Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Three-Tier Confidentiality Framework for Cloud Data Security and Integrity

Gurjot Kaur, Naveen Kumari

Department of Computer Science and Engineering

Punjabi University Regional centre for IT and Management, Mohali, Punjab, India

Abstract— Cloud computing is a term coined for something which involves delivering hosted services over internet. The major advantage of cloud computing is reduction in cost and for this very reason this paradigm is being readily adopted by many software enterprises. In that pretext, none can still leave their data at risk with a firm which claims that it would secure it. Hence forth, it becomes a liability on our part to ensure data security before we outsource it. In this paper, architecture to cloud data security has been proposed. This architecture distributes the entire framework into different platforms. The whole of data will only be accessible if the hacker or any malicious intruder reaches to all the networks involved. The main idea of this proposed work is to design and validate a unique framework which combines different existing platforms of third party authentication, encryption scheme and access control techniques into a single environment.

Keywords— Authentication, cloud computing, confidentiality, encryption, integrity.

I. INTRODUCTION

In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy [4]. To maximize the effectiveness and minimize the cost, security and privacy must be considered from the initial planning stage at the start of the systems development life cycle. Attempting to address security after implementation and deployment is not only much more difficult and expensive, but also more risky. Cloud computing is an emerging technology which is not yet completely established in terms of data storage and security. We do expect it to be implemented in the upcoming years.

Classification of cloud Models [9]: There exist three types of service models namely SaaS, PaaS and IaaS for providing services to the cloud. Apart from the service models, cloud computing has four deployment models which include public, private, community and hybrid cloud.

Concerns regarding the adoption of cloud are interoperability, latency, platform or language constraints, regulations, reliability, resource control, and security [11]. Out of which all, security poses a real threat. In the discussion of cloud environment, major task of securing the data is done through encryption mechanisms, effective access control and/or third party authentication. There has been an introduction of various changes to these mechanisms as no traditional assumption of access control technique is directly applicable as the data owner and the cloud server are most likely to be in different domains [3]. In lieu to the cloud computing discussion, another cumbersome task of maintaining data security is to uphold the integrity of the data being held over the cloud server. Data integrity can be assured in many ways. The inclusion of the proposed integrated mechanism decreases the time and cost associated with the data integrity checking mechanism. An integrated architecture can be designed which collectively holds Encryption mechanisms, Access control and Third party authentication in a single framework [3].

II. PROPOSED WORK PLAN

The algorithm for this proposed framework is divided into three sub-algorithms, namely:

a. Sub-Algorithm for File Storage
b. Sub-Algorithm for File Downloads
c. Sub-Algorithm for TPA -Integrity Check

(a) Sub-Algorithm for File Storage

The stepwise description of this part of algorithm is as follows:

STEP I New user signs up for the service. Admin grants role-based access to the user.
STEP II If the user chooses to upload either a text or animation data onto the cloud database, otherwise, goto step VII.
STEP III The auto-Encryption mechanism comprising MD5 and Triple DES is executed.
STEP IV File is encrypted and a key to decryption is generated.
STEP V Append the key to a given signature; send to the email address of the current user (data owner).
STEP VI Add a static four-bit binary code to the file at the storage time. File is stored.

STEP VII Exit.

(b) Sub- Algorithm for File Download

The modular detail of this part of algorithm is as follows:

STEP I User logins on to the cloud periphery.
STEP II User may ask for his files to the server.
STEP III User will select the file for download.
STEP IV If the user attempts to access or download a file other than his/hers, Goto Sub-Algorithm for TPA - integrity check. Otherwise Goto step V
STEP V Download the file and decrypt it using the private key and signature from the mail. Goto step VII
STEP VI If user wants another file from his account, Goto step II. Otherwise, Goto Step VII
STEP VII Exit.

(c) Sub-Algorithm for TPA -Integrity Check

The third-party Auditor is basically concerned with the maintenance of data integrity. The step by step description of this sub-algorithm is as follows.

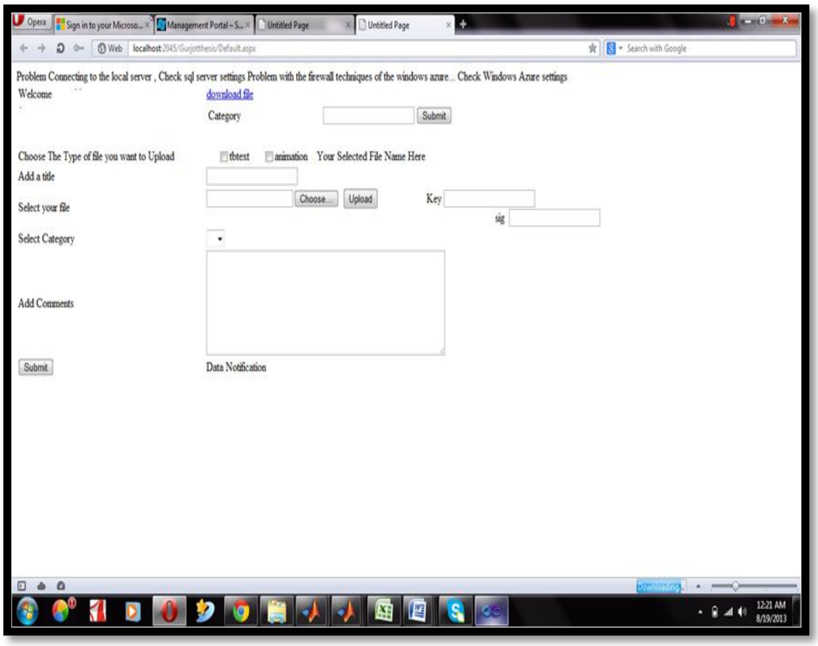
STEP I A user (other than the data owner), has made an attempt to access a stored file.
STEP II The binary format attached to that particular file is altered.
STEP III Thereby, a message of this attempt of an unauthorised access is reported to the Admin. Along with, following notifications:
(a) Id of the offending user
(b) Previous history of attempts if it is true Goto step IV, otherwise step V.
STEP IV The nature of breach is severe, permanently block the user.
STEP V Send a warning message to the user, instructing him not to repeat this again.
STEP VI Repeat from Step I, if there is other such attempt.
STEP VII Exit.

III. DESIGN MODULE

Module 1

To establish role based access control, admin assigns user an access depending upon his/her username. Only the signed up users will be allowed to proceed further. This authentication will be checked online on cloud itself.

Module 2



Problem Connecting to the local server , Check sql server settings Problem with the firewall techniques of the windows azure... Check Windows Azure settings

Welcome

download file

Category

Choose The Type of file you want to Upload □ tbtext □ animation Your Selected File Name Here

Add a title

Select your file

Key

sig

Select Category

Add Comments

Data Notification

Fig 3.1: file upload interface to the cloud

For the implementation of encryption in module 2, an encryption algorithm based on combination on md5 and tdes have been generated (in order to have better security than both md5or tdes alone). This combination has been used to encrypt the data files before being stored onto the cloud (confidentiality).

Module 3

(a) it describes the file download section of the proposed environment. Whenever a user wants to download his files, he/she has to select a file, which is available in the encrypted format. The decryption of the file would be done, if the user produces the key and signature associated with the same file.

(b) it also covers the scenario of the proposed framework which computes the average time taken by the existing as well as the proposed framework for the same amount of data. The time calculated here is in seconds.

IV RESULTS AND DISCUSSIONS

The performance of each existing individual mechanisms is compared with those deployed in the proposed integrated framework. The comparison has been on the basis of time taken in seconds. The results obtained are discussed in detail.

Encryption mechanism

The encryption time taken by the proposed hybrid technique (MD5 and TDES) has been compared to the time taken by RSA while encrypting the same file. The values obtained from subsequent simulations are shown in the table below. From the table 4.1, it can be noted that the time taken by RSA is lesser than that of the proposed integrated technique.

Table 4.1: Average Encryption time

Number of simulations	Time taken by the hybrid approach(in seconds)	Time taken by the RSA (in seconds)
1	6	2.8
2	7.3	4
3	8	4.4
4	9	5
5	11	5.9

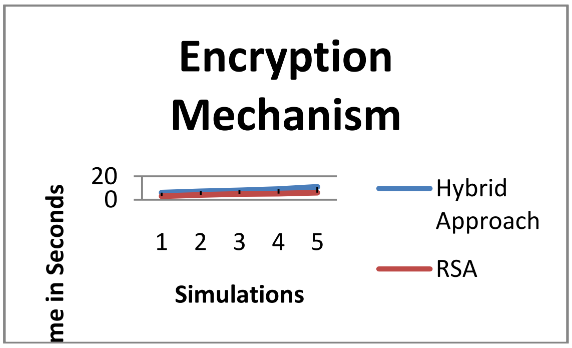


Figure 4.1 Average time taken by hybrid approach and RSA

From the graph, it is inferred that the time taken by RSA to encrypt a given file is less than the time taken by the proposed approach.

Third party authentication mechanism

There is method to add TPA approach externally to any framework but it has its own limitations in terms of increased overhead in calling routines. The time taken by an external TPA scheme and the proposed integrated TPA is shown in the table 4.2.

Table 4.2 Average Authentication time

Number of simulations	Time taken by the hybrid approach (in seconds)	Time taken by the external TPA (in seconds)
1	2	6
2	3.2	7.3
3	4	8.5
4	4.7	8.7
5	5	10

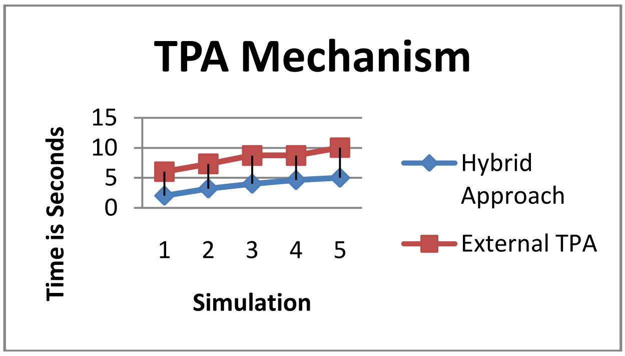


Figure 4.2: Average time taken by the hybrid approach and existing TPA

From the figure 4.2, it can be inferred that the average time taken by the hybrid approach is less than the external TPA. There is much of the overhead involved in calling the external libraries in the case of the existing approach. Therefore, it is depicted from the above graph that the proposed integrated approach takes less operational time on an average.

Signature verification

From the table 4.3, it is indicated that there is a meagre difference in the time taken by the RSA algorithm and the proposed hybrid approach. Although, a minute improvement is there, this is even unnoticeable practically.

Figure 4.3: Average time taken for Signature Verification

Number of simulations	Time taken by the hybrid approach (in seconds)	Time taken by RSA (in seconds)
1	1.2	1.4
2	2	2.3
3	2.5	2.6
4	3	3
5	4	4.1

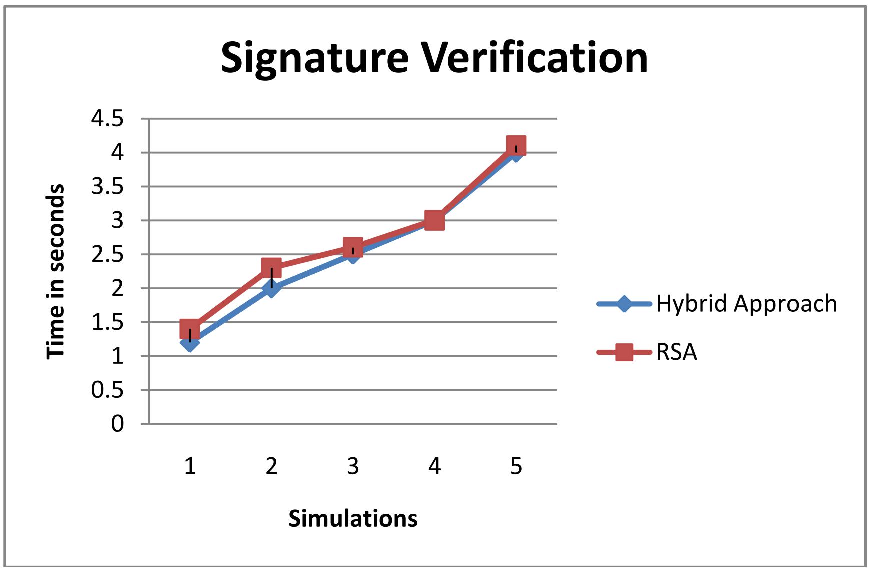


Figure 4.3: Average time taken for Signature Verification

From the figure 4.3, it is concluded that there is only a little improvement in the Signature Recognition process. In the proposed scheme, signatures are provided externally by the data owner whereas in RSA the case in not the same.

Accuracy

Accuracy in the existing approach and the proposed three-tier framework is measured in terms of data loss in the downloaded file. The average value of accuracy for both the approaches is shown in the table 4.4

Table 6.4 Average Accuracy of both approaches

Number of simulations	Downloaded content accuracy with existing approach (given in %)	Downloaded content accuracy with the proposed approach (given in %)
1	87	92
2	88	91
3	89	93
4	89.3	94

The figure 4.4 depicts that the content accuracy of the decrypted file is more in the proposed framework than the existing approach.

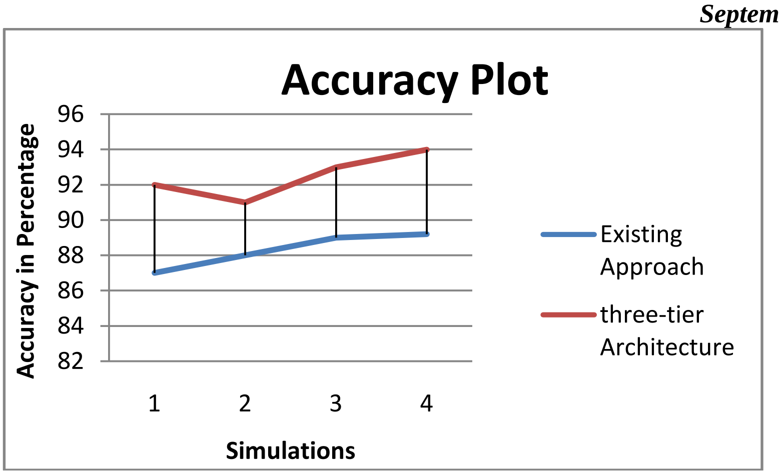


Figure 4.4: comparison of accuracy

This concludes that the time taken for encryption by the proposed hybrid approach is more than the RSA algorithm, the integrated TPA is efficient in terms of time as compared to the external TPA and the signature verification is also optimal in the proposed approach. The bottom line of all the discussion is that the proposed framework is capable of storing and retrieving a more accurate file both in terms of content accuracy and integrity, but the time taken for encryption is relatively more.

IV CONCLUSION

In this article, a three-tier confidentiality cum integrity framework has been proposed, as an attempt to design a combined platform which reflects the collaboration of benefits of all its components as well. All the primary concerns of the data security namely confidentiality, authentication and integrity have been addressed within in a single environment. Apart from designing the proposed solution, its implementation is also done using Dot Net framework over Microsoft Azure server. Moreover, in order to reflect the optimal efficiency of this composite platform in comparison to their individual counterparts, performance analysis has been done on the basis of average execution time and the outcome is graphically reflected and thoroughly discussed. Thus, from the analysis, we conclude here that the proposed framework results in an optimal behaviour in terms of confidentiality, encryption, TPA and authentication.

V FUTURE SCOPE

The proposed solution is implemented at a very smaller level where only a small amount of data is being outsourced to cloud. This could be extended for any huge data. The proposed framework may be extended to include many other management or operational controls. Role-based access provided to the new and existing users can be refined to categorize normal and premium users. Premium users may be entitled to access data uploaded by admin on pay-per usage basis.

REFERENCES

[1] Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou.," Secure ranked keyword search over encrypted cloud data", In Proc.of ICDCS, 2010.

[2] Cong Wang, S. Chow, Q. Wang, K. Ren, and W. Lou.,"Privacy-preserving public auditing for secure cloud storage", Computers, IEEE Transactions,pp(99):1, 2011.

[3] Gurjot Kaur and Naveen Kumari,"Secure cross cloud platform for efficient data storage and backup",International journal of Advances in Science and Technology,vol.7,No.1,July 2013.

[4] K.Govinda, V.Gurunathaprasad and H.Sathishkumar,"Third party authentication for secure data storage in cloud through digital signature using RSA ",International Journal of Advanced Scientific and Technical Research,vol.4,Issue 2,August 2012.

[5] Microsoft Windows Azure" http://www.microsoft.com/windowsazure/.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou.," Privacy-preserving multi keyword ranked search over encrypted cloud data", In Proc. of INFOCOM, 2011.

[7] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li,"Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, 2010.

[8] S.Sajithabanu and Dr.E.George Parkash Raj," Data Storage security in cloud",International Journal of Science and Technology,vol.2,Issue 4,pp.436-440,Dec 2011.

[9] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in Proc.of IEEE INFOCOM 2010, 2010.

[10] Wayen Jansen and Timothy Grance. Guidelines on security and privacy of Pubic Cloud Computing. Technical Report SP 800-144 Draft, National Institute of Standards and Technology, Information Technology Laboratory, January 2011.

[11] William Stallings:Cryptography and Network Security[book style]