Implementation of Shared Authority based Privacy-Preserving Authentication Protocol in Cloud Computing

Miss. Suvidha S. Sangole[1] Prof. M. R. Ingle[2] Prof. Dinesh S. Gawande[3]
[1]PG Student [2,3]Assistant Professor
[1,2,3]Department of Computer Engineering
[1,2,3]DBACER, Nagpur, India

Abstract— Cloud computing has a lot of security crises that are acquirement great concentration nowadays, including the data shelter, network security. Data protection is one of the most important security crises that arise in real world, because associations won't relocate its data to isolated machines if there is no definite data protection from the cloud service providers. Many procedures are suggested for data shelter in cloud computing, but there are still a lot of difficulties in this subject. The most popular security method includes SAPA i.e. "shared Authority based Privacy preserving Authentication Protocol". Ambition of this paper is to investigate and estimate the most important security techniques for data sheltering in cloud computing. We have proposed SAPA, the shared access authority is achieved by unidentified access request and privacy contemplation, attribute based access control allows the single user to access own data. To provide the data invoking from the other trustworthy party and sharing among the multiple users proxy re-encryption scheme is used by the cloud server. It indicates that the proposed scenario is possibly applied for enhanced privacy-preservation and security in cloud applications. We have done the review study on this scenario. In this paper we will focused on implementation of this review with assuring a improved result.

Key words: RSA, Pseudo–Random Number Key Generation, Privacy, Cloud Computing, Data Security, Authentication, Authorization

I. Introduction

Cloud computing is the aptitude to access a group of computing resources owned and continued by a third party via the Internet. It is not a new technology but a way of distribute computing possessions. Cloud computing usually involves the relocate, storage, and dispensation of data. There are a lot of security techniques for data security that are acknowledged from the cloud computing providers, and they all make available verification, confidentiality, access control and agreement. We propose a shared authority based privacy-preserving authentication protocol (SAPA) to concentrate on above privacy issue for cloud storage.

In the SAPA,

1) Shared access authority is accomplished by unidentified access demand corresponding mechanism with security and privacy contemplations (e.g., authentication, data ambiguity, user privacy, and forward security);
2) Attribute based access control is approved to appreciate that the user can only admittance its own data pasture;
3) Proxy re-encryption is functional by the cloud server to supply data sharing along with the multiple users. Meanwhile, universal compensability (UC) model is established to prove that the SAPA hypothetically has the plan correctness. It designated that the proposed protocol recognizing privacy-preserving data access authority sharing, is attractive for more than one user mutual cloud applications.

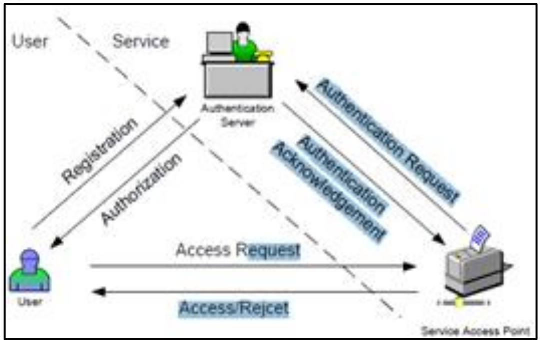


Fig. 1: System Architecture

II. Related work

Chia-Mu Yu, Chi-Yuan Chen, and Han-Chieh Chao [1] they have aspired to plummeting both the server side dormancy and the user side dormancy, they proposed an alternative POW design on the problem of unlawful file downloading in de-duplicated cloud storage. Deyan Chen, Hong Zhao [2] they have make available a diminutive but all-round analysis on data security and privacy defence issues associated with cloud computing across all phases of data life cycle. Ramgovind S, Eloff MM, Smith E [3] they have offer an generally security observation of Cloud computing. P. Vidhya Lakshmi, Dr. S. Sankar Ganesh [4] they have introduced a new privacy dispute during data accessing. Data confidentiality and data integrity is assured by authentication. H. Wang **[5]** have revision proxy provable data possession (PPDP). Apurva Gomase, Prof.Vikrant Chole [6] has projected re-encryption in which the data is encrypting twofold. Somesh P. Badhel, Prof. Vikrant Chole [7] have given a brief review on different issues of data backup and resurgence of data after damage for Cloud Computing such as retaining the cost of functioning and functioning complexities as low as possible. Somesh P. Badhel, Prof. Vikrant Chole [8] have offered attribute design of proposed Backup recovery technique for cloud computing.

III. Security issues and challenges of cloud computing

Security is measured as one of the most crucial aspects in everyday computing and it is not altered for cloud computing due to sensitivity and significance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully estimated with respect to the security. Cloud Computing has several most important issues and disquiets, such as data security, conviction, potential, convention, and performances issues. One issue with cloud computing is that the administration of the data which might not be fully dependable; the risk of malicious insiders in the cloud and the failure of cloud services have arriving a strong attention by companies. Whenever we talk about security of cloud computing, there are various security issues occur in path of cloud.

IV. Proposed Work Plan

We have proposed different security algorithms to purge the apprehensions regarding data loss, isolation and privacy while accessing web purpose on cloud. In this paper, we address the abovementioned privacy issue to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which appreciates authentication and authorization without negotiation a user's private information.

The major assistance is as follows:

1) Categorize a new privacy dispute in cloud storage, and deal with a restrained privacy issue throughout a user demanding the cloud server for data sharing, in which the disputed request itself cannot make public the user's privacy no matter whether or not it can obtain the access authority.
2) Propose an authentication protocol to improve a user's access appeal related privacy, and the shared access authority is accomplished by unidentified access request matching system.
3) Apply cipher text policy feature based access direct to appreciate that a user can consistently access it disseminate data fields, and assume the proxy re-encryption to provide stand-in authorized data sharing among numerous users.

The remainder of the paper is organized as follows. Section 2 introduces related works. Section 3 introduces the system model challenges, and Section 4 presents the proposed Authentication protocol system model. The UC model based formal security analysis is performed in Section 5 Finally, Section6 draws a conclusion.

V. Security Algorithm Used in Cloud Computing

A. *RSA Algorithm*

The most common Public (Shared) Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). RSA is essentially an asymmetric encryption /decryption algorithm. It is asymmetric in the logic, that here public key disseminated to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not commune to everyone.

How RSA is going to employment in cloud upbringing is explained as: RSA algorithm is used to make sure the protection of data in cloud computing. In RSA algorithm we have encrypted (from plain text to cipher text) our data to make available security. The principle of securing data is that only fretful and approved users can access it. After encryption data is stored in the cloud storage. So that when it is mandatory then an appeal can be positioned to cloud provider. Cloud provider validates the user and relinquishes the data to user. As RSA is a Block Cipher in which every significance is mapped to an integer. In the projected cloud environment, Public key is known to all users who are using it, whereas Private Key known only to user who initially owns the data. Thus encryption is done by the cloud service provider or contributor and decryption is done by the cloud user or customer. Once the data is encrypted with the Public key, it will be decrypted using the corresponding Private Key only which is allotted only to the authenticated trusted user.

B. *Pseudo-random Number Generators*

"Random" numbers are more appropriately mention to as pseudo-random numbers, and pseudo-random sequences of such numbers. A pseudo-random number generator (PRNG), also known as a deterministic random bit generator (DRBG) algorithm, is an algorithm for producing a progression of numbers whose properties fairly accurate the properties of progressions of random numbers. The PRNG-generated progression is not accurately random, because it is entirely indomitable by a comparatively small set of preliminary values, called the PRNG's seed (which may include truly random (dissimilar) values). Even though progressions that are closer to accurately random can be produced using hardware random number production, pseudo-random number generators are significant in preparation for their speed in number productions and their reproducibility.

PRNGs are innermost in relevance's such as reproduction (e.g. for the Monte Carlo method), electronic games (e.g. for bureaucratic generation), and cryptography. Cryptographic applications necessitate the output not to be unsurprising from previously outputs, and more complicated algorithms, which do not come into the linearity of simpler PRNGs, are needed.

- Approximately all network security protocols depend on the arbitrariness of certain parameters.
  - Nonce - used to avoid rerun
  - Conference(session) key
  - Exceptional parameters in digital signatures
- Monte Carlo reproduction is a statistical procedure for mathematically solving differential equations. Randomly generates state of affairs for accumulate information.

1) *Algorithm*

- Separate the series of the random number generator into equivalent intermission.
- (Divide into 4 intervals for a random walk in two dimensions)
- Produce a number, if the number falls in:

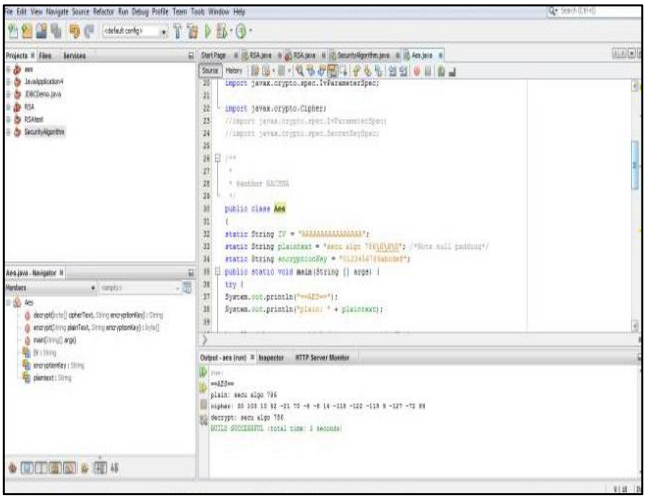
1) First intermission, increment X
2) Second intermission, increment Y
3) Third intermission, decrement X
4) Fourth intermission, decrement Y

- Produce t steps for a random walk for n walks.
- Compute the means squared distance reached.
- Connive this distance against time.
- A plot for several values of t and distance should approximately be linear.
- Else the random numbers are not in the approved manner disseminated.

VI. Implementation and Results

Implementation of algorithms has been done using Eclipse with Java. Coding's used for algorithms have shown below:

A. *Coding 1 used for making Cloud data secure*

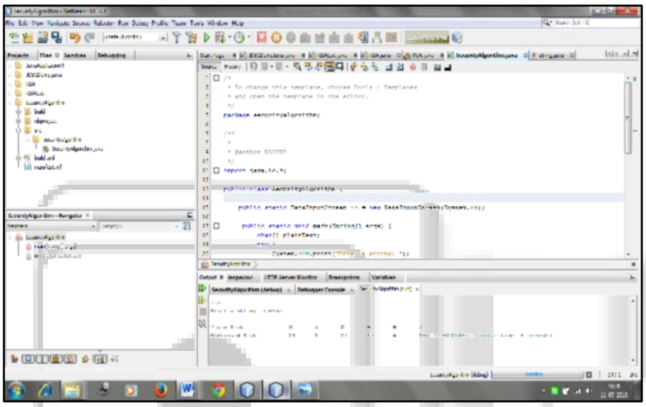


```
import javax.crypto.spec.IvParameterSpec;

import javax.crypto.Cipher;
//import javax.crypto.spec.IvParameterSpec;
//import javax.crypto.spec.SecretKeySpec;

/**
 *
 * @author RACHNA
 */
public class Aes
{
static String IV = "AAAAAAAAAAAAAAAA";
static String plaintext = "secu algo 786\0\0\0"; /*Note null padding*/
static String encryptionKey = "0123456789abcdef";
public static void main(String [] args) {
try {
System.out.println("==AES==");
System.out.println("plain: " + plaintext);
```

```
run:
==AES==
plain: secu algo 786
cipher: 30 103 10 92 -21 70 -8 -8 14 -118 -122 -118 9 -127 -72 88
decrypt: secu algo 786
BUILD SUCCESSFUL (total time: 1 seconds)
```

Fig. 1: Coding 1

B. *Coding 2*



```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */
package securityalgorithm;

/**
 *
 * @author [illegible]
 */
import java.io.*;

public class SecurityAlgorithm {

    public static DataInputStream in = new DataInputStream(System.in);

    public static void main(String[] args) {
        char[] plainText;
        try {
            System.out.print("Enter a string: ");
```

Fig. 2: Coding 2

VII. Conclusion and Future Prospects

In this paper, we have projected a privacy preserving access authority sharing in cloud computing environment. Where we will acknowledge a new privacy task during data retrieve. Data confidentiality (do not release data to anyone) and data integrity (reliability) will be exact by authentication. During the broadcast the combined values will be swapped hence data inscrutability will be achieved. User privacy is improved by unspecified access demand to confidentially report to the cloud server about the user's access need. We have projected a shared access authority by unidentified access request corresponding device with security and privacy considerations , characteristic based access control will help to be aware of that the user can only access its own data fields; proxy re-encryption by the cloud server will offer data allocation between the multiple users. This shows that the projected method can functional for enhanced privacy conservation in cloud application.

References

[1] Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , Cloud Computing System Based on Trusted Computing Platform, International Conference on Intelligent Computation Technology and Automation, Volume 1, May 2010, On page(s): 942-945.

[2] Rachna Arora, AnshuParashar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.

[3] KireJakimoskiInternational Journal of Grid and Distributed Computing Vol. 9, No. 1 (2016), pp.49-56.

[4] Wei-Fu Hsien1, Chou-Chen Yang1, and Min-Shiang Hwang2;3 International Journal of Network Security, Vol.18, No.1, PP.133-142, Jan. 2016.

[5] Pearson, S., Benameur, A., Privacy, Security and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference 2010, On page(s): 693-702.

[6] RohitBhadauria and SugataSanyal, A Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, Volume 47- Number 18, June 2012, On page(s): 47-66.

[7] C. Liu, J. Chen, L. T. Yang, X. Zhang, C. Yang,R. Ranjan, and K. Ramamohanarao,\Authorized public auditing of dynamic big data storage on cloud with efficient variable _ne-grained updates," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2234{2244, 2014.

[8] [8] C. Liu, C. Yang, X. Zhang, and J. Chen, \External integrity verification for outsourced big data in cloud and IoT: A big picture," Future Generation Computer Systems, vol. 49, no. 6, pp. 58{67, 2015.

[9] Chia-Mu Yu, Chi –Yuan Chen, Han-ChiehChao,"proof of ownership in de-duplicated cloud storage with mobile efficiency".

[10] Deyanchen, hongzhao, "Data security and privacy protection issue in cloud computing"IEEE conference of computer science and electronics engg, 2013.

[11] Ramgovind S, Eloff MM, Smith E, "The management of security in cloud computing".

[12] P.VidhyaLlakshmi,Dr.s.Sankar Ganesh, "A secure cloud storage system with data forwarding using proxy re-encryption scheme", international journal for trends in engg and tech , April 2015.

[13] Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, [online]ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.

[14] L. Badger, T. Grance, R. Patt-Corner and J. Voas, "Cloud computing synopsis and recommendations (draft), nist special publication 800-146", Recommendations of the National Institute of Standards and Technology, Tech. Rep. (2011).

[15] U. Khalid, A. Ghafoor, M. Irum, and M. A. Shibli, "Cloud based secure and privacy enhanced authentication & authorization protocol", Procedia Computer Science, 22, (2013), 680-688.

[16] T. Acar, M. Belenkiy and A. Küpçü, "Single password authentication", Computer Networks, 57(13), (2013), 2597-2614.

[17] G. Wang, Q. Liu, J. Wu and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Computers & Security, 30(5), (2011), 320-331.

[18] C. I. Fan and S. Y. Huang, "Controllable privacy preserving search based on symmetric predicate

encryption in cloud storage", Future Generation Computer Systems, 29(7), (2013), 1716-1724.

[19] D. W. Chadwick and K. Fatema, "A privacy preserving authorisation system for the cloud", Journal of Computer and System Sciences, 78(5), (2012), 1359-1373.

[20] Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp? tp=& arnumber=6374615, 2012.