

Multi-Layer Data Security in Cloud Computing

Lovejeet Kamboj, Pawan Luthra

Department of Computer Science and Engineering
Shaheed Bhaghat Singh State Technical Campus, Firozpur

ABSTRACT

In the digital world, the users stores digital data on clouds and according to requirement access the data. So, authentication and confidentiality is a big concern. To resolve these attacks cryptography and steganography algorithms are used. In this paper, an overview of cloud, its architecture, and attacks defined. Also, a literature survey is done and based on survey a multi-layer security algorithm is designed by hybrid the cryptography and steganography algorithm. Moreover, the performance analysis is done on the basis of correlation factor, MSE and PSNR values.

Keywords—Cloud Attacks, Security, MSE, PSNR, Cryptography, Steganography.

Date of Submission: 30-09-2017

Date of acceptance: 23-10-2017

I. INTRODUCTION

Cloud computing is recently a rising model of distributed computing. Cloud computing is not a new idea that emerged recently. L. K Leinrock in 1969 [1] anticipated that "The computer networks are still in their babyhood. But, as they build up and become more and more complicated, than there is a probability to see the spread of 'computer utilities' just like present electric utilities and telephone utilities, and will provide service to individual homes and offices across the country." His fantasy was the true sign of today's utility based computing paradigm. In the mid-1990s, grid computing was first allotted to allow consumers to obtain computing power on demand was a crucial step taken by this world. The beginning of cloud computing can be regarded as an evolution of grid computing technologies. In late 2006, Google's CEO Eric Schmidt was the first to prominence the term cloud computing. So, the birth of cloud computing is a very recent phenomenon, but its origins belong to some old concepts with new scientific, business and social perspectives. The cloud is usually built on existing grid based architecture and used the grid services and adds some technologies like virtualization and some business models. By introducing computation, storage, and software-based services, cloud computing has gained popularity among individuals and as well as for the organization. To address the insufficient resource issue of their clients, they provide them on-demand pay-per-use services [2]. It incorporates a centralized collection of resources called a cloud connected through a high-speed network. Due to the global availability of high-performance resources, it can support a large number of services and also has the ability to store a large amount of data.

Even with the modern smart phones, the cloud computing is able to serve multiple purposes ranging from a backup of contacts to the execution of complex applications through computation offloading [3-4]. Moreover, the reduced cost of services and an assurance regarding quality make it an attractive solution for mitigating the issue of constrained resources. Since a cloud computing platform provides services by sharing valuable resources, an adequate usage of these resources may be achieved by ensuring that the platform is able to counter security threats which may otherwise deteriorate its performance and reliability.

1.1 CLOUD ARCHITECTURE

The cloud providers actually have the physical data centers to provide virtualized services to their users through Internet. The cloud providers often provide separation between application and data. This scenario is shown in the Figure 2. The underlying physical machines are generally organized in grids and they are usually geographically distributed. Virtualization plays an important role in the cloud scenario. The data center hosts provide the physical hardware on which virtual machines resides. User potentially can use any OS supported by the virtual machines used. Operating systems are designed for specific hardware and software. It results in the lack of portability of operating system and software from one machine to another machine which uses different instruction set architecture. The concept of virtual machine solves this problem by acting as an interface between the hardware and the operating system called as system VMs [5].

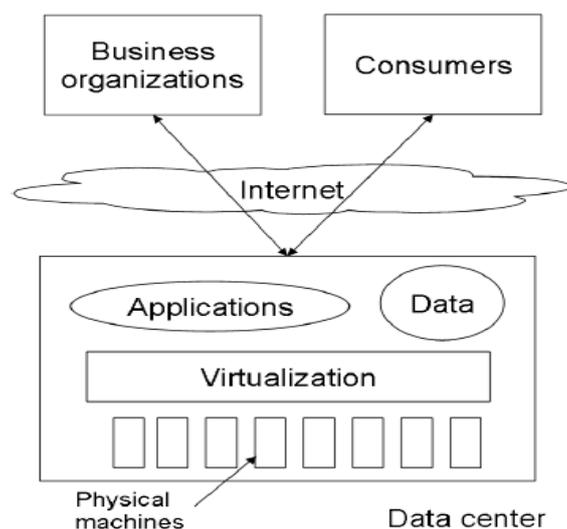


Fig 1 Basic Cloud Computing Architecture

1.2 Types of cloud

Clouds can be of three types [6].

- **Private Cloud** - This type of cloud is maintained within an organization and used solely for their internal purpose. So, the utility model is not a big term in this scenario. Many companies are moving towards this setting and experts consider this is the 1st step for an organization to move into cloud. Security, network bandwidth are not critical issues for private cloud.
- **Public Cloud** - In this type an organization rents cloud services from cloud provider's on-demand basis. Services provided to the users using utility computing model.
- **Hybrid cloud** - This type of cloud is composed of multiple internal or external clouds. This is the scenario when an organization moves to public cloud computing domain from its internal private cloud.

1.3 Advantages of using cloud

The advantages for using cloud services can be of technical, architectural, business etc. [7-8].

1.3.1 Cloud provider's point of view-

- Most of the data centers today are underutilized. They are mostly 15% utilized. These data centers need spare capacity just to cope with the huge spikes that sometimes get in the server usage. Large companies having those data centers can easily rent those computing power to other organizations and get profit out of it and also make the resources needed for running data center (like power) utilized properly.
- Companies having large data centers have already deployed the resources and to provide cloud services they would need very little investment and the cost would be incremental.

1.3.2 Cloud user's point of view-

- Cloud users need not to take care about the hardware and software they use and also, they don't have to be worried about maintenance. The users are no longer tied to someone traditional system.
- Virtualization technology gives the illusion to the users that they are having all the resources available.
- Cloud users can use the resources on demand basis and pay as much as they use. So, the users can plan well for reducing their usage to minimize their expenditure.

1.4 Attacks on Cloud Computing

In this section, attacks on cloud data are defined.

- **Cross VM side channel attacks:** The VM based side channel attacks are able to extract information regarding resource usage, cryptographic keys and other information from a target VM which is residing on the same physical machine as that of the attacker VM. These attacks may exploit timing information from resources such as cache and shared memory. The counter-measures for side channel attacks use authentication mechanisms, cryptographic algorithms or deterministic execution to mitigate the risk of side channels [20].
- **Denial of Service Attack:** In this attack, the attacker is jamming the whole network.
- **Eavesdropping attack:** In this attack the attacker monitors the whole communication.
- **Malware injection and steganography attacks:** A malicious code may be inserted in an application if a cloud platform allows for an insecure interface for application development. With a steganography attack,

the attackers embed malicious code within files being transmitted over network. The transmission of malicious code may then be ignored by security systems for which it seems as if a normal file is being sent.

1.5 Overview of Cryptography and Steganography Algorithms

In the last section, attacks are highlighted. To resolve these attacks cryptography and steganography algorithms are used.

- **Cryptography:** In cryptography the data is change into another form which is not easily understandable by third person. The cryptography algorithms security depends on their mathematical models. Some of the mathematical models on which algorithms are based are discrete logarithm, Galois field *etc.*
- **Steganography:** In steganography the data is hided in another media in such a way that the media quality never degraded. The most used technique for data hiding is LSB technique. In which the data bits are hide in the LSB bits of cover image.

The paper outline as follows the section II defined the literature survey and section III defined the algorithms are used for multi-layer security. In section IV simulation is done on MATLAB results shown using qualitative and quantitative analysis. The V section shows the conclusion.

II. LITERATURE SURVEY

In this section, cloud computing attacks and their countermeasure algorithms survey is done.

M. A. Hasan et.al [9]Cloud computing confers strong economic advantages, but many clients are reluctant to implicitly trust a third-party cloud provider. To address these security concerns, data may be transmitted and stored in encrypted form. Major challenges exist concerning the aspects of the generation, distribution, and usage of encryption keys in cloud systems, such as the safe location of keys, and serving the recent trend of users that tend to connect to contemporary cloud applications using resource-constrained mobile devices in extremely large numbers simultaneously; these characteristics lead to difficulties in achieving efficient and highly scalable key management. In this work, a model for key distribution based on the principle of dynamic data re-encryption is applied to a cloud computing system in a unique way to address the demands of a mobile device environment, including limitations on client wireless data usage, storage capacity, processing power, and battery life. The proposed cloud-based re-encryption model is secure, efficient, and highly scalable in a cloud computing context, as keys are managed by the client for trust reasons, processor-intensive data re-encryption is handled by the cloud provider, and key redistribution is minimized to conserve communication costs on mobile devices. A versioning history mechanism effectively manages keys for a continuously changing user population. Finally, an implementation on commercial mobile and cloud platforms is used to validate the performance of the model.

Y. Bassil et.al [10], Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and the receiver would realize that a secret communicating is taking place. Unlike cryptography which only scrambles secret data keeping them overt, steganography covers secret data into medium files such as image files and transmits them in total secrecy avoiding drawing eavesdropper's suspicions. However, considering that the public channel is monitored by eavesdroppers, it is vulnerable to stego-attacks which refer to randomly trying to break the medium file and recover the secret data out of it. That is often true because steganalysts assume that the secret data are encoded into a single medium file and not into multiple ones that complement each other. This paper proposes a text steganography method for hiding secret textual data using two mediums; a Pangram sentence containing all the characters of the alphabet, and an uncompressed image file. The algorithm tries to search for every character of the secret message into the Pangram text. The search starts from a random index called seed and ends up on the index of the first occurrence of the character being searched for. As a result, two indexes are obtained, the seed and the offset indexes. Together they are embedded into the three LSBs of the color channels of the image medium. Ultimately, both mediums mainly the Pangram and the image are sent to the receiver. The advantage of the proposed method is that it makes the covert data hard to be recovered by unauthorized parties as it uses two mediums, instead of one, to deliver the secret data.

Z. Alani et.al [11], Developers of cloud computing systems are responsible for identifying the requirements of Quality Attributes and developing security of cloud computing systems. Developing some quality cloud computing systems needs to satisfy interoperability, security, safety, dependability, performance, and other. Security of cloud computing services represents another incentive that will promote the use of cloud services by related stakeholders. Also, security is considered as an important issue when dealing with cloud services' interoperability. Using good protected access control technique can prevent many security problems. This paper proposes steganography scheme as a new architecture to secure the data in cloud computing by exploiting text properties. Also, it describes the implementation of the data steganography technique, which could provide more security to the cloud computing environment to achieve the trusted computing technology.

S. N. Brohi et.al [12], Despite several cost-effective and flexible characteristics of cloud computing, some clients are reluctant to adopt this paradigm due to emerging security and privacy concerns. Organization such as Healthcare and Payment Card Industry where confidentiality of information is a vital act, are not assertive to trust the security techniques and privacy policies offered by cloud service providers. Malicious attackers have violated the cloud storages to steal, view, manipulate and tamper client's data. Attacks on cloud storages are extremely challenging to detect and mitigate. In order to formulate privacy preserved cloud storage, in this research paper, we propose an improved technique that consists of five contributions such as Resilient role-based access control mechanism, Partial homomorphic cryptography, metadata generation and sound steganography, Efficient third-party auditing service, Data backup and recovery process. We implemented these components using Java Enterprise Edition with Glassfish Server. Finally, we evaluated our proposed technique by penetration testing and the results showed that client's data is intact and protected from malicious attackers.

III. OVERVIEW OF ALGORITHMS

In this section, the encryption and hiding algorithm explanation given which are used for multi-layer security in cloud computing.

3.1 OVERVIEW OF LEOPARD ENCRYPTION ALGORITHM [13]

The LEOPARD algorithm is derived from AES algorithm. The Encryption Algorithm is given as

```

Round (State, Round Key)
{
  Mix-Column (State)
  Add Round Key (State, Round Key)
  Shift-Rows (State)
}
Sub Byte (State)
Shift-Rows (State)
Add Round Key (State, Round Key)

```

The Key Scheduling Algorithm: The keys are arranged into 4x4 matrixes.

```

1. The 4th Column is Circular Rotate and passed through S-Box.
2. The next key matrix is generated as
Key Column1' = (original Key Column1 XOR Updated 4th Column Value) XOR R-Constant
Key Column2' = Key Column1' XOR Original 2nd Key Column
Key Column3' = Key Column2' XOR Original 3rd Key Column
Key Column4' = Key Column3' XOR Original 4th Key Column

```

3.2 OVERVIEW OF IMPROVED LSB TECHNIQUE [14]

3.2.1 **2:2:4 Ratio**: In 2:2:4 Ratio the data is split into 2:2:4 Ratio and hide in RGB plane simultaneously. As shown in table [4.6-4.8]

Let suppose data bits: **10100011, 01010111, 11001100, 01000111**

Table 1: Red Plane for 2:2:4 Ratio

10010111	11100011	01110000	01111111
10001001	01010101	10101110	00011001

Table 2: Green Plane for 2:2:4 Ratio

10010100	11100001	01110011	01111101
10001001	01010101	10101110	00011001

Table 3: Blue Plane for 2:2:4 Ratio

10011010	11100101	01111100	01110111
10001001	01010101	10101110	00011001

3.3 Proposed Improved LSB Technique

In the proposed technique in place of replacing EXOR of cover LSB bits with data bits is done. The EXOR principle reduces the error factor as compared to LSB technique in the image.

Let suppose data bits: **10100011,01010111, 11001100, 01000111**

Table 4: Red Plane for 2:2:4 Ratio

10010101	11100001	01110000	01111110
00000011	00000011	00000000	00000011
10010110	11100010	01110000	01111101

Table 5: Green Plane for 2:2:4 Ratio

10010110	11100001	01110010	01111110
00000000	00000001	00000011	00000001
10010110	11100000	01110001	01111111

Table 6: Blue Plane for 2:2:4 Ratio

10011110	11100001	01111011	01110011
00001010	00000101	00001100	00000111
10010100	11100100	01110111	01110100

IV. PROPOSED ALGORITHM

In the proposed algorithm, a multi-layer data security algorithm is designed using cryptography and steganography.

1. Read the data.
2. Encrypt the Data using LEOPARD technique.
3. Break the encrypted data stream into 2:2:4 ratios.
4. The data bits hide in image using EXOR principle in place of replacing technique.
5. Performance analysis is done on the basis of qualitative and quantitative analysis parameters such as correlation factor, MSE, PSNR.

V. SIMULATION RESULTS

The proposed technique is simulated in MATLAB 2013a using different videos. Also we have done Qualitative and Quantitative analysis for the proposed work as shown in table 1 and 2.

5.1 Qualitative Analysis

For Qualitative Analysis different videos are taken from MATLAB database.

Table 7: Qualitative Analysis between Cover and Stego Frame

File Name	Cover Image	Stego Image
Football.jpg		

The Qualitative analysis shows that after data hiding the output frame looks like input frame so, it's doesn't give attention to third person when data is communicated.

5.2 Quantitative Analysis

5.2.1 Correlation Factor: Correlation is used to measure the level of security of encrypted information. Correlation is given as [9]

REFERENCES

- [1] Leonard Klein rock. An internet vision: the invisible global infrastructure. *Ad Hoc Networks*, 1(1):3 {11, 2003.
- [2] Buyya, R., Bromberg, J., Goscinski, A.M., 2011. *Cloud Computing Principles and Paradigms*. Wiley Publishing, New Jersey, USA.
- [3] Kumar, K., Liu, J., Lu, Y.-H., Bhargava, B., 2013. A survey of computation offloading for mobile systems. *Mob. Netw. Appl.* 18(1), 129–140.
- [4] Sanaei, Z., Abolfazli, S., Gani, A., Buyya, R., 2014. Heterogeneity in mobile cloud computing: taxonomy and open challenges. *IEEE Commun. Surv. Tutor.* 16(1), 369–392
- [5] J.E. Smith and R. Nair. An overview of virtual machine architectures. pages 1, 20, October 2001.
- [6] Bhaskar Prasad Rimal, Eunmi Choi, and Ian Lumb. A taxonomy and survey of cloud computing systems. *Networked Computing and Advanced Information Management, International Conference on*, 0:44{51, 2009.
- [7] Michael Armbrust, Armando Fox, Rean Grith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. Above the clouds: A Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.
- [8] F.M. Aymerich, G. Fenu, and S. Surcis. An approach to a cloud computing network. *Applications of Digital Information and Web Technologies*, 2008. ICADIWT 2008., pages 113 {118, August 2008.
- [9] Tysowski, P. and Hasan, M. (2011) Re-Encryption-Based Key Management towards Secure and Scalable Mobile Applications in Clouds. *IACR Cryptology Eprint Archival*, 668-678.
- [10] Bassil, Y. (2012) A Text Steganography Method Using Pangram and Image Mediums. *International Journal of Scientific & Engineering Research*, 3, 2229-5518.
- [11] Al-Khanjari, Z. and Alani, A. (2014) Developing Secured Interoperable Cloud Computing Services. *The European Interdisciplinary Forum 2014 (EIF 2014)*, Vilnius, 18-19 June 2014, 341-350.
- [12] Brohi, S., Bamiah, M., Chuprat, S. and Manan, J. (2014) Design and Implementation of a Privacy Preserved Off-Premises Cloud Storage. *Journal of Computer Science*, 10, 210-223.
- [13] R.D. Sparrow, A.A. Adekunle, R.J. Berry, "LEOPARD: Lightweight Encryption Operation Permutation Addition Rotation and Diffusion," *10th International Conference on Signal Processing and Communication Systems*, February 2017.
- [14] Amritpal Singh, Harpal Singh, "An improved LSB based Image Steganography Technique for RGB images", *IEEE*, pp.1-4, 2015.

International Journal of Computational Engineering Research (IJCER) is UGC approved Journal with Sl. No. 4627, Journal no. 47631.

Lovejeet Kamboj "Multi-Layer Data Security in Cloud Computing." *International Journal of Computational Engineering Research (IJCER)*, vol. 7, no. 10, 2017, pp. 01–07.