International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Mobile Cloud Data Privacy using Lightweight Data Sharing System

Kundan.B, T.Rakesh Kumar, Sarangam Kodati

Abstract: ***The data security problem in mobile cloud becomes more and more severe and it prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However the most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. So we propose a light weight data sharing scheme (LDSS) for mobile computing it adopts CP-ABE (Cipher text policy attribute based encryption) an access control technology using normal cloud environment but changes a structure of access control tree to make suitable for mobile cloud environment. It is important to use the resources provided by Cloud Service Provide to store and share data. Thus LDSS can effectively reduce the over head on the mobile device side when users are sharing a data in mobile cloud environment..***

Keywords: LDSS, CP-ABE, Mobile Cloud Computing, Data Security, CSP, Data Encryption, Access Control.

I. INTRODUCTION

The rise of cloud technology and mobile applications allows personal information to be saved retrieved from just about anywhere. The data security concern is becoming increasingly acute in mobile cloud and helps to prevent further mobile cloud development. Significant studies have been carried out to enhance cloud protection, but most are not relevant to the mobile cloud since only limited software space and power is available for mobile devices. Mobile cloud applications with minimal cognitive efficiency are required. We therefore deliver a Lightweight Data Sharing Framework for Mobile Cloud computing. Services with low calculation payload are needed. The plan was designed to deliver lightweight and safe data storage processing and data recovery from the cloud, as well as to reduce mobile equipment load. Cloud- provides computer system resources, notably data storage and computer power, on-demand without user-active direct management. The term usually serves to describe data centers that are accessible to many users of the internet. Wide clouds, nowadays primarily, are often spread across a variety of central network locations and can be used as an edge database when the client interfaces are relatively close to each other.

The document discusses the supplier and the processing of knowledge, data owner and the role of the employee in the cloud. Safe and efficient access to outsourced software and internet access to large-scale information in a vital sector work in a safe and competent manner. The element does not simply ensure safe entry to the externalized information but depends on encryption-based access control and over-encryption. Where organizations share information across their centralized database systems, cohesive partnerships, worries over possible risks of information spills or software abuse avoids cloud alliances. The existing system takes about half an hour to perform the same work on a mobile device when encrypting takes one minute on pc. In comparison, current approaches do not address very well the issue of user privilege transfer, which could contribute to a very large revocation value. To mobile devices this does not happen either. There is clearly no correct solution to solve the problem of secure data sharing in mobile cloud. As the mobile cloud is increasingly popular, it is urgently needed to provide an active and secure data sharing system for mobile cloud.There is no acceptable framework for data security in the mobile cloud. The price of user authentication and cancelation is high. The protection for single person details is instable to the software proprietors. It will be a real stress. We are not able to satisfy each one of the needs of information holders. You are consuming a large amount of data. What are more important resources that are not available to mobile phones. Every high rejection price could be reached.

For cell phones, this is not a fact. Obviously, no course is going to suit. Such apps allow individuals (informational proprietors) to upload images, records, files and various documents to the cloud and to exchange them with other persons (informational customers). For some data holders, the security of knowledge on the person sensitive information is a major concern.

II. PROPOSED SYSTEM

In this we propose a small weight data sharing (LDSS) system for mobile cloud computing. In order to effectively control access to cipher code, we have developed an algorithm named LDSS-CP-ABE, focused on the attributes dependent encryption approach. For encrypting and decrypting activities they use proxy servers.

Manuscript published on November 30, 2019.
* Correspondence Author
Kundan.B*, CSE Department, Teegala Krishna Reddy Engineering College, Computer Science and Engineering, Telangana, India. Email: tkrcsekundan@gmail.com
T.Rakesh Kumar, CSE Department, Teegala Krishna Reddy Engineering College, Computer Science and Engineering, Telangana, India. Email:rakesh903262@gmail.com
Sarangam Kodati,CSE Department, Teegala Krishna Reddy Engineering College, Computer Science and Engineering, Telangana, India. Email: k.sarangam@gmail.com

In our methodology, ABE's complex calculation operations on proxy servers minimize the computing overhead substantially on mobile devices on the client side. We have benefits such as having effective data access methods. Yet performance and cost management have been enhanced. Information confidentiality through LDSS-CPABE is also protected. The changed decryption key edition is sent to the proxy servers in a safe way.

Advantages:

Overhead data storage is very small. If the multiple cancelation operations are combined together, the overhead is shortened. LDSS reduces the overhead on the client side by reducing the additional server costs. By using this strategy, data sharing protection on mobile devices has improved. LDSS produces better performance results dependent on cipher text access control systems compared to the existing ABE.

III. ANALYSIS OF USER LOGGING IN TO THE CLOUD

Cloud Service Models

3.1 Software-as-a-Service (SaaS): SaaS service model provides services, as apps to the user utilizing default frameworks, on top of a cloud infrastructure that is transparent to the customer. software as - a-service (SaaS) The cloud provider manages the system, operating systems and underlying infrastructure. Only some specific user application interface configurations are controllable to the consumer: Sources include: Yahoo!, Gmail and Google Docs, etc.

3.2 Platform-as-a-Service (PaaS): The business model PaaS provides to the consumer services as channels of activity and growth. The user can create and operate his own applications with a cloud based framework on the web "Consumers do not operate or monitor the cloud infrastructure, like network, databases, operating systems and processing, but regulate the applications installed and likely database host setups." E.g.Google Aps, Microsoft Server, etc.

3.3 Infrastructure-as-a-Service (IaaS): IaaS Service Model is the lowest service model for the technological framework providing raw data collection, energy management, and network capacity connectivity as products. Customers may install their own operating systems and software through the services offered by IaaS and provides customers with a wider range of depletion features than those provided through PaaS or SaaS. "Consumers do not own, monitor and maintain the underlying cloud infrastructure, but have operating system access, space, software installed, and perhaps limited control over specific network elements, for instance host firewalls." Instance: AWS (S3, EC2), Microsoft Azure, etc.

A technical specification determines the role of a device or part in software engineering or process design. A task is defined as a collection of inputs, actions, and outputs The equations, technical detail, data manipulation, storage and other basic functions which determine the mechanism to be executed can be functional specifications. Compartmental requirements which describe all cases in which functional requirements are taken into account by the system. Functional specifications are accompanied by non-functional (so-called reliability criteria) requirements, which enforce development or execution constraints (e.g. performance, safety and dependability). Functional specifications, as specified in specifications technology, have basic process outcomes. That is in contrast to non-functional requirements this define total functionality such as price and performance.

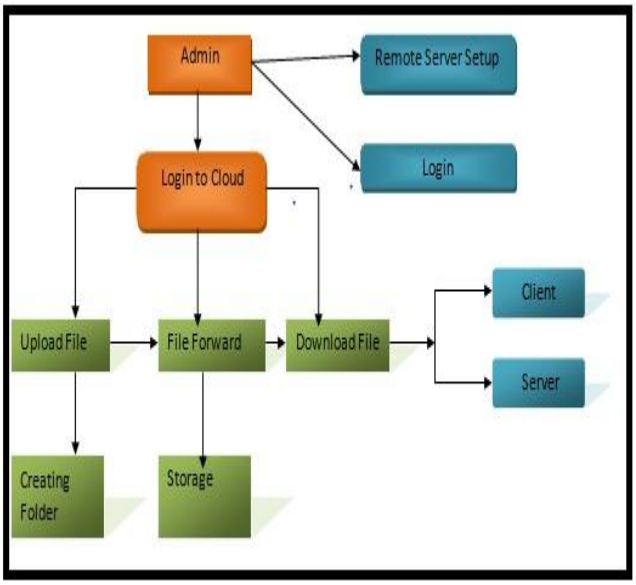

Figure 1: User Logging in to the Cloud

System design involves conversion from a client-oriented file into a device or server personnel. The development is a means of how a new system can be developed. It consists of many levels. It provides the required interpretation and operational knowledge for the implementation of the program proposed in the feasible analysis. The planning process takes place through conceptual or practical creation processes, the logical model analyses the current physical structure, schedules input and output requirements, designs specifics and produces a logical layout advancement. The database tables were constructed by way of study of system functions and field formats. Fields in the database tables must describe the function of the database in the process. To order to ensure a user-friendly interface in the output and feedback display, it is necessary to avoid redundant fields because it impact the space zones of the device. The list must be precise and lightweight. It offers on-demander computer facilities to that pool of resources, i.e. client, space, networking, code, database, applications etc., over the internet. Cloud is a distributed consumer services system. It is a template to enable omnipresent on-demand access to a popular package of configurable computer resources, which can be easily delivered and published with minimal management effort. The course would present different areas of cloud computing including the concepts, management problems, security problems and future trends in science.

The LDSS is referred to as the stable Lightweight Data Sharing System. The LDSS-CP-ABE algorithm is used here. This contains the following algorithm layout. The first download, (A, V)—Creates a personal master key and a public key on the array of attributes, A, V. The second produces a password (Au, MK). This is used for creating attribute keys in the Software User based on the collection of A and MK attributes. The fourth is Encryption focused on symmetrical key K, CT cipher text generation of the public key PK and the Control Access tree T.

Third, decryption is performed using the main attribute and access control chain. Cipher code decrypts. LDSS is but one form of software that guarantees the Light weight sharing of information on mobile cloud.

This uses attribute-based encoding in LDSS, which has two other components….

CP-ABE: Chip text policy Encryption based on attribute.

KP-ABE: Encryption based on key policy attributes.

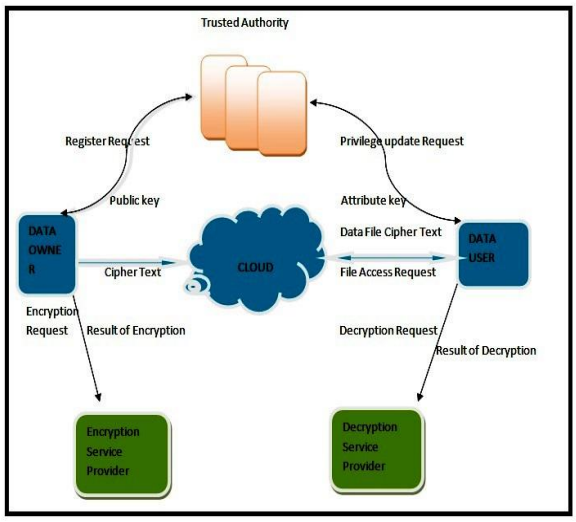

Figure 2: System Architecture

IV. IMPLEMENTATIONS OF USER LOGGING IN TO THE CLOUD

4.1 File Owner: DO uploads or exchanges file with peers into the phone cloud. DO defines the access control rules.

4.2 Software user: DU gathers wireless cloud data.

4.3 TA: TA's function in creating and transmitting attribute keys.

4.4 Service Provider Authentication (ESP): ESP offers DO data encryption operations.

4.5 DSP Provider of Decryption Products (DSP): DSP offers DU decryption.

4.6 Cloud Service Provider (**CSP):** DO information is saved by CSP. It performs trustworthily the operations demanded by DO when accessing the data stored by DO in the cloud.

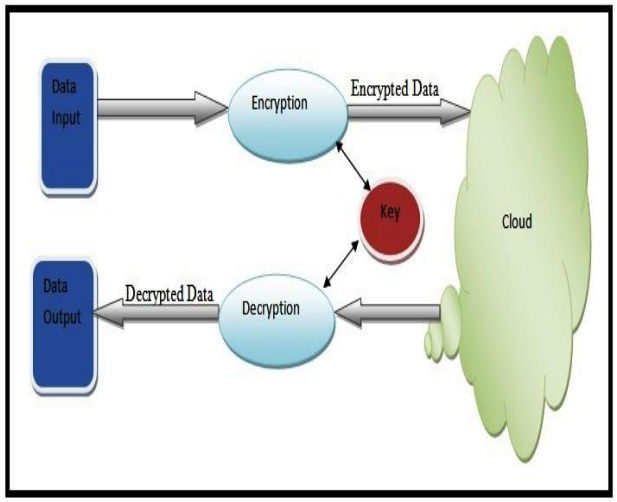

Figure 3: Encryption & Decryption Operations from End user to Cloud and then to End User using Key

The databases are sent to the cloud by a computer administrator. For certain security reasons, they can't blindly transmit to the cloud so that information are secured prior to being submitted to the cloud. The Software Manager accesses the software file control tree to delegate which allocates to a software client the ability to get certain data files, although we have a control policy for access. The LDSS data files are encryptable, with symmetric data encryption by Attributes Based Authentication (ABE) utilizing symmetric device keys. The cipher text embeds the symmetric key, Access Control Procedure. The software client with authority will access the coded control policy, then decode it and get the symmetric key.

4.7 Encryption and decryption of texts

User encrypts the plain text to encrypted format and uploads it to the server. Using a keyword, authentication is completed. Only one can decode the cryptographic text using the key. The client also needs encrypted data when saving the code. The requesting user is responsible for passing the password to the next client.

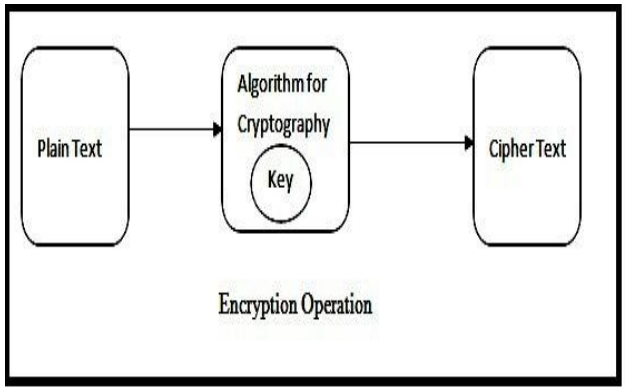

Figure 4: Operation for Encryption

V. RESULT

5.1 Image Encryption and decryption

The crypt picture and key is also uploaded to the internet, as is the case with the crypt and the decryption of text, and the authorized authority ID tasked with enforcing the code on to the intended client.

5.2 Text request

The file uploaded to the server can be viewed by any user. Every single file is encrypted. By recognizing the password, the client can not access data. The first client has to query the Trusted Authority for the key to open such documents. The Authority must explain whether or not the client is real. After the client has been validated with the particular details, the Authority issues a correct user key.

5.3 Image request

The demand for an image is close to the application for text too. In the form, the set of photos can be accessed. But after acquiring the code from the trusted authority, users can only display the pictures.

5.4 View Encrypted Data

On server side the client uploads the encrypted data. As a database, the trusted authority is responsible for providing the requested Client with its username.

5.5 View user request

Once you have accessed the encrypted data, you must query for the symmetric encryption key. The authorized authority will show this client application.

5.6 Provide password

On receiving the report, the Authorized Authority can then provide the code for the file provided to the user concerned via e-mail and the client is legitimate. The client will encrypt the folder with this key.

5.7 Attribute-Based Encryption

Sahai and Waters are offered attribute-based encryption (ABE). It is a function of Identity-Based Encryption (IBE). It is particularly suitable for decentralized and transparent network systems for one to several data sharing scenarios. Encryption with attributes is broken down into two categories. One is the chip text-policy-based encryption attribute (CP-ABE) which contains the access management policy in chips. The other is the Key-Policy Attribute Based Encryption (KP-ABE), which integrates the authentication rules into the key attributes of the client. CP-ABE is more suited for real implementations as it appears like tasks dependent access control. The information holder establishes the Access Control Program in CP-ABE and grants data users attributes. If the user's characteristics align with the Access Control Protocol, users may encrypt data properly.

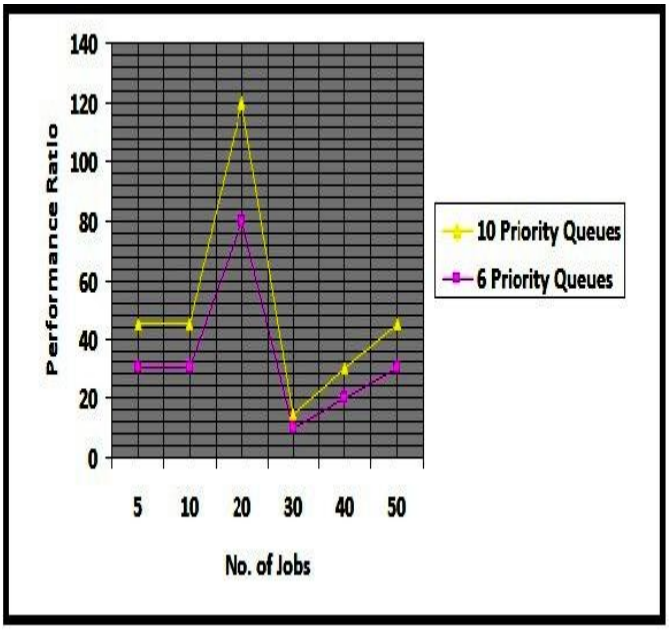

Figure 5: The job quality proportion

Throughout LDSS, all data files are authenticated using the symmetrical encryption scheme, and the symmetric data encryption key (ABE) is also encrypted. The access control protocol is included in the symmetric key cipher file. The cipher text can be decrypted and the symmetrical key can only be found by an DU with attribute keys that meet the Access Control Policy. The computer-intensive encryption and decryption introduces heavy burdens for mobile users. The encryption service provider (ESP) and decryption services provider (DSP) were used to reduce the burden on smart phones on the customer side. That happens. The provider of encryption and decryption services is also semi-confident. In order to secure data privacy when outsourcing computer functions to ESD and DSP We change the traditional algorithm for the CP-ABE and design a LDSS-CP-ABE algorithm.

The computer-intensive encryption and decryption introduces significant burdens for mobile users. Encryption-Service Provider (ESP) as well as Decryption Service Provider (DSP) are used to loosen payload on customer side mobile platforms.

5.8 Trusted Authority:

A trustworthy individual (TA) is given to full LDSS that is available through and through. It can carry accessible and underground keys and disperses the keys to customers. The audience must delegate and accept the authentication and adaptation practices following an ecological cycle with this part. In the course of the TA and anniversary client we apprehend TA as completely credible and trustworthy. The way a trusted approach can be found did not imply that the advice can be combined via the trusted channel, since the advice could be in a huge amount. TA is carefully acclimated (in a small amount) to barter keys between customers. In addition, TA is asked to be online to help the consultants whenever possible and to pin TA's keys.

VI.CONCLUSION

This paper presents a new stable framework and application for information management. In order to address this issue, we suggest LDSS. This displays a new LDSS-CP-ABE equation to transfer notice worthy calculations overhead to intercom from devices, so that the question of safe data sharing in the open cloud can be dealt with. In this article we propose the LDSS system to safe data sharing on mobile cloud and we can also use the Advance Encryption Standard (AES) to encrypt and decrypt data. The results of the exploration show that LDSS can ensure data safety in comfortable cloud and reduce customer-side overhead in flexible cloud. We also refer to the Authentication Authorization of Third Parties (TPA). By using TPA, they can control the validity, reliability and accuracy of associated documents that are transferred to the cloud by the software holder. Feature enhancements are resilient to the storage compromise on mobile devices, and cloud servers are distrusted. Thus, they provide a stronger protection for more general and realistic application scenarios comparing with the previous work.

REFERENCES

1. Rakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE.in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011.
2. Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009.
3. Cong Wang, KuiRen, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012
4. Junzuo Lai, Robert H. Deng, Yingjiu Li, et al. Fully secure key-policy attribute-based encryption with constant size cipher texts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

5. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attributeIEEE Transactions on Cloud Computing, January 2017 based encryption. in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.
6. Di Vimercati S D C, Foresti S, Jajodia S, et al. Over-encryption: management of access control evolution on outsourced data. In: Proceedings of the 33rd international conference on Very large data bases. Vienna, Austria: ACM, pp. 123-134, 2007
7. 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.
8. Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.
9. Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010.
10. Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs.. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012.
11. Sahai A, Waters B. Fuzzy identity based encryption. in: Proceedings of the Advances in Cryptology. Aarhus, Denmark: Springer-Verlag, pp.457-473, 2005.

AUTHORS PROFILE

Kundan.B is an Assistant Professor in Computer Science & Engineering Department at TKREC R9 affiliated to JNTUH. I received M.Tech & B.Tech both the degrees from JayaPrakash Narayan College of Engineering affiliated to JNTUH. I have 4+ years of Real Time Experience in MNC's. My areas of interests are Computer Networks, Internet of Things, and Data Mining

T.Rakesh Kumar, is a Assistant Professor, CSE, Teegala Krishna Reddy Engineering College at Hyderabad, Telangana, India. He received the B.Tech degrees in Computer Science Engineering from SCET College of engineering, Ranga Reddy and M.Tech degree in Computer Science Engineering from S.V College of engineering and technology, Ranga Reddy,Telangana.

Dr.Sarangam Kodati, He is a Associate Professor, CSE, Teegala Krishna Reddy Engineering College at Hyderabad, Telangana, India. His research interests include Data mining, Bioinformatics, Internet of Things. He had much teaching and research experience with a good number of publications in reputed International Journals & Conferences. He awarded Ph.D at Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal, M.P,India. M.Tech completed at JNTU-CEH (Autonomous), Kukatpally, Hyderabad. B.Tech completed VNR VJIET, Hyderabad.