



INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 2)

Available online at: www.ijariit.com

Secured Data Access in Cloud Computing

Mayank Milind Murdio

Mayankmrd3@gmail.com

Rajiv Gandhi College of Engineering and Research,
Nagpur, Maharashtra

Shrirang Rajiv Paretkar

shrirang.paretkar@gmail.com

Rajiv Gandhi College of Engineering and Research,
Nagpur, Maharashtra

Saurabh Sanjay Vaidya

saurabhvaidya474@gmail.com

Rajiv Gandhi College of Engineering and Research,
Nagpur, Maharashtra

Rushikesh Gajanan Duve

duverushikesh@gmail.com

Rajiv Gandhi College of Engineering and Research,
Nagpur, Maharashtra

ABSTRACT

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. This paper proposed some services for data security and access control when users outsource sensitive data for sharing on cloud servers. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data to access control to untrusted cloud servers without disclosing the underlying data contents.

Our proposed scheme enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.

Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability and achieves fine - grainedness, scalability and data confidentiality for data access control in cloud computing. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

Keywords: *Cloud Computing, Database, Encryption Techniques and Decryption Techniques.*

1. INTRODUCTION

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. Our proposed scheme enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. Our proposed scheme has been divided into various modules which have its specific work. Each module is different from other. Our proposed scheme is highly efficient and provably secures under existing security models.

2. METHODS

We have researched on various encryption and decryption methods for the security of data. In our proposed scheme there are various modules which are used to build our scheme.

- Owner Module
- User Module
- Authentication

a) Owner Module

In this module, the owner will log in to his account and he can view the user details, Files which are downloaded and he can upload the files.

b) User Module

In this module, the user has to register and he will get the user id, key, and secret key. Using that user id and key the user has to login and by using the secret key the user has to download the file.

c) Authentication

Authentication means providing the access controls to the users. Each and every user has to register and he has to login with that user id and password. If the user wants to download the files he has to enter the secret key.

3. CONCLUSION

This paper aims at fine-grained data access control in cloud computing. One challenge in this context is to achieve finegrainedness, data confidentiality, and scalability simultaneously, which is not provided by current work. In this paper, we propose a scheme to achieve this goal by exploiting KPABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption. Moreover, our proposed scheme can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved. Formal security proofs show that our proposed scheme is secure under standard cryptographic models.

4. ACKNOWLEDGEMENT

At every outset, I express my gratitude to the almighty lord for showering his grace and blessings upon me to complete this project.

Although our name appears on the cover of this book, many people had contributed in some form or the other form to this project Development. I could not have done this project without the assistance or support of each of the following and I thank you all for the same.

I wish to place on my record my deep sense of gratitude to my project guide, **Mr. Akhil Anjekar**, for his constant motivation and valuable help through the project work. I also extend my thanks to other Faculties for their Cooperation during my Course. Finally, I would like to thank my friends for their cooperation to complete this project.

5. REFERENCES

- [1] www.support.mircosoft.com
- [2] www.developer.com
- [3] www.15seconds.com
- [4] www.msdn.microsoft.com
- [5] Asp.Net 3.5 Unleashed www.msdn.microsoft.com/net/quickstart/aspplus/default.com
- [6] www.asp.net
- [7] www.fmexpense.com/quickstart/aspplus/default.com
- [8] www.asptoday.com
- [9] www.aspfree.com
- [10] www.4guysfromrolla.com/index.aspx