Proc. of Int. Conf. on Advances in Computer Science and Application, CSA

Double Level Security Provisioning in Cloud Networks

Sagarkumar V. Budihal[1], Dr. Jayashree D. Mallapur[2], Shivanand C. Hiremath[3] and Renuka T. Ambiger[4]
[1, 2]Department of Electronics and Communication, [3,4]Department of computer science engineering,
[1]Maratha Mandal Engineering College, Belagavi, Karnataka, India
[2]Basaveshvara Engineering College, Bagalkot, Karnataka, India
[3] R N Shetty Polytechnic, Belagavi, Karnataka, India
[4]B.V.V.S. Polytechnic (Autonomous), Bagalkot, Karnataka, India
Sagar.budihal@yahoo.com,bdmallapur@yahoo.co.in,shivshiv44@gmail.com,renukaran@yahoo.com

***Abstract*—In the emerging computing paradigm known as cloud computing, there are significant issues that need to be addressed in order for cloud computing to be adopted as universally as the Internet. The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by Companies before they decide to do so. One of the most important aspects refers to security. The proposed methodology provides two levels of security mechanisms for securing a cloud networks. The integrity and confidentiality of the data uploaded by the user is ensured by authentication and encryption of the files to be uploaded on the cloud or fetch by the cloud.**

***Index Terms*— Security, Cloud Network, Provisioning.**

I. 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. 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. There is a critical need to securely store, manage, share and analyze massive amount of complex data. Many organizations tried to enhance for their security constraints, for their secured data base, for their web applications but they have not achieved a high-level security for their organization. Data integrity quality of correctness, completeness and compliance with intension of the creator of the data. It is achieved by preventing and accidental or deliberate but unauthorised insertion, modification or destruction of the data in database.

There are many issues in cloud networks which are listed below:

- **Abuse and Nefarious Use of Cloud Computing:** Abuse and nefarious use of cloud computing is

Grenze ID: 02.CSA.2015.4.12

the top threat identified by the Cloud Security Alliance. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.

- **Insecure Interfaces and APIs:** As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.
- **Malicious Insiders:** The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.
- **Shared Technology Issues:** Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required.
- **Data Loss or Leakage:** Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe.
- **Account or Service Hijacking:** Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of service attacks.

In the above issues, unauthorised access to the data is one of the important issue in cloud computing. So in this attempt we are trying to provide security to the data in the cloud by implementing two levels of security while accessing the data using some of the cloud security mechanisms.

We are proposing two way of security mechanism in order to provide security for cloud networks. Authentication and encryption mechanisms are the most efficient mechanisms, in order to avoid unauthorised access to the data. Authentication is the mechanism in which the system will accept the user name and password from the user. Once the two are verified, the user is given access to his files. Only if the entered name and password are valid, the system will establish a connection with the cloud. If the entered name and password are not valid, the system shows an error and rejects the user. The encryption algorithm used here is the substitution mechanism which uses a key to generate a cipher code of the file to be encrypted and the same key will be used for the decryption of the file. The substitution mechanism is a symmetric key algorithm which uses the same key for encryption and decryption. The system manager generates the key for the encryption process.

II. Related Works

In [1], this paper explains about the authentication and authorization for data in cloud networks. So in order overcome security threats here they propose a method i.e. encrypting a file before it is uploaded on to the cloud. AES (Advanced Encryption Standard) is one of the most secure encryption algorithms and not many attacks are successful on data which is encrypted using AES .The integrity and confidentiality of the data uploaded by the user is ensured doubly by not only encrypting it but also providing access to the data only on successful authentication.

In [2], the main objectives of this paper is to prevent Data access from unauthorized access, it proposes a distributed scheme to provide security of the data in cloud ,which could be achieved by using homomorphism token with distributed verification of erasure-coded data. 2) Proposed scheme perfectly stores the data and identifies the any tamper at the cloud server.3) and also performs some of the tasks like data updating, deleting, appending. This paper also provides a process to avoid Collusion attacks of server modification by unauthorized users.

In [3], this paper gives importance on cloud data storage security. To ensure the correctness of users' data in the cloud, they propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior works they claim that the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append.

Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.
In [4], this main objective of this paper is that use a Multi-Level Security model. This includes introducing workflow transformations that are needed where data is communicated between clouds. In specific cases these transformations can result in security breaches, but the paper describes how these can be detected. The tool developed to implement the method has proved invaluable in two ways. Firstly, it removes the chance of human error in applying the various stages of the method to the input workflow and Secondly developing the tool forced them to think about how best to structure the implementation of the method, which resulted in a very general system that operates on rules, transforms and cost models.
In [5] , in this paper they have proposed encryption algorithms to make cloud data secure and also comparisons have been made between AES,DES, Blowfish and RSA algorithms which has to be used in cloud computing for making cloud data secure and not to be hacked by attackers. The major security concerns they address are 1) Secure data transfer 2) Secure Software Interfaces 3) Data Separation 4) Secure Stored Data 5) User Access Control.
In [6], in this paper authors make an attempt to review the encryption techniques used in data confidentiality and they classify the results on the basis of type of approach and the type of validation used to validate the approach and they also provide literature review of the works regarding to usage of encryption techniques in the area of cloud computing data security.
In [7], this paper proposes a scheme' such that they are encrypting the whole data along with the cryptographic key, in existing solutions of protection of data with cryptographic key there is a chance of theft or getting the key by another person. In order to avoid that, encrypt the key at the time when it is generated or periodically change the key at the same time encrypt the data using encryption algorithms like RSA, Blow fish etc.
In [8], this paper talks about the data security and privacy protection issues associated with cloud computing across all stages of data life cycle. The typical systems that require privacy protection are e-commerce systems that store credit cards and health care systems with health data. The ability to control what information to reveal and who can access that information over the Internet has become a growing concern. Finally, this paper describes future research work about data security and privacy protection issues in cloud.
In [9], this paper analyses the feasibility of applying encryption algorithm for data security and privacy in cloud storage, the main objective of this paper is to 1) To develop a system that will provide security and privacy to cloud computing. 2) To establish an encryption based system for protection data on the cloud and storage service provider to operate on encrypted data. 3) To develop a retrieval system in which the data is retrieved by the user in encrypted form.

III. PROPOSED WORK

The work presented here attempts to overcome the issues and threats that are dealt in the cloud environments. The proposed methodology suggests the encryption of the files to be uploaded on the cloud. The integrity and confidentiality of the data uploaded by the user is ensured doubly by not only encrypting it but also providing access to the data on successful authentication.
The schematic of the proposed methodology is as shown below:

A. File upload

The process of file upload can be shown diagrammatically as:

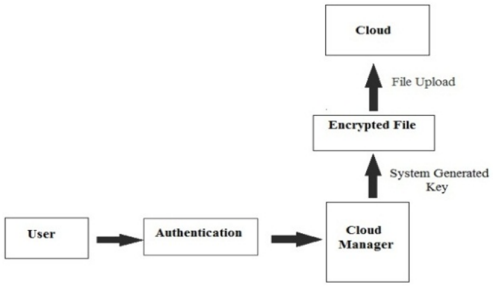

Fig. 1. Process of file upload

Block diagram description:

- **User:** User in this context is the cloud consumer who is keeping his data in the cloud. The user is supposed to specify his requirements regarding the amount of space required and the time for which he wants to use the cloud services. Generally user negotiates with the cloud manager regarding the money he has to pay in order to access cloud services and to securely store his files onto the cloud.
- **Authentication:** This is the first level of security where the user is supposed to give his credentials like the username and password for successful access to his files. This allows only the right person to access the file and deny the same by an unauthorized party. The permissions and folders returned define both the environment the user sees and the way he can interact with it, including hours of access and other rights such as the amount of allocated storage space.
- **Cloud Manager:** Cloud Manager is a backend application that generates a key for encryption of the file. Cloud manager not only generates key but also generates normalised cost for the user depending upon user's requirement. Normalized Cost Generation is the mechanism in which the generation of the cost for the cloud resources that are used by the cloud consumer, that takes into consideration the size of the storage space required by the consumer and the total time (in hours) the cloud resources are being used. The user has to provide the amount of space required and the time for which he/she is using the cloud resources at the beginning. This mechanism then generates the cost based on the data entered by the consumer. This is a very effective mechanism for the generation of the cost for the use of the cloud resources. The key generated is random and no user interference is involved here. This helps in not disclosing the key to the user. The user knows the key only on successful authentication to the cloud. The cloud manager takes the file and encrypts it and uploads it to the cloud. At the time of access the file is decrypted by the cloud manager. The cloud manager in its essence protects the confidentiality of the user data.
- **Cloud:** Cloud is a computing environment where our encrypted file is uploaded for future access. Here the files are kept safe by the cloud provider. No third party is involved in the process of file upload to the cloud.

The methodology suggested here aims to prevent every possible attack on the user data. The first step towards the same is authentication. The system will accept the user name and password from the user. Once the two are verified, the user is given access to his files. Only if the entered name and password are valid, the system will establish a connection with the cloud. If the entered name and password are not valid, the system shows an error and rejects the user. Then user is asked to enter the amount of storage space and the time of usage of the data. Depending upon these requirements cloud manager generates normalised cost for the use of cloud network.

Now when the user has access to his files he can keep any content in it and even modify the previous data. Once the user has entered the data and the file is selected to be uploaded, the next step asks the user for a password for the encryption process. The user is supposed to give an eight digit password. This password is used for generation of a key for the successful encryption of the file. The encryption algorithm used here is the substitution mechanism which uses a key to generate a cipher code of the file to be encrypted and the same key will be used for the decryption of the file. The substitution mechanism is a symmetric key algorithm which uses the same key for encryption and decryption. The system manager generates the key for the encryption process. The user is not involved in process of generation of the key. Every time the user tries to access his files or modify it, a new key is generated for the process. This ensures that even if any unauthorized person tries to breach into the user's data he cannot access the contents of it without knowing the key for decryption. The user's data is doubly secured because one, a person can access the data only when the entered username and password are valid and two, even if the login password of the user is attacked, the uploaded file is encrypted which can be decrypted only if the user enters the password which he entered during the encryption process. This ensures confidentiality. Also, since the uploaded data is encrypted, no modification can be made to the cipher text. This ensures data integrity. Ones the cipher text file is successfully uploaded on the cloud and the user has no more file to be uploaded, the system logs out of the user account and disconnects the established connection with the cloud.

B. File download

The process of file download can be shown diagrammatically as:

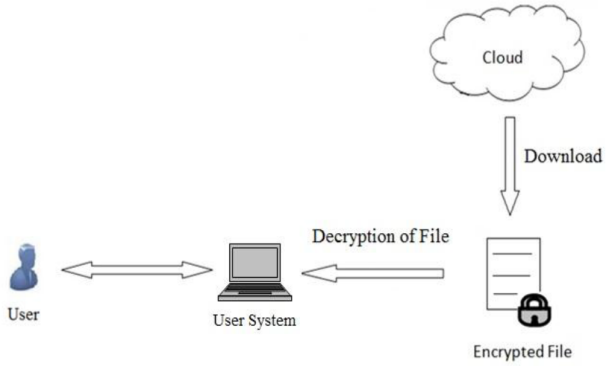

Fig. 2. Process of file download

The initial procedure for file download is as same as the file upload process, which begins by authenticating the user by specifying the username and the password to enter the cloud environment. The system manager generates the user specific key for the decryption of the encrypted file. The cipher text file uploaded by the user will only be decrypted and downloaded if the password entered is same as the password entered during the file encryption. This is the reason that the password is saved during the encryption process, that is, the stored password is used to validate the entered password. The substitution encryption needs the same key to encrypt and decrypt the data. This is possible only if the same password is entered into the key generator function to generate the key. If the password is not validated an error message will be shown and the password will be rejected. Once the user does not wish to download anymore files from the cloud, logout of the user account and disconnect the established connection with the cloud. This is the last step of the download process.

IV. Results And Discussion

A. Number of Acceptance/ Number of Users

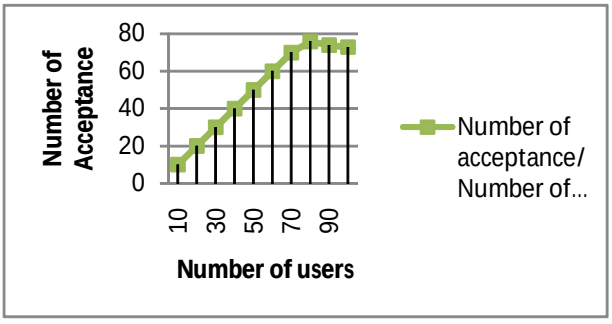

Fig. 3. No. acceptance/No. of users

The above graph shows the plot of the number of acceptance vs. number of users for the allocation of the available storage space in the cloud. The graph shows a linear variation of the number of acceptance/hits for the available space. That is, the number of users almost remains the same depending on the available space. For successful allocation of memory limited number of users should get access to the cloud.

B. Number of Rejections/ Number of Users

The below graph shows a plot of number of rejections vs. number of users for the allocation of the available storage space in the cloud. The graph depicts that as the number of users goes on increasing the less and less number of users get access to the memory i.e. to say that the number of rejections go on increasing.

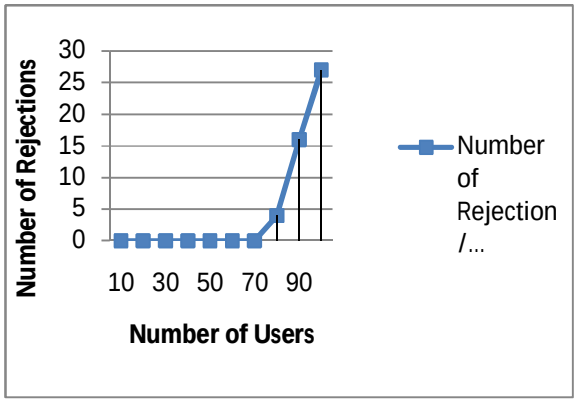

Fig. 4. No. rejection/No. users

C. Encryption time / File size

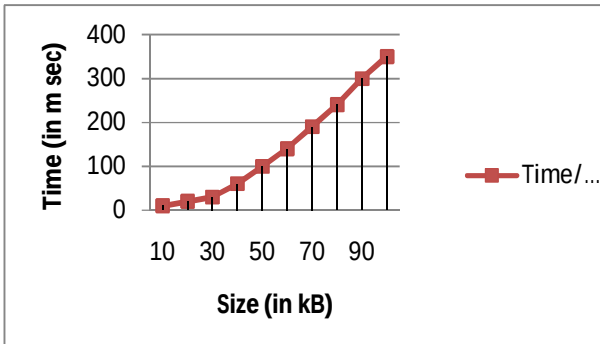

Fig. 5. Encryption time

The above graph shows a plot of the encryption time vs. the file size of the file to be uploaded to the cloud. As the file size increases so does the required time to encrypt the file increases. The time usually is in milliseconds.

D. Decryption time / File size

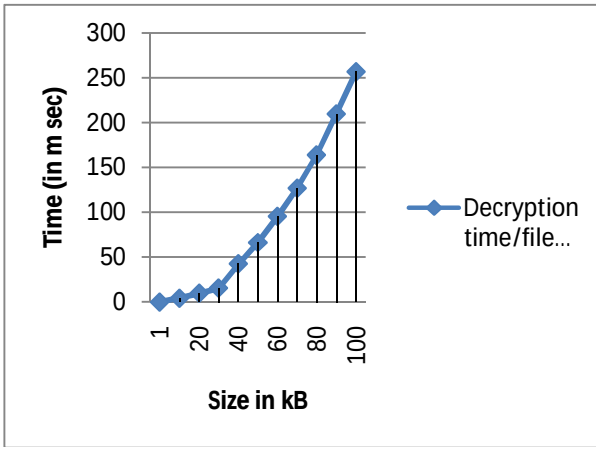

Fig. 6. Decryption time

The above graph shows a plot of the decryption time vs. the file size of the file to be uploaded to the cloud. As the file size increases so does the required time to decrypt the file increases. The time usually is in milliseconds

REFERENCES

[1] Debajyoti Mukhopadhyay, Gitesh Sonawane, Parth Sarthi Gupta, Sagar Vibha Mittal. "Enhanced Security for Cloud Storage using File Encryption", Maharashtra Institute of Technology Pune, India.

[2] Deepanchakravarthi Purushothaman and Dr.Sunitha Abbauru,"An Approach for Data Storage Security in Cloud Computing", International Journal of Computer Science Issues(IJCSI), Vol. 9,Issue 2, No 1, March 2012

[3] Cong Wang, Qian Wang, and Kui Ren,"Ensuring Data Storages Security in Cloud Computing". Illinois Institute of Technology, Worcester Polytechnic Institute respectively.

[4] Paul Watson, "A multi-level security model for partitioning work flows over federated clouds", Watson Journal of Cloud Computing: Advance Systems and applications, 2012.

[5] Geetha Thomas, Prem Jose, P.Afsar."Cloud Computing Security using Encryption Techniques".

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

[7] Monjur Ahmed and Mohammad Ashraf Hossain."Cloud Computing and Security Issues in Cloud". International Journal of Network Security and Its Applications(IJNSA), Vol. 6 , No. 1, January 2014.

[8] Vahid Ashktorab, Syed Reza Taghizadeh. " Securit Threats and Countermeasures in Cloud Computing" , International Journal of Application or Innovation in Engineering and Management, Vol. 1, Issue 2, October, 2012.

[9] Mohit Marwaha, Rajeev Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", International Journal of Computer Science Issues(IJCSI), Vol.10, Issue 1, No 1, January 2013.

[10] Robert Denz and Stephen Taylor. "A Survey on Securing Virtual Cloud", Denz and Taylor Journal of Cloud Computing: Advances, Systems and applications, 2013.

[11] Pradeep Kumar Tiwari, Dr. Bharat Mishra. "Cloud Computing Security Issues Challenges and Solutions", International Journal of Emerging Technology and Advanced Engineering(IJETAE), Vol. 2 , Issue 8 , August 2012.

[12] Rajkumar Buyyaa, Chee Shin Yeoa, Srikumar Venugopala, Ivona Brandic. "Cloud Computing and emerging IT platforms:Vision,hype reality for delivering computing as the 5th utility". University of Melbourne, Australia. Future generation computer systems, 2009.