Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 6, May-2019, ISSN 2230-7540

Privacy of Big Data in Cloud Computing for Super Marketing

Dibakar Panigrahi*

Research Scholar, Pacific University, Udaipur, Rajasthan

Abstract – Cloud computing is a technological advancement that focuses on the way in which we design computing systems, develop applications, and leverage existing services for building software. It is based on the concept of dynamic provisioning, which is applied not only to services, but also to compute capability, storage, networking, and Information Technology (IT) infrastructure in general. Resources are made available through the Internet and offered on a pay-per-use basis from Cloud computing vendors. Today, anyone with a credit card can subscribe to Cloud services, and deploy and configure servers for an application in hours, growing and shrinking the infrastructure serving its application according to the demand, and paying only for the time these resources have been used.

This vision of computing utilities based on a service provisioning model anticipated the massive transformation of the entire computing industry in the 21st century whereby computing services will be readily available on demand, like other utility services such as water, electricity, telephone, and gas available in today's society. Similarly, users (consumers) need to pay providers only when they access the computing services. In addition, consumers no longer need to invest heavily, or encounter difficulties in building and maintaining complex IT infrastructure.

Keywords – Cloud Computing, Model, Resource

----------X----------

INTRODUCTION

In such a model, users access services based on their requirements without regard to where the services are hosted. This model has been referred to as utility computing, or recently (since 2007) as Cloud computing. The latter term often denotes the infrastructure as a "Cloud" from which businesses and users can access applications as services from anywhere in the world on demand. Hence, Cloud computing can be classified as a new paradigm for the dynamic provisioning of computing services supported by state-of-the-art data centers employing virtualization technologies for consolidation and effective utilization of resources.

The concept expressed above has strong similarities with the way we make use of other services such as water and electricity. In other words, Cloud computing turns IT services into utilities. Such a delivery model is made possible by the effective composition of several technologies, which have reached the appropriate maturity level. Web 2.0 technologies play a central role in making Cloud computing an attractive opportunity for building computing systems. They have transformed the Internet into a rich application and service delivery platform, mature enough to serve complex needs. Service-orientation allows Cloud computing to deliver its capabilities with familiar abstractions while virtualization confers Cloud computing the necessary degree of customization, control, and flexibility for building production and enterprise systems.

Besides being an extremely flexible environment for building new systems and applications, Cloud computing also provides an opportunity for integrating additional capacity, or new features, into existing systems. The use of dynamically provisioned IT resources constitutes a more attractive opportunity than buying additional infrastructure and software, whose sizing can be difficult to estimate and needs are limited in time. This is one of the most important advantages of Cloud computing, which made it a popular phenomenon. With the wide deployment of Cloud computing systems, the foundation technologies and systems enabling them are getting consolidated and standardized. This is a fundamental step in the realization of the long-term vision for Cloud computing, which provides an open environment where computing, storage, and other services are traded as computing utilities.

Cloud computing allows anyone having a credit card to provision virtual hardware, runtime environments, and services. These are used for as long as needed and no upfront commitments are required. The entire stack of a computing system is transformed into a collection of utilities, which can be provisioned and composed together to deploy systems in hours, rather than days, and with virtually no maintenance costs. This opportunity, initially met with skepticism, has now become a practice across several application domains and business sectors. The demand has fast-tracked the technical development and enriched the set of services offered, which have also become more sophisticated and cheaper.

Despite its evolution, the usage of Cloud computing is often limited to a single service at time or, more commonly, a set of related services offered by the same vendor. The lack of effective standardization efforts made it difficult to move hosted services from one vendor to another. The long term vision of Cloud computing is that IT services are traded as utilities in an open market without technological and legal barriers.

In this Cloud marketplace, Cloud service providers and consumers, trading Cloud services as utilities, play a central role. Many of the technological elements contributing to this vision already exist. Different stakeholders leverage Clouds for a variety of services. The need for ubiquitous storage and compute power on demand is the most common reason to consider Cloud computing. A scalable runtime for applications is an attractive option for application and system developers that do not have infrastructure or cannot afford any further expansion of existing one.

These are all possibilities that are introduced with the establishment of a global Cloud computing market place and by defining an effective standard for the unified representation of Cloud services as well as the interaction among different Cloud technologies. A considerable shift towards Cloud computing has already been registered, and its rapid adoption facilitates its consolidation. Moreover, by concentrating the core capabilities of Cloud computing into large datacenters, it is possible to reduce or remove the need for any technical infrastructure on the service consumer side. This approach provides opportunities for optimizing datacenter facilities and fully utilizing their capabilities to serve multiple users. This consolidation model will reduce the waste of energy and carbon emission, thus contributing to a greener IT on one end, and increase the revenue on the other end.

PROPOSED SYSTEM

Nowadays Cyber Criminals can easily access data storage. In Personal Cloud Storage important data, files and records are entrusted to a third party, which enables Data Security to become the main security issue in Cloud Computing. In Cloud Storage any organization‟s or individual‟s data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task.

A. System Analysis

A document management system (DMS) is a system used to track, manage and store documents. Most are capable of keeping a record of the various versions created and modified by different users. Generally, Organizations or individual uses Premise-based document management system. But Premise-based document management systems are not reliable, they have following limitations.

- Initial investment is high.
- The logistics of capturing, storing, retrieving, indexing, sharing, and securitizing documents is complex.
- It needs software licenses, server modules, hardware and need to assign storage, databases, and web servers.
- Did not provide Top Level Security

Because of these limitations, each and every organization is moving its data to the cloud based document management system, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc. In Cloud Storage any organization‟s or individual‟s data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task.

B. System Architecture

The proposed system is designed to maintain security of files. The name of our system is "Cloud-Based Document Management System" or "Cloud-Based DMS". Our System provides Software-as-a Service (SaaS) document management solutions. Cloud-based DMS uses an enterprise’s existing equipment eliminating the need for high-powered servers or complex onsite architectures. The following figure illustrates the architecture of cloud-based Document Management System (DMS).

The proposed system architecture focuses on the following objectives which are helpful in increasing the security of data storage.

Scalability:

The system is scalable because it provides server, storage capabilities and collaboration from one to thousands of users.

Security:

The cloud offers better security by using multilevel encryption. Also, you're able to quickly and easily recover files if they lose during a break-in, network breach or natural disaster.

Use of Web Browser:

Cloud-based DMS is available through a simple Web browser Internet connection. The system needs little or no software to install; no firewalls to configure; no backups to set up.

Storage and Backup:

The system scrambled the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage using multilevel encryption algorithms.

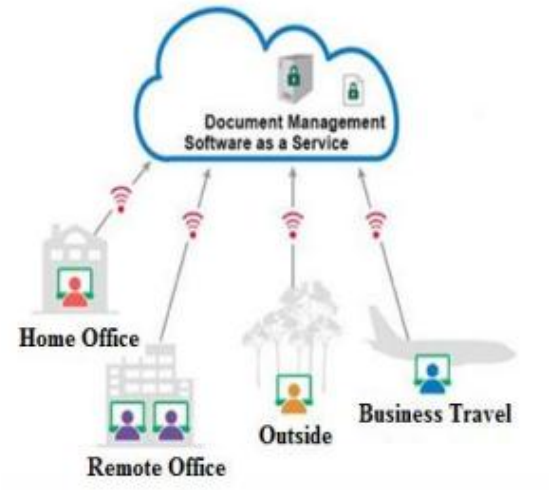

Fig. 1. Architecture of Cloud-Based DMS

C. Proposed System Design

The proposed system "Cloud-Based DMS" is designed to maintain security of data files stored in cloud. This proposed system is a combination of two different security algorithms to eliminate the security challenges of Personal Cloud Storage. We have taken a combination of algorithms like: DES and RSA. DES (Data Encryption Standard) is a symmetric key algorithm, in which a single key is used for both encryption/decryption of data.

Whereas RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. A user can upload data files such as text, mp3, images, pdf etc in Personal Cloud Storage. While uploading file DES and RSA Encoding schemes are used to encrypt data.

The steps of Multi-tier encryption will be as follows;

- Upload the file
- Now implementation of DES Algorithm takes place. The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The actual key used by DES algorithm for encryption is 56 bits in length. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds.
- DES has 16 rounds, means the main algorithm is repeated 16 times to produce cipher text. As number of rounds increases, the security of system increases exponentially.
- The first level encryption is generated using DES algorithm.
- Now apply RSA algorithm on encrypted output of DES algorithm to generate second level encryption.
- In RSA algorithm public key is used for encryption. RSA is a Block Cipher in which every message is mapped to an integer.
- Once the data is encrypted using RSA algorithm, it will be stored in Database of Cloud Storage.

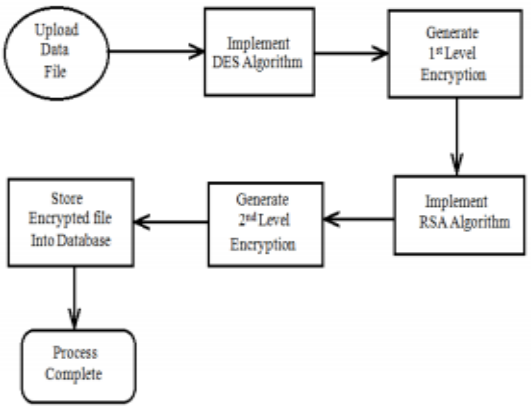

Fig. 2: Block diagram of Multi-tier Encryption

And while downloading file inverse DES and RSA algorithms are used to decrypt data. The Block Diagram of proposed work at multilevel decryption is shown in following figure 3.

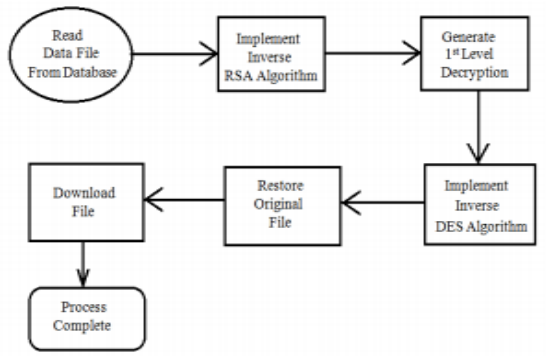

Fig. 3: Block diagram of Multi-tier Decryption

As Shown in figure 3, the steps of Multi-tier decryption will be as follows;

1. Inverse DES and RSA algorithms are used to decrypt data

2. First apply the Inverse RSA algorithm (decryption scheme) using private key. This algorithm will generate first level decrypt data

3. Now apply the DES decryption algorithm on first level decrypted data.

4. DES decryption algorithm uses the same 56 bit length key for decryption.

5. DES algorithm of decryption will generate Plain text.

6. Now Plain Text will be displayed to the User.

In Our proposed System, implementation of the DES algorithm takes place to generate first level encryption. And then we apply the RSA algorithm on the encrypted output of DES algorithm to generate second level encryption. And same process takes place for decryption using inverse DES and RSA algorithms. Means we applied multi-tier Encryption and Decryption to cloud-based DMS for security purpose.

CONCLUSION AND FUTURE SCOPE

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. Encryption algorithms play an important role in data security on cloud. But these existing cryptographic algorithms are single level encryption algorithms. Cyber criminals can easily cracked single level encryption. Hence we propose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage. In our proposed work, only the authorized user can access the data. If some intruder (unauthorized user) tries to get the data directly from the database, he must have to decrypt the data at each level which is a very difficult task. It may be expected that multilevel encryption will provide more security for Cloud Storage than single level encryption.

FUTURE SCOPE

We are working on betterment of decryption techniques. The decryption techniques must be more precise as compared to what we have presently. The applied multilevel decryption algorithm needs to be modified so as to improve the decryption of files. Thus in a nutshell, further experiments are required to confirm these justifications. In addition, firewall and VPN (Virtual Private Network) technology will be improved to protect data transfer. These are some justifications that are expected in the future, the future of cloud based DMS is not limited to these justification.

REFERENCES

[1] A. L. Jeeva, Dr. V. Palanisamy, K. Kanagaram (2012). “Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms” International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp. 3033-3037.

[2] Neha Jain, Gurpreet Kaur (2012). "Implementing DES Algorithm in Cloud for Data Security", VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321.

[3] Brian Hay, Kara Nance, Matt Bishop (2011). “Storm Clouds Rising: Security Challenges for IaaS Cloud Computing” Proceedings of the 44th Hawaii International Conference on System Sciences, pp. 1-7.

[4] Kevin Curran, Sean Carlin, Mervyn Adams (2011). “Security issues in cloud computing”, Elixir Network Engg.38 (2011), pp. 4069-4072.

[5] Randeep Kaur, Supriya Kinger (2014). "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847), Volume-3 Issue-3, pp. 171-176.

[6] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI (2012). “Homomorphic Encryption Applied to the Cloud Computing Security”, World Congress on Engineering, Volume I, ISBN: 978- 988-19251-3-8;

ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online).

[7] Dr. Chander Kant, Yogesh Sharma (2013). "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3 Issue 5, pp. 571-575.

[8] S. C. Rachana, Dr. H. S. Guruprasad (2014). “Emerging Security Challenges in Cloud Computing”, International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3 Issue 2, pp. 485-490.

Corresponding Author

Dibakar Panigrahi*

Research Scholar, Pacific University, Udaipur, Rajasthan