PROVIDING COMPLETE SECURITY TO OUTSOURCED HIGH SENSITIVE DATA IN A CLOUD ENVIRONMENT

Suresh Krishna.S

Vijaya Sarathy.A.C

Arun Prasad.G

Mrs.V.Kavitha Priyadarshini, Assistant Professor

Jerusalem College of Engineering (Affiliated to Anna University), Chennai, India

Abstract

In this paper, we propose the idea of providing the attribute of 'absolute security' to the sensitive and confidential data outsourced by organizations. The organization mentioned here, maybe a space research organization, defense organization or a similar one. The main constraint involved in these cases is the privacy of data exchanged. Outsourcing helps with the attributes of cost efficiency, scalability and flexibility but puts up the danger of the data being revealed to the service provider or an illegal user. Thus, here we present a system that operates in a cloud where the data exchanged is just known to the trusted users and the admin, and not to anyone else including the service provider. The proposed system is provided with a 4-layer security checkpoint so that the security can never be breached under any circumstances. The search efficiency is also kept intact by not altering any of the constraints or algorithms of storage on the server side. Here, we insist on the point that securing the key is always less costly than securing the data.

Keywords: Security, Cloud, Protection

Introduction

In the present scenario, organizations prefer to move their huge amount of data collected to the cloud. The organizations prefer the outsourcing [Agrawal, Divyakant, 2009] of data or cloud storage due to low storage costs and instant access from anywhere. But while considering cases like an army information center or a space research organization, the information involved may be highly sensitive and confidential. So, storing such information

on to a cloud involves the serious danger of such information being exposed to an intruder or an un-trusted user. Therefore, the privacy of the information in the cloud [Zhou, Minqi, 2010] must be guaranteed. At the same time, the provided security must not reduce the search efficiency. Initially watermarking [R. Agrawal, P.J. Haas, and J. Kiernan, 2003] techniques were used but they can establish only the ownership of data and not guarantee the authorized access to data.

For, example consider the following situation, a research organization's head needs to store and exchange an important and sensitive piece of research information on to the cloud and the organization trusts only the top scientists of the organizations and no one else. That is, the organization's head doesn't even trust the other employees of the organization other than the top scientists (Ex: Mars Express). In such a case, storing the information on to the cloud would be a challenging job since the information's privacy must be preserved. There is also a danger of the service provider leaking the data or obtaining the information in the data for personal gain [Kimery, Kathryn M, 2002]. To sort out this problem, the service providers like Amazon offer a contract agreement promising not to leak out the data or use it to gain. But, still there lies a problem of trust. The question, "does a contract really guarantee the words exchanged in it?" cannot be answered with surety. Moreover, there is always a threat from hackers or intruders.

Thus, summarizing the above discussed points in short we understand that the outsourced sensitive and valuable data must be highly secured and also the search efficiency must be guaranteed.

Drawbacks of the Existing systems

Existing implemented systems [M.L. Yiu, I. Assent, C.S, 2010] either provide efficiency in terms of searching or in terms of privacy. Moreover considering the level of the sensitivity of the information in a research organization like ISRO, the security provided in the present scenario is too low. The single layer of security provided can be cracked very easily in spite of security playing a major part in these situations than the search efficiency.

Objective

The main objective of this study is to ensure that, even in the worst case, the attacker doesn't gain access to the key. The cost of securing the key from the intruder is always cheaper than implementing a method for securing the information after the intruder has obtained the key. The encryption is applied not just to the data but also to the key Separate encryption algorithms are used for the encryption of the key and the data. Thus, we propose a

system with 4 layer security checkpoint mechanism such that the key as well as the data is secured from any intruders or hackers. The key used is a one-time key.

Generalized Attacks on the present System

Several attacks can be carried out on the present single layer security systems. A few are discussed below:

Site Cloning and ARP poisoning attacks

The site cloning attack and ARP redirection/poisoning **[**Janbeglou, Maziar, 2010] attacks can be collectively used to obtain the user's login ID and password. The site user logs in into is replicated and then the ARP and DNS are poisoned to achieve this.

Social Engineering Techniques

Several advanced social engineering techniques like tabnabbing [http://en.wikipedia.org/wiki/Tabnabbing] and pharming **[**http://www.technicalinfo.net/papers/Pharming.html] can be used steal the user's credentials and obtain the key which in turn can be used to get access to the high sensitive information etc.,

Prevention of similar attacks on the proposed system

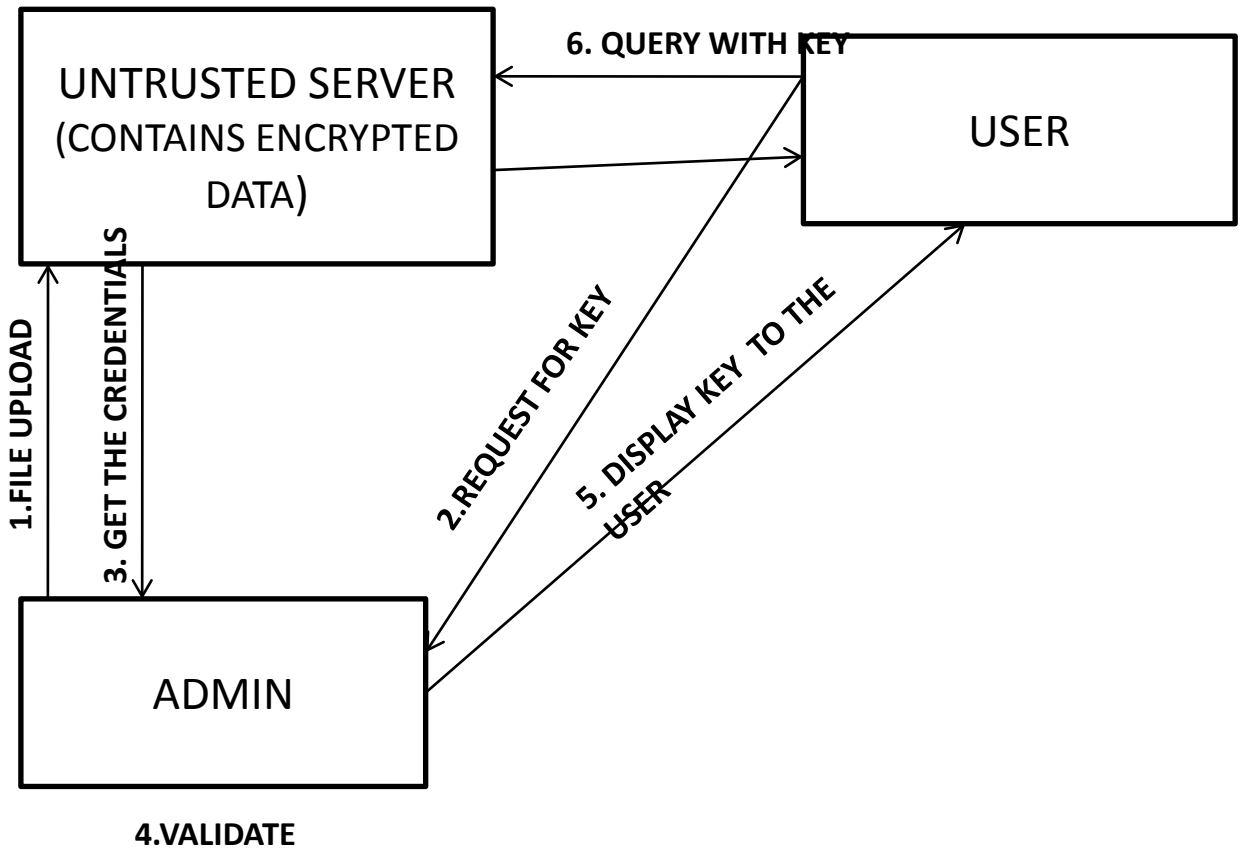
In our proposed system, the access to the organization's cloud is granted only if the user is authenticated. Moreover, the security checks are done stage by stage. That is, the user can't directly move on to the second stage verification. Even if the hacker directly enters the second stage verification by breaking the security, he will need to have type in the decrypted key, team name and the secret ID where he'll fail since these credentials are the output of registration and the first stage verification respectively. In the other case if the user gains the user's login ID and password and then cracks the user's mail by some means and gets the decrypted key the user will still fail in finding the team name and secret ID. Moreover, the key used here is a one time key. Therefore, absolute security is guaranteed by this.

Problem Definition

The systems at present involve the direct exchange of key and a single login system. That is, when the user enters his login ID and the password, the key is provided to the user. Thus, the existing systems are vulnerable to several security threats. For instance, consider that an intruder has obtained the user's ID and password by some means. Therefore, in such a case, the intruder can obtain the key instantly and easily obtain the data/files from the cloud.

Security Risks

The present systems operate as follows:



The users are first registered by the admin with a login ID and a password. Then the user uploads the content on to the un-trusted server. The content is encrypted and then uploaded. The user then requests the admin for the key. The admin validates the user using the credentials stored in the un-trusted server and then displays the key to the user. The user queries the un-trusted server with the key to obtain the decrypted data. Thus analyzing the process, a major security risk lies in the part that the user credentials are stored in the un-trusted server. Moreover, the single security verification system turns out to be a main vulnerability. That is, once the user credentials are stolen, the system provides no further security.

Proposed Solution

The security is enhanced by using the 4 layer security checkpoint mechanism and the search efficiency is guaranteed by not altering any constraints or algorithms of storage on the server side.

Four- Layer Security Checkpoint mechanism

To handle these situations, we propose a 4 layer security verification system.

Layer 1

First, the admin registers the users with their login ID (usually a mail ID) and password. Each registered user is provided with a Secret ID and team name. Only, those registered can request for the key later.

Layer 2

Then, the user has to enter his/her login ID and password to obtain the decrypted key. The key is a one-time key. That is, each time the user logs in, a new key is generated. The admin verifies the login ID and password and then sends the decrypted key to the user's login ID. The user is recommended to use different passwords for the organization and the mail for security reasons. Finally, the user logs into his mail by providing his ID and password to obtain the decrypted key.

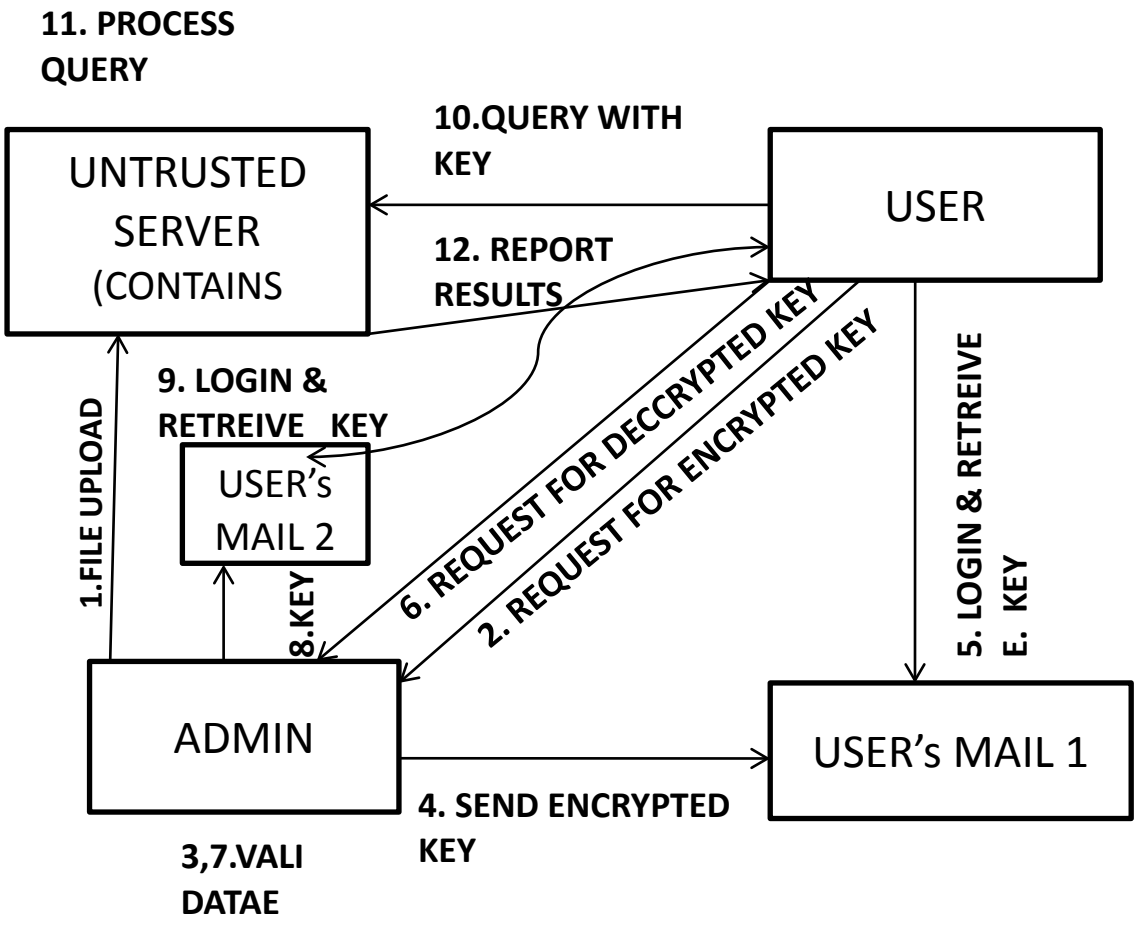
Layer 3 and Layer 4

After that, the user has to submit the following credentials to the admin:

1) The login ID
2) The password of the login ID
3) The secret team name
4) The secret ID
5) The decrypted key
6) A dynamic mail ID to send the key

If any of the parameters from 1) to 5) are incorrect, the user is simply logged out of the system. If all the details supplied are correct, the user is granted access to the cloud and the key is mailed to the user's dynamic mail ID. The user then logs into the dynamic mail ID and gets the key. The user is recommended to use a different mail ID rather than the one provided for the organization as the dynamic mail ID for security purposes. The user finally, queries the cloud for the file required and then supplies the key to decrypt the data.

Proposed Model and Operation



(Proposed Model Architecture)

The proposed model architecture consists of three entities, the data owner/admin, user and the server. The admin registers the users of the organization (each user registered by the admin is provided with a secret ID and team name) and uploads sensitive and confidential files onto the cloud/server. The admin trusts no one else except himself and the trusted users. That is, he doesn't even trust the service provider. Thus, he encrypts the data/files using a key K and then stores the data in the server. To retrieve the data, the user needs to get the key from the admin and then supply the key to obtain the decrypted data from the server. In this way the privacy constraints of the data are maintained.

Note: The credentials of the registered users are contained in the local server of the admin and not in the un-trusted server or cloud.

As, shown in the figure, the model operates as follows

1. First, the administrator/data owner uploads the data onto the cloud.

The user can then retrieve the data by using the following steps:

2. The user requests the admin to send the encrypted key to his/her mail ID using the organizational login ID and password.

3,4. Once, the user is authenticated, the encrypted key will be sent the user's E-mail.

5. The user now logs in to his mail ID to retrieve the encrypted key. This key is a one-time key. (ie., each time the user logs in a new encrypted key is generated).

6. Now, the user requests for the decrypted key by supplying in the, encrypted key, organization login Id and password, secret Id and team name and then enters a dynamic E-mail ID to send the key. (This may by some other Mail ID of the user or even the same one as before but supplied dynamically during the second phase verification)

7,8. Once the user is authenticated, then the decrypted key is sent to the user's dynamic mail ID. In case of any deviations in the credentials provided, the user is simply logged out of the system.

9. The user then logs in to the dynamic mail ID he/she mentioned and then retrieves the key\

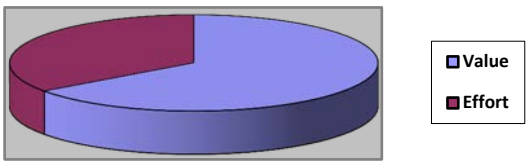
10. The user supplies the key to get the decrypted data from the cloud

11,12. The query is processed and if the key is valid the decrypted data is returned, or else the encrypted data are returned back from the server.

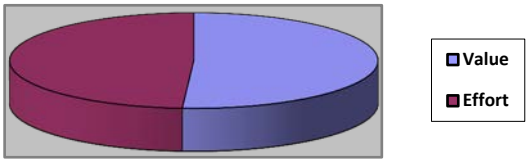
Comparative Analysis

Security

Comparing the security of our proposed system, with the present systems on the basis of Value/Effort Ratio, we find that the value/effort ratio is considerably reduced and is almost equal to 1. Therefore, the system turns out to be totally secure. By theoretical analysis and surveys we present the following data:



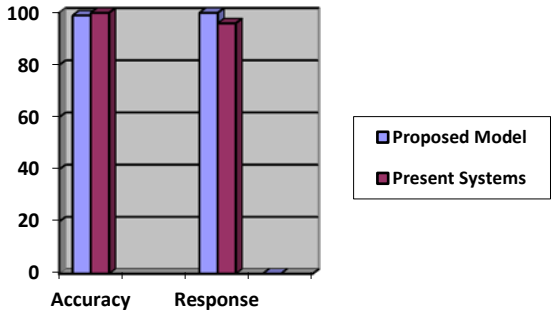
(Present Systems)



(Proposed System)

Search Efficiency

In this case we just guarantee that the search efficiency of our proposed system doesn't get reduced by the introduction of security features. Thus, experimentally evaluating the response time and the accuracy of the present and proposed systems, we present the following data:



(Search Efficiency Comparison)

Note: The graph denotes just the comparative values. That is, the percentage of efficiency of the proposed model when compared with present systems. (This doesn't mean that the efficiency or accuracy of the present system is 100%)

Conclusion

The proposed system has a key advantage in terms of privacy over the present systems. We now briefly summarize our understanding of the proposed solutions. The system comes out with both the features of efficiency and security. Existing systems involve the direct key exchange without encryption of the key. Also, the number of layers of security is restricted to a maximum of 2. Thus, these systems are vulnerable to several security breaches. Therefore, here we introduce the concept of 4 layer security, and also the direct key exchange mechanism is modified by putting in encryption. In the proposed system, the user is first

authenticated by the administrator using the four layer security and then the key is granted on successful authentication. Once the user gets the key, the uses the key to decrypt and view the information in the third party database (cloud). Thus, the information is secured not only from the un-trusted users but also from the "service provider" in a cloud environment but also the flexibility and the efficiency of the search are guaranteed. Therefore, the trade off between security, efficiency and flexibility is maintained. For carrying out the search efficiently secure k-NN compuation may be used [W.K. Wong, D.W. Cheung, B. Kao, and N. Mamoulis, 2009].

References:

R. Agrawal, P.J. Haas, and J. Kiernan, "Watermarking Relational Data: Framework, Algorithms and Analysis," The Int'l J. Very Large Data Bases, vol. 12, no. 2, pp. 157-169, 2003.

W.K. Wong, D.W. Cheung, B. Kao, and N. Mamoulis, "Secure k-NN Computation on Encrypted Databases," Proc. 35th ACM SIGMOD Int'l Conf. Management of Data, pp. 139-152, 2009.

Agrawal, Divyakant "Database Management as a Service: Challenges and Opportunities", Data Engineering, .ICDE '09. IEEE 25th International Conference, pp. 1709-1716, 2009.

Zhou, Minqi, "Security and Privacy in Cloud Computing: A Survey", Semantics Knowledge and Grid (SKG), Sixth International Conf, pp. 105-112, 2010.

http://www.technicalinfo.net/papers/Pharming.html

http://en.wikipedia.org/wiki/Tabnabbing

Kimery, Kathryn M, "Third-party assurances: the road to trust in online retailing", System Sciences, HICSS. Proceedings of the 35th Annual Hawaii International Conf., 2002

M.L. Yiu, I. Assent, C.S. Jensen, and P. Kalnis, "Outsourced Similarity Search on Metric Data Assets," DB Technical Report TR-28, Aalborg Univ., 2010.

Janbeglou, Maziar, Redirecting network traffic toward a fake DNS server on a LAN, Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conf., pp. 429-433, 2010.