ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

A Secure Mechanism for Data Distribution, Storage and Privacy in Cloud Application

R. Deshmukh, B.kulkarni, S.Kalekar, A.Deshmukh, S.Shinde

Department of IT, MMCOE, Pune, India

ABSTRACT: Cloud computing technology is mostly preferred now-a-days. People store their data in cloud instead of storing on their device, but the security of data and issues of trusted third party are still present in the cloud. We can solve the issues by avoiding the trusted third party in communication between data owner and data consumer and security of data can be maintained by giving two-level encryption to data stored in cloud. Compared to single level encryption of data we can add one more level of security, by adding second encryption to data present in cloud which provides more data security. Verifying the data owner and data consumer is important in case of data security in order to avoid the unauthorized access to data. This is done by providing the One Time Password authentication. Security is also enhanced by asking random questions to data consumers while downloading the file which can be asked to the consumer while registering to the system. Category-wise data is getting stored on cloud and consumer can access the data according to categories. The data distribution process is done by categorizing data with different sections like distinction, first class, second class in MNC based application which can be stored with secure mechanism. The mechanism used provide privacy to the data with two level encryption.

General Terms

Security, data distribution, privacy, data owner, data consumer, cloud service provider.

KEYWORDS: Cloud Computing, secure data distribution, data integrity, storage, privacy.

I. INTRODUCTION

In cloud computing high scalable computing resources are supplied as services through internet on pay as usability basis. Cloud is a platform where we can use several resources over the internet. There are different advantages of using cloud like easily accessible, easily available, low cost and efficient. We can store big amount of data without bothering of hardware, but storing data on cloud requires more security and trust. The security issues like data integrity, privacy loophole can damage data in system. Perhaps two of the more hot button issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally slow down the deployment tent of the cloud service provider. The security mechanisms between organization and the cloud need to be robust. In this work, we are presenting an efficient data distribution system by using web application so that the users can efficiently store their data on cloud and can share their data to the authorized person. Where we are storing our data in the form of category. For example, suppose we have college based web application which is storing details of its student, teacher staff, non-teaching staff and workers. If any MNC want to access the data from student category, then he can access data through the category only if data owner gives him access permission. We are authorizing both consumer and owner for giving permission to access the data for providing more security. For authentication of owner we are providing one time password (OTP) so that any fake or unauthorized owner will not be able to do any operation into the system .The consumer will be identified by using image processing on security basis; We are providing data security by using algorithms blowfish,IDEA,MD-5 . We firstly design blowfish algorithm which allows consumer with a single secret key to keep the data privacy and flexibly share his data to authorized person under permission. We are also using IDEA algorithm for double encryption to protect integrity and privacy of data. To protect our data from data theft which acquires data services from different service providers because those services are cost

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

efficient and flexible for sharing data. To provide more security, our data distribution system ID designed without trusted third party. So that the data owner is only the authorized person to control and share his own data.

1. Related Work

There are lot of works focusing on the issues of security, privacy of data in cloud [1], [8]. Proxy re-encryption (PRE) is one of the solution to share data on public cloud [3], [6].This benefit of PRE is that user have to maintain the secrete key. Now, new TB-PRE concept is used for the access control in cloud computing where system is enough powerful for

Many application in which data is naturally classified into different categories for different users [1], [4]. Some systems work over the concept of identity-based encryption in their work [2], [8].

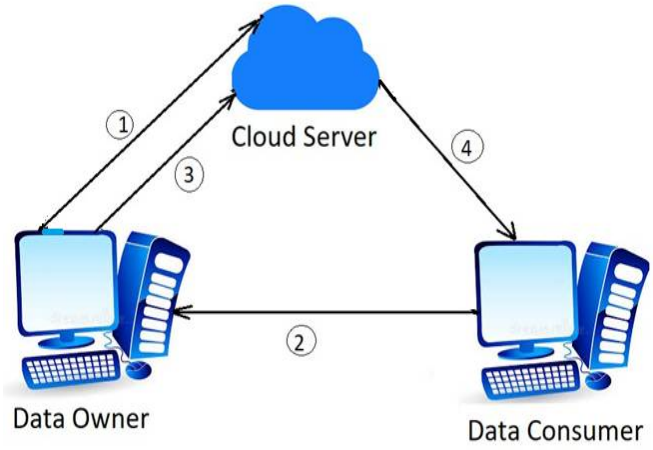
Any loophole in the system may cause damage to the system, that loophole in system may be arise through some attacks [6], [7]. Cryptography refers to the secure communication in the system [2], [6].

Lots of research has been done in the aspect of cryptography and its techniques in cloud.

II. PROBLEM STATEMENT

Security is big concern in cloud computing, we are providing security w.r.t to data security, data privacy, data distribution in our system by eliminating the interference of third party.

1.1 Basic System Model



In basic architecture diagram the basic idea about the flow of system is discussed. Here data owner can store his data on cloud and allow number of consumers to access them.

Step 1: Data owner stores the data on cloud server.

Step 2: Data consumer takes permission from data owner to access data.

Step 3: Data Owner asks the Cloud Server to provide data to data consumer.

Step 4: Cloud Server gives the data to data consumer.

1.2 Detailed System Model

In our system, we are having data owner, data consumer, UI system and Cloud service provider where each one is performing its vital role. Data owner is a user who can register into the system first, then login with the OTP generated by the system. OTP will be generated by using the algorithm which will send the required key on mobile phone by using HTTP protocol and also on an email by using API and upload the data through various categories like distinction, first class, higher second class and so on. Cloud service provider is admin who login to the system for data encryption which is done at second level using IDEA where simple txt file is processed, BLOWFISH Algorithm is used for double

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

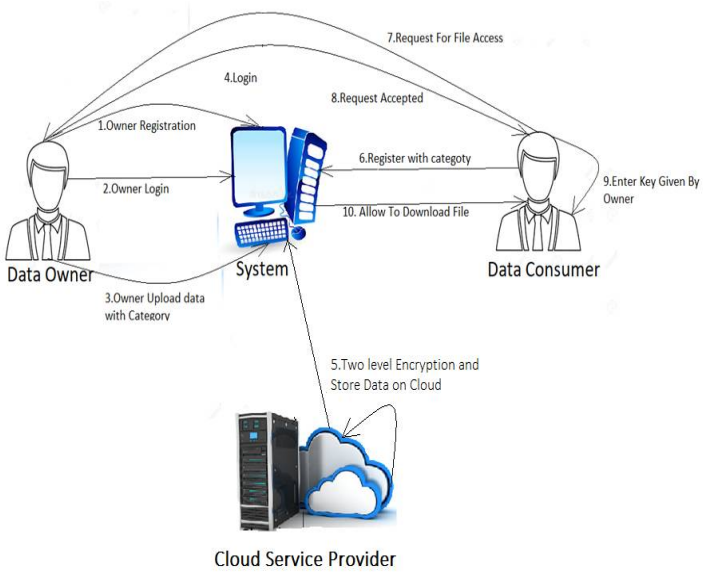
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

encryption to provide more security to the system, MD-5 for generating key algorithms and stores the encrypted data on cloud. Cloud Consumer request for the data access directly to the data owner without interference of third party. Data consumer can access or download the requested file only if the request accepted by the data owner and key is sent by owner to the consumer for downloading the requested file.



1.3 Design Goals

To ensure the correctness of users' data in cloud, we propose an effective and flexible distributed method which allow end users to retrieve data with different categories from cloud service provider.
To allow data owner to upload data on cloud with different categories and who is also able to upload text, images for files till 52428800bytes.
To maintain the privacy using two level encryption that is with IDEA, Blowfish algorithms and integrity using MD-5 key generation algorithm for uploaded data.
To authenticate data consumer with random questioning.

III. A NEW METHOD FOR DATA DISTRIBUTION, SECURITY AND PRIVACY

3.1.Algorithms

1.3.1 IDEA Algorithm

The input.txt file is given to IDEA algorithm. In IDEA algorithm input.txt file is divided into 4 parts such as P1, P2, P3, and P4. Total keys used are 52keys. Total there are 8 rounds and in each round we use 6keys. 6 Keys are K1, K2, K3, K4, K5, and K6. Round 1:

Step1- P1*k1 Step2- P2+k2
Step3- P3+k3 Step4- P4*k4 Step5- Step1 XOR Step3 Step6- Step2 XOR Step4 Step7- Step5*K5
Step8- Step6+Step7 Step9- Step8*k6
Step10-Step7+Step9 Step11-Step1 XOR Step9 -R1
Step12-Step3 XOR Step9 -R2 Step13-Step2 XOR Step10 -R3 Step14-Step4 XOR Step10 -R4

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

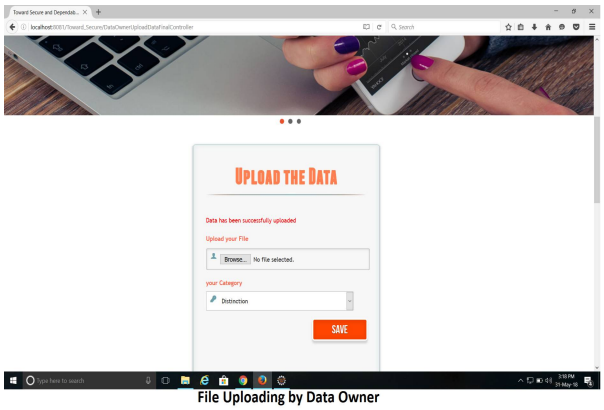
Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

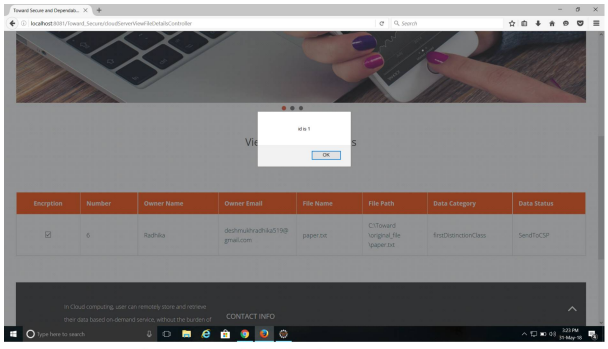
First round output R1 R2 R3 R4 But while giving input to second round, input will be R1 R3 R2 R4 Similarly the 8 rounds will take place. But after the eight rounds, in each round we have just used 6 keys so 8 rounds * 6 = 48 keys so till now we have just used 48 keys still 4 keys are remaining. Output of eight round we will get R1, R2, R3, R4
R1 * k49 -C1 R2 + k50 -C2 R3 + k51 -C3 R4 * k52 -C4 finally cipher text will be generated as: C1+C2+C3+C4=C

1.3.2 Blowfish Algorithm
-Output of IDEA algorithm is given as input to Blowfish algorithm.
Output of IDEA algorithm is C.
Blowfish consist of total 16 rounds. P1-P18 is the keys.
-Divide C into two 32bit: XL, XR XL-Left text, XR-Right text for i=1 to 16; (because of 16 rounds)
XL = XL XOR P1 XR = F (XL) XOR XR
Swap XL and XR Swap XL and XR (Undo the last swap)
XR = XR XOR P17 XL = XL XOR P18
Cipher text: Concatenation of XL XR
MD-5 algorithm is used to maintain the integrity of data stored on cloud

3.2 Snapshots of the system



File Uploading by Data Owner


File Encryption with Two Level

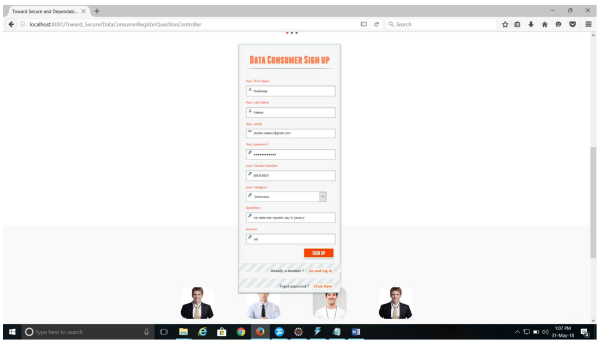
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

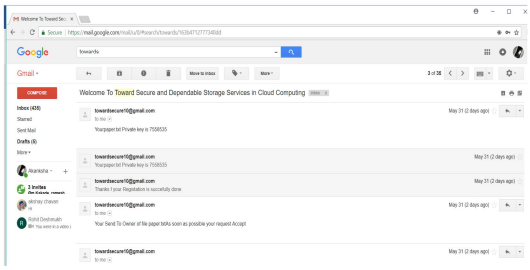
(A High Impact Factor, Monthly, Peer Reviewed Journal)

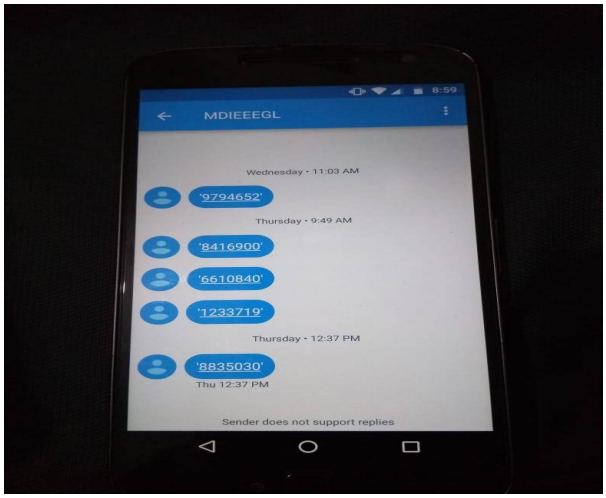
Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018



Data Consumer Registration





IV. CONCLUSION AND FUTURE WORK

In this system, security is provided by two level of encryption on data and by not involving trusted third party. Algorithm used in system are Blowfish, IDEA and MD-5. To get access only to required data, categories-wise data is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

stored in cloud. Verifying data owner and data consumer by One Time Password is done to enhance the security of the system.

Future Work: 1. Security of data stored on cloud is becoming more important, we can add more level of encryption to the data stored in cloud. 2. Data consumer can also give rating to data owner, according to rating given to data uploaded by data owner. 3. System can be used in Training and Placement applications.

V. ACKNOWLEDGMENTS

The authors would like to thank Mr. Swapnil.S.Shinde (Assistant Professor) at MMCOE College of Engineering, Marathwada Mitra Mandal's College of Engineering for guiding and motivating us for this research work.

REFERENCES

1. Jiang Zhang, Zhenfeng Zhang, and Hui Guo, Towards Secure Data Distribution Systems in Mobile Cloud Computing, IEEE Transactions on Mobile Computing (Volume: 16, Issue: 11, Nov. 1 2017).
2. Dan Boneh and Xavier Boyen,Efficient selective identity-based encryption without random oracles ,Journal of Cryptology (JoC), 24(4):659693, 2011 , early version in Eurocrypt 2004.
3. Benot Libert and Damien Vergnaud,Unidirectional chosen ciphertext secure proxy re-encryption ,tInformation Theory, IEEE Transactions on, 57(3):1786 1802, march 2011.
4. Jae Woo Seo, Dae Hyun Yum, and Pil Joong Lee, Proxy-invisible cca-secure typebased proxy re-encryption without random oracles , Theoretical Computer Science, (0):, 2012.
5. Qiang Tang,Type-based proxy re-encryption and its construction, In DipanwitaRoy Chowdhury, Vincent Rijmen, and Abhijit Das, editors,Progress in Cryptology-INDOCRYPT 2008, volume 5365 of Lecture Notes in Computer Science, pages 130144. Springer Berlin Heidelberg, 2008.
6. Jian Weng, Yanjiang Yang, Qiang Tang, Robert Deng, and Feng Bao, Efcient conditional proxy re-encryption with chosenciphertext security, In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Ardagna, editors, Information Security, volume 5735 of LNCS, pages 151166.Springer Berlin / Heidelberg,2009.
7. Qin Liu, Guojun Wang, and Jie Wu, Clock-based proxy reencryption scheme in unreliable clouds, In Parallel Processing Workshops (ICPPW), 2012 41st International Conference on, pages 304305, 2012.
8. https://en.wikipedia.org/wiki/Boneh