A Novel Approach for Security Enhancement and Efficient Data Recovery in Cloud Computing

J.Velmurugan [1] S.Aadhithyan[2] T.Naveenkumar[3]
[1]Reseach Scholar of Anna University [2&3] UG Stdents of Anna University
Veltech Hightech Dr.Rangarajan Dr.Sakunthala Engineering College
Avadi, Chennai, India

Abstract: Cloud Computing is a set of services and resources always offered only through internet. Here the services are always provided from the database throughout the world. In other words or simply cloud computing can be defined in simple words as service providing through internet. But the main drawback of this concept is that the security is really on the lower side as all the encryption or the decryption is done by the agent himself. This means that he has access to the vendors account at any time leaving the account holder vulnerable to all interior attacks. This paper mainly concentrates on these interior attacks where the service provider himself cannot access the account even in case of emergency without the vendors permission.

Keyword: Public audit, Data dynamic,Data availability,Cloud Storage, Data integrity, Security,Proxy Server, Third Party Auditor, RSA, ECC.

Introduction:

Network first was introduced in the year 1969 where a simple ARPANET was used to transfer a packet. Then after years of research in the year 1995 first wireless network was established. Though various technologies emerged making our life more comfortable and easy came along with it the danger. Security became a big issue in network. Cloud computing which is an emerging and latest technology developed has serious loop holes in security.

Rivest-Shamir-Adleman(RSA):

It is one of the popular encryption algorithm used in the world. It works on the fact that there is no efficient way to factor or find a very large encrypted number(100-200).The key length of this algorithm is 1024bits(1024 bit RSA).

Algorithm:

Step1:get two prime numbers l and k.

Step2:multiply a=l*k.

Step3:GCD=(d,((l-1) * (k-1))) = 1.

Step4:calculate the value of e using d.e * d = 1 (mod ((l-1) * (k-1))).

Elliptic Curve Cryptography(ECC):

It is a public-key cryptography on the algebraic structure of the elliptic curves over a finite field. Requires smaller keys when compared to RSA algorithm.256 bit key=3072-bit RSA key length. It is very secure a small point which is taken from a curve is used to encrypt and generate a password which is really hard to find and break through even by brute force.

Algorithm:

Step1:Take the curve equation into account
$y^2=x^3+ax+b$ where

e- Elliptic Curve
t Point on the curve
n Maximum limit

Step2:decide a number d in the range of n.

Step3:To generate public key x = d * t
d is the random number which is chosen in between 1 to n-1.p is point of the curve.

Step4:Encryption technique:
a1 = j*t
a2 = m + j*x

Step5:Decryption:
M = a2 – d * a1

Proxy Server:

Its is a simple dummy server where it can handle all the request and the response from the user and the cloud service provider. It is generally placed in a DMZ where no man has the access to the server.

Existing System:

a. In paper [1], the v-grt has been used where a user simply uses the encryption algorithm and encrypts his data and sends it to the storage area. But the problem here is that again a normal encryption technique has been used like AES and DES and the encryption has been done. Also that the encryption is only at database level and not at the entry level it is highly risky that there is a possible way where a user can easily take the required data from inside the organization.
b. In paper [2], the technique called claim-based solution has been used. Here any user who is to be the owner of the account can have access to the account of the rightful. But the security is that any user can easily break into the account and get the rightful claim. It is easy to get the token and pretend as if the original user has given request.
c. In paper [3],A efficient dynamic auditing protocol has been used for securing the data that a vendor has ut into his cloud server. Here privacy preserving protocol has been used a new concept to protect the data.
d. In paper [4], In this paper the same concept as that of 2nd has been used but along with it an efficient access control strategy has been given to improve the security of the vendors or the user in other words who upload their data in the cloud.
e. In paper [5], The concept of identity management has been used where each user gets a unique identity to access his account to prevent various attack like account hijacking, spoofing etc..As there are various ways for any hacker to get into the system identity management has been used.
f. In paper [6], the concept of cloud computing security management has been implemented. It is a simple encryption technique where normal security is provided to the management of cloud tools. The security is nothing but the username and the password and to generate these keys either generally RSA or DES or AES is used.
g. In existing system, while uploading, the entire data were uploaded as single block, so we couldn’t find the particular data loss.
h. Do not support efficient data dynamics and/or suffer from security vulnerabilities when involving dynamic data operations. Here they haven’t used any network codes or erasure codes hence they faced many difficulties while finding the redundancies.

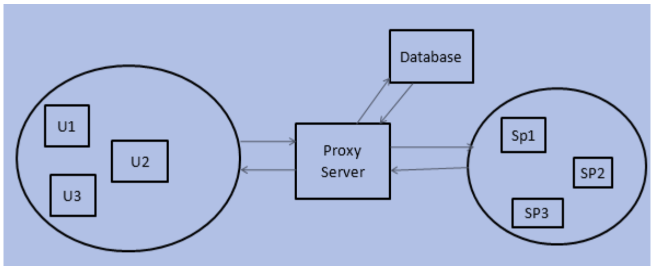
i. No file audit report and file audit delegation. Data corruption caused by server hacks or Byzantine failures. Get network overload on every servers.
j. Security issues such as data integrity and availability are the main obstacles in this system.

Proposed System:

In our proposed system we have brought about a new concept called as a proxy server which is to be placed between the user and the Cloud service provider. The concept has been introduced in this paper because every organization has its own security perimeter and the firewall to protect the external attacks. The security perimeter generally separates the organization and the external world. Its main purpose is to protect the company from external attacks. But the biggest drawback of this inclusion is that it cannot literally protect any attack which comes from inside. It is always said that the greatest threat to an organization is its employee where he is capable of pulling the company to zero point with in a night. So by the existing concept it is clear that the vendor who puts his data in a cloud generally encrypts and decrypts his data using the algorithm that the service provider has put in the server. But the real problem is that an employee who is a grave danger of the organization can easily put an decryption algorithm and take all the required details. Hence in this paper the concept of a proxy server has been implemented such that the direct connection between the user and cloud service provider is broke and the proxy server acts as an security for even the internal attack.

At first the request is sent to the proxy server by the user. The proxy server checks for the authentication in the database and checks the user. If the user is not valid then the server rejects it. If valid then the request is sent to the cloud service provider. Now the CSP provides the required service to the user through the proxy server. By this first the external attacks are stopped by this. Second the internal attack is also stopped as the encryption is done by the proxy server and not the service provider. Thus by this simple implementation of a proxy server the internal attacks can be avoided thus improving a little bit of security

Proposed System Architecture:

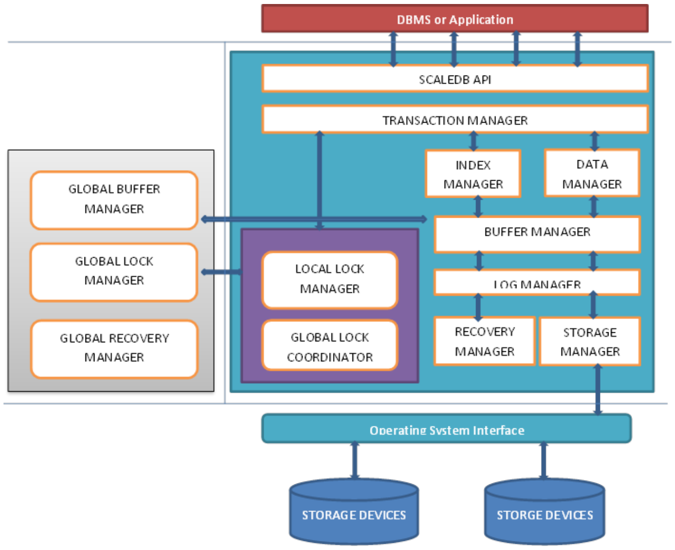


As mentioned in the diagram user gives request to proxy server. Proxy server checks and authenticates the user. After verification the service request is sent to the CSP and the service is provided to the user through the proxy server.

We propose an enhanced dynamic proof of retrieve ability for public audit ability and communication-effective recovery from data corruptions. To this end, we split up the data into small data blocks and encode each data block individually using network coding.

Network coding and erasure codes are adopted to encode data blocks to achieve within server and cross server data redundancy, tolerating data corruption.

By combing range based on encrypted Base64 method and improved version of aggregately signature based broadcast encryption, our construction can support efficient data dynamics while defending against data replay attack.



Conclusion:

On the whole this paper is purely based on the security of a user account on the basis that what if an internal attack on the user accounts is done. Work on this paper is further possible by implementing more good encryption technique and give a good security to the user. The drawback of this paper is that we have used only single proxy server and encryption technique. Still more servers can be added for more tighter security and can be give more complicated algorithms. The encryption methods can be effective more and the security of the users or the vendors can improved thus by this improving the security in the cloud computing.

References:

[1] Data security model or Cloud Computing using V-GRT methodology Thamizhselvan,M. Dept.of Inf. Technol., Sri ManakulaVinayagar Eng. Coll., Puducherry, India

[2] Singh.A. Comput.Sci.&Eng., Nat. Inst. of Technol., Patna,India Chatterjee,K. Identity Management in Cloud Computing through Claim-Based Solution.

[3] Dominick Baier, Vittorio Bertocci, Keith Brown, Scott Densmore, Eugenio Pace and MatiasWoloski , "A GUIDE TO CLAIMS-BASED IDENTITY AND ACCESS CONTROL" , *Authentication and Authorization for Services and the Web* [online] Available: http://msdn.microsoft.com/en-in/library/ff423674.aspx

[4] Cloud Computing Security Management : Sameera AbdulrahmanAlmulla, Chan YeobYeunKhalifa University of Science, Technology and Research (KUSTAR), Shrjah Campus

[5] Security Schemes in Distributed Data Storage Using Proxy Re-encryption G. Srilakshmi PG Scholar, Dept of CSE, Kakatiya Institute of Technology and Science, Warangal, India

[6] Proxy Re-encryption Schemes for Data Storage Security in Cloud- A SurveyW. Sharon Inbarani1 , PG Scholar,Department of CSE, A.S.L Pauls College ofEngineering andTechnology,India

[7] A Secure Code Based Cloud Storage System Using Proxy Re-Encryption Scheme in Cloud Computing Priyadharshini. B. Mrs. Carmel Mary Belinda M. Ramesh Kumar VelTechMultiTech Dr. Rangarajan Dr. Sakunthala Engineering College.

[8] Providing A Secure Data Forwarding In Cloud Storage System Using Threshold Proxy Re-Encryption Scheme: S.Poonkodi, V.Kavitha, K.Suresh, KarpagaVinayaga College of Engineering & Technology, KanchipuramDt, Tamil Nadu, India