Original Article

Encryption Algorithm for Data Security and Privacy in Cloud Storage

Manisha R. Shinde* and Rahul D. Taur

Radhai Mahavidyalaya, Aurangabad, Maharashtra, India

Address for Correspondence

Radhai Mahavidyalaya, Aurangabad, Maharashtra, India.
E-mail: mnisha.shinde@gmail.com

ABSTRACT

Cloud computing is the concept implemented to decipher the Daily Computing Problems. Cloud computing is basically virtual pool of resources and it provides these resources to users via internet. Cloud computing is the internet based development and used in computer technology. The prevalent problem associated with cloud computing is data privacy, security, anonymity and reliability etc. But the most important between them is security and how cloud provider assures it. In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using encryption algorithms to enhance the security in cloud as per different perspective of cloud customers. Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private key encryption to hide the sensitive data of users, and cipher text retrieval. The paper analyzes the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage.

Keywords: Cloud, Cloud storage, Cipher text retrieval, Encryption algorithm.

INTRODUCTION

Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or consumer IT services over the Internet. Cloud computing supports distributed service oriented architecture, multi-users and multi-domain administrative infrastructure, it is more prone to security threats and vulnerabilities. At present, a major concern in cloud adoption is its security and Privacy. Intrusion prospects within cloud environment are many and with high gains. Security and Privacy issues are of more concern to cloud service providers who are actually hosting the services. In most cases, the provider must guarantee that their infrastructure is secure and clients' data and applications are safe by implementing security policies and mechanisms. While the cloud customer must ensure that provider has taken proper security measures to protect their information. The issues are organized into several general categories: trust, architecture, identity management, software isolation, data protection, availability Reliability, Ownership, Data Backup, Data Portability and Conversion,

Multiplatform Support and Intellectual Property.

OBJECTIVE OF OUR SYSTEM

1. To develop a system that will Provide Security and Privacy to Cloud Storage.
2. To Establish an Encryption Based System for protecting Sensitive data on the cloud and Structure how owner and storage Service Provider to operate on encrypted Data.
3. To Create a System where the user store its data on the cloud the data is sent and stored on the cloud in encrypted form As in normal cases in cloud computing when a user login to the cloud and they store data on cloud storage device the data stored on the server cloud is not much secure as it can be readable to anyone which have permission to access and Leaving data vulnerable.
4. To Develop a retrieval System in which the data is retrieved by the user in encrypted form and is decrypted by the user at its own site using a public and private key encryption both the keys working at the user level.

Cloud deployment models

There are three types cloud Deployment models that widely used are:

Public

It is referred as external cloud or multi-tenant cloud, this model represents an openly accessible cloud environment in this cloud can be accessed by general public. Customer can access resources and pay for the operating resources. Public Cloud can host individual services as well as collection of services.

Private

It is also known as internal cloud or on-premise cloud, a private cloud provides a limited access to its resources and services to consumers that belong to the same organization that owns the cloud. In other words, the infrastructure that is managed and operated for one organization only, so that a consistent level of control over security, privacy, and governance can be maintained.

Hybrid

A hybrid cloud is a combination of public and private cloud. It provides benefits of multiple deployment models. It enables the enterprise to manage steady-state workload in the private cloud, and if the workload increases asking the public cloud for intensive computing resources, then return if no longer needed.

Community

This deployment model share resources with many organizations in a community that shares common concerns (like security, governance, compliance etc). It typically refers to special-purpose cloud computing environments shared and managed by a number of related organizations participating in a common domain or vertical market. (See figure 1.)

Benefits of cloud computing

- Cloud Computing has numerous advantages. Some of them are listed below:
- One can access applications as utilities, over the Internet.
- Manipulate and configure the application online at any time.
- It does not require to install a specific piece of software to access or manipulate cloud application.
- Cloud Computing offers online development and deployment tools, programming runtime environment through Platform as a Service model.

- Cloud resources are available over the network in a manner that provides platform independent access to any type of clients.
- Cloud Computing offers on-demand self-service. The resources can be used without interaction with cloud service provider.
- Cloud Computing is highly cost effective because it operates at higher efficiencies with greater utilization. It just requires an Internet connection.
- Cloud Computing offers load balancing that makes it more reliable.

Compute clouds

Compute clouds allow access to highly scalable, inexpensive, on-demand computing resources that run the code that they're given. Three examples of compute clouds are

• Amazon's EC2

• Google App Engine

• Berkeley Open Infrastructure for Network Computing (BOINC)[10].

Compute clouds are the most flexible in their offerings and can be used for sundry purposes; it simply depends on the application the user wants to access. You could close this book right now, sign up for a cloud computing account, and get started right away. These applications are good for any size organization, but large organizations might be at a disadvantage because these applications don't offer the standard management, monitoring, and governance capabilities that these organizations are used to. Enterprises aren't shut out, however. Amazon offers enterprise-class support and there are emerging sets of cloud offerings like Terre mark's Enterprise Cloud, which are meant for enterprise use.

Issues in cloud data storage

Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud.

Trust

Trust is defined as reliance on the integrity, strength, ability and surety of a person or thing. Entrusting your data on to a third party who is providing cloud services is an issue.

Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

Security

Cloud service providers employ data storage and transmission encryption, user authentication, and authorization. Many clients worry about the vulnerability of remote data to criminals and hackers. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigate this problem.

Ownership

Once data has been relegated to the cloud, some worry about losing their rights or being unable to protect the rights of their

customers. Many cloud providers address this issue with well-skilled user-sided agreements. According to the agreement, users would be wise to seek advice from their favorite legal representative.

Performance and availability

Business organizations are worried about acceptable levels of performance and availability of applications hosted in the cloud.

Data backup

Cloud providers employ redundant servers and routine data backup processes, but some people worry about being able to control their own backups. Many providers are now offering data dumps onto media or allowing users to back up data through regular downloads.

Proposed algorithm

Proposed technique emphasizes on improving classical encryption techniques by integrating substitution cipher and transposition cipher. Both substitution and transposition techniques have used alphabet for cipher text. In the proposed algorithm, initially the plain text is converted into corresponding ASCII code value of each alphabet. In classical encryption technique, the key value ranges between 1 to 26 or key may be string (combination alphabets). But in proposed algorithm, key value range between 1 to 256. This algorithm is used in order to encrypt the data of the user in the clouds. Since the user has no control over the data after his session is logged out, the encryption key acts as the primary authentication for the user. Proposed algorithm is described below.

Encryption algorithm

Followings are the steps in proposed encryption algorithm.

Encryption Algorithm

Step 1

Count the No. of character (N) in the plain text without space.

Step 2

Convert the plain text into equivalent ASCII code. And form a square matrix (S X S >=N).

Step 3

Apply the converted ASCII code value from left to right in the matrix. Divide matrix into three part namely upper, diagonal and lower matrix.

Step 4

Read the value from right to left in each matrix.

Step 5

Each matrix use three different key K=K1, K2, K3 for encryption. Do the encryption.

Step 6

Apply the encrypted value into the matrix in the same order of upper, diagonal and lower.

Step 7

Read the message by column by column. Here the order in the columns read from the matrix is the key K4.

Step 8

Convert the ASCII code into character value.

Overview of our approach

Our goal is to build up a repository to facilitate the data integration and sharing across cloud along with preservation of data confidentiality. For this we will be using an encryption technique to provide data security on data storage.

CONCLUSION

Our research indicates that that Security and Privacy are the major issues that are needed to be countered, efforts are being made to develop many efficient System That can Provide Security and privacy at the user level and maintain the trust and intellectual property rights of the user. Our method States Encryption is one such method that can provide peace of mind to user and if the user have control over encryption and decryptions of data that will boost consumer confidence and attract more people to cloud platform.

REFERENCES

1. http://en.wikipedia.org/wiki/Cloud_computing.
2. Rich Maggiani,solari communication. "Cloud computing is changing how we communicate".
3. Randolph Barr, Qualys Inc, "How to gain comfort in losing control to the cloud".
4. Greg Boss, Padma Malladi, Dennis Quan, Linda Legregni,Harold Hall, HiPODS, www.ibm.com/ developerworks/ websphere/ zones/hipods.
5. http://www.roughtype.com.
6. Tharam Dillon, Chen Wu, Elizabeth Chang, 2010 24th IEEE International Conference on Advanced Information Networking and Applications, "Cloud computing: issues and challenges".
7. Armbrust, Fox, Griffith, Joseph, "Above the clouds:A Berkeley view of cloud computing"[2009].
8. Buyya, Venugo, "Cloud Computing and emerging IT platforms: Vision, hype, and reality for delivering Computing as the 5th Utility", [2008].
9. Caceres, Lindner, Vaquero, "A break in the clouds:towards a cloud definition", [2008].
10. Keahey, Fortes, Freeman, "Science Clouds:Early Experiences in Cloud Computing for scientific applications" [2008].
11. Moretti, Thain, Flynn, "All-pairs: An abstraction for data inexpensive cloud computing", [2008].
12. Nurmi, Woloski, Obertelli, "The Eucalyptus Opensource Cloud computing" [2009].
13. Quist-Aphetsi Kester, "A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher", International Journal of Advanced Technology & Engineering Research (IJATER), Volume 3, Issue 1, pp 141-147, 2013.
14. Dr. A. Padmapriya, P. Subhasri," Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security", International Journal of Engineering Trends and Technology (IJETT) – Volume 4, Issue 4, pp 1067-1071, 2013.

 ISSN 2349 – 7238

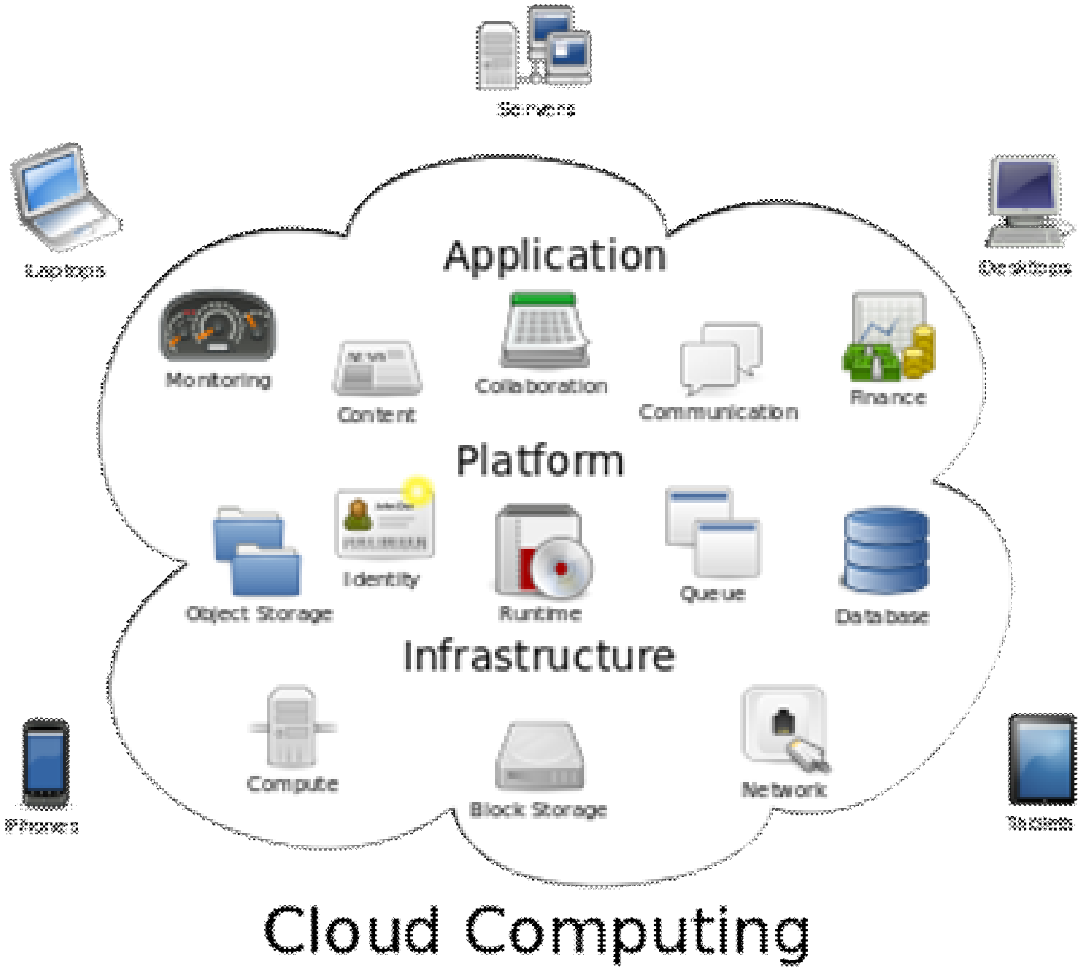

Figure 1. Cloud computing