds offer several key benefits to customers, including no initial capital investment on infrastructure, lower costs and shifting of risks to providers' infrastructure.

However, customers have a low degree of control in these kind of control compared with private clouds, which raises a huge amounts of security and privacy concerns that are the basis of this document, as public clouds are the main traditional way of deploying Cloud Computing architectures.

C. Hybrid Clouds

A hybrid cloud is a combination of public and private cloud models that tries to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds (e.g. core applications, sensitive data) while the remaining part runs in public clouds (e.g. non-core applications). Hybrid clouds provide more control and security over data compared to public clouds while still facilitating on-demand service and elasticity. However, the design of hybrid clouds require to carefully determine what should be split into public and private cloud components.

III. CLOUD COMPUTING SERVICE MODELS

A. Software-as-a-Service

Software-as-a-Service (SaaS) is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying

cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

B. Platform-as-a-Service

Platform-as-a-Service (PaaS) is a model of software deployment whereby the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The development environment is typically special purpose, determined by the cloud provider and tailored to the design and architecture of its platform. The cloud subscriber has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud subscriber.

C. Infrastructure-as-a-Service

Infrastructure-as-a-Service (IaaS) is a model of software deployment whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. The cloud subscriber generally has broad freedom to choose the operating system and development environment to be hosted. Security provisions beyond the basic infrastructure are carried out mainly by the cloud subscriber.

IV. LITERATURE SURVEY

Mr. Shrikant D. Bhopale [1], Cloud computing is one of the emerging fields in the computer world these days. Cloud computing is attracting everyone with its benefits. Now companies are shifting their focus onto cloud computing. But to be a part of cloud computing environment and to take advantages of cloud computing, legacy applications need to be migrated to cloud. Cloud migration is the process of transitioning all or part of a company's data, applications and services from onsite computers behind the firewall to the cloud or moving them from one cloud environment to another. After migrating to the cloud, the information will be available on the internet so that more people can have access to it as needed.

J. Priya Shanthi [2], Cloud computing is a form of parallel and distributed system where the resources are shared dynamically and services are provided to customers on demand. It is a new, rapidly growing technology. Hosting applications on a cloud saves a lot of time and effort for the organization as well as their clients. This paper addresses the security issues in cloud computing and computing paradigm called DPaaS which is used as a suite for security and how migration is possible for existing applications to the cloud and among clouds.

Y. Ghebghoub[3], Cloud Computing has been developed to deliver information technologies services on demand to organizations such as well as individual users, this technology is still in its early stages of development because it suffers from different security threats that prevent users trust it In this paper, we identify different security problems existing in the cloud from several research papers and we show suggested solutions.

Anjali Patel[4],Cloud computing is rapidly growing due to the provisioning of elastic, flexible, and on-demand storage and computing services for users. In cloud based storage concept, data owner does not have full control

over own data because data controlled by the third party called cloud service providers (CSP). Data security is challenging problem when data owner shares own data to another known as data sharer on cloud. Many researchers have addressed this issue by cryptography with different encryption schemes that provides secure data sharing on cloud. Here, author propose system model for secure data sharing on cloud with intension to provides data confidentiality, access control of share data, removes the burden of key management and file encryption/decryption by users, support dynamically changes of users membership, owner not be always online when the user wants to access the data.

V. EXISTING TECHNIQUES FOR CRYPTOGRAPHY

Cryptography is the art and science of study of designing or generating the secret message i.e. code or ciphers of the original message for the secure communication between sender and the receiver. The main goals of cryptography are (1) Authentication, (2) Privacy, (3) Integrity, (4) Non-repudiation [3] and (5) Access Control. Encryption is basically a process or algorithm to make information hidden or secret. It is considered as the subset of cryptography. It is the actual process of applying cryptography. It is the process to transform or converting the data into some another form that appears to be random, meaningless and unintelligible. It can also be said that encryption is the process of transforming plaintext into the ciphertext where plaintext is the input to the encryption process and ciphertext is the output of the encryption process.

D. DES

DES is a block cipher that uses shared secret key for encryption and decryption. DES algorithm takes a fixed length of string in plaintext bits and transforms it through a series of operations into cipher text bit sting of the same length and its each block is 64 bits. There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation which named as IP and FP.

E. 3DES

3DES is an enhancement of DES and it is 64 bit block size with 192 bits key size. In this standard the encryption of method is similar to the one is the original DES and increase the encryption level and the average safe time.

In 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence order of Encrypt-Decrypt-Encrypt.

TDES algorithm with three keys require 2168 chances of combinations and with two keys requires 2112 combinations; and the disadvantage of this algorithm is too time consuming problem.

F. AES

In AES is the almost identical of block cipher Rijndael cipher developed by two Belgian cryptographers, Joan and Vincent Rijmen. The algorithm explains about by AES is a secret-key algorithm which means of the same key is used for both encrypting and decrypting the data.

AES on the other hand which encrypts all 128 bits in one iteration. This is one reason why it has a comparably small number of rounds. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices.

G. Blowfish

Blowfish is one of the most common public domain encryption algorithm provided by Bruce Schneier one of the worlds leading cryptologists, and the president of Counterpane Systems and a consulting firm specializing in cryptography and computer security

Blowfish encrypts 64-bits block cipher with variety length key and it contains two parts.

- Data Encryption: It involves the iteration of a simple function of 16 times. Each round contains a key dependent permutation and data dependent substitution.
- Subkey Generation: It involves converts the key upto 448 bits long to 4168 bits.

H. RSA

RSA is a public key algorithm invented by Rivest, Shamir, Adleman. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages.

Messages encrypted with the public key can only be decrypted using the private key. These keys for the RSA algorithm are generated in many ways.

VI. EXISTING TECHNIQUES FOR STEGNOGRAPHY

I. Spatial Domain Methods

In this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories: i)Least significant bit (LSB) ii) Pixel value differencing (PVD) iii) Edges based data embedding method (EBE) iv) Random pixel embedding method (RPE) v)Mapping pixel to hidden data method vi) Labelling or connectivity method vii) Pixel intensity based.

i) LSB: this method is most commonly used for hiding data. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image.

ii) BPCP: In this segmentation of image are used by measuring its complexity. Complexity is used to determine the

noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data.

iii) PVD: In this method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an edge area or smooth area.

J. Spread Spectrum Technique

The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it become difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data

completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.

K. Satistical Technique

In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.

L.Transform Domain Technique

In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain techniques are broadly classified such as

i) Discrete Fourier transformation technique (DFT)

ii) Discrete cosine transformation technique (DCT)

iii) Discrete Wavelet transformation technique (DWT)

iv) Lossless or reversible method (DCT)

v) Embedding in coefficient bits

M. Distortion Techniques

In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.

N. Masking and Filtering

These techniques hide information by marking an image. Steganography only hides the information where as watermarks becomes a potion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grey scale images.

VII. CONCLUSION AND FUTURE SCOPE

In this paper, we have presented a review on cloud security using stegnography and cryptography. In this paper, we have discussed various features of cloud computing, cloud models etc. Various cryptography techniques and stegnography techniques has been discussed in detail in this paper. In future a robust system can be developed based on cloud computing using stegnography and cryptography to secure the data.

REFERENCES

[1] Mr. Shrikant D. Bhopale,"Cloud Migration Benefits and Its Challenges Issue", IOSR Journal of Computer Engineering (IOSR-JCE) ISSN : 2278-0661, ISBN : 2278-8727, PP : 40-45

[2] J. Priya Shanthi, Parsi Kalpana,"Migration of Existing Applications to Cloud and Among Clouds", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[3] Y. Ghebghoub, S. Oukid, and O. Boussaid,"A Survey on Security Issues and the Existing Solutions in Cloud Computing", International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013.

[4] Anjali Patel,Nimisha Patel, Dr. Hiren Patel,"Secure Data Sharing Using Cryptography in Cloud Environment", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. IV (Jan – Feb. 2016), PP 58-62.

[5] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha "Performance Evaluation of Symmetric Cryptographic Algorithms", International Journal of Electronics and Communication Technology Vol 2 Issue 3, Sep 2011.

[6] Nirmaljeet Kaur, Harmandeep Singh "Efficient and Secure Data Storage in Cloud Computing Through Blowfish, RSA and Hash Function", International Journal of Science and Research (IJSR), Vol. 4 Issues 5, May 2015.

[7] Gurpreet Singh, Supriya, "A Study of Encryption Algorithm(RSA,DES,3DES and AES) for information Security" , International Journal of Computer application, Vol. 67- No 19, april 2013.

[8] Deepanshi Nanda, Sonia Sharma, "Security in Cloud Computing using Cryptographic Techniques", IJCST Vol. 8, Iss ue 2, April - June 2017

[9] E.Thmbiraja, G.Ramesh, Dr.R.Umarani, "A survey on various most common encryption techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7, July 2012.

[10] Minu George, Dr. C.Suresh Gnanadhas and Saranya.K, "A Survey on Attribute Based Encryption Scheme in Cloud Computing" , International Journal of Advanced Research in Computer and Communication Engineering 2, no. 11,2013,4408-4412.

[11] Santosh Kumar and R. H. Goudar, "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012.

[12] Vishwanath S Mahalle , Aniket K Shahade , "Enhancing the Data security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm" , 978-1-4799-7169-5/14/$31.00 ©2014 IEEE

[13] Vijay Dhaka, Ankit Dhamija, "A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration", 978-1-4673-7910-6/15/$31.00_c 2015 IEEE.