International Journal of Multidisciplinary Engineering in Current Research
Volume 6, Issue 1, January 2021, http://ijmec.com/

A NOVEL MODEL OF PRIVATELY DATA SHARING SERVICES FOR MOBILE CLOUD COMPUTING

,SinghSoniaandGuptaNitin**

**AssistantProfessor,departmentofPhysiotherapy,PunjabiUniversity,Patiala
***Endocrinologist, FortisEscortsHospital,Amritsar

Abstract— Mobile devices may now store and access personal data from almost anywhere, thanks to the growing popularity of cloud computing. Mobile cloud data security is becoming more and more of a challenge, which impedes the growth of mobile cloud. The cloud security has been the subject of much research. Since mobile devices have limited processing capabilities and power, most aren't appropriate for mobile cloud. Mobile cloud applications are in desperate need of low-computing-overhead solutions. A lightweight data sharing strategy (LDSS) for mobile cloud computing is proposed in this work. An access control system utilised in regular cloud settings, CP-ABE has been modified to work better in mobile cloud environments by reorganising its access control tree. As part of CP-ABE, LDSS shifts a major piece of the compute expensive access control tree transformation to external proxy servers. Lazy revocation, a tricky problem in CP-ABE systems based on programmes, is handled using attribute description fields to cut down on user revocation costs. It was shown that LDSS may significantly minimise mobile device overhead while transferring data across devices in mobile cloud scenarios.

Index Terms— encryption, access control, and revocation of user permissions are all terms related to mobile cloud computing.

INTRODUCTION

There are several advantages to cloud computing for corporations and end consumers. Cloud computing has three key advantages.

An end user may provide computer resources for nearly any form of task, on demand, via self-service provisioning

Companies have the ability to scale up and down as their computing requirements change, allowing them to adapt to changing demand.

Pay per use : Users may pay only for the resources and workloads they use, since computing resources are assessed at a granular level.

Private, public, or hybrid clouds are all viable options for cloud computing.

Private cloud services are those that are only available to the employees of a company. With this design, you get the best of both worlds: flexibility and ease of use, while yet maintaining administration, control, and security. IT

International Journal of Multidisciplinary Engineering in Current Research
Volume 6, Issue 1, January 2021, http://ijmec.com/

chargeback may or may not be used to bill internal consumers for services.

The cloud service is delivered via the Internet by a third party under the public cloud model. On-demand public cloud services are offered on a per-minute or per-hour basis. In other words, customers only pay for the resources they really use. Google Compute Engine (GCE) and Amazon Web Services (AWS) are among the top public cloud service providers.

On-premises private cloud services are combined with public cloud services through orchestration and automation. Private clouds may be used for mission-critical workloads, whereas public clouds can be used for bursty workloads that need to be scaled on demand. As the name suggests, this approach combines the benefits of on-premises infrastructure with those of the public cloud, all while preserving control over mission-critical data.
Cloud, Provider, and User are the three main players in the typical encoded search architecture via the cloud. In the Provider's records and files, there is an arrangement. Search management will be moved to the cloud, where customers will be able to access it. Generally referred to as a "cloud" administration, the Cloud is a corporate association that provides calculation and capacity assets as virtual computers. The User is a person who enters watchwords into search records that include these catchphrases. Customers in our circumstance would send in requests for new looks through mobile devices like smartphones and tablets. Three basic streams are shown in Figure 1: the transfer of archives and lists (steps 1 to 4), the erasure of the trapdoor (steps 5 to 8), and the retrieval of reports (steps 9 to 12). (steps 9 to 11). There is an indication of how much information is being shared by the weight of the lines.

EXISTING SYSTEM

There are four main forms of access control: basic cypher text, hierarchical access control, completely homomorphic encryption, and attribute-based encryption access control (ABE). All of these ideas are geared toward a cloud computing environment that is not transportable.
Cloud computing environments with resource-constrained mobile devices have been studied by Tysowski et al., who proposed novel modifications to ABE that assigned the higher computational overhead of cryptographic operations to the cloud provider and reduced total communication costs for the mobile user in this specific case.

DISADVANTAGES OF EXISTING SYSTEM

I.Many data owners are concerned about the privacy of their customers' personal information.
II.The CSP's cutting-edge privilege management and access control techniques are either insufficient or inconvenient for data owners' needs.
III.They use up a lot of storage and processing power, which isn't accessible on portable devices.
V.The issue of changing a user's privileges isn't well-solved by current methods. A costly revocation might be the outcome of such an operation. This doesn't apply to mobile devices either, unfortunately. In the mobile cloud, there is clearly no practical answer to the issue of safe data exchange.

VII.**PROPOSED SYSTEM**

For mobile cloud computing environments, we have developed a light-weight data sharing scheme (LDSS).

International Journal of Multidisciplinary Engineering in Current Research
Volume 6, Issue 1, January 2021, http://ijmec.com/

For efficient access control over cypher text, we build an algorithm based on the Attribute-Based Encryption (ABE) approach.

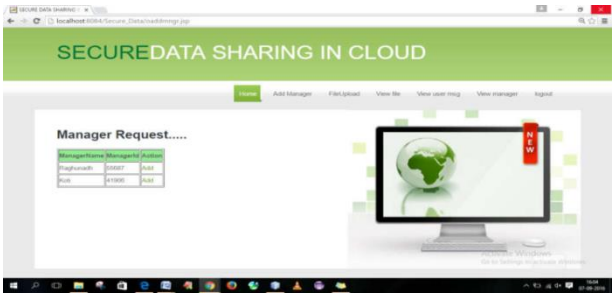
In order to encrypt and decode data, proxy servers are used by us. Client-side mobile devices benefit considerably from our method, which uses proxy servers to perform ABE's most computationally expensive processes. As part of the access structure for LDSS-CP-ABE, the version property has also been included in order to guarantee data privacy. In order to send the decryption key to the proxy servers safely, the file format has been updated.
For the user revocation issue, we provide sluggish re-encryption and attribute description fields to decrease revocation cost.
Finally, we provide a prototype framework for data exchange based on LDSS.

ADVANTAGES OF PROPOSED SYSTEM

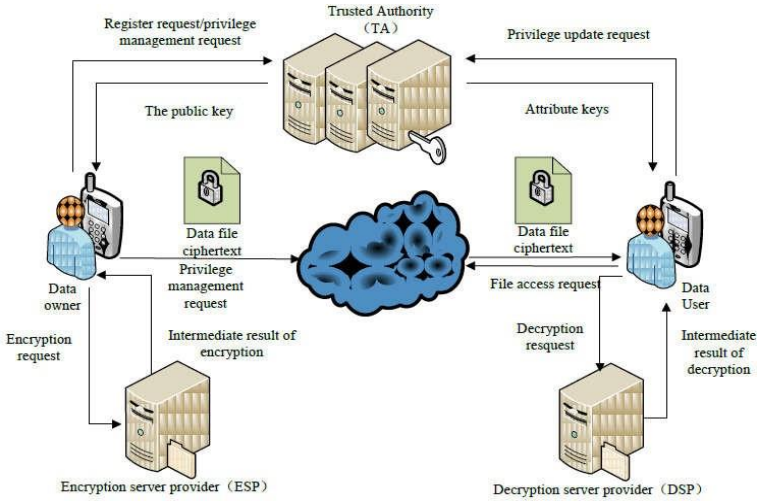
Client-side overhead may be considerably reduced with LDSS, with just a minor extra cost on the server side.
A realistic data sharing security mechanism for mobile devices may be implemented using this method.
LDSS outperforms previous ABE-based access control systems in terms of cypher text performance, according to the findings.

As a result, the total amount of time spent on revocations is reduced.

When compared to data files, the storage overhead required for access control is negligible with LDSS.



VIII. **SYSTEM ARCHITECTURE**



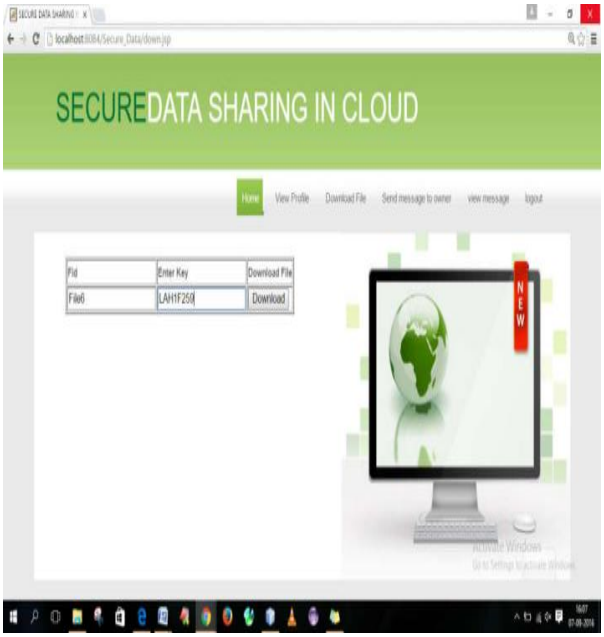
We provide LDSS, a mobile cloud architecture for lightweight data sharing (see Fig. 1). This is made up of the following six parts.
When a user is a Data Owner (DO), he or she uploads data to the mobile cloud and shares it with other users. It is up to DO to set the rules for access restriction.
When you're using the mobile cloud, you're using a Data User (DU).

Attribute keys are generated and distributed by the Trust Authority (TA).

In order to protect DO's data, ESP acts as an encryption service provider.

There are a number of DSPs that offer decryption services to the Data Unlocker.

International Journal of Multidisciplinary Engineering in Current Research
Volume 6, Issue 1, January 2021, http://ijmec.com/



(CSP): Cloud Service Providers hold DO's information. Despite the fact that it may peep into data that DO has saved in the cloud, it faithfully performs DO's requests.

Data is sent to the cloud using DO. Before uploading data to the cloud, it must be encrypted. For data files, the DO sets an access control policy in the form of an access control tree (see Definition 2 in Section 3.2) to designate which characteristics a DU should receive in order to access a particular data file.. When employing LDSS, the symmetric encryption technique is used to encrypt all data files, and the symmetric key for data encryption is encrypted using attribute-based encryption (ABE). The symmetric key's ciphertext has an embedded access control policy. Decryption of the ciphertext and retrieval of the symmetric key are both possible only for a DU with access control policy-compliant attribute keys. Encryption and decryption require a significant amount of processing power, which might place a strain on mobile devices
users. Encryption service provider (ESP) and decryption service provider (DSP) are used to reduce the burden on mobile devices. Neitthe encryption service provider nor the decryption service provider are fully trusted. When computing activities are outsourced to ESP and DSP, we use an LDSS-CP-ABE method, which is a modification of the classic CP-ABE technique.

IX.**SCREEN SHOTOS**

MANAGER VIEW USER REQUEST

International Journal of Multidisciplinary Engineering in Current Research
Volume 6, Issue 1, January 2021, http://ijmec.com/

MANAGER VIEW USERS

VIEW FILES PAGE

DOWNLOAD FILES PAGE

X.**CONCLUSION**

The mobile cloud-based EnDAS encrypted search system that we suggested in this research reduces network traffic and increases search time efficiency compared to the current method. We began by an in-depth assessment and redesign of the present encrypted search system To deal with inefficient search time, we used the TMT module and the RSS algorithm, while a trapdoor compression approach was used to cut network traffic expenses. After analysing these bottlenecks, we designed an efficient EnDAS architecture that is appropriate for the mobile cloud. Finally, our investigation shows that EnDAS is superior in terms of performance.

XI.**FUTURE ENHANCEMENT**

XII.We are employing effective grouping and feedback forms for this project's improvement purposes. It's possible to utilise the newest encryption and decryption methods to speed up decryption and just one key is sent over the internet to view and download files.

XIII.**REFERENCES**

Implementing Gentry's fullyhomomorphic encryption technique [1]. Gentry C, Halevi S. Proceedings of the 13th European Conference on Cryptology (EUROCRYPT 2011). Germany: Springer, 2011, pp. 129-148

The efficient use of (standard) LWE for complete homomorphic encryption [2]. Proceedings of the IEEE Symposium on Foundations of Computer Science. IEEE Press, California, USA, pp. 97-106, October 2011.

The 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011. Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaborative clouds."

The authors of this article are Mohammad Mannan and Adam Skillen. On Deniable Storage Encryption for Mobile Devices. Network and Distributed System Security Symposium (NDSS), Feb. 2013, 20th anniversary.

5] Wang W, et al. Secure and efficient access to outsourced data: Proceedings of the 2009 ACM symposium on Cloud computing security, pp. 73–78. ACM, pp. 55-66, Chicago, IL, 2009.

It is possible to establish a trustworthy database system using untrusted storage, according to Maheshwari, Vingralek, and Shapiro. Volume 4, USENIX Association, pp. 10-12, 2000, Proceedings of the 4th Symposium on Operating System Design & Implementation.

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