

SECURITY AND PRIVACY OF DATA IN MULTI CLOUD WITH DATA BACKUP AND DATA RECOVERY SERVICE

¹HENAL KOTHADIYA, ²DR. VIPUL VEKARIYA, ³DR. G.R. KUKARNI

*1 PG Scholar, Computer Science & Engineering, Noble Group of Institutions, Junagadh,
Gujrat, henal.kothadiya@ngivbt.edu.in*

*2 Associate Professor, Computer Science & Engineering, Noble Group of Institutions,
Junagadh, Gujrat, vp@ngivbt.edu.in*

*³ Principal, S.S.Agrawal Institute of Engineering and Technology,
Navsari, 396445 Gujarat, drgopalrkulkarni8@gmail.com*

Abstract— Cloud computing is important in IT industry. Cloud service has a widespread acceptance but the fear pertaining to security and privacy of these services still continue to be an open challenge. While talking about cloud security there are many aspects which one needs to consider such as trusted authentication, authorization, data security. There are different algorithms for data encryption like RSA, AES, DES, RC4, 3DES etc. These algorithms are broadly classified as being symmetric or asymmetric in nature. While creating a secure cloud there are faced too many challenges like data protection, loss of data etc. Many security services which are certain by the secure cloud system. In that system hybrid cryptographic approach used which gives benefits of both symmetric and asymmetric encryption. That system is for single cloud and it was implemented on cloud sim framework. In cloud computing, data generated in electronic form are large in amount. To maintain this data efficiently, there is a necessity of data recovery services. This paper is about the reviews on data security and data backup/recovery in multi cloud.

Keywords—Single Cloud; Multi Cloud; Data Privacy; Data Backup/Recovery; cloud Storage

I. INTRODUCTION

Cloud computing has become a vital technology where Cloud services providers make available computing resources to their consumers to host their data or execute their computing Tasks. Cloud computing can be catalog into unusual service Distribute models such as Software as a Service, Platform as a Service, Infrastructure as a Service.[5] Today, Cloud Computing is itself a gigantic technology which is Surpassing all the previous technology of computing (like Cluster, grid, distributed etc.) of this competitive and challenging IT world. The need of cloud computing is increasing day by day as its advantages overcome the disadvantage of various early computing techniques.[8] The use of cloud computing has increased rapidly in many organizations.[1]

Dealing with “single cloud” providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards “multi clouds”, “inter cloud” or “cloud-of-clouds”. [1] This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider This paper is also focus on multi cloud based data recovery.

A. Cloud Computing: Preliminary

Cloud computing is define as “a style of computing where massively scalable IT-enabled capabilities are delivered ‘as a service’ to external customers using Internet. [2] Cloud computing consist of three components such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). [1]

B. Cloud Service Provider

Cloud service providers should ensure the security of their customers’ data and should be responsible if any security risk affects their customers’ service infrastructure. A cloud provider offers many services that can benefit its customers, such as fast access to their data from any location, scalability, pay-for-use, data storage, data recovery, protection against hackers, on-demand security controls, and use of the network and infrastructure facilities [1]

C. Security Concern in Cloud

Security in cloud plays an important role in creating a sense of belief and confidence between the customer and Cloud Service Provider (CSP). Since, the entire user data is stored, managed and processed at the cloud end thus it is the duty of the CSP to mitigate any kind of risks pertaining data security and privacy. Following are certain Cloud security which a CSP

needs to keep in mind while dealing with user data [4];

- Data Protection
- Loss of Data
- Traffic Hijacking
- Isolation of Resources
- Malicious Insider

D. Moving From single to Multi Cloud

After all, we need to know what Multi cloud is. Clearly, it is a more complex system than a hybrid cloud, which is usually a combination private and public cloud. [6] The main purpose of shifting towards inter clouds is to improve whatever was offered in single cloud by distributing the reliability, trust and the security among multiple cloud providers. Multi-cloud add more clouds to the mix (i.e. possibly two or more public IaaS providers, a private PaaS, private use-based accounting, etc.) which aims at reducing the risk of service availability failure, exploitation of data, loss of privacy, and the possibility of malicious insiders in the single cloud.[6]

II. LITERATURE REVIEW

A. Data Security

N.Jayapandian [3] uses DES algorithm as a symmetric encryption and RSA algorithm as a asymmetric encryption. In DES same key is used for encryption and decryption and mainly secured by secret key method. RSA is mainly exposing an asymmetric method in the encryption and decryption algorithm. It is a method of asymmetric Technique, that here public key distributed to all through which one can encrypt data of the original message and private key which is used for decryption is maintained for more privacy to keep secret and it will not share to every person.

Akshay Arora [4] uses hybrid algorithm for data security in cloud. Here it's give benefits of both symmetric and asymmetric encryption. He use AES and RSA algorithm. First the RSA generates Public and Private Keys which are later used by the AES in order to commence data encryption. The Private key of the AES again undergoes encryption through RSA and is saved in the data base after adding salt to it. In this way the user data is stored in an encrypted form at the Cloud end and whenever the user wishes to access it will be available after successful decryption.

Kunal V. Raipurkar [5] uses LDAP and two way encryption algorithm. The LDAP authentication method is used for identification of valid user. LDAP authentication Based on TCP/IP protocol therefore it is very easy to implement on any system. In two way encryption algorithm key generation is done by Secure Hash Algorithm (SHA-512) and this key is passed to the Advanced Encryption Algorithm (AES).

This two way encryption algorithm provides more security for users and cloud providers.

B. Data Backup And Recovery Service

In cloud, as number of user shares the storage and other resources, it is possible that other customers can access your data. Either the human error, faulty equipment's, network connectivity, a bug or any criminal intent may put our cloud storage on the risk and danger. And changes in the cloud are also made very frequently; we can term it as data dynamics. The data dynamics is supported by various operations such as insertion, deletion and block modification. Since services are not limited for archiving and taking backup of data; remote data integrity is also needed. [8] Because the data complete state of the server that takes care of the heavily generated data which remains unchanged during storing at main cloud remote server and transmission. Integrity plays an important role in back-up and recovery services. There are many techniques have been proposed HSDRT, PCS, ERGOT, Linux Box, Cold/Hot backup strategy etc. that, discussed the data recovery process.

Ms. Kruti Sharma [8] discussed about a smart remote data backup algorithm, Seed Block Algorithm (SBA). SBA helps the users to collect information from any remote location in the absence of network connectivity and also help to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason. It basically uses the concept of Exclusive-OR (XOR) operation of the computing world. SBA is very much robust in maintaining the size of recovery file same as that the original data file.

Yu Gu [7] discussed about DR-Cloud which is multi cloud based disaster recovery service. With DR-Cloud, resources of multiple cloud service providers can be utilized cooperatively by the data disaster recovery service provider. And customers only need to deal with that service provider, using very simple and unified service interface, without concerning the internal processes between heterogeneous clouds. DR-Cloud can ensure high data reliability, low backup cost, and short recovery time by using intelligent data scheduling strategies. In this replica scheduler is important. [7]

C. Multi cloud Security

Multi-cloud computing is relatively new concept, biggest security aspects in cloud computing basically are data intrusion, data integrity and service availability are handled in much better way in multi-cloud than single cloud computing.

Mohammed A. AlZain[2] is discussed about multi cloud security. It proposes a Multi-clouds Database Model (MCDB) which is based on Multi-clouds service providers instead of using single cloud service provider. MCDB ensures security and privacy in

cloud computing environment and is based on multi-clouds service providers and the secret sharing algorithm. The purpose of this model is to avoid the risk of malicious insider in the cloud and to avoid the failing of cloud services. MCDB contains three layers: the presentation layer, the application layer, and the data management layer. The presentation layer contains the end user's browser and HTTP server. The application layer contains servlet engine. The management layer consists of the Database Management System (DBMS) and the database service provider.

Arun Singh [6], use Shamir secret sharing algorithm for securing multi cloud. a secret sharing scheme is a method for distributing a secret amongst a set of participants, each of which is allocated a share of the secret. The secret can be recreated when the shares are united together; individual shares are of no use on their own. In secret sharing scheme there is only one dealer and n player. The dealer a secret to the players, but only when specific conditions are fulfilled. This secret sharing Algorithm is threshold sharing scheme and is based on the Lagrange polynomial interpolation.

III. PROPOSED WORK

A. Data Security

The prevalent Problem associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network. With the help of different encryption algorithms, Users are able to enhance the data security of cloud computing. [10] There are many different algorithms for data security. Mainly two types of encryption algorithm: symmetric encryption and asymmetric encryption.

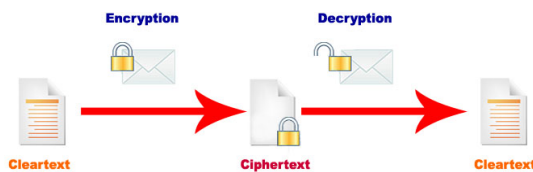


Fig. 1. Encryption/Decryption Process

Here in this system hybrid cryptography is used which is combine benefits of both symmetric encryption and asymmetric encryption.

B. Workflow of System

In this sub section we would be discussed the workflow of system.

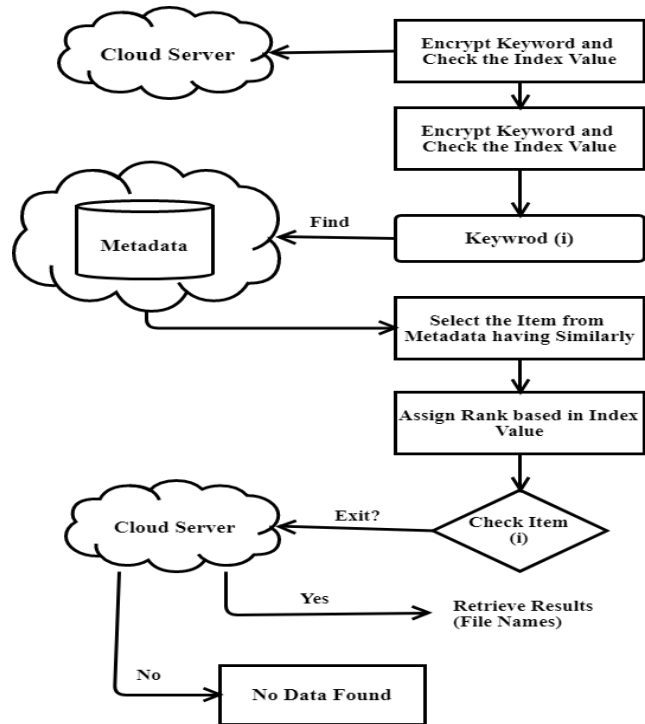


Fig. 2. System Work Flow

First of all encryption process is done. This is done by a hybrid algorithm. Here we use AES and RSA algorithm. The private key of RSA is used by AES and encrypts data. After that, decryption process was completed. In between them if any issue occurs like a threat or any other than cloud provider will not allow access service. Here another service also provided by a system which is data backup and recovery service so the user can retrieve their files easily after deletion of a file or any other issues.

IV. ALGORITHM

The working of our proposed system is explained through the illustration of the algorithm that forms the core for it. The algorithm depicts the functioning of the system by representing the entire process from user authentication to storage and retrieval of user data from Cloud.

- Step 1:** Create Username & Password
- Step 2:** Password Creation using CSPRNG
- Step 3:** SHA512 and bcrypt function used for password protection
- Step 4:** SHA512 key is protected using HMAC algorithm
- Step 5:** Enter login Credentials
- Step 6:** Make use of OTP for Multifactor authentication. Validity of OTP is 5 minutes
- Step 7:** User store data on cloud
- Step 8:** SSL & TLS1.2 are used for conducting transfer user data over the network
- Step 9:** RSA algorithm is used for public private key generation

- Step 10:** AES algorithm encrypts data using RSA private key
- Step 11:** Private key encrypted using RSA
- Step 12:** User request to access data
- Step 13:** RSA generates decryption key
- Step 14:** Decryption process takes place

In this system we also used seed block algorithm for data backup and recovery service. SBA is robust in helping the users to collect information from any remote location in the absence of network connectivity and also to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason. This algorithm steps are as following:

Initialization: Main cloud: M_C , Remote Server: R_S , Client's Main cloud: C_i , Files: a_1 & a_1' , Seed Block: S_i , Random Number: r , Client's ID: $client_Id_i$

Input: a_1 creates by C_i , R is generated at M_C

Step 1: Generate a random number $int\ r=rand()$

Step 2: Create a seed block: S_i for each C_i and store S_i at R_S (Repeat step 2 for all client)

Step 3: If c_i /Admin creates/modifies a a_1 and stores at M_C , Then a_1' create as

$$a_1' = a_1 \oplus S_i$$

Step 4: Store a_1' at R_S

Step 5: If server crashes a_1 deleted from M_C , Then we do EXOR to retrieve original a_1 as:

$$a_1 = a_1' \oplus S_i$$

Step 6: Return a_1 to C_i

Step 7: END

V. IMPLEMENTATION

The above mentioned algorithm is implemented on CloudSim framework. CloudSim [12] is a simulation toolkit which comprises of various predefined classes that provide a simulation environment for Cloud computing. It is a java based simulation toolkit and can be implemented either using Eclipse or Net Beans IDE. In our case we would be using the Net Beans IDE. To run CloudSim on Net Beans, we first need to download the Net Beans IDE and install it. After successful installation of eclipse IDE, download the latest CloudSim package, extract it and import it in Net Beans. Talking of our proposed work we have created our own classes in CloudSim and have portrayed our algorithm in form of java code. The following are the screenshots that depict the working of our algorithm on CloudSim framework.



Fig. 3. Successful Authentication

In above snapshot authorization process is successfully completed. If any unauthorized person will try to login or upload data, then cloud service provider will check this using a secret key and then they add unauthorized person into fraud list.

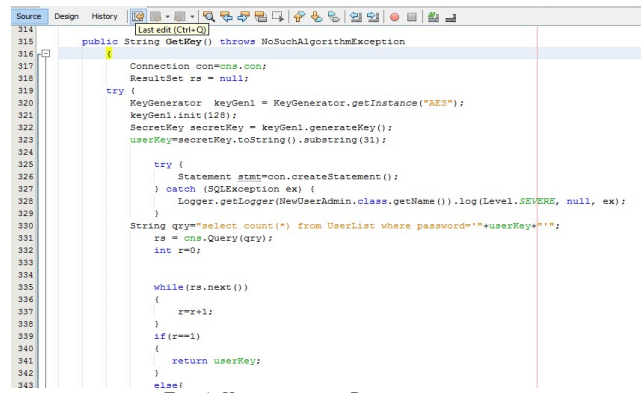


Fig. 4. Key generation Process

In the next screenshot is about the process of key generation. The private key of the RSA algorithm is used by AES to encrypt the data. The Fig-5 shows the experimental result of proposed SBA. As fig-5 (a) shows the original file which is uploaded by the client on the main cloud. Fig-5 (b) shows the EXORed file which is stored on the remote server. This file contains the secured EXORed content of the original file and seed block content of the corresponding client. Fig-5 (c) shows the recovered file.

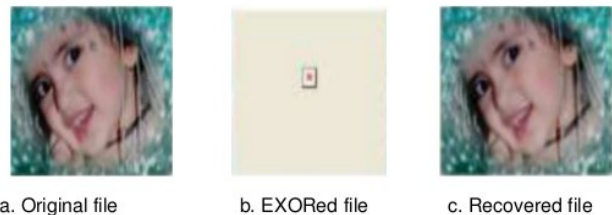


Fig. 5. Sample output image of SBA algorithm.

VI. CONCLUSION

In this paper, we present a Hybrid Cryptographic System (HCS) that combines the benefits of both symmetric and Asymmetric encryption. The system also makes use of certain hashing and salting techniques which even strengthens the entire encryption process. Proposed SBA is robust in helping the users to collect information from any remote location in the absence of network connectivity and also to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason. Experimentation and result analysis shows that proposed SBA also focuses on the security concept for the back-up files stored at remote server, without using any of the existing encryption techniques. The time related issues are also being solved by proposed SBA such that it will take minimum time for the recovery process.

References

- [1] Mohammed A. AlZain , Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds" 2012 45th Hawaii International Conference on System Sciences
- [2] Mohammed A. AlZain, Ben Soh and Eric Pardede, "MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing", 2011. IEEE
- [3] N.Jayapandian, Dr.A.M.J.Md.Zubair Rahman, S.Radhikadevi, M.Koushikaa, "Enhanced Cloud Security Framework To Confirm Data Security on Asymmetric And Symmetric Key Encryption", 2016 IEEE
- [4] Akshay Arora, Abhirup Khanna, Anmol Rastogi, Amit Agarwal, "Cloud Security Ecosystem for Data Security & privacy", 2017 IEEE
- [5] Kunal V. Raipurkar, Anil V. Deorankar, "Improve Data Security in Cloud Environment by Using LDAP and Two Way Encryption Algorithm", 2016. Symposium on Colossal Data Analysis and Networking (CDAN)
- [6] Arun Singh, Darshan Jain, Paresh Chavan, Sweta Jain, "Multi Cloud Data Security" 2016 International Research Journal of Engineering and Technology (IRJET)
- [7] Yu Gu, Dongsheng Wang, Chuanyi Liu, "DR-Cloud: Multi-Cloud Based Disaster Recovery Service", 2014. TSINGHUA SCIENCE AND TECHNOLOGY I SSN 1007- 0214 02/ 10 pp13-23 Volume 19, Number 1, February 2014
- [8] Ms. Kruti sharma, Prof. Kavita R Singh, "Seed Block Algorithm: A Remote Smart Data Backup Technique For cloud", 2013 International Conference on Communication Systems and Network Technologies
- [9] M.Muhil, U.Hemanth Krishna, R.Kishore Kumar, E. A. Mary Anita, "Securing Multi-Cloud using Secret Sharing Algorithm", 2015 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)
- [10] N.Thillaiarasu, Assistant Professor, Dr.ChenthurPandian.S, Principal, "Enforcing Security and Privacy over Multi-Cloud Framework Using Assessment Techniques", 2015 IEEE
- [11] Manpreet Kaur, Rajbir Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", 2013 International Journal of Computer Applications (0975 – 8887)Volume 70– No.18, May 2013
- [12] Calheiros, Rodrigo N., et al. "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms." Software: Practice and Experience 41.1 (2011): 23-50