International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue:2 March-April 2017 p-ISSN: 2394-8280

SECURITY MODEL FOR SECURE STORAGE IN CLOUD ENVIRONMENT

Prativesh Pawar[1], Prof. Rashid Sheikh[2]
Computer Science and Engineering, M-Tech, Final year, Sri Aurobindo Institute of Technology
Indore, India, prativesh.sait@gmail.com
Associate Professor, Sri Aurobindo Institute of Technology , Indore, India
rashid.sheikh@sait.ac.in

ABSTRACT: ***The cloud computing is a technology used to organize and manage resources and services. Cloud based Web applications help for enabling convenient and on demand resource access with resource shared pool. Cloud Computing application provides platform for various computation, software access and data handling for betterment of proposed solution. Security is primary requirement to maintain trust and authenticity of information and services. This research work observes that there is big gap into security issue of existing system. Confidentiality, authentication, access control and integrity are the major ideology of security and one of the essential requirements for any software. This paper investigate existing solution for SaaS model of Cloud computing and explore the various flaw in context of security. Here, work concludes with the comparative study of different existing solution and address the common problems and excuses.***

Keywords: Hybrid Cloud, Mobile Authentication, OTP, RSA Algorithm

INTRODUCTION

Cloud computing technology is seen as the collection of internet based services for better utilizing the resources and services. It is the new utility which provides virtualization, parallel and distributed computing into single unit. It implies the sharing of resources to handle applications with reduces capital and low maintenance cost. It gives increased scalability and ease of access feature with low complexity.

Cloud computing can be defined " A model for enabling ubiquitous, convenient, on –demand network access to a shared pool of resources (e.g., networks, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Cloud security is the most critical task while considering its working environment, i.e. outsourced, distributed and utility based. In such cases making the users data confidential, increases the trust over the system. Also the security procedure does not make the availability affected in any ways. The users of these kind of systems is always retains the services and securities preliminaries with respect to data itself. As the cloud user can access its data frequently and if here some encryption is used which requires decryption and the repetitive process continues to increase the overheads. It requires some mechanism in which encryption

is performed and if the user requires performing some operations on secure file without decrypting it can be fulfilled. Thus encryption lets the user facilitates about the performing operations on encrypted data which reduces the complexity of confidentiality operations.

The cloud computing service can support the computer hardware or software resources to user conveniently. The cloud computing service can support the computer hardware or software resources to user conveniently. The cloud computing service can support the computer hardware or software resources to user conveniently.

But they are able occur privacy, availability, or man-in-the-middle attack problems in the wired or mobile communication environments. So, public cloud user is lower about 22%.The private cloud services can provide only users who are allowed from the inside of the enterprise. The private cloud service is very expensive method and it has many restrictions. So only the enterprises of 20% degree are using a service only from domestic. Therefore, hybrid cloud services are only hopeful services. This service selects strong points between the public cloud service and private cloud services. This service must agree network, database, and security services between service providers before make services. And this is a very difficult. Hybrid cloud services must understand secure weak points of private cloud services and public cloud services. And they must support a way of resolving the security threats. They must provide a secure authentication system for hybrid cloud services in mobile communication environments. Therefore, hybrid cloud service provider must understand secure weak points for private and public cloud service and they must support suitable security services to hybrid cloud service users such as user and device authentication service.

The purpose of the project is to find out the benefits and drawbacks in regards with data security and data availability; enterprise can have by the use of Cloud Computing for the implementation and management of their information system. Finally concluding the factors in terms of cost and data security, enterprises should keep in mind while adopting Cloud Computing for the effective and efficient use of their information system.

EXISTING SOLUTION

Sushil Kr Saroj et. al. [] state that "Cloud computing can be listed as the one of the most fast growing technology can be used for better computation and storage performance. The basic advantage of such technology is to develop cost effective application with minimum resource requirement. This statement can be creating complex contradiction about to enhance system performance and cost effective solution with minimum resources. This technology helps to share various resources and storage capacity along with services to reduce individual cost and create a sharable environment. Author suggest that there are five feature of cloud computing can be listed as below;

1. On-Demand Service,
2. Self Service,
3. Location Independent,
4. Rapid Elasticity And
5. Measured Scale Service.

However, security is one of the major hurdles in the way of cloud computing due to sharable environment. User avoids using of common resources due to worry of information leakage Computing. Here author observe that "people feel that cloud is unsafe place and once you send your data to the cloud, you lose complete control over it".

They conclude that many schemes are given to confirm these security requirements however they're affected by collusion attack or information leakage attack by malicious users due to weak cloud service provider and serious computation (due to massive no keys). To deal with these problems author propose a algorithm, integrated by several security approach. During this theme, there are essentially three entities: Data Owner (DO), Cloud Service supplier (CSP) and Users. Users are divided in teams on some basis like location, project and department and, cherish every group, there's one key for secret writing and cryptography of data. Every user within the cluster shares elements of the key. Data can be decrypted once a minimum of threshold variety of users can present. This theme not solely provides information confidentiality by all means that however additionally reduces the quantity of keys. To achieve fine-grained information access management, the approach has used capability list. To explain the complete phenomena they propose a architecture view explained in figure 2.2.

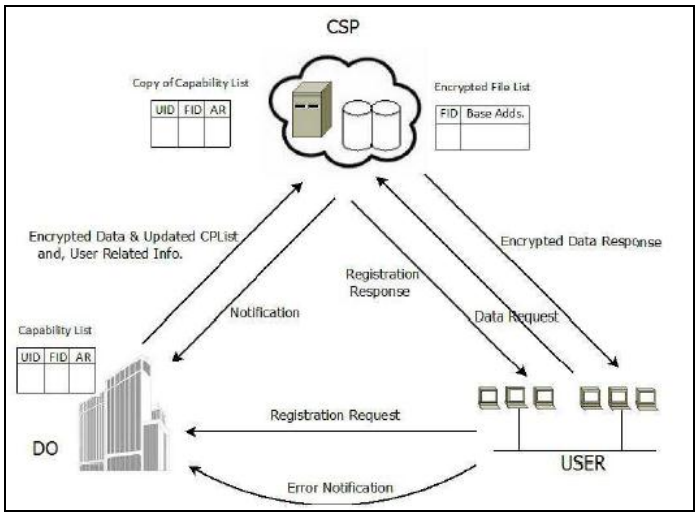


Figure 2.2: Communication Model with Security

PROBLEM STATEMENT

Cloud computing environment has wide application area and may deploy with various purpose. Although, security was primary concern since inception of internet due to its public connection, it becomes very critical due to involvement of internet with cloud computing. Cloud computing gives wide computing nature environment with distributed storage with parallel execution facility. It requires internet to enhance its scope from intranet to worldwide and uses internet services to access cloud application from outside the network.

Any organization or computer node that process data through public network is subject for security breach and may be target for various security threats and attackers. It

creates dilemma in user's mind about the trust and privacy of information. Any user who access or store their confidential information using cloud applications always required assurance about safety and security of content.

The study of complete existing system explore that, existing solutions provides security but either one or two level. They do not gives complete security model or framework to integrate security with cloud applications. They address a very strong need of security model which should provide security not as the requirement but as essential component of application. Following major problems has been observed during the study of Base Paper [Base Paper Citation].

- Poor Privacy and Confidentiality Approach
- Single Authentication Approach
- No User Role Classification
- Absence of storage level privacy

In the existing work author attempt to provide security for public cloud environment. They do not consider trusted node may spy the network security policy and can support security breaching. Capability list base access control classifies the user based on user involvement but does not stand arise the involvement of user into system. Role specification can not help to avoid such situation but may enhance the scalability of user addition.

Furthermore, work also examine the need of privacy maintenance at database level. Previous work do not consider such critical issue and store data into plain format. They only concentrate to maintain privacy at communication level not background level.

The study of complete existing system explore that, existing solutions provides security but either one or two level. They do not give complete security model or framework to integrate security with cloud applications. They address a very strong need of security model which should provide security not as the requirement but as essential component of application.

PROBLEM STATEMENT

This research work proposes an efficient technique to establish strong security policy for real cloud (Red hat-Open Shift). The complete system is classified into two ends. One end is client end, use to generate request for service. Subsequently, another end is server end use to process and manage incoming requests and provide interface between database, user and service provider.

The user management of proposed system is classified into three users which are listed below;

1. **General User**
2. **Manager**
3. **Administrator**

All the above three users are classified according to their rights of access. User / Basic user can only perform upload or download action. User is very limited user type can perform limited task. The advance user type super user is co-administrator of proposed solution used

to manage uploaded files. This user can also delete the uploaded files. Administrator is the root authority of proposed system give approval for user. It is the only authority who is responsible for user creation. The rights and working capabilities of each user can defined below.

User / Basic User: Following steps are used for user creation and service access.

Step 1: It is the primary step where user request for access by registration form to create new user profile. Default scripts retrieve the IP address of requested node and attach with user request. Afterwards, User has to re-login and generate IP-request for administrator approval. Administrator approval provides permission for user to login from requested IP address. Furthermore, it also adds the requested IP address with user information in database for authentication purpose.

Step 2:

Afterwards, user can upload and download the document file. When user requests to upload a file, it request to upload service and file up-loader convert the requested file into byte format and store into database

The complete system is implemented into web based environment and available on red-hat server. Thus the entire uploaded file can be accessed and download from any location. This feature may create opportunity for attacker to get access from public network. Thus IP-Verification process is integrated with authentication service. When user attempt to login from non-recognized computer system, it required fresh approval from administrator before login. Thus, non-recognized node can't be used for login purpose.

Manager User: This is more privilege user than basic user who not only upload or download file but also delete respected files. All the authentication and approval process is same for super user as basic user.

Administrator: It is the root user of the proposed system who allow user and super user to access the requested services as per there privilege. It is shown in figure 4.4.

Confidentiality	RSA
Authentication	1. User Id-Password Mechanism 2. IP-Based Authentication [**Private Cloud Authentication**] 3. Token Based Authentication [OTP]**[Public Cloud Authentication**]
Integrity	MD5
Access Control Mechanism	Role Based Access Control

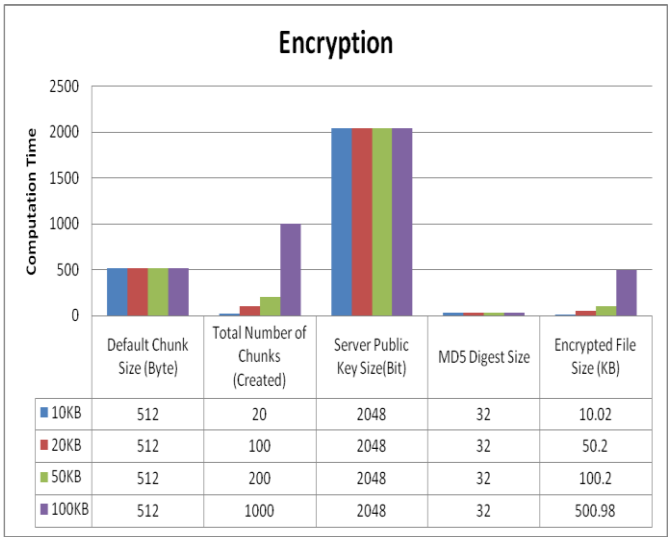
Implementation of Security Principles & Suitable Algorithms is shown in Table 1.

RESULT ANALYSIS

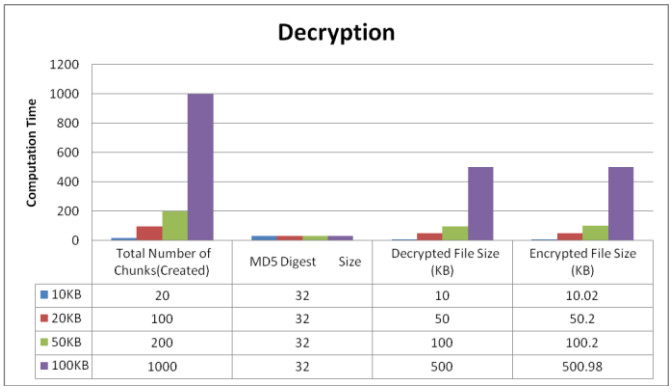
Analysis of system performance is done in two manners. The first way is observation of performance in terms of computation time with respect to single node and three nodes. And the second way is execution of testing and verification of developed application with respect to proposed solution.

The complete solution has been deployed into two way; public and private cloud. Subsequently results are observed in terms of computation time for both.

We have calculated results on the basis of file size after encryption. It is expected that file size should not grow in huge way and should remain almost same in size after encryption. The proposed system is working in the expected manner and file size is getting increased with less than 1% of the total file size. The below table justifies the same result.



	Default Chunk Size (Byte)	Total Number of Chunks (Created)	Server Public Key Size(Bit)	MD5 Digest Size	Encrypted File Size (KB)
10KB	512	20	2048	32	10.02
20KB	512	100	2048	32	50.2
50KB	512	200	2048	32	100.2
100KB	512	1000	2048	32	500.98



	Total Number of Chunks(Created)	MD5 Digest Size	Decrypted File Size (KB)	Encrypted File Size (KB)
10KB	20	32	10	10.02
20KB	100	32	50	50.2
50KB	200	32	100	100.2
100KB	1000	32	500	500.98

4. CONCLUSION

As on now cloud is changing the way a user works over the network. It continuously reduces the load on users in terms of cost and complexity. It also lets the organization feel safe about their data against security breaches and fault interruptions. It provides a robust way of serving

user through a service based model. In a way to achieve its goal, the changed computing also demands some of modified operation of security control for more protection.

With Reference to comparison graph shown in above figures a significant enhancement has been observed into both public and private cloud. To highlight the complete goodwill of proposed solution, following points are expressed.

1. Previous work [Base Paper] only performs solution for public cloud not for private. This work gives solution for both public and private cloud environment.
2. Here, approximately 16% hike in upload and 33 % in download service has been observed.
3. Subsequently, Base paper work only concentrates on confidentiality and gives poor authentication scheme and access control policy.

In this paper a solution is proposed to provide confidentiality, authentication and integrity with access control scheme as a service and inside a data storage environment. At the initial level of analysis, the system seems to satisfy all the demands of security in an effective manner.

5. REFERENCES

[1] Nasrin Khanezaei, Zurina Mohd Hanapi "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia

[2] Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering.

[3] Bokefode Jayant D, Ubale Swapnaja A, Pingale Subhash V, Karande Kailash J., Apate Sulabha S., "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model" International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015

[4] Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh babu "An enhanced data security and trust management enabled framework for cloud computing systems" IEEE 5th International Conference on Computing, Communications and Networking Technologies July 11-13, 2014, Hefei, China

[5] Shilpi Singh, Vinod Kumar "Secured User's Authentication and Private Data Storage-Access Scheme in Cloud Computing Using Elliptic Curve Cryptography" 2015 IEEE 2nd International Conference on Computing for Sustainable Global Development.

[6] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012

[7] Babu, Sriramoju Ajay, and Namavaram Vijay. "Image Tag Ranking for Efficient Matching and Retrieval." (2016).

[8] Babu, Sriramoju Ajay, and Namavaram Vijay. "Design and Implementation of a Framework for Image Search Reranking." (2016).
[9] Babu, Sriramoju Ajay, and S. Shoban Babu. "International Journal of Research and Applications Jan-Mar© 2016 Transactions 3 (9): 422-426 eISSN: 2349–0020."
[10] Bhoyar, Mayur R., Suraj Chavhan, and Vaidehi Jaiswal. "Secure method of updating digital notice board through SMS with PC monitoring system." IOSR Journal of Computer Science (IOSRJCE), e-ISSN (2014): 2278-0661.
[11] Bhoyar, Mayur Ramkrushna. "Home automation system via internet using Android phone." InternationalJournal of Research in Science and Engineering. CSE Department, JDIET, Yavatmal: 6.
[12] Haridass, R., et al. "PERFORMANCE IMPROVEMENT OF POLLUTION CONTROL DEVICE USED IN SMALL SCALE FOUNDRY INDUSTRY." PERFORMANCE IMPROVEMENT 3.1 (2017).
[13] Bhoyar, Mayur Ramkrushna. "Home automation system via internet using Android phone." InternationalJournal of Research in Science and Engineering. CSE Department, JDIET, Yavatmal: 6.
[14] Maulana, Bagoes, and Robbi Rahim. "GO-BACK-N ARQ APPROACH FOR IDENTIFICATION AND REPAIRING FRAME IN TRANSMISSION DATA."
[15] Nofriansyah, Dicky, and Robbi Rahim. "COMBINATION OF PIXEL VALUE DIFFERENCING ALGORITHM WITH CAESAR ALGORITHM FOR STEGANOGRAPHY."