
NEED AND IMPORTANCE OF SECURITY OF DATA IN CLOUD COMPUTING

***Dr. Gnyanganga Vishwanath**

*Guest Lecturer, Department Computer Science, Government First Grade College, Bidar

ABSTRACT

Cloud computing is an innovative progression that spotlights on the manner by which we design computing systems, foster applications, and influence existing services for building software. It is based on the idea of dynamic provisioning, which is applied not exclusively to services, yet additionally to figure capability, storage, networking, and Information Technology (IT) infrastructure overall. Resources are made accessible through the Internet and presented on a compensation for every utilization premise from Cloud computing sellers. Today, anybody with a credit card can buy into Cloud services, and send and configure servers for an application in hours, developing and contracting the infrastructure serving its application as indicated by the interest, and paying just for the time these resources have been utilized.

This vision of computing utilities based on a service provisioning model expected the monstrous change of the whole computing industry in the 21st century by which computing services will be promptly accessible on request, as other utility services like water, electricity, phone, and gas accessible in the present society. Also, users (customers) need to pay suppliers just when they access the computing services. In addition, customers never again need to contribute vigorously, or experience troubles in building and keeping up with complex IT infrastructure.

KEYWORDS:

Cloud computing, model, resource

INTRODUCTION

In such a model, users access services based on their prerequisites without respect to where the services are facilitated. This model has been alluded to as utility computing, or as of late (beginning around 2007) as Cloud computing. The last option term regularly signifies the infrastructure as a "Cloud" from which organizations and users can get to applications as services from anyplace on the planet on request. Henceforth, Cloud computing can be delegated another worldview for the dynamic provisioning of computing services upheld by best in class data focuses utilizing virtualization innovations for solidification and successful use of resources.

The idea communicated above has solid similarities with the manner in which we utilize different services like water and electricity. As such, Cloud computing transforms IT services into utilities. Such a conveyance model is made conceivable by the compelling composition of a few advancements, which have arrived at the proper maturity level. Web 2.0 advances assume a focal part in making Cloud computing an appealing opportunity for building computing systems. They have changed the Internet into a rich application and service conveyance stage, mature to the point of serving complex requirements. Service-direction permits Cloud computing to convey its capabilities with recognizable reflections while virtualization gives Cloud computing the fundamental level of customization, control, and flexibility for building creation and endeavor systems.

Besides being a very adaptable climate for building new systems and applications, Cloud computing likewise provides an opportunity for incorporating additional capacity, or new elements, into existing systems. The utilization of progressively provisioned IT resources constitutes a more alluring opportunity than purchasing additional infrastructure and software, whose measuring can be hard to gauge and needs are limited on schedule. This is one of the main benefits of Cloud computing, which made it a well known peculiarity. With the wide sending of Cloud computing systems, the establishment advancements and systems empowering them are getting solidified and standardized. This is a basic advance in the acknowledgment of the drawn

out vision for Cloud computing, which provides an open climate where computing, storage, and different services are exchanged as computing utilities.

Cloud computing permits anybody having a credit card to arrangement virtual equipment, runtime conditions, and services. These are utilized however long required and no forthright commitments are required. The whole heap of a computing system is changed into an assortment of utilities, which can be provisioned and created together to send systems in hours, as opposed to days, and with virtually no support costs. This opportunity, initially met with suspicion, has now turned into a training across a few application areas and business areas. The interest has optimized the specialized turn of events and enhanced the arrangement of services offered, which have likewise become more refined and less expensive.

Despite its development, the utilization of Cloud computing is regularly limited to a solitary service at time or, all the more normally, a bunch of related services presented by a similar seller. The absence of compelling standardization endeavors made it hard to move facilitated services starting with one seller then onto the next. The drawn out vision of Cloud computing is that IT services are exchanged as utilities an open market without mechanical and legitimate obstructions.

In this Cloud commercial center, Cloud service suppliers and purchasers, exchanging Cloud services as utilities, assume a focal part. Large numbers of the mechanical components adding to this vision as of now exist. Various partners influence Clouds for an assortment of services. The requirement for ubiquitous storage and figure power on request is the most well-known motivation to consider Cloud computing. A scalable runtime for applications is an appealing choice for application and system developers that don't have infrastructure or can't manage the cost of any further extension of existing one.

These are for the most part possibilities that are presented with the foundation of a worldwide Cloud computing commercial center and by characterizing a powerful standard for the brought together portrayal of Cloud services as well as the communication among various Cloud advances. An extensive shift towards Cloud computing has previously been enlisted, and its fast

reception facilitates its union. In addition, by concentrating the center capabilities of Cloud computing into enormous datacenters, it is feasible to lessen or eliminate the requirement for any specialized infrastructure on the service buyer side. This approach provides opportunities for improving datacenter facilities and completely using their capabilities to serve multiple users. This solidification model will diminish the hopeless cause and fossil fuel byproduct, along these lines adding to a greener IT toward one side, and increment the income on the opposite end.

PROPOSED SYSTEM

Presently a-days Cyber Criminals can without much of a stretch access data storage. In Personal Cloud Storage significant data, files and records are shared with an outsider, which empowers Data Security to turn into the principle security issue in Cloud Computing. In Cloud Storage any association's or alternately individual's data is stored in and open from multiple distributed and associated resources that contain a cloud. To give secure communication over distributed and associated resources authentication of stored data turns into a compulsory errand.

A. System Investigation

A document management system (DMS) is a system used to follow, oversee and store documents. Most are fit for tracking the different versions made and adjusted by various users. By and large, Organizations or individual purposes Reason based document management system. However, Reason based document management systems are not solid, they have following limitations.

- Initial speculation is high.
- The operations of catching, putting away, recovering, ordering, sharing, and it is complicated to securitizing documents.
- It needs software licenses, server modules, equipment and have to relegate storage, databases, and web servers.
- Didn't give High Level Security

Due to these limitations, every single association is moving its data to the cloud based document management system, implies it utilizes the storage service given by the cloud supplier. So there is a need to safeguard that data against unapproved access, adjustment or refusal of services and so on. In Cloud Storage any association's or alternately individual's data is stored in and available from multiple distributed and associated resources that contain a cloud. To give secure communication over distributed and associated resources authentication of stored data turns into a required undertaking.

B. System Architecture

The proposed system is designed to keep up with 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 utilizes a venture's current hardware disposing of the requirement for powerful servers or complex onsite architectures. The accompanying figure represents the architecture of cloud-based Document Management System (DMS).

The proposed system architecture centers around the accompanying targets which are useful in expanding the security of data storage.

Scalability:

The system is scalable on the grounds that it provides server, storage capabilities and joint effort from one to thousands of users.

Security:

The cloud offers better security by utilizing multilevel encryption. Additionally, you're ready to rapidly and effectively recuperate files in the event that they lose throughout a break-in, network break or catastrophic event.

Utilization of Web Browser:

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

Storage and Backup:

The system mixed the substance of the data, like text, picture, sound, video, etc to make the data garbled, undetectable or trivial during transmission or storage utilizing multilevel encryption algorithms.

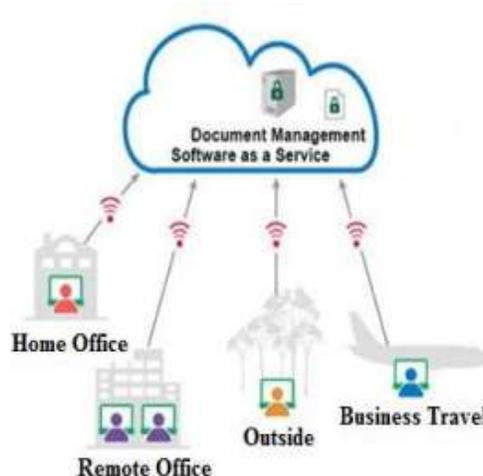


Fig. 1: Architecture of Cloud-Based DMS

C. Proposed System Design

The proposed system "Cloud-Based DMS" is designed to keep up with security of data files stored in cloud. This proposed system is a mix of two unique security algorithms to dispense with the security difficulties of Personal Cloud Storage. We have taken a blend of algorithms like: DES and RSA. DES (Data Encryption Standard) is a symmetric key algorithm, where a solitary key is utilized for both encryption/decryption of data.

Though RSA is a lopsided key algorithm, the algorithm that involves different keys for encryption and decryption purposes. A user can upload data files like text, mp3, images, pdf and so on in Personal Cloud Storage. While uploading file DES and RSA Encoding plans are utilized to encrypt data.

The means of Multi-tier encryption will be as per the following;

- Upload the file

- Presently execution of DES Algorithm happens. 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 contribution to DES, which produces 64 bits of cipher text. The genuine key utilized by DES algorithm for encryption is 56 bits long. The encryption cycle is made of two permutations (P-boxes), which we call initial and last permutation, and sixteen Feistel rounds.
- DES has 16 rounds, implies the fundamental algorithm is rehashed 16 times to create cipher text. As number of rounds builds, the security of system increments dramatically.
- The main level encryption is created utilizing DES algorithm.
- Presently apply RSA algorithm on encrypted result of DES algorithm to produce second level encryption.
- In RSA algorithm public key is utilized for encryption. RSA is a Block Cipher in which each message is planned to a whole number.
- When the data is encrypted utilizing RSA algorithm, it will be stored in Database of Cloud Storage.

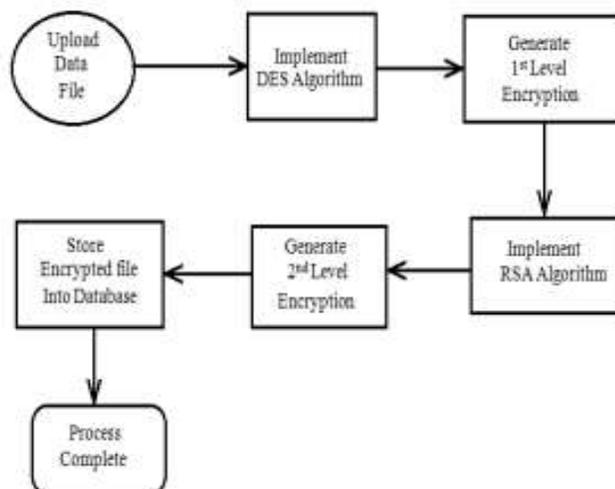


Fig. 2: Block diagram of Multi tier Encryption

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.

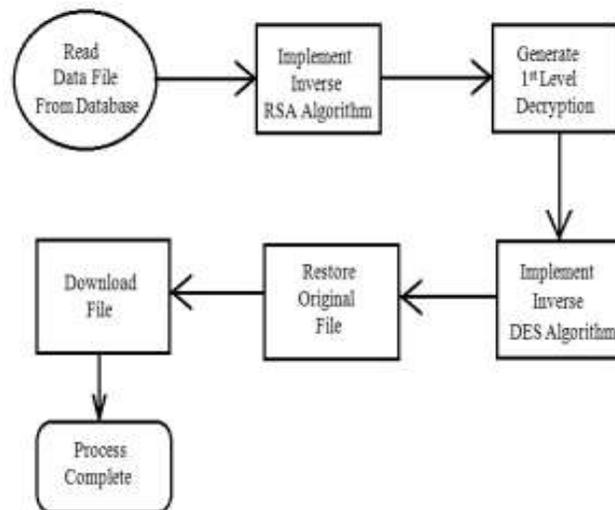


Fig. 3: Block diagram of Multi-tier Decryption

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, execution of the DES algorithm happens to create first level encryption. And afterward we apply the RSA algorithm on the encrypted result of DES algorithm to create second level encryption. What's more, same interaction happens for decryption utilizing inverse DES and RSA algorithms. Implies we applied multi tier Encryption and Decryption to cloud-based DMS for security reason.

CONCLUSION

Cloud computing is arising as another thing and a large number of the organizations are pushing toward the cloud yet missing because of security reasons. So cloud security is must which will break the prevention the acknowledgment of the cloud by the organizations. Encryption algorithms assume a significant part in data security on cloud. However, these current cryptographic algorithms are single level encryption algorithms. Cyber criminals can undoubtedly broke single level encryption. Henceforth we propose a system which involves multilevel encryption and decryption to give greater security to Cloud Storage.

In our proposed work, just the approved user can get to the data. If some interloper (unapproved user) attempts to get the data straightforwardly from the database, he should need to decrypt the data at each level which is an undeniably challenging undertaking. It might be normal that multilevel encryption will give more security to Cloud Storage than single level encryption.

We are working on advancement of decryption procedures. The decryption methods should be more exact when contrasted with what we have as of now. The applied multilevel decryption algorithm should be changed in order to work on the decryption of files. In this manner more or less, further investigations are expected to affirm these avocations. In addition, firewall and VPN (Virtual Private Network) technology will be improved to safeguard data move. These are a few defenses that are normal later on, the eventual fate of cloud based DMS isn't limited to these avocation.

REFERENCES

- [1] AL. Jeeva, Dr. V.Palanisamy, K.Kanagaram, "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, May-Jun 2012.
- [2] Neha Jain, Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security", VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

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

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

[5] Randeep Kaur, Supriya Kinger, "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, March 2014.

[6] Maha TEBA, Saïd EL HAJJI, Abdellatif EL GHAZI, “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) , 2012.

[7] Dr. Chander Kant, Yogesh Sharma, "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, May 2013.

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