ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURITY FOR DATA STORAGE IN CLOUD COMPUTING

Prof. S.A.Gade*, Mukesh P.Patil, Ganesh D. Bagul
* Project Guide SVIT, Chincholi, Computer Department.

ABSTRACT

Cloud computing is nothing but a specific style of computing where everything from computing power to business apps are provided facility. This application moves the various data to the large data centers through computing where security provided fully trustworthy.

The data stored in the cloud may be frequently updated by the users (registered user) including actions like insertion, deletion, modification etc. To ensure that data storage in cloud this web application implements. This application is implemented to protecting data from unauthorized disclosure and modification. Cloud information security can encrypt & decrypt data, generate OTP (one time password) and transfer file.

INTRODUCTION

From initial concept building application to current actual deployment, cloud computing is growing so fast. Now a day in many industries, like Small Scale and medium industries are increasingly by submitting their various application and data into the cloud. The use of cloud computing may lead to gains in efficiency lead to gains in efficiency and effectiveness in developing and deployment the application. And to save the cost in purchasing and maintaining the environment made by cloud.

Centralized data store is a suitable model for the online access to computer services or resources on-demand network access or to shared resources like application or peripheral devices connected to network with minimum effort or service provider interaction.

Commonly security issues are not managing properly in cloud. But as industries boundaries have been extended to the cloud, so traditional security mechanisms are no longer for application and data in cloud.

In this paper we describe the data security through data can be transfer from one place to another place. And user can manage privacy through authentication in cloud environment. In this paper 2nd section describe that what data transfer on network in cloud resources.3rd section shows how security can be managed.4th section shows solution for protecting data. And 5th section recaps the work done.

PROPOSED SYSTEM

The main objectives of this project is to establish the precision of user's data in the cloud, we introduce a powerful and extensible scheme with two features. By handling the OTP (One Time Password) token with confirmation of encrypted data. Our design manages the sending of file from sender to licensed receiver surly and data without loss. Unlike most prior works, the new scheme further supports secure and efficient runtime operations on data section. Large security and working analysis shows that the suggested scheme is deeply efficient and elastics against failure like Byzantine or malicious and server colluding attacks.

SYSTEM ARCHITECTURE

In cloud computing system there are number of security problem identified and they can be field into any number of element. In cloud system information are carried from client to server by using Cloud Service Provider (CSP) and security is main aspects.

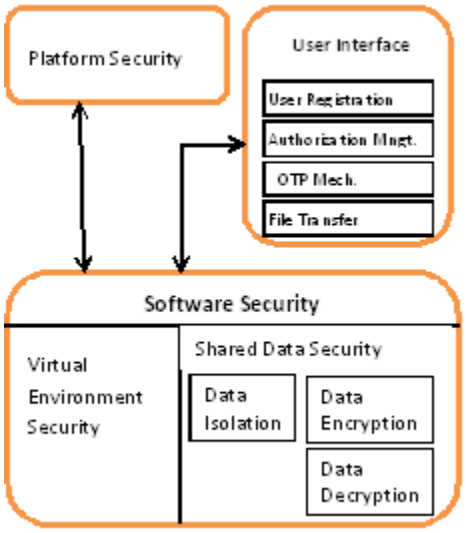

Fig 1: Data Security Architecture

For the security purpose following are certain conditions:

1. Developing the threat of attacks.
2. Rapidly growth of networking for information sharing.
3. Absence of particular resources that can affect the securing system. In the network level, host level, application level there are security issues in all aspects of the infrastructure.

- Platform Security:
  We know that there are various type platforms as Linux, windows etc. And every OS has their different security mechanism and Kernel runs security mechanism
- Software Security:
  Virtual Environment Security- It is the security of our application. That security provided by system OS.
  Shared Data Security- It include following subpart as,

Data Isolation: - primarily data that we will Transfer to other system which are stored in own system. The data are isolated before take part in cloud computing.

Data Encryption: - before sending data to other user it will be encrypted for the security purpose.

Data Decryption: - data decryption can be decrypted by only authenticate person by using the OTP(One Time Password)

- User Interface:
  - ✓ User Registration
  - ✓ Authorization Management
  - ✓ OTP Mechanism
  - ✓ File Transfer

ALGORITHMS

In this we are using RSA algorithm.

The algorithm was designed by Ron Rivest, Adi Shamir and Leonard Adleman and it's their last names which make up the name of the algorithm. The RSA algorithm is given in following steps.
1. Two prime numbers p and q are taken.
2. A new number n is calculated by multiplying p and q.

n=pq

3. Another number φ(n) is generated by using formula:

φ (n)= (p-1)(q-1)

4. Another integer e is to be found such that e lies between 1 and φ(n). Also, e and φ(n) must be coprimes. Mathematically

1 < e < φ(n)Where

gcd(e,φ(n))=1

(gcd=Greatest Common Divisor)

5. Another number d is to be found such that

de % mod(φ(n))=1

i.e. when the product d and e is divided by mod (φ(n)), the remainder should be 1.

The number e and n make up the public key, while d and n make up the private key. The calculation is given as follows (m is the message to be encrypted and c is cipher text produced after encryption):

For encryption $c=m^e(\text{mod } n)$

For decryption $m=c^d(\text{mod } n)$

RESULT & DECLARATION

File Transfer:

In the file transfer user can be send file to another user. The snapshot can be given as below figure.

Fig 2: File Transfer

Inbox

In the inbox all incoming messages can be shown with detail like sender name, subject, date etc. The snapshot can be given as below figure.

OTP Generation

In the OTP generation one time password can be send to users verified mobile number and then other action like reading message or any other activity can be done by user.

CONCLUSION

We can conclude that this system provide security for data which is stored in cloud. System asks one time password to receive stored data and the password is generate by using RSA algorithm. If any unauthorized users try to access data without OTP then System will show encrypted data. In this way our system provides security to cloud data.

REFERENCE

[1] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," *Proc. of SecureComm '08*, pp. 1–10, 2008.
[2] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175, 2008, http://eprint.iacr.org/.
[3] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," *Proc. 11th USENIX Workshop on Hot Topics in Operating Systems (HOTOS '07)*, pp. 1–6, 2007.
[4] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," *Proc. of the 2003 USENIX Annual Technical Conference (General Track)*, pp. 29–41, 2003.
[5] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasurecoded Data," *Proc. 26th ACM Symposium on Principles of Distributed Computing*, pp. 139–146, 2007.
[6] Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," *Proc. of CCS '07*, pp. 584–597, 2007.
[7] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," *Proc. of IEEE INFOCOM*, 2009.
[8] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.