Efficient Cryptographic Algorithms for Cloud Storage Security

Prof. Sawan Baghel
PRMITR Badnera, Maharashtra, India.

Prof. Gaurav Saboo
PRMITR Badnera, Maharashtra, India.

Abstract – The cloud computing is the information technology where user can store remotely data so as to enjoy on demand high quality application and recourses. The security is a major issue in cloud computing where privacy issues and security that need to be considered are authentication, correctness of data, availability, no storage overhead and easy maintenance, no data leakage, no data loss. Up to this system, third party demanding the confined copy of user's data, this will increase the possibility of client files to be scarf by third party auditor. So, this system will not provide any pledge on data integrity and availability. To avoid previously mentioned problem, the client can stores their data on the server without keeping a confined copy of data and thus can provide privacy against third-party auditor. So, this system will not leak any private information to the third party auditor. To achieve this objective, this system have implemented Kerberos as a Third Party Auditor, RSA algorithm for secure communication, MD5 algorithm is used to verify data integrity, Data centers is used for storing of data on cloud in effective manner with secured environment and provides Multilevel Security to Database.

Index Terms – Public Auditing, Cloud Computing, Third Party Auditor, Multilevel Security, Data centers.

1. INTRODUCTION

Cloud computing is a model for enabling services such as user's networks access, servers access, storage access, and the applications that can be quickly provision and free with minimal management effort or service provider communication. The security architecture and functions highly depend on the reference architecture, and this paper shows the reference architecture and the main security issues regarding this architecture [1].

The rest of paper is organised as follows: section 2 introduce system architecture where it gives different technique to solve problem related cloud storage security but they have some shortcoming which can overcame by our result which is explain in section 3 that means it provide efficient solution against problem of security issue where it gives result of our implemented system. Finally section 4 gives the concluding remark of this paper [2].

2. SYSTEM ARCHITECTURE

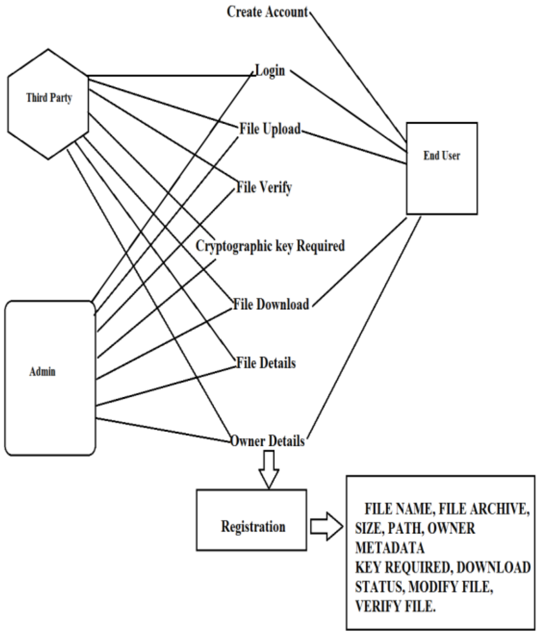

Create Account
Third Party
Login
File Upload
End User
File Verify
Cryptographic key Required
File Download
Admin
File Details
Owner Details
Registration
FILE NAME, FILE ARCHIVE, SIZE, PATH, OWNER METADATA
KEY REQUIRED, DOWNLOAD STATUS, MODIFY FILE, VERIFY FILE.

Figure.1. System Architecture

In this system, there are five main models such as cloud server, third party, end user, admin, and last one is user registration. The working steps of this system architecture are as follows:

- ✓ Step1: In this step, end user's have to register himself on cloud environment i.e. user has to create an account on this system for accessing cloud services.
- ✓ Step2: After the creating account of new user the request of this account is sent directly to the admin for activation of the user.
- ✓ Step3: The admin have to check the documents of new user account physically. After verifying the

documents the admin decide the activation of new user. Only after that the user is able to login.

- ✓ Step4: So in login form, we provide userid and password so that any user who is an authenticated person is able to login in the system to enjoy the environment provided by the cloud for communication.
- ✓ Step5: Whenever the end user login to the service he has to go from an authentication process of third party which identifies and verifies the end user before the cloud services started. As soon as the user login with the system it generates the two keys of RSA algorithm, one key which is public key is sent to the Third party for the encryption of session key and secret key.

3. RESULTS AND DISSCUTION

TECHNIQUES	PARAMETERS							
	Authentication	Key Management	key Transport	key Agreement	Fast	Slow	Best for 32 bit and 64 bit machines	Best for 32 bit machines
Diffie-Hellman Algorithm	Poor	Good	Poor	Good	Poor	-	-	-
Digital Signature Algorithm (DSA)	Good	Poor	Poor	Poor	Good	-	-	-
RSA Algorithm	Better	Better	Good	-	Better	-	-	-
MD5 Algorithm	-	-	-	-	Better	-	Better	Better
Secure Hash Algorithm	-	-	-	-	-	Yes	Poor	Good
Kerberos as a Third Party	Better	-	-	-	Better	-	-	-
Public Key Infrastructure	Poor	Good	Poor	Poor	-	Yes	-	-
Remote Authentication Dial-In User Service	Good	-	-	-	Poor	Yes	-	-
Directory-Based Services	Good	-	-	-	Poor	Yes	-	-

Table1: Analysis of different crypto graphical Algorithms

1. User Registration:

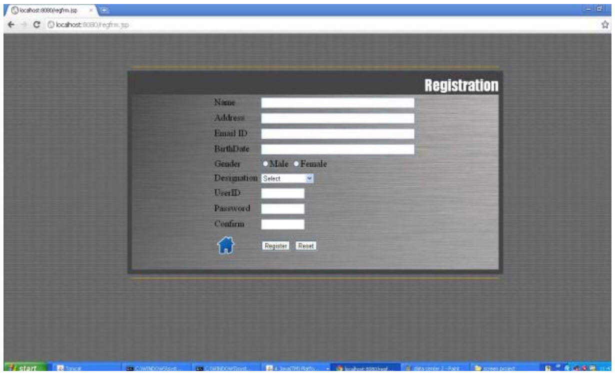


Figure2: Registration form

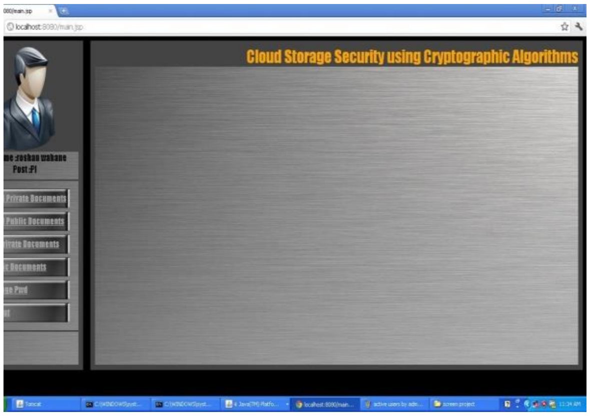


Figure.3: End User Account

2. Admin login page:

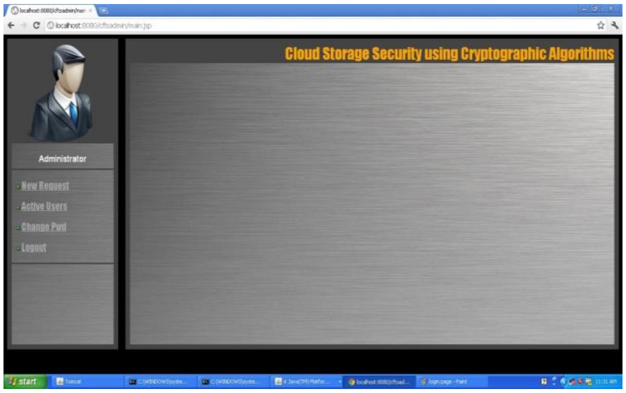
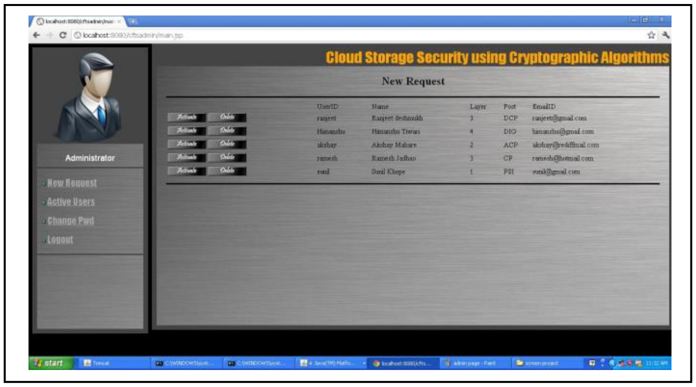


Figure 4: Admin

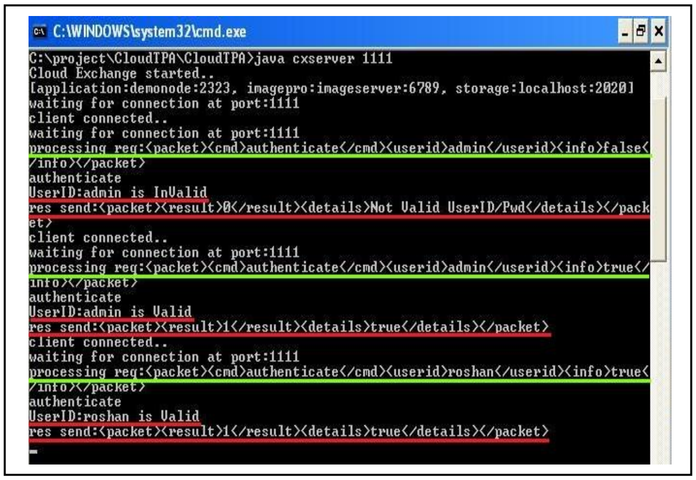

localhost:8080/cftsadmin/main.jsp
Cloud Storage Security using Cryptographic Algorithms
Administrator
New Request
Active Users
Change Pwd
Logout

New Request

		UserID	Name	Layer	Post	EmailID
Activate	Delete	ranjeet	Ranjeet deshmukh	3	DCP	ranjeet@gmail.com
Activate	Delete	Himanshu	Himanshu Tiwari	4	DIG	himanshu@gmail.com
Activate	Delete	akshay	Akshay Mahare	2	ACP	akshay@rediffmail.com
Activate	Delete	ramesh	Ramesh Jadhao	3	CP	ramesh@hotmail.com
Activate	Delete	sunil	Sunil Khope	1	PSI	sunil@gmail.com

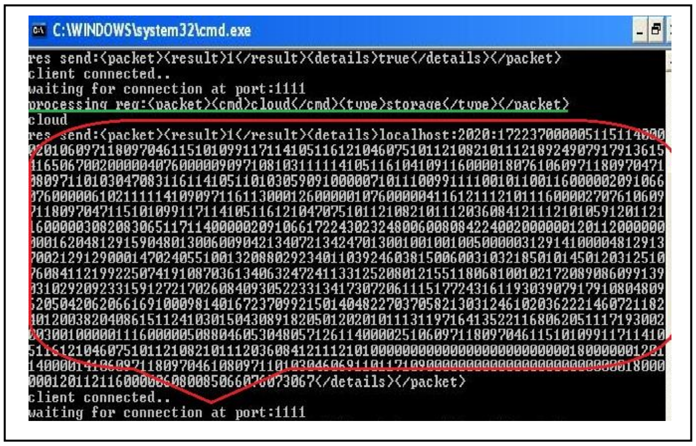
Figure 5: Active Users

3. Third party:



```
C:\project\CloudTPA\CloudTPA>java cxserver 1111
Cloud Exchange started..
[application:demonode:2323, imagepro:imageserver:6789, storage:localhost:2020]
waiting for connection at port:1111
client connected..
waiting for connection at port:1111
processing req:<packet><cmd>authenticate</cmd><userid>admin</userid><info>false<
/info></packet>
authenticate
UserID:admin is InValid
res send:<packet><result>0</result><details>Not Valid UserID/Pwd</details></pack
et>
client connected..
waiting for connection at port:1111
processing req:<packet><cmd>authenticate</cmd><userid>admin</userid><info>true</
info></packet>
authenticate
UserID:admin is Valid
res send:<packet><result>1</result><details>true</details></packet>
client connected..
waiting for connection at port:1111
processing req:<packet><cmd>authenticate</cmd><userid>roshan</userid><info>true<
/info></packet>
authenticate
UserID:roshan is Valid
res send:<packet><result>1</result><details>true</details></packet>
_
```

Figure.5. End user Authentication by the TPA



```
res send:<packet><result>1</result><details>true</details></packet>
client connected..
waiting for connection at port:1111
processing req:<packet><cmd>cloud</cmd><type>storage</type></packet>
cloud
res send:<packet><result>1</result><details>localhost:2020:172237000005115114000
02010609711809704611510109911711410511612104607510112108210111218924907917913615
41650670020000040760000090971081031111141051161041091160000180761060971180970471
08097110103047083116114105110103059091000007101110099111100101100116000002091066
07600000610211111410909711611300012600000107600000411612111210111600002707610609
71180970471151010991171141051161210470751011210821011120360841211121010591201121
16000003082083065117114000002091066172243023248006008084224002000000120112000000
00016204812915904801300600904213407213424701300100100100500000312914100004812913
70021291290001470240551001320880292340110392460381500600310321850101450120312510
76084112199225074191087036134063247241133125208012155118068100102172089086099139
03102920923315912721702608409305223313417307206111517724316119303907917910804809
52050420620661691000981401672370992150140482270370582130312461020362221460721182
40120038204086151124103015043089182050120201011131197164135221168062051117193002
00300100000111600000508804605304805712611400002510609711809704611510109911711410
51161210460751011210821011120360841211121010000000000000000000000000001800000012 01
14000014106097118097046108097110103046069110117109000000000000000000000000000018000
00012011211600000608000850660760073067</details></packet>
client connected..
waiting for connection at port:1111
```

Figure.6. Encryption of session and secret key

4. CONCLUSION

This paper provides the efficient data storage security in cloud services by considering various security issues in the system. For getting better one algorithm for efficient cloud storage security, system analyzes the different crypto graphical algorithms which are used for Securing cloud Communication. So from these different algorithms we are considering RSA algorithm for secure communication, MD5 algorithms for data integrity and Kerberos type of authentication system as third party auditor which then improve the security message flow between user and cloud sever through third party which does not demand local copy of user data information.

REFERENCES

[1] Kangchan Lee,” Security Threats in Cloud Computing Environments” International Journal of Applications and Security , Vol. 6, No. 4, October, 2012.

[2] Baghel, S.V. , Theng, D.P. , “A Survey for Secure Communication of Cloud Third Party Authenticator ” International Conference on Electronics and Communication Systems (ICECS-15), vol.. 1 , pp. 51-54, February 2015.

[3] C. Wang, Sherman S. M. Chow, Q. Wang, K. Ren and W. Lou, “Privacy-Preserving Public Auditing for SecureCloud Storage”, IEEE Transaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.

[4] A.Mohta, Lalit Kumar Awasti,“Cloud Data Security while using Third Party Auditor”, InternationalJournal of Scientific & Engineering Research, Volume 3,Issue 6, ISSN 2229-8 June 2012.

[5] Q. Wang, W. Lou and Jin Li, C. Wang,K.Ren “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, Parallel and Distributed System on IEEE Transaction, vol. 22, no. 5, pp. 847and 859,2011.

[6] C. Wang, W. Lou, and Q. Wang, K. Ren “Privacy-Preserving Public auditing for storage security in cloud computing,” in Proc.of IEEE INFOCOM’10, March 2010.

[7] C. Papamanthou, C. Erway, and R. Tamassia A. Küpçü, , “Dynamic provable data possession,” in the 16th ACM conference on Computer security and communications, 2009, pp. 213–222.

[8] C. Wang, Q. Wang and K. Ren, “Ensuring Data Storage security in Cloud Computing”, IEEE Conference Publication, 17th International Workshop on Quality ofService (IWQoS), 2009.

[9] Theng, D.; Hande, K.N., "VM Management for Cross-Cloud Computing Environment," Communication Systems and Network Technologies (CSNT), 2012 International Conference on , vol., no., pp.731,735, 11-13 May 2012.

[10] Theng, D., "Efficient Heterogeneous Computational Strategy for Cross-Cloud Computing Environment," Emerging Research in Computing, Information, Communication and Applications (ERCICA), 2014 Second International Conference on, vol., no., pp.8,17, 1-2 August 2014.

[11] Gourkhede, M.H.; Theng, D.P., "Analysing Security and Privacy Management for Cloud Computing Environment," Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on , vol., no., pp.677,680, 7-9 April 2014.