Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Apurva Kale, IJPRET, 2014; Volume 2 (9): 1076-1080 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

CROSS-LAYER KEY MANAGEMENT USING CLOUD COMPUTING

MISS. APURVA KALE[1], DR. H. R. DESHMUKH[2], N. S. BAND[3], S. H. KUCHE[3]

1. M. E. First Year, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
2. Prof and HOD, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
3. Asst. Prof, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Ever-increasing number of cloud based service providers takes cloud computing based paradigm as an advantage in order to efficiently offer services to private users, businesses, and governments. However, while cloud computing allows to transparently scale back-end functionality such a computing and storage, the implied distributed sharing of resources has severe implications when sensitive or otherwise privacy-relevant data is concerned. These privacy implications primarily stem from the in-transparency of the involved backend providers of a cloud-based service and their dedicated data handling processes. Likewise, back-end providers cannot determine the sensitivity of data that is stored or processed in the cloud. Hence, they have no means to obey the underlying privacy regulations and contracts automatically. As the cloud computing paradigm further evolves towards federated cloud environments in terms of secure data background, the envisioned integration of different cloud platforms adds yet another layer to the existing in-transparencies. In this paper, we discuss initial ideas on how to overcome these existing and dawning data handling in-transparencies and the accompanying privacy key-pathway based concerns. To this end, we propose to annotate data with sensitivity information as it leaves the control boundaries of the data owner and travels through to the cloud environment. This allows signaling privacy properties across the layers of the cloud computing architecture and enables the different stakeholders to react accordingly.

Keywords: Cloud computing, Data handling, key-pathway, back-end, privacy, secure data background.

PAPER-QR CODE

Corresponding Author: MISS. APURVA KALE

Access Online On:

www.ijpret.com

How to Cite This Article:

Apurva Kale, IJPRET, 2014; Volume 2 (9): 1076-1080

INTRODUCTION

The endeavor of cloud based background underlies in terms of the proper data based secure process in terms of background [1]. Data which is sensitive in nature [2] must be protected over the cloud which works upon the key-secure pathway and encryption of data while sending the same data to the server. Multi-Key though has been previously has hindrance of secure key with re-generating key trusted party [4] [5]. The hierarchical access can be efficiently achieved for users of different access class privileges [6] with re-encryption task required whenever group membership changes. Cloud-based data privacy and secure- pathway with the vanish system having data encryption and decryption [7].Key share can be distributed on demand by some authority and accessibility is subject to degradation [8] over time with multi user key handling over varied pathways. The client requests storage of data in the cloud without assurance of exactly where it is stored, whether it is replicated and how long it is kept for and who exactly will access to it with encryption mode and decryption mode valid for key secured processing [1] [9]. In existing system there is one time login and also with no constraint with consideration parallel processed data [10] such as time constraint and validation [11].

OBJECTIVE

According to the propose method which works on key management and encrypt the data while sending that to the server. It makes use of the cloud economical storage cost to maintain key material, and to degrade it over time, so that the cost of key re-generation is minimized. The main contribution of this work is the novel utilization of a cloud's centralized data storage facility to store encryption key material.

METHODOLOGY

We are creating one application with Graphical User Interface (GUI) which will communicate with cloud storage for data transfer. Actual implementation of algorithm: The key management algorithm will be implemented in this step. We are generating one key for users and once the user will access the task then the key will be regenerated for other user. The encryption process will be applied in this level to make data confidentiality with refined analysis and testing in reference to its added pathway.

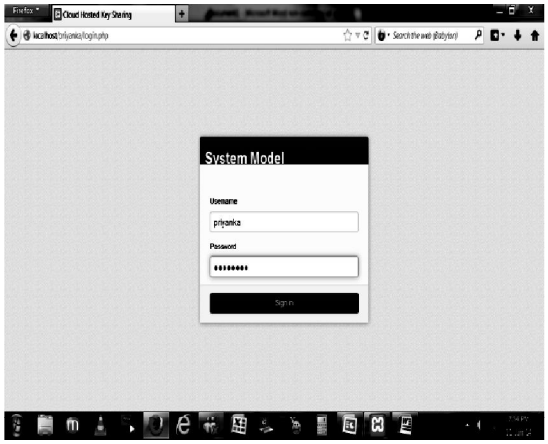

Fig. 1. System Model

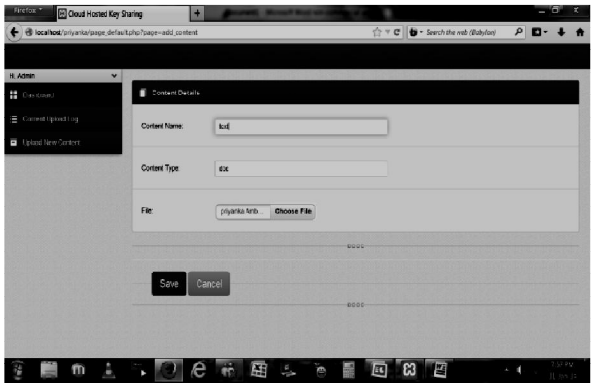

Fig. 2. Cloud Computing Security: From Single to Multi-clouds

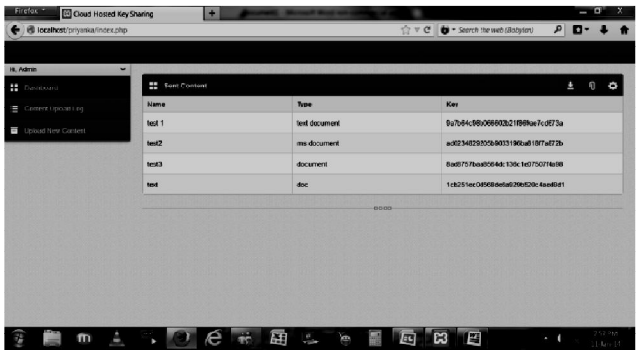

Fig. 3. Cloud Secured Key with their Pathway's

Tools required

Operating system compatible with Windows 95/98/2000/XP

provided with tomcat 5.0/6.X server having front end HTML, Java, JSP, AJAX applied with javascript. Data base connectivity applied with Mysql speed varied with 1.1GHz HDD performed with 20GB.

ADVANTAGES

Preserving the privacy of user data stored in the cloud in terms of its secured pathway. User oriented approach with client server key match having mixed mode operating system with full control over share management. The inexpensive storage capacity and high accessibility offered by a cloud provider.

CONCLUSION

This method implements the secure key sharing with secured-pathway as best way of storing data over the cloud in encrypted format. This method can help the data owner to keep their data secure from cloud provider. At same time it allows user the constraint based access to the cloud data.

REFERENCES

1. Cloud-Hosted Key Sharing Towards Secure and Scalable]Mobile Applications in Clouds by Piotr K. Tysowski and M. Anwarul Hasan International Conference paper 2013.

2. S. Jahid, P. Mittal, and N. Borisov, "EASiER: encryption-based access control in social networks with efficient revocation," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '11. New York, NY, USA: ACM, 2011, pp. 411–415.

3. Bessani, M. Correia, B. Quaresma, F. Andre,´ and P. Sousa, "Depsky: dependable and secure storage in a cloud-of-clouds," in Proceedings of the sixth conference on Computer systems, ser. EuroSys '11. New York, NY, USA: ACM, 2011, pp. 31–46.

4. P. Zimmermann, "Pretty good privacy: public key encryption for the masses," in Building in big brother, L. J. Hoffman, Ed. New York, NY, USA: Springer-Verlag New York, Inc., 2009, pp. 93–107.

5. T. Tiemens. (2012, May) Shamir Secret Sharing in Java. [Online]. Available: http://sourceforge.net/projects/secretsharejava Schneier, Applied Cryptography: Protocols, algorithms, and source code in C. Wiley, 2009.

6. J. Baek and Y. Zheng, "Identity-Based Threshold Decryption," in *Public Key Cryptography – PKC 2004, ser. Lecture Notes in Computer Science,*F. Bao, R. Deng, and J.Zhou, Eds. Springer Berlin / Heidelberg,2004,vol. 2947, pp. 262–276.

7. R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in *Proc. of the 18th USENIX Security Symposium, 2009.*

8. Avinash Mehta, Mukesh Menaria, Sanket Dangi and Shrisha Rao,밿nergy Conservation in Cloud Infrastructures?IEEE(2011).

9. Hao Li, Jianhui Liu, Guo Tang, A Pricing Algorithm for Cloud Computing Resources, International Conference on Network Computing and Information Security, IEEE (2011).

10. Janki Akhani, Sanjay Chuadhary, Gaurav Somani,?Negotiation for Resource Allocation in IaaS Cloud ACM,COMPUTE11, March 25-26, Bangalore, India(2011).

11. Jianfeng Yan, Wen-Syan Li, Calibrating Resource Allocation for Parallel Processing of Analytic Tasks?, IEEE International Conference on e-Business Engineering, IEEE (2009).