Survey on Cloud computing security using steganography

Sandeep Sahu
HoD CSE, SRIT
Jabalpur, MP

Aditi Bhadoria
M.Tech Scholar, SRIT
Jabalpur, MP

Abstract:

IT technologies are growing very rapidly, now the information technology has become the revolution. All the other business domain and technologies are also experiencing the IT waves. One of the core working force behind the IT revolution is "Cloud Computing", which has attracted major SMB and SME to migrate their data and applications to the cloud infrastructure. As every technologies has some pros and cons, cloud computing also have a major limitation that is security and privacy. In this paper we have discussed about the proposed technique by which we can improve the cloud user's experience in terms of security and data privacy.

Keyword:

Cloud Computing, Steganography, and Information privacy

Introduction:

In the emerging world of technology, the term cloud computing has transformed the way users manage, process, distribute, and store data. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, and applications) that can be quickly provisioned and released with minimal management efforts or service provider interactions. Cloud computing promotes availability and is composed of five essential characteristics, three service models, and four deployment models. The five essential characteristics within the cloud model include [1]:

• On Demand self-service- A cloud customer may individually obtain computing capabilities, such as the usage of various servers and network storage, on demand without the need of human interaction at each cloud provider.

• Broad network access- Services are delivered across the Internet by standard mechanisms that allows customer to access the services through heterogeneous client platforms (e.g., Personal Computers (PCs), and mobile phones).

• Resource pooling- The cloud provider employs a multitenant model to serve multiple customers by pooling computing resources dynamically assigned or reassigned according to customer demand.

• Rapid elasticity- Capabilities may be rapidly and elastically provisioned in order to quickly scale out or rapidly release to quickly scale in. From customer's viewpoint, the available capabilities should appear to be unlimited and have the ability to be purchased in any quantity at any time.

• Measured Service- The service purchased by customers can be quantified and measured. For both the provider and customer, resource usage will be monitored, controlled, metered, and reported.

The five essential characteristics within the cloud model make cloud computing a very unique and attractable infrastructure, which provides its consumers a wide array of functionalities and resources with the avoidance of capital expenditures. Three service models are provided within the cloud model including [1]:

• Cloud Software as a Service (SaaS)- The capability provided to the consumer is to use the provider's applications running on the cloud infrastructure.

• Cloud Platform as a Service (PaaS)- The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired application using programming languages and tools supported by the provider.

• Cloud 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. Cloud computing provide different deployment models that makes the entire cloud architecture complete [2]:

• Public Cloud- The cloud infrastructure is made available to the general public or a large industry group and is owned by organization selling cloud services.

• Private Cloud- The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises

• Community Cloud- The cloud infrastructure is shared by several organizations and supports a specific community that has common concerns (e.g., mission, security requirements, policy, or compliance considerations).

ISSN: 2278 – 7798

• Hybrid Cloud- The cloud infrastructure is composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). As one can see, cloud computing offers its consumer's endless functionality and resources within a large variety of cloud environments. One of the most appealing services offered within cloud computing is cloud storage. Cloud storage allows consumers to store their data on the cloud service provider's servers instead of storing their data on their own servers. Having the ability to store data on the service provider's servers allows consumers to easily access their data from any geographical region where the Cloud Service Provider's network or Internet is accessible.

2. Literature Survey:

Image steganography and cloud computing security domain is one of the popular domain for researchers, many concrete and outstanding research milestones are achieved in this field. Some of constructive works are as follow:

G. Shaik Abdullah and B. Muthulakshmi [2] have following finding, the method of applying steganography in conjunction with cryptography, referred to as twin steganography, develops a durable model that adds a lot of challenges in distinguishing any hidden and encoded information. Therefore using steganography within steganography, create to better interpretation of twin steganography which is able to give higher security in cloud. A ProofLess Public Key Encoding (PL: PUKE) clears the key written agreement drawbacks in identity free-based encoding and certification annulment drawbacks in PU Key cryptography. A tends to (PL: PUKE) design while not exploitation matching operations. Each Data owner first register in the cloud service provider. It can submit Thumb Finger Print and Aadhaar Card Number. Both Finger Print and Aadhar Card Number are stored in the Security- as- a- Service (SEaaS). The Key Provider – as – a – Service (KPaas) to provide key to Cloud data
owner. The cloud is applied as safe compute storage as well as Key Creating Center – as – a - Service (KCCaaS). The data owner encrypts the sensitive data using the cloud, KCCaaS making user key (UR Key) based on its data owner public key (PU Key) and upload the encoding data store to the STorage – as – a – Service (STaaS) in the cloud. Upon successful authorization, the cloud partly decipherment the encoding data for the users by using Security Negotiation Host – as – a - Service (SNHaaS). The users subsequently fully decoding the partially decrypted data using their private key (SEC Key) as well as UR Key. A method for concealment knowledge with two level of security to plant knowledge at the side of sensible sensory activity transparency and high payload capability. A tend to carry out a CL-PUKE theme and the overall cloud primarily based system and assess its security and performance.

Garima Saini and Naveen Sharma [3] worked for research work titled "Triple Security of Data in Cloud Computing", in their proposed work they provide security by implementing three algorithm DSA, DES and steganography together to cloud network. To implement these three algorithm we use Asp.net as a platform. In proposed system for encryption first apply DSA for authentication of data. Then apply AES algorithm for encryption and then hiding data within audio file for provide maximum security to the data. Receiver can get original plain text by reversing the steganography, AES and DSA.

They implements Digital signature Algorithm, Data Encryption Standard and Steganography to provide maximum security in cloud computing. By implementing these three algorithm provide authenticity, security and data integrity to the data. Then find that the time complexity is high because it is a one by one process but in future this time complexity could be reduced.

Another paper "Enhancing Data Storage Security in Cloud Computing through Steganography"[4], proposed model aims to secure data-at-rest, not by physically storing files, instead of the data present in a files are somehow stored within some images. This underlining concept is known as steganography which tells- "The art and science of writing hidden messages in such a way that no one apart from the sender and the intended recipient, suspects the existence of the message, a form of security through obscurity". The security model give a detailed description of how the system will be worked. The users will perform their computations in CSP-3. Whenever user wants to save their data, the following operation will be happen:

1. CSP-3 requests set of images from CSP-1.
2. CSP-1 acknowledges CSP-3 by providing a set of valid images.
3. CSP-3 requests the data hiding algorithm which is stored in CSP-2.
4. CSP-2 provides the algorithm to CSP-3.

ISSN: 2278 – 7798

5. According to the algorithm the data are saved within the pixels of the images which are taken from the CSP-1.
6. The images containing the data will be stored in CSP- 1.

Later whenever user wants to view or retrieve his/her data the following mechanisms will be followed:
1. CSP-3 requests set of images which are associated with the file that users want to view/retrieve.
2. CSP-1 acknowledges to CSP-3 by providing the associated set of images.
3. CSP-3 requests the data retrieval algorithm which is stored in CSP-2.
4. CSP-2 provides the algorithm to CSP-3.
5. CSP-3 processes the algorithm on the images which are provided by CSP-1, and store the data after retrieval into a temporary file. This file is displayed to the user and after any operation on this data; it will be deleted from it. Before user log-out from CSP-3, the temporary file will be automatically de-allocated from the system.

C. Design Goal

To ensure the security for cloud data storage from unauthorized users, we have designed efficient mechanism for data-at-rest in cloud data storage centers. As our used techniques highlights hiding data within digital image, this steganography technique exploits the weakness of Human Visual System (HVS). HVS cannot detect the variation in luminance of grayscale vectors at higher frequency side of the visual spectrum. An image is a collection of pixels (Picture Elements), where each pixel of grayscale image is composed of 8 bits. If we change the last bit, the color information may be varying within +1 to -1. This change of the intensity will not be perceived by human eye. Now data consist of characters representing ASCII values. Idea is to store each character into the last bit of consecutive 8 pixels. So by storing data within images, which are located in remote cloud servers, we can achieve the following goals.
1. Correctness: Data can be stored correctly within images.
2. Availability: An authorized user can retrieve the information from an image when required.
3. Protection: It is fully protected from unauthorized user because, perceiving an image does not provide any idea of the original information.

In this work, they have investigated the problem of security in cloud computing, which is essentially a distributed storage system. To ensure the security of user' data in cloud storage, proposed an effective and efficient steganography strategy for enhancing security on data-at-rest. So, when these images are stored in the cloud data center, no one can view the original content of the data without any proper identification. Through detailed security and performance analysis, we have seen that our scheme almost guarantees the security of data when it is residing on the data center of any Cloud Service Provider (CSP). The concept we have discussed here, will help to build a strong architecture for security in the field of cloud computation. This kind of structure of security will also be able to improve customer satisfaction to a great extent and we will attract more investor in this cloud computation concept for industrial as well as future research farms. Security in a very large scale cross cloud environment is an active issue. This present scheme is able to handle only a limited number of security threats in a fairly small environment. It need further simulations to verify the performance.

3. Discussion:

In the promoting of cloud computing services, the issue of data security is one of the most important problems to be solved. Today's network construction, safety products, and encryption protocol have been protected the safety of data transmission basically; Data storage security can be solved through technical means in the design stage of cloud services, such as redundancy, parity, user authentication and access control; Data management security involves many aspects, the first is to improve the relevant laws and regulations as soon as possible, and the second is compatible with data between cloud computing service providers to ensure that users can seamlessly pan data, and service providers should establish a rapid and effective disaster recovery mechanisms to guarantee the availability of the data. At present, in a short period of time, the cloud computing cannot completely replace traditional computing. It is still not being fully accepted that to manage data by a third party, especially for large enterprises and government departments. In order to take full advantages of cloud computing characteristics, some large enterprises with strong economic and technological strength have begun to try to establish their own cloud computing platforms, such as China Mobile Big Cloud, but the Chinese government is still in a wait-and see. It is foreseeable that in the near future, the average user will not shift entirely to the cloud computing model, firstly, because of the aforementioned security reasons, and secondly, they also hoard some computing devices, turning to cloud computing means to abandon existing investments. But some businesses with low level data confidentiality or even completely

ISSN: 2278 – 7798

open can use commercial cloud computing model, such as some entertainment sites, SNS sites as well as public service platform, such as network library and public information release platform and so on. In addition, enterprises can also try to separate from the business, one part of the businesses involves confidential information are still running in the local network in accordance with the original mode and the other part complete by the cloud computing platform.

4. Proposed Idea:

The proposed solution for cloud computing security is a novel method, where we are using image or part of image as encryption key to encrypt the data and information. The complete work flow of the method is as follow:

Step 1: Get the data or information which is going to be on cloud infrastructure.

Step 2: Now choose any image, and apply differential evolution algorithm. This will perform an intelligent segmentation process and will differentiate between objects and background of the image.

Step 3: Now the encryption key will be generate by using segmented objects of the image.

Step 4: Encryption will be process using the generate key.

Step 5: System will use KDC for third party authentication.

Step 6: Cloud computing infrastructure will communicate with both KDC and PKI for the secure transaction of data and information over the network.

5. Conclusion:

To ensure information and data privacy over the cloud, application are encrypting the user data before sending it over the cloud. Hackers and cryptanalyst are capturing the data using various illegal practices over the communication network. In this paper we have proposed a method, where data is encrypted using image as encryption key and to generate this encryption key from image, we used differential evolution algorithm for multi-level segmentation. Results are compared with other nature inspired algorithms.

6. References:

[1] Chao Yang, "A novel triple Encryption Scheme for Hadoop based cloud computing", in Emerging intelligent data and web technologies , IEEE , Sep-2013.

[2] Patidar , S "Survey on cloud computing" , in Advanced computing and communication technologies , IEEE , Jan- 2012..

[3] M. Vijayapriya, "Security algorithm In Cloud Computing: Overview"/ International Journal of Computer Science & Engineering Technology (IJCSET)

[4] Rashmi Nigoti, Manoj Jhuria & Dr. Shailendra Singh," A Survey of Cryptographic algorithms for Cloud Computing. In International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), ISSN (print) 2279-0047, ISSN (online):2279-0055.

[5] B.Arun & S,K. Prashanth, " Cloud Computing Security Using Secret Sharing Algorithm" in Indian Journal of Research, ISSN- 2250-1991, Volume:2|Issue: 3| March 2013.

[6] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan &

Bhavani Thuraisingham, "Security Issues for Cloud Computing" in International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.

[7] Ew Approach to Hide Text in Images Using Steganography" in International Journal of advanced Research in Computer Science and software Engineering, ISSN:2277 128X, Volume 3, Issue 4, April 2013.

[8] V.K. Zadiraka & A. M. Kudin, " Cloud Computing In Cryptography And Steganography", in Cybermetics and Systems Analysis, Vol. 49, No. 4, July-2013, UDC 681,3;519,72;003,.26

[9] Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing ", Journal of Network and Computer Application, vol. 34, issue 4, pp 1113-1122, July 2011, Academic Press td London, UK.

[10] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," Proc. of ICDCS '08, pp. 411–420, 2008.

[11] S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. of ICDCS '06, pp. 12–12, 2006.

[12] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. Of CCS '07, pp. 598–609, 2007.

[13] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Of Secure Comm. '08, pp. 1–10, 2008.

[14] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," Proc. of ICDCS '08, pp. 411–420, 2008.

ISSN: 2278 – 7798