JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-8, Issue-3, Mar 2020 E-ISSN: 2347-2693

Reliability and Integrity in Lightweight Data Exchange for Mobile Cloud Computing

K.S. Bhosale[1*], M.R. Kshirsagar[2], K.L. Jadhav 3, S.G. Sayyad[4]

Dept. of CSE, Shivaji University / Karmaveer Bhaurao Patil College of Engineering, Satara, Maharashtra

DOI: https://doi.org/10.26438/ijcse/v8i3.9596 | Available online at: www.ijcseonline.org

Received: 26/Feb/2020, Accepted: 09/Mar/2020, Published: 30/Mar/2020

Abstract— Cloud computing being the latest technology, the storage and retrieval of personal data from mobile devices can be done from any location at anytime. The data security problem in mobile cloud is preventing development of mobile cloud. Studies have been conducted in various aspects to provide improved solutions to the cloud security. As mobile devices only have limited power and computing resources most of the solutions are not favorable for mobile cloud.. In this paper, we propose a reliable lightweight data exchange scheme for mobile cloud computing. The results show that the overhead on the mobile device side when users are sharing data in mobile cloud environments is effectively reduced using this technology.If the user wants to upload or download the data publicly then there wont be any encryption made over that data and if the data is confidential then certain algorithms for encryption can be applied to maintain the integrity.

Keywords— *Reliable, Integrity,Encrypted Data;*

I. Introduction

Cloud computing means storing data and accessing that data from the web rather than Using Traditional hardware for many of the operations. More than 50% of IT companies have moved their Business to the cloud. Sharing of knowledge over the cloud is that the new trend that's being assail . The amount of knowledge generated on each day to day life is increasing and to store that each one of the info in traditional hardware isn't possible due to limited storage capacity. Therefore, transferring the info to the cloud may be a necessity where the user can get unlimited storage. Security of that data over is the next big concern for most of us. After uploading the data to the cloud use loses its control over that data.

Since personal data files are sensitive, data owners are allowed to settle on whether to form their data files public or can only be shared with specific data users. Therefore, privacy of the private sensitive data may be a big concern for several data owners. When any of the people upload the data onto the cloud they are leaving their data in a place where monitoring over that data is out of their control, the cloud service provider can also spy on the personal data of the users. When someone has to share data over the data they have to share the password to each and every user for accessing the encrypted data which is cumbersome. Therefore, to solve this problem data should be encrypted before uploading it onto the cloud which can be safe from everyone. Now the data encryption part brings some new problems such as we have to provide an efficient encryption algorithm such that if the data Is in encrypted format it cannot be easily to get break or get accessed by any exploiters. The next big concern is time consumption for encryption. Traditional Hardware with big configuration can encrypt data in short amount of time but limited resource devices suffer from this problem. They require more amount of time of encryption and decryption. So, an efficient crypto system is to be proposed which can worked equally or heterogeneously on all of the devices.

II. Related Work

With the event of cloud computing and therefore the popularity of smart mobile devices, people are gradually getting familiar with a replacement era of knowledge sharing model during which the info is stored on the cloud and therefore the mobile devices are wont to store/retrieve the info from the cloud. Typically, mobile devices only have limited space for storing and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to realize the satisfactory performance, it's essential to use the resources provided by the cloud service provider to store and share the info . the development of cloud computing and therefore the popularity of smart mobile devices, people are gradually getting familiar with a replacement era of knowledge sharing model during which the info is stored on the cloud and therefore the mobile devices are wont to store/retrieve the info from the cloud. Typically, mobile devices only have limited space for storing and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to realize the satisfactory performance, it's essential to use the resources provided by the cloud service provider to store and share the info .

III. Methodology

There are various problems of data security therefore the data to be uploaded can be made secure by applying some encryption mechanisms like ciphertext policy attribute based encryption .The data encryption is a bit tedious task and also comes up with certain problems. To access the data by decrypting it can be challenging to the users as all the users cannot have knowledge regarding it. Proper access control mechanisms and priviledges must be provided to the users such as grant/revoke. Many researchers have worked on the issues related to the cipher text. The assumptions made in these researches are that the files to uploaded should have access priviledges. Files that are public can be uploaded and downloaded without any encryption decryption. The files that have confidential data can be encrypted.

ALGORITHM

```
Step-1: Start
Step-2: Accept the data from the user.
Step-3: The Attributes of the data from the users
formats are obtained by the Attribute-Based
Encryption.
Step-4: With the assistance of those Attributes,
Random key's generated, and sort of knowledge is
obtained for encryption by BRE algorithm.
Step-5: the info is converted into equal number of
blocks and N x N matrix are going to be generated
on the idea of those blocks.
Step-6: Based on number of blocks, pool of threads will
be created.
Step-7: Run the threads in multi core system to
make encrypted data briefly amount of your time .
Step-8: A secret key's generated so as to open the
encrypted file which is stored within the cloud.
Step-9: The secret key is shared to the user via email or
mobile number of the authorized user. This key are
going to be wont to decrypt the encrypted file.
Step-10: The file selected are going to
be decrypted within the original form using the key.
Step-11: Stop.
```

IV. RESULTS AND DISCUSSION

The data can securely be transmitted and downloaded according to the requirement of the user and hence RISS provides feasibility of access and reliability in data exchange.Secure transmission and storage over cloud provides enough space by allowing mobile storage space to be free for other purpose.

V. CONCLUSION AND FUTURE SCOPE

In recent years, many studies on access control in cloud are supported attribute-based encryption algorithm (ABE). However, traditional ABE isn't suitable for mobile cloud because it's computationally intensive and mobile devices only have limited resources. during this paper, we propose RILDE to affect this issue. It introduces completely unique RILDE-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that RILDE can ensure data privacy in mobile cloud and reduce the overhead on users side in mobile cloud. within the longer term work, we'll design new approaches to make sure data integrity. To further tap the potential of mobile cloud, we'll also study the thanks to do cipher text retrieval over existing data sharing schemes.

ACKNOWLEDGMENT

We take this opportunity to express our gratitude to “Karmaveer Bhaurao Patil college of Engineering, satara” and computer science & engineering department for sanctioning us the project topic “a light weight secure data sharing scheme for mobile cloud computing” & for allowing access to varied facilities. We sincerely wish to express hearty thanks to our project guide Dr.Sayyad S.G. For her encouraging & inspiring guidance. Her valuable suggestions were constant source of inspiration for us.we wish to express our thanks to our Hod prof. Ghatge D. D. for encouragement & providing us with the best facilities for our project work. We would also like to thanks to other teaching & non teaching staff.last but not the least we would like to thank all our friends, who helped us directly or indirectly. Helpful hand rendered by all of them will remain for while in our memory. Finally we admit the cooperation, coordination & diligence are our keywords for fulfillment.

REFERENCES

[1] Ruixuan Li, Member,IEEE, Chenglin Shen, Heng He, Zhiyong Xu, and Cheng-Zhong Xu, Member, IEEE,“A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing”,Volume: 6 , Issue: 2 , April-June 1 2018.

[2]Cheung, L., Newport, C.: Provably secure ciphertext policy abe. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2009, pp. 456–465. ACM, New York (2007)

[3]Shubham Chandugade, Prachi More, Shaikh Mohammad Shafi Rafiq ,IRJET,”Survey on Lightweight Secured Data Sharing Scheme for cloud computing”, Volume: 04 Issue: 10, p-ISSN: 2395-0072,Oct -2017

[4] K. Liang et aI., "A OFA -based functional proxy reencryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security,vol. 9, no. 10, pp. 1667-1680, Oct. 2014.

[5] H. Hong, Z. Sun. "An efficient and traceable KP-ABS scheme with untrusted attribute authority in cloud computing", JoCCASA, 5(2).pp.I -8,201 6.

[6] J. Liu, X. Huang, and 1. K. Liu, "Secure sharing of personal health records in cloud computing: Cipher textpolicy attribute-based signcryption," Future Gene rat. Com put. Syst., vol. 52, pp. 67-76, Nov. 2015.