Data Security In Cloud Computing Using RC6 Encryption and Steganography Algorithms

Sirisha Aguru¹, Batteri MadhavaRao²

¹Dept. of CSE, Sri Vasavi Engineering College, JNT UK, Kakinada, India
²Corresponding Author: sirib4u1@gmail.com, Tel.: +91-8978284214

Available online at: www.isroset.org

Abstract—Cloud computing is one of the emerging technologies. The cloud environment is a large open distributed system. Cloud Computing provides various services to the customers with price as pay for use such services are Infrastructure as a service (IaaS), Platform as a service (PaaS), software as a service (SaaS) and Data base as service (DaaS) like so many services. And all these services provide various benefits to its customers, but there are still some challenges. One among them is to protect the data, as well as, privacy of users. The data saved at remote servers is under the control and observation of unknown people who can do anything with our data, thus there are some Security risks. So, these data security risks are causing a hindrance in the development of the field of cloud computing. This paper has designed a scheme that can help, solve this Security issue. This paper proposes an improved way in guaranting information security by utilizing RC6 algorithm and Steganography algorithms.

Keywords—Cloud Computing, Data Security, Encryption, RC6 Encryption, Steganography.

I. INTRODUCTION

Cloud computing is emerging as a dominant technology category in the business community. While the benefits of cloud computing are clear, it also introduces new security challenges. Cloud Computing is considered as Service oriented. This service oriented nature of Cloud Computing not only reduces the overhead of infrastructure and cost of ownership but also provides flexibility and improved performance to the end user. A major concern in usage of cloud for data is security and privacy. It is very important for the cloud service to provide the data integrity, privacy and protection. A Survey on various security issues in cloud environments [4] gives a detailed knowledge on how insecure is the data on cloud. Storing data in the cloud has become a trend [2], [3].

An increasing number of clients store their important data in remote servers in the cloud, without even leaving a copy in their local computers. Sometimes, the data may be so sensitive to be stored on a public cloud, for example, highly confidential future project information etc. This type of data can be extremely sensitive and the consequences of exposing this data on a public cloud can be serious. In such cases, it is highly recommended to store data using internal organizational cloud. This approach can help in securing data by enforcing on-premises data usage policy. However, it still does not ensure full data security and privacy, since many organizations are not qualified enough to add all layers of protection to the sensitive data.

In cloud storage setting, the loss of physical possession of data, is a major issue. If the cloud servers are not fully trusted, the integrity of stored data could not be ensured. Consequently, there is a need for the development of protocols allowing the data owners to verify that their data are securely stored in the cloud.

This paper is the study of data security techniques used for protecting and securing data in cloud. The remainder of the paper is organized as follows. Section 2 is the review of literature that provides an insight into the work already done in this area. Section 3 discusses the types of threats to data in cloud. Section 4 examines a solution adopting an efficient data security technique that uses both RC6 algorithm and Steganography. The final section is the conclusion which provides summary for this study.

II. RELATED WORK

Here the authors provide a very solid technique of maintaining the integrity of data. In this model, the data being sent to server is saved behind the images. Thus, the unauthorized access cannot perceive the data as it is hidden. The proposed model makes use of steganography using images for protecting the integrity of data which is a very good approach. However, the security of data during transmission is not handled at all. Hence, even though it’s a very unique approach but could have been much better if integrity and confidentiality of data can be handled while uploading to cloud server.

**Robust Data Security for Cloud while using Third Party Auditor by Ravi Kant Sahu and Abhishek Mohta**

This paper uses the services of a third party auditor for checking cloud server provider reliability. Also it verifies that the data is intact and is responsible for its accountability. In short it deals with the problem of data privacy and its integrity.

**Cloud Computing Security and encryption by Varsha Alangar**

In this paper the author has tried to attract analyst attention towards the problem of data security and as firmly believe that data encryptions can help to solve this issue. The author has provided a list of various encryption techniques such as RSA, DES, etc.

**Improve Cloud Computing Security Using RSA Encryption With Fermat’s Little Theorem by Balkees M. Shereek, Zaiton Muda, Sharifah Yasin**

This paper provides a new method for Cloud Computing Security by applying RSA algorithm and Fermat’s theorem together to keep user’s data highly secured against unauthorized servers and from malicious dangers. Their purpose work using Fermat’s theorem to speed up the RSA Encryption and helping to build a new trusted environment of cloud computing.


This paper discusses a problem statement, when storing the data on cloud there are number of issues. The main issues of cloud computing are data security, integrity, authentication and confidentiality. This paper provided a survey of different symmetric and asymmetric algorithms to provide the solution for these security issues.

**Security Storage Model of Data In Cloud by Sonia Arora & Pawan Luthra**

This paper discussed a security model for data storage to eliminate Security and trust issues in cloud. They proposed system that provides security for data by using encryption algorithms, such as RC6, RC4, Blowfish, AES and others to encrypt the file and then transfer it to the cloud and they used hashing algorithms to check integrity of the data being stored.

### III. SECURITY CONCERNS IN CLOUD

Several risks and security concerns are associated with cloud computing and its data. Here we will discuss about the virtualization, storage in public cloud and multi-tenancy which are related to the data security in cloud computing [1].

A. **Virtualization**

Virtualization is a technique in which a fully functional operating system image is captured in another operating system to utilize the resources of the real operating system fully. Virtualization is a foundational element of cloud computing which helps in delivering the core values of cloud computing. However, virtualization poses some risks to data in cloud computing. One possible risk is compromising a hypervisor itself. A hypervisor can become a primary target if it is vulnerable. If a hypervisor is compromised, the whole system can be compromised and hence the data [5].

Another risk with virtualization is associated with allocation and de-allocation of resources. If VM operation data is written to memory and it is not cleared before reallocation of memory to the next VM, then there is a potential for data exposure to the next VM which might be undesirable [6].

A solution to above mentioned issues is, a better planning of the use of virtualization. Resources should be carefully used and data must be properly authenticated before de-allocating the resources.

B. **Storage in Public Cloud**

Storing data in a public cloud is another security concern in cloud computing. Normally clouds implement centralized storage facilities, which can be an appealing target for hackers. Storage resources are complicated systems that are combination of hardware and software implementations and can cause exposure of data if a slight breach occurs in the public cloud [7]. In order to avoid such risks, it is always recommended to have a private cloud if possible for extremely sensitive data.

C. **Multi-tenancy**

Shared access or multi-tenancy is also considered as one of the major risks to data in cloud computing [8]. Since multiple users are using the same shared computing resources like CPU, Storage and memory etc. it is threat to not only a single user but multiple users. In such scenarios there is always a risk of private data accidentally leaking to other users. Multi-tenancy exploits can be exceptionally risky because one fault in the system can allow another user or hacker to access all other data [9]. These types of issues can be taken care of by wisely authenticating the users before they can have access.
to the data. Several authentication techniques are in use to avoid multi-tenancy issues in cloud computing [10].

IV. PROTECTING DATA USING ENCRYPTION

Here we are proposing a data security algorithm using encryption, decryption with RC6 algorithm while we are transferring it over the network. The proposed system is based on the principle of securing data both during transmission and while data at rest at servers. Data at rest refers to data in cloud, or any data that can be accessed using Internet. This includes backup data as well as live data.

A. Working of proposed model

Our proposed model uses RC6 algorithm for encryption and decryption and Steganography. RC6 is a symmetric key algorithm in which encryption and decryption are performed utilizing a similar key. RC6 algorithm is a block cipher derived from RC5. The generated key is embedded into an image and then shared with the destination. This is where Steganography plays its role. We explain RC6 Algorithm in two steps:

1. Storing Process
2. Retrieval Process.

1. Storing Process

Storing Process is explained in the following steps:-

1) The user selects the data to be uploaded and this selected data gets encrypted using RC6 algorithm.
2) The encrypted data is then uploaded to server.
3) On receiving the data, a Hiding algorithm[11] is applied which randomly selects the bits positions from images where data is to be stored. The bit position is either 0th, 1st or 2nd position.
4) This Hiding algorithm[11] is used to save the files or data behind the images. This process is called Steganography.

B. Retrieval Process

Retrieval process is explained in the following steps:

1) When user demands data, Retrieval algorithm extracts images and separates user data from the decrypted data.
2) This extracted data is then sent to client.
3) On client side, the encrypted data is decrypted using RC6 algorithm and the original data is retrieved.

V. ENCRYPTION ALGORITHM USING RC6

RC6, like RC5, consists of three components: a key expansion algorithm, an encryption algorithm, and a decryption algorithm. Select a file to store in the cloud before applying RC6 algorithm. Read a selected file and convert data into byte array. Then perform following operations:

1. Key Expansion

The key expansion algorithm is used to expand the user-supplied key to fill an expanded array S, so S resembles an array of t random binary words. The user must supply a key of b bytes, where 0 ≤ b ≤ 255, and from which (2r+4) words are derived and stored in a round key array. Zero bytes are appended to give the key length equal to a “non-zero integral number”. The (2r+4) derived words are stored in array for later decryption or encryption.
2. Encryption and Decryption Function

The \((2r+4)\) derived words i.e. the key must be passed in the form of a byte array. The Encryption function returns encrypted data in the form of byte array. The data in this byte array is stored in the cloud. When a client requires some data from cloud, Decryption Function is applied on the data. The obtained decrypted data is stored in a temporary file. User now can view their required data from this temporary file.

VI. CONCLUSION

This paper deals with data security issues related to cloud. The above mentioned algorithm revolves around the problem of data security and with the help of encryption at client side and steganography at server side it provides a highly secure model. Symmetric algorithms gives better performance in terms of speed when compared to asymmetric algorithm, while Asymmetric algorithms provide better security when compared with symmetric algorithm. RC6 algorithm gives better performance in terms of speed when compared to AES algorithm.

REFERENCES


Authors Profile

Ms. Sirsha Aguru pursued Bachelor of Technology from Jawaharlal Nehru Technological University, Kakinada in 2005 and Master of Science from Jawaharlal Nehru Technological University in 2012. She is currently working as Assistant Professor in the Department of Computer Science and Engineering, Srivasavi Engineering College, Autonomous since 2007. She is a life time member of CSI.

Mr. Batteri Madhava Rao pursued Master of Science from Jawaharlal Nehru Technological University in 2010. He is currently working as Assistant Professor in the Department of Computer Science and Engineering, Srivasavi Engineering College, Autonomous since 2007. He is a life time member of CSI.