International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

Academic Science

A Heuristic Approach to Provide Security For Data Storage In Cloud Computing Environment

C.Kamalanathan[1] R S Valarmathy[2] and S Karthick[3]

[1] Assistant Professor (Sr.G)/ECE, Bannari Amman Institute of Technology, Sathyamangalam, TamilNadu, India

[2] Senior Professor & Head/ECE, Bannari Amman Institute of Technology, Sathyamangalam, TamilNadu, India

[3] Assistant Professor (Sr.G)/ECE, Bannari Amman Institute of Technology, Sathyamangalam, TamilNadu, India

ABSTRACT *- Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Security issues such as data loss, phishing pose serious threats to organizations data and software. So, for the protection of data privacy, sensitive data usually have to be encrypted before outsourcing.*

In this paper, the data is encrypted using RSA algorithm, a public-key cryptography technique. The project is developed in the Windows XP environment. The project design is made using J2EE framework. The tools used in the scripting of the project are done with JSP. The Client scripts are made with HTML and Java Script. The data sharing of the cloud requirements are stored in relational database management system.

Keywords — Cloud computing, RSA algorithm

I. INTRODUCTION

Cloud Computing has been envisioned as the next generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history such as on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud. From users perspective, including both individuals and IT enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits such as relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances.

While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons.

First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time.

Secondly, for the benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsourced data. Examples include cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed or even hiding data loss incidents so as to maintain a reputation. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

does not offer any guarantee on data integrity and availability.

So, for the protection of data privacy, sensitive data usually have to be encrypted before outsourcing. Internet Protocol (IP) security is used for the tunneling, which provides a single authenticated, encrypted security associate, thus providing integrity control and secrecy. Here, the data is encrypted using RSA algorithm, a public-key cryptography technique.

II. EXISTING METHODS

Data encryption makes effective data utilization a very challenging task given that there could be a large amount of outsourced data files. Moreover, in Cloud Computing, data owners may share their outsourced data with a large number of users. The individual users might want to only retrieve certain specific data files they are interested in during a given session. One of the most popular ways is to selectively retrieve files through keyword-based search instead of retrieving all the encrypted files back which is completely impractical in cloud computing scenarios.

Keyword-based search technique allows users to selectively retrieve files of interest and has been widely applied in plaintext search scenarios, such as Google search [1]. Unfortunately, data encryption restricts user's ability to perform keyword search and thus makes the traditional plaintext search methods unsuitable for Cloud Computing. Besides this, data encryption also demands the protection of keyword privacy since keywords usually contain important information related to the data files. Although encryption of keywords can protect keyword privacy, it further renders the traditional plaintext search techniques useless in this scenario. To securely search over encrypted data, searchable encryption techniques have been developed in recent years [2]–[10].

Searchable encryption schemes usually build up an index for each keyword of interest and associate the index with the files that contain the keyword. By integrating the trapdoors of keywords within the index information, effective keyword search can be realized while both file content and keyword privacy are well-preserved. Although allowing for performing searches securely and effectively, the existing searchable encryption techniques do not suit for cloud computing scenario since they support only exact keyword search. That is, there is no tolerance of minor typos and format inconsistencies.

It is quite common that users' searching input might not exactly match those pre-set keywords due to the possible typos, such as Illinois and Ilinois, representation inconsistencies, such as PO BOX and P.O. Box, and/or her lack of exact knowledge about the data.

Traditional searchable encryption [2]–[8], [10] has been widely studied in the context of cryptography. Among those works, most are focused on efficiency improvements and security definition formalizations. The first construction of searchable encryption was proposed by Song et al. [3], in which each word in the document is encrypted independently under a special two-layered encryption construction.

Goh [4] proposed to use Bloom filters to construct the indexes for the data files. To achieve more efficient search, Chang et al. [7] and Curtmola et al. [8] both proposed similar "index" approaches, where a single encrypted hash table index is built for the entire file collection. In the index table, each entry consists of the trapdoor of a keyword and an encrypted set of file identifiers whose corresponding data files contain the keyword.

As a complementary approach, Boneh et al. [5] presented a public-key based searchable encryption scheme, with an analogous scenario to that of [3]. These existing schemes support only exact keyword search, and thus are not suitable for Cloud Computing.

III. PROPOSED METHOD

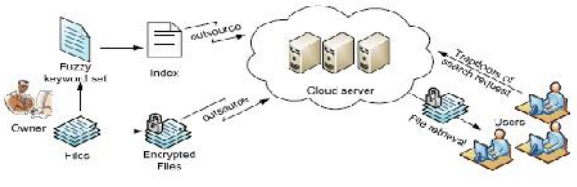

Figure1. Architecture of Fuzzy Keyword Search

In this paper, we formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when *exact* match fails.

IV. RESULTS AND DISCUSSION

Figure2. Screenshot for user login area

The user log in window created using J2EE frame work is shown in figure2. The user has to provide the user id and password by entering into the link provided by the server owner through the browser.

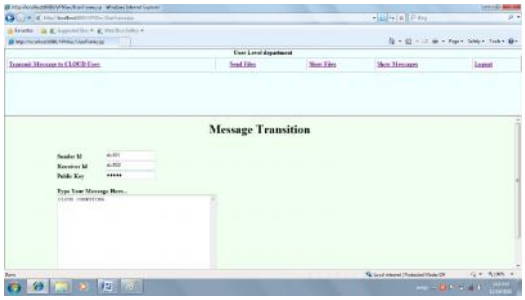

Figure3. Screenshot For Message Transition

Once logged in various options are provided such as send files, show files, show messages. The user can send message in the window as shown above. Here the user has to give the details such as sender id, receiver id and public key as provided by the server owner. Next the user can type the message in the dialog box appearing next to public key. The window appears as shown in figure3.

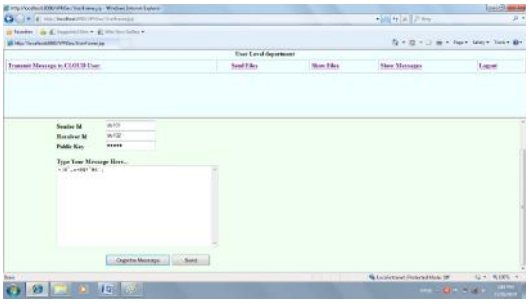

Figure4. Screenshot of Crypted message

After entering the text, there is tab named crypt the message by clicking it the message can be encrypted and finally the message can be sent as shown in figure 4.

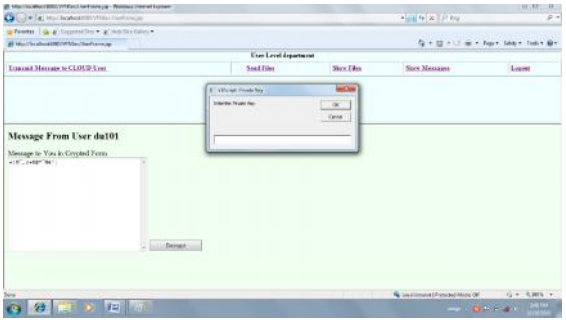

Figure5. Sreenshot for decrypting the message

The receiver can view the message by decrypting the message using the public key as shown in figure5.

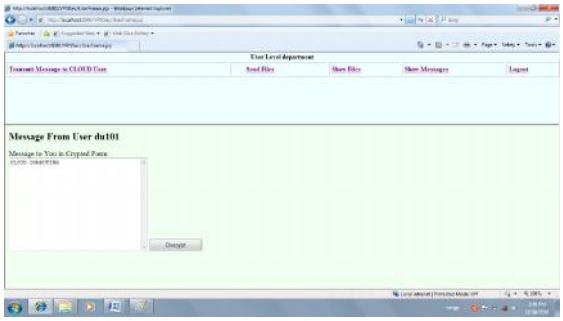

Figure6. Screenshot Showing The Decrypted Message

After decryption the original message can be retrieved as shown in the figure6.

V. CONCLUSION AND FUTUREWORK

As discussed earlier, cloud computing is the long dreamed vision of computing as utility. The major issue is security of outsourced data. So for the protection of data, it is encrypted using RSA algorithm before outsourcing the data. The project design is made using J2EE framework. The tools used in the scripting of the project are done with JSP. The Client scripts are made with HTML and Java Script. The data sharing of the cloud requirements are stored in RDBMS.

For the effective data utilization, of the outsourced encrypted data, fuzzy keyword search is used to securely search over encrypted data through keywords and to selectively retrieve files of interest, while maintaining keyword privacy. The goal is to explore new mechanism for constructing storage efficient fuzzy keyword sets (Wildcard-based

technique), to design efficient and effective fuzzy search scheme based on the constructed fuzzy keyword sets and to validate the security of the proposed scheme.

REFERENCES

[1] Google, *Britney spears spelling correction*, Referenced online at http://www.google.com/ jobs/ britney.html, June 2009.

[2] M.Bellare, A.Boldyreva, and A.O'Neill, *Deterministic and efficiently searchable encryption*, in Proceedings of Crypto 2007, volume 4622 of LNCS. Springer-Verlag, 2007.

[3] D.Song, D.Wagner, and A.Perrig, *Practical techniques for searches on encrypted data*, in Proc. of IEEE Symposium on Security and Privacy'00, 2000.

[4] E.-J.Goh, *Secure indexes*, Cryptology ePrint Archive, Report 2003/216, 2003, http://eprint.iacr.org/.

[5] D.Boneh, G.D.Crescenzo, R.Ostrovsky, and G.Persiano, *Public key encryption with keyword search*, in Proc. of EUROCRYP'04, 2004.

[6] B.Waters, D.Balfanz, G.Durfee, and D.Smetters, *Building an encrypted and searchable audit log*, in Proc. of 11th Annual Network and Distributed System, 2004.

[7] Y.-C.Chang and M.Mitzenmacher, *Privacy preserving keyword searches on remote encrypted data*, in Proc. of ACNS'05, 2005.

[8] R.Curtmola, J.A.Garay, S.Kamara, and R.Ostrovsky, *Searchable symmetric encryption: improved definitions and efficient constructions*, in Proc. of ACM CCS'06, 2006.

[9] D.Boneh and B.Waters, *Conjunctive, subset, and range queries on encrypted data*, in Proc. of TCC'07, 2007, pp. 535–554.

[10] F.Bao, R.Deng, X.Ding, and Y.Yang, *Private query on encrypted data in multi-user settings*, in Proc. of ISPEC'08, 2008.

[11] www.sunmicrosystems.com.