SECURE AND EFFICIENT ACCESS FOR MOBILE CLOUD COMPUTING

[1]Seema Sultana,[2] Shailaja.S

[1] PG student,[2] Assistant Professor
[1,2] Department Of Computer Science,
[1,2] PDA College of Engineering, Kalaburagi, India.

Abstract : *As people are nowadays moving from storage devices to clouds for storing their personal data. Mobile devices can store and retrieve data whenever they want from wherever they want. But there is data security problem in storing the data in cloud. This data security problem in cloud is becoming more and more severe which is in turn preventing the further development of mobile cloud computing. There are many studies that have been conducted to improve the data security in cloud. Since mobile devices have only limited computing power and resources ,they are not applicable to mobile cloud computing hence solutions with low computational overhead are in need for mobile cloud applications*

***IndexTerms* – Mobile cloud computing, data encryption , AES, Idea, lightweight data sharing ,**

I. INTRODUCTION

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. More than 50% of IT companies have moved their Business to the cloud. Sharing of data over the cloud is the new trend that is being set on. The amount of data generated on a day to day life is increasing and to store that all of the data in traditional hardware is not possible because of limited storage capacity. Therefore, transferring the data to the cloud is a necessity where the user can get unlimited storage. Security of that data is the big concern for most of the data owners. After uploading the data to the cloud user loses its control over that data. As personal data files are very sensitive, data owners should allow to choose whether to make their data files public or can only be shared with specific data users. Therefore, privacy of the personal sensitive data is a big concern for many data owners.

When user 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. Another big concern here is the 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.

As the development and popularity of cloud computing and the mobile devices is increasing, people are gradually getting accustomed to a new era of data sharing model in which the data is being stored on the cloud and they are using mobile devices to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data.

Nowadays, various cloud mobile applications have been widely used. In these applications, people (data owners) can upload their photos, videos, documents and other files to the cloud and share these data with other people (data users) they like to share. Cloud service providers also provide data management functionality for data owners. As data owners are sharing their personal data-files they should be allowed to choose whether to make their data files public or can only be shared with specific data users. Clearly, data privacy of the personal sensitive data is a huge concern for many data owners.

The state-of-the-art privilege management access control mechanisms provided by the cloud service provider are either not sufficient or not very convenient. They cannot full fill all the requirements of data owners. First, when people upload their data files onto the cloud, they are leaving the data in a place where is out of their control, and the cloud service provider may spy on user data for its commercial interests and/or other reasons. Second, people have to send password to each data user if they only want to share the encrypted data with certain users, which is very cumbersome. To simplify the privilege management, the data owner can divide data users into different groups and send password to the groups which they want to share the data. However, this approach requires fine-grained access control. In both cases, password management is a big issue.

II. RELATED WORK

Shubham Chandugade, Prachi More ,Shaikh Mohammad, Shafiq Rafiiq [1] To overcome the challenge to share the data security over the cloud in this paper they have used combination of attribute-based encryption and byte-rotation encryption algorithm for encrypting the data before sending it to the cloud. This will help the user to securely store and share the data in encrypted form.

Chandini patel , Sameer Singh Chaubhan, Bharesh Patel[2] In this proposed data security framework they have used three different cryptographic implementation techniques for improving the security and privacy of data

1. Counter modes of block based encryption and decryption (CTR) for cryptographic functions by using simply XOR operations on block and key.

MAC-message authentication code for validating the integrity of file or data. Here hash function is used to generate the integrity key from password provided by mobile user.

. Blowfish symmetric cryptographic algorithm is used to improve the security of data.

Zhibin Zhou, Dijiang Hua [3] This paper presents a secure data enquiry framework for mobile cloud computing that includes two major component

PP-CP-ABE (privacy preserving-cipher policy-Attribute-based encryption) is for encryption and decryption to the cloud without revealing data content and secret keys and ABDS (Attribute based data storage) is to achieve scalable and fine-grained data access control and with this user's attribute are organized in a carefully constructed hierarchy so that the cost of membership revocation can be minimized.

Abdul Nasir Khan, M.L.Mat.Miah,Samee.U.Khan,Sajad.A.Madani [4] This Survey paper critically investigate different security frameworks proposed for the mobile cloud computing environment and most of the discussed security framework overlooked the trade-off between the energy consumption on the device and the expense of using cloud resources while designing a security framework.

A.Jyothi, Dr.B.Indira [5]This paper presents some of data security , storage and distribution mechanisms, such as it explains that the encryption alone is not the solution for data security because traditional data encryption scheme limits the data access by only allowing the user with corresponding decryption key to read the data. so to have an efficient data sharing with access control over the private data in the cloud, advanced cryptographic encryption schemes such as broadcast encryption(BE),Attribute-based encryption(ABE), Proxy encryption (PRE) have been employed in the design of cloud storage system.

Maheshwari U, Vingrablek R, Shaprio W[6] In this paper they framework a door control structure for conveyed capacity frameworks that accomplished fine-grained get with control perspective about a balance cipher text policy attribute-based encryption (CP_ABE) methodology in the recommend conspire, a proficient characteristics refused techno babble may be suggested on adjusting of the changing transforms for client's door reductions to immense scale frameworks. The examinations show that suggested get should control plot is probably secure in the discretionary prophet model and proficient should make associated with preparing.

Kan Yang, Xiaohua Jia, Kul Ren[7] In this paper they have examined the issue for secure what is more compelling similarly search again outsourced cloud data. Likeness search is the vital further more extra ordinary instrument flying arrangement initial endeavors a smothering strategy with fabricate stockpiling profitable likeness catchphrase set from a provided for record accumulation, for adjusting uproots as that similarity metric. The perspective of that, they toward that purpose amass a private trie-navigate gazing document what's more hint at it viably accomplishes those described similarity look convenience steady chase duration of the time multifaceted nature

III. Problem statement:

Personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the cloud service provider. However, the data encryption brings new problems. How to provide efficient access control mechanism on cipher text decryption so that only the authorized users can access the plaintext data is challenging. In addition, system must offer data owner's effective user privilege management capability, so they can grant/revoke data access privileges easily on the data users.

IV. SYSTEM ANALYSIS

EXISTING SYSTEM

As the development and popularity of cloud computing and the mobile devices is increasing, people are gradually getting accustomed to a new era of data sharing model in which the data is being stored on the cloud and they are using mobile devices to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data

PROPOSED SYSTEM

Apparently, to solve the above problems, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the cloud service provider. However, the data encryption brings new problems. How to provide efficient access control mechanism on cipher text decryption so that only the authorized users can access the plaintext data is challenging. In addition, system must offer data owners effective user privilege management capability, so they can grant/revoke data access privileges easily on the data users. There have been substantial researches on the issue of data access control over cipher text. In these researches, they have the following common assumptions. First, the cloud service provider is considered honest and curious. Second, all the sensitive data are encrypted before uploaded to the Cloud. Third, user authorization on certain data is achieved through encryption/decryption key distribution. In general, we can divide these approaches into four categories: simple cipher text access control, hierarchical access control, access control based on fully homomorphism encryption and access control based on attribute-based encryption (ABE). All of these proposals are for non-mobile cloud environment.

Propose a lightweight data sharing scheme for mobile cloud computing environment. The proposed method design an algorithm called LDSS-CP-ABE based on Attribute Based Encryption (ABE) method to offer efficient access control over cipher text. The proposed model uses proxy servers for encryption and decryption operations. In this designed approach, computationally intensive operations in ABE are conducted on ESP DSP that is proxy servers, which greatly reduce the computational overhead on client-side mobile devices. Further we analysis performance of Advances Encryption Standard (AES) and International Data Encryption Algorithm (Idea) algorithms for data sharing in mobile cloud computing.

SYSTEM DESIGN AND METHODOLOGY:

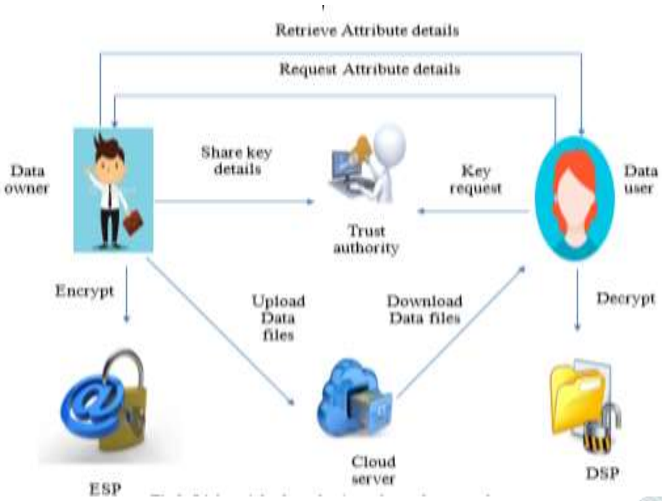

Fig 1-Secure and Efficient Access for Mobile Cloud Computing

The fig-1 demonstrates how a file can be stored in the cloud in encrypted format. If data owner wants to upload a file then that file has to encrypt before uploading it to the cloud. The proposed method includes proxy server's ESP and DSP for file encryption and decryption respectively. And trusted authority (TA) is responsible for generating the keys. This proposed method offers two types of encryption to the data owner that is AES encryption method and Idea encryption method . After each encryption we can observe the block size , key size and number of rounds for the selected encryption algorithm and based on this we can compare both the algorithms. The work flow is as shown in below flow diagram.

FLOW DIAGRAM

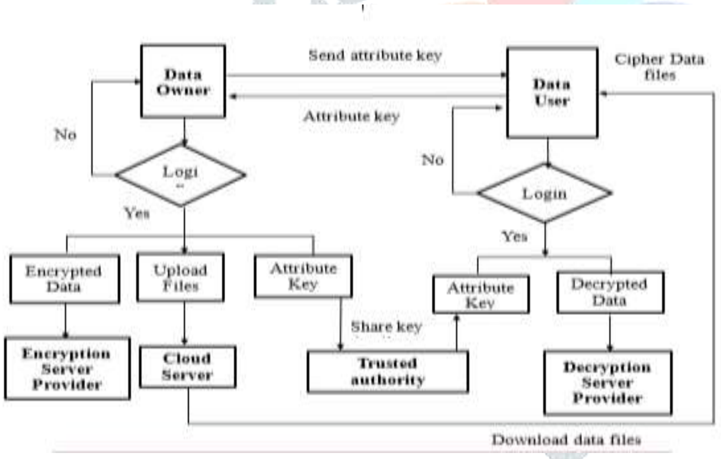

Fig 2-Application Flow Diagram

PERFORMANCE ANALYSIS DIFFERENT ALGORITHM

- Block size (in bits)
- Key size (in bits)
- No of Rounds

1. USER MODULES

Text Encryption and Decryption

- Text request

2. SERVER SIDE:

- View encrypted data
- View user request
- Provide key

Text Encryption and Decryption

In this module user encrypt the plain text to encrypted format and upload to the cloud. The encryption is done by using a password/key. Only using this password one can decrypt the text. The user uploads the password also include with encrypted data. The trusted authority is responsible for passing the password to the requested user

Text request

Any user can view the file uploaded in the server. All the files are in encrypted format. User can't view the files without knowing the password. For view the file first user need to request the password to Trusted Authority. The Authority checks the user and provides the key for valid user.

View Encrypted Data

The user uploaded encrypted data can be view in the server side. The trusted authority act as server they have the responsibility to provide key for the requested user.

View user request

After user viewing the encrypted data, they can request the key for encrypted data. This user request can be view in the trusted authority

Provide key

After view the request Trusted authority validating the user and if the user is valid the Trusted authority provide key for the requested file. Using this key user can decrypt the file

V. CONCLUSION

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm. However, traditional attribute-based encryption is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. Proposed lightweight data sharing scheme is used to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from devices onto proxy servers, thus it can solve the secure data sharing problem in cloud. After this we can finally analysis the performance of AES algorithm and Idea algorithm for mobile cloud computing.

REFERENCES

[1] Shubham Chandugade, Prachi More ,Shaikh Mohammad, Shafiq Rafiiq: Survey on lightweight secured data sharing scheme for cloud computing.IRJET 2017 p-ISSN:2395-0072

[2] Chandini patel , SameerSingh Chaubhan, Bharesh Patel:A data security framework for mobile cloud computing. IJARCCE vol 4,issue 2,2015 p-ISSN:2319-5940

[3] Zhibin Zhou, Dijiang Hua:Efficient and secure data storage operation for mobile cloud computing.2012 8th International Conference on Network and Service Management.

[4] Abdul Nasir Khan, M.L.Mat.Miah,Samee.U.Khan,Sajad.A.Madani: Towards secure mobile cloud computing www.elsevier.com/locate/fgcs

[5] A.Jyothi, Dr.B.Indira: Secure storage distribution and processing of IoT based data through mobile cloud computing. 2017 IJARSE volume 6 special issue(01) ISSN 2319-8354

[6] Maheshwari U, Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage.in: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation-Volume 4. USENIX Association, pp. 10-12, 2000

[7] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528,2013.