ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Mobile Cloud Computing for Secure Light weighted Data Sharing with Time Factor

Pallavi.G[1], Daina K.K[2], Nithya.B.M[3], Vaibhavi.K[4]

Assistant Professor, Department of Information Science Engineering, SKIT, Bengaluru, Karnataka, India[1]

Assistant Professor, Department of Computer Science Engineering, CIT, Ponnampet, Karnataka, India[2]

U.G Student, Department of Information Science Engineering, SKIT, Bengaluru, Karnataka, India[3]

U.G Student, Department of Information Science Engineering, SKIT, Bengaluru, Karnataka, India[4]

ABSTRACT: With the arising demand of cloud computing , people can access their desired data whenever and wherever required by using their mobile devices .Further development of mobile cloud is comparatively restricted due to their security issues .The emerging studies are taking place to improvise cloud security. Due to their bounded computing resources this application is not much considerable. In this paper, we propose a mobile cloud computing for secure light weighted data sharing along with time constraints .The access control technology used here is CP-ABE , which is normally used in cloud environment , but this CP-ABE suitably changes the access control tree with time revocation to make mobile cloud environment more efficient .LDSS transfers more computation intensive access control tree to external proxy servers using mobile devices. Extensive performance and security analysis shows that the proposed scheme is providing high efficiency.

KEYWORDS: CLOUD COMPUTING, CP-ABE , ACCESS CONTROL TREE , PROXY SERVERS.

I.INTRODUCTION

Cloud computing is an emerging technology in the field of information technology .Cloud computing means storing data and accessing that data from the internet .More or less cloud computing describes highly scalable computing resources supplied as an outer service through internet on pay-as-usability basis. Generally , mobile devices have limited storage space and computing power .In adverse , the cloud has large amount of resources . So to achieve the adequate performance , it imperatively uses the provided resources from the cloud service provider(CSP) that stores and shares the data .Presently ,the distinct cloud mobile applications are greatly come in use .In this scheme, people can upload there photos ,videos ,documents and files to cloud and the data can be shared with other people with whom they want to share .Data providers can provide data management functionality by the CSP's. Data shared is sensitive because it may contain personal data files ,and hence data providers are let to make their data files public or can be shared only with distinct users .In this paper we propose Mobile Cloud Computing For Secure Light weighted Data Sharing With Time Constraint. LDS provides the following main contributions:

1. To provide efficient access control over cipher text ,the LDS-CP algorithm was developed which is based on Attribute Based Encryption(ABE).
2. To reduce revocation problem we have developed lazy re-encryption and description field to reduce revocation cost.
3. The operations, encryption and decryptions works on proxy servers.
4. In access structure a version attribute is added to give data privacy in LDS-CP-ABE. Decryption key is passed onto the proxy servers in a secured way along with time constraint.
5. Lastly, LDS framework is created to implement data sharing prototype.

This analysis helps us to reduce LDS overhead cost on the client side, which can build a minimal additional cost on the server side. Hence, this analysis is advantageous to implement a realistic data sharing security on mobile devices. Time

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

factor also plays a major role in dealing with mobile cloud computing. As soon as the Data Provider uploads the encrypted data the intended users will be able to access their data within the given span of time. Data which is stored in cloud can be protected by using an efficient method like information access mechanism.

II.RELATED WORK

Z. Qin, el. at[], worked on proxy re-encryption provides a optimistic solutions to safe guard the data which is being shared in the cloud. This enables the data provider to share the encrypted data in the cloud by using its own public key, which is later reorganized by a semi-trusted cloud server into an encryption purposefully for the authorized recipient for access control[1].

G. O. Karame, el. at[], worked on cloud storage providers like Drop box and Google drive which completely depend on data de-duplication to retain storage costs only by storing one copy of each uploaded file. A novel storage solution, checkbox, which allows a storage service provider to transparently provides its customers the de-duplication pattern of the encrypted data which has to be stored[2].

R. Masood, el. at[], worked on a planned analysis of the existing authorization solutions in cloud and then estimate their effectiveness against firmly established industrial standards that adapts to the distinctive access control requirements in the domain[3].

Junzuo Lai, el. at[], worked on Attribute-Based Encryption(ABE) which is a upcoming cryptographic primitive, which is extensively applied to implement fine-grained access control system for encrypted data. In this key-policy hint, attribute sets are used to explicate cipher text and secret keys which are connected to the access structures which specifies the entitled cipher text to be decrypted[4].

III.PROPOSED SYSTEM

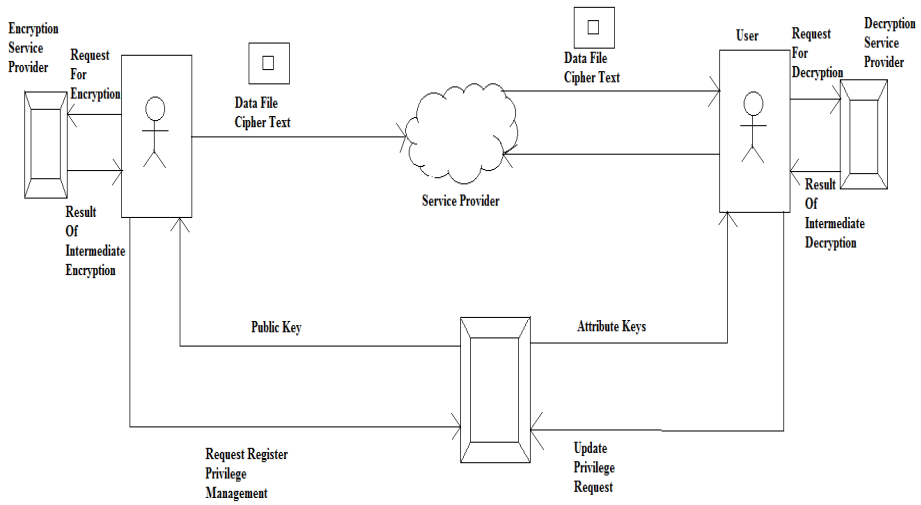

Fig 1:Lightweighted Data Sharing Framework

Considering, the problem in the existing system to overcome these flaws of existing system ware proposing LDS technique. To provide security against the CSP, the data is better to be encrypted before they are uploaded on to the cloud. This leads to the new problem on data encryption. The objection is how to provide an adaptive access control mechanism on cipher text decryption, where the plain text data can be accessed by the certified user. In addition, to

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

grant/revoke access opportunities to data user the system provides data owner an effective user privilege management capability. Abundant researches have been taken place to solve the problem of data access control over cipher text. Here are some common assumptions which are made as follows. First, the data that is sent to cloud which contains sensitive data are encrypted. Second, the honest and curious CSP is taken into consideration. Third, by encryption/decryption key distribution the user data is kept legitimated. These approaches are divided into four categories: simple cipher text access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attribute-based encryption. All these are designed for non-mobile cloud environment.

Text Encryption and Decryption In this system, the plain text uploaded to the cloud will be first encrypted by the user. Using the password method encryption is done. Using this password only the authorized password holder can decrypt the data. The user will uploaded the encrypted data with password. When the user appeal for the password it is the trusted authorizes duty to pass the password.

Text Request The file uploaded on the server is viewable to any user. The files are all in their encrypted format. Without the password the user can not view files. If the user wants to view then, the user first needs to request for the password to Trusted Authority then the authority checks for the user and then the valid user is provide password.

View Encrypted Data The uploaded encrypted data can be seen on the server side. When the user requests for the password the trusted authority, acting like a server provides the password.

View User Request The user requests for the password for encrypted data. The user request is viewed in Trusted Authority.

Provide Password The requested Trusted Authority validates the user and if the user is accurate then the Trusted Authority provide the password for the requested file by email. The decryption of file is done by using this password.

IV.RESULT

In this application, using ABE the LDS algorithm was developed, that provides efficient access control over cipher text. Revocation problem have been reduced due to the development of lazy re-encryption and decryption. We provide data privacy by using LDS-CP-ABE. As the decryption key will be passed on in secured way, which provides more security. This framework is mainly created for data sharing prototype. In this system, we have introduced an addition feature that is the time factor. This also helps us to keep our data more secure from unauthorized users.

V.CONCLUSION AND FUTURE WORK

In recent years, many studies on access control in cloud are based on Attribute Based Encryption (ABE). Due to limited computational resources of mobile devices traditional ABE is not suitable for mobile cloud. We proposed LDS system to overcome this issue. There are many issues regarding security of data sharing in mobile cloud. So the proposed LDS algorithm shifts the major computation overhead from mobile devices onto proxy servers. Thus, to assure that data privacy is maintained in mobile cloud and to reduce the computation overhead on mobile cloud LDS is an accurate algorithm as shown by many experiments. In further experiments we will undertake new approaches to ensure data integrity. And to increase the capacity of mobile cloud study, is taken place that, how to do cipher text retrieval over existing data sharing schemes.

REFERENCES

[1] Z. Qin, H. Xiongb, S. Wu, and J. Batamuliza, "A Survey Of Proxy Re- encryption For Secure Data Sharing In Cloud Computing," IEEE Transactions on Services Computing, Avaliable online, 2016.

[2] F. Armknecht, J.-M. Bohli, G. O. Karame, and F. Youssef, "Transparent data de-duplication In Cloud," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security ,pp. 886-900,ACM,2015.

[3] R. Masood, M. A. Shibli, Y. Ghazi, A. Kanwal, and A. Ali, "Cloud Authorization: Exploring Techniques And Approach Towards Effective Access Control Frame Work," Frontiers of Computer Science, vol. 9, no. 2, pp. 297–321, 2015.

[4] Junzuo Lai, Robert H. Deng, Yingjiu Li, et.al, "Fully Secure Key Policy Attribute-Based Encryption Constant-Size Cipher Text And Fast Decryption". In Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp.239-248, Jun 2014.