A LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

Mrs. K. Kiranma, Assistant Professor, Dept. Of Computer Science & Engineering, Dhanekula Institute of Engineering and Technology, A.P., India.
M. Manisaradhi, K. Praneeth, G. Kalyan Kumar, A. Lakshmi Kantha Reddy Students, Dept. Of Computer Science & Engineering, Dhanekula Institute of Engineering and Technology, A.P., India.

Abstract:
Mobile devices can now access personal data from anywhere at any time thanks to cloud computing, but this also raises the possibility of data security breaches in mobile cloud settings. Despite the fact that numerous studies have been done to enhance cloud security, the majority of methods do not work with mobile clouds due to the constrained computing power and resources of mobile devices. Therefore, for mobile cloud apps, there is a need for lightweight solutions with low computational overhead. In this paper, we suggest a lightweight data sharing scheme (LDSS) for mobile cloud computing that makes use of CP-ABE, a cloud access control technology, but modifies the access control tree structure to fit mobile cloud environments. Through the use of external proxy servers, LDSS moves the highly demanding CP-ABE access control tree transformation away from mobile devices. Additionally, it adds attribute description fields to implement lazy revocation, which is a challenging problem in program-based CP-ABE systems, to lower the cost of user revocation. According to the findings of the experiments, LDSS can significantly lower the overhead incurred by mobile devices when users exchange data in mobile cloud environments.

Keywords: Cloud Computing, LDSS(Lightweight Data Sharing Scheme), CP-ABE(Ciphertext-Policy Attribute-Based Encryption), DO(Data Owner), DU(Data User), TA(Trusted Authority), Cloud, Encrypt, Decrypt.

INTRODUCTION

In the cloud computing model, computing hardware and software tools are made available as a service over a network, frequently the Internet. The use of a cloud-shaped symbol to symbolize the intricate infrastructure involved gave rise to the term "cloud".
By linking systems together, cloud computing aims to make it possible to use high-performance computing capacity, which was previously only available in military and research facilities. The National Institute of Standards and Technology (NIST) lists on-demand self-service, wide network access, resource pooling, quick elasticity, and measured service as the primary attributes of cloud computing

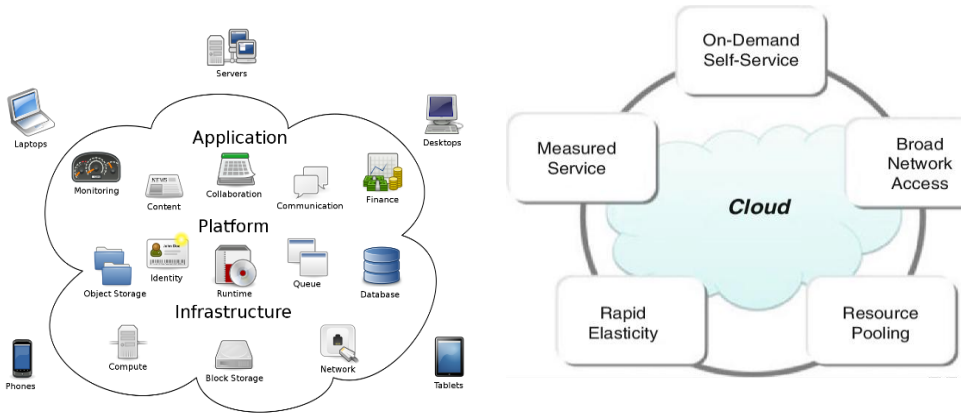


Figure. 1 Structure & Characteristics of cloud computing

 DOI: 10.36893.DRSR.2023.V13I0.0189-0194

LITERATURE SURVEY

[1] Due to the exponential growth in data generated by individuals and businesses that require storage and utilization, there is a growing incentive for data owners to transfer their complex local data management systems to the cloud. This is because of the cloud's high level of flexibility and cost-effectiveness. [2] Although data access control is a reliable method for guaranteeing data security in cloud storage, it becomes a difficult issue due to data outsourcing and untrustworthy cloud servers. Consequently, traditional access control schemes are no longer suitable for cloud storage systems. [3]Attribute-based proxy re-encryption scheme (ABPRE) is a novel cryptographic primitive that expands the conventional proxy re-encryption (either public key or identity-based cryptosystem) to the attribute-based equivalent. This extension empowers users with the capability to delegate in the access control environment. [4]A cloud storage service allows data owner to outsource their data to the cloud and through which provide the data access to the users. Because the cloud server and the data owner are not in the same trust domain, the semi-trusted cloud server cannot be relied to enforce the access policy. [5] The attribute-based proxy re-encryption scheme (ABPRE) is a recently developed cryptographic primitive that enhances the traditional proxy re-encryption (whether public key or identity-based) to its attribute-based equivalent. As a result, users are endowed with the ability to delegate in the access control environment.

EXISTING SYSTEM

Access control for data encryption generally refers to four different methods:
simple ciphertext access control, hierarchical access control, access control based on completely homomorphic encryption, and access control based on attribute-based encryption. (ABE).
These strategies aren't mainly made for mobile devices, but rather for cloud computing environments.
Tysowski et al. acknowledged this restriction and suggested changes to ABE to accommodate mobile devices with constrained resources getting cloud-based data. By making these changes, the mobile user's computational burden for cryptographic operations is transferred to the cloud provider, lowering the former's overall transmission cost.

PROPOSED SYSTEM:

Our proposal is a Lightweight Data Sharing Scheme (LDSS) specifically designed for mobile cloud computing environments. The key contributions of LDSS are:

- ✓ We introduce an algorithm, called LDSS-CP-ABE, which employs Attribute-Based Encryption (ABE) to provide efficient access control over ciphertext.
- ✓ We utilize proxy servers to handle encryption and decryption operations, enabling computationally intensive ABE operations to be offloaded from mobile devices to proxy servers.
- ✓ We develop and implement a data sharing prototype framework based on the LDSS approach.

METHODOLOGY

MODULES:

- ❖ System Framework
- ❖ Data Owner
- ❖ Data User
- ❖ Trusted Authority
- ❖ Cloud Service Provider

MODULES DESCRIPTION:

System Framework:

A new age of data sharing where data is stored in the cloud and accessed through mobile devices has emerged with the introduction of cloud computing and the rising popularity of smart mobile devices.

DOI: 10.36893.DRSR.2023.V13I0.0189-0194

Data owners can upload their private files and papers to the cloud and share them only with specific users using such applications. Data owners can control the privacy of their data by choosing whether to share it openly or only with specific users thanks to the functionality that cloud service providers (CSPs) offer.
Due to the sensitivity of personal data files, data privacy is a top worry for many data owners. We suggest LDSS, a lightweight data sharing framework for mobile cloud
computing, to solve this issue. This structure is made up of six essential parts:

1. Owner of Data (DO)
2. User of Data (DU)
3. rely on authority (TA)
4. Provider of Encryption Services (ESP)
5. Cloud Service Provider (CSP): Decryption Service Provider (DSP)

LDSS uses proxy servers to manage computationally demanding encryption and decryption operations and is intended to provide effective access control over ciphertext using Attribute-Based Encryption (ABE). By doing this, it protects confidential personal information while facilitating safe data exchange between parties they can trust.

Data Owner (DO):
A data owner (DO) registers with the Trust Authority to commence the process of setting up the LDSS framework. (TA). Using the Setup() algorithm, the TA creates a public key (PK) and a master key (MK), sending PK to the DO while keeping MK on its own computer.
The contacts are given attributes by the DO, which specifies its own attribute set, and are then sent to the TA and the cloud for storage. The DO then uploads data to the mobile cloud, shares it with peers, and establishes access control rules there.
Since the cloud cannot be trusted, the DO must encrypt the data before uploading it, ensuring data protection. The DO then establishes an access control policy, represented as an access control tree, for each data file, defining the qualifications a Data User (DU) must meet in order to view a given file.

Data User (DU):
When a Data User (DU) logs into the system, they submit the Trust Authority (TA) an authorization request that contains their attribute keys. (SK). The request is verified by TA, who also creates more attribute keys (SK) for the DU.
The cloud then determines whether the DU satisfies the access requirements for the requested data before the DU transmits it to it. The symmetric key and the data files' ciphertext are sent to the DU by the cloud after successful authentication.
The Decryption Service Provider (DSP) helps the DU decode the symmetric key's ciphertext after which the symmetric key is used to decrypt the data files' ciphertext.
Trusted Authority:
A Trusted Authority (TA) is introduced to guarantee the viability of the Lightweight Data Sharing Scheme (LDSS) in actual use. Users can share and access data without being conscious of the underlying encryption and decryption operations thanks to the TA's creation of attribute keys, public and private keys, and other information.

It is assumed that the TA is fully reliable and that each user has access to a secure channel. The fact that a secure channel exists does not, however, guarantee that the data being shared can be transmitted through it, especially if the data is big. Instead, the TA is only used to safely transfer users' comparatively small keys from one to the other.
Additionally, it is critical that the TA is always online because data users may need to access data at any moment, necessitating the updating of attribute keys by the TA.

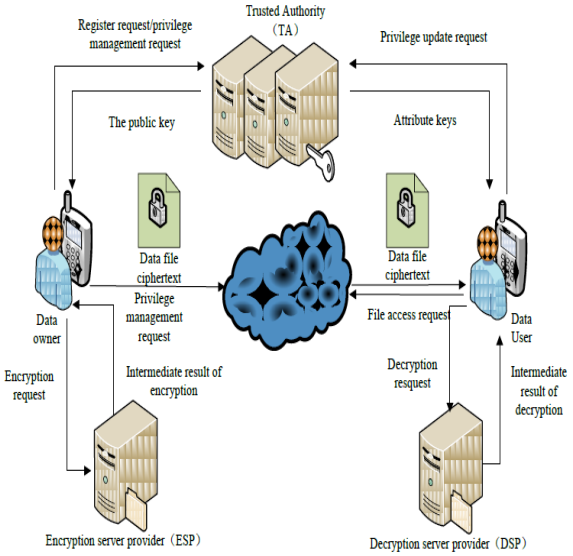
 DOI: 10.36893.DRSR.2023.V13I0.0189-0194

Cloud Service Provider:

Data storage for the Data Owner is the responsibility of the Cloud Service Provider (CSP). (DO). CSP may have access to the data that DO has kept in the cloud while faithfully performing the tasks asked by DO.

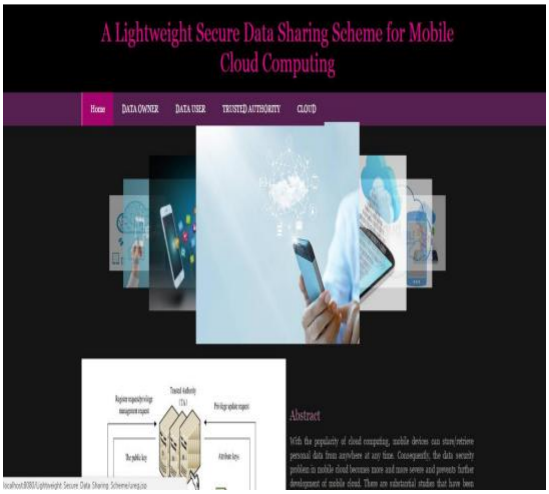
The cloud gets a request for data from the Data User (DU) and checks to see if the DU complies with the access requirements. The proposal is turned down if the DU is unable to fulfil the conditions. The cloud transmits the ciphertext to the DU if it satisfies the requirements.

The Uploaded Files must also be managed by CSP.



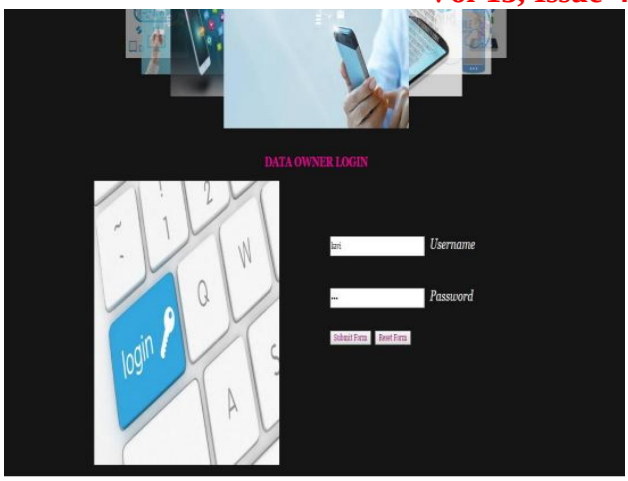
RESULT

With hidden access control policy, CP-ABE (Ciphertext-Policy Attribute-Based Encryption) allows data owners to share their encrypted data via cloud storage with authorized users without revealing the access control policies.

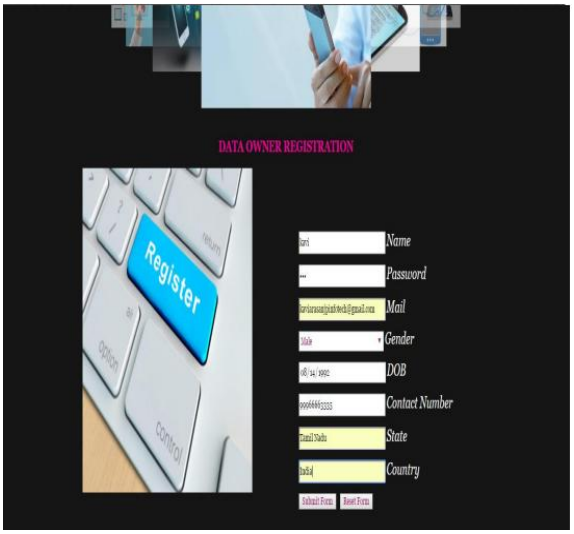


The LDSS-CP-ABE algorithm utilizes Attribute-Based Encryption (ABE) to enable efficient access control over ciphertext. Compared to the regular ABE operation that runs 27 times slower on mobile platforms, LDSS-CP-ABE reduces this overhead**.**

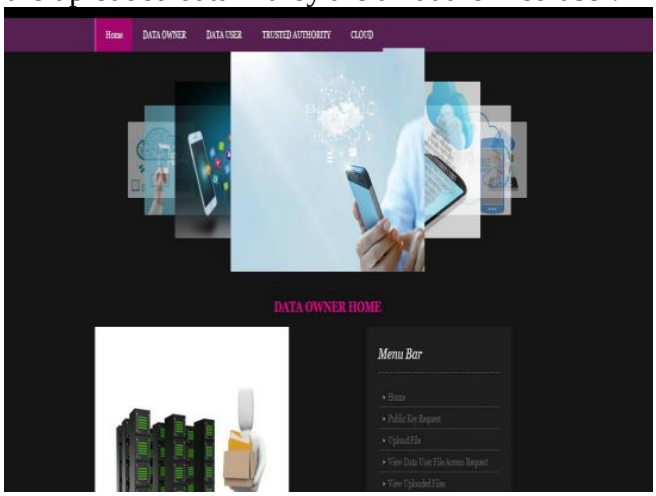
DOI: 10.36893.DRSR.2023.V13I0.0189-0194



A system has been established with four modules: Data Owner (DO), Data User (DU), Trusted Authority (TA), and Cloud.



The DO is responsible for uploading data into the cloud.
The DU is only allowed to access the uploaded data if they are an authorized user.



The TA holds information about the DO and DU, including their access privileges, and generates public and attribute keys for them. The Cloud stores the encrypted files uploaded by the DO, and will only grant access to them when a data access request is made by an authorized DU. Once the Cloud acknowledges the request, it sends a File Decryption Key to the DU, allowing them to download the requested file.

 DOI: 10.36893.DRSR.2023.V13I0.0189-0194

CONCLUSION

Attribute-based encryption (ABE) algorithms have been widely studied for access control in cloud computing, but the computational demands of conventional ABE make it unsuitable for mobile cloud environments with constrained device resources. To solve this problem, we suggest the Lightweight Data Sharing Scheme (LDSS), which transfers the processing load from mobile devices to proxy servers using the LDSS-CP ABE algorithm.

Experimental findings demonstrate that our suggested scheme is efficient in protecting data privacy and minimising the burden on users in mobile cloud environments. To fully realise the potential of mobile cloud computing, we will investigate cypher text retrieval in current data sharing schemes and investigate methods to ensure data integrity.

REFERENCES

[1] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

[2] Brakerski 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.

[3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16thACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.

[4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20thAnnual Network and Distributed System Security Symposium (NDSS), Feb. 2013.

[5] 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.

[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]T. Ormandy, An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments, Whitepaper, (2008).

[8]El-Sofany, H. F., El-Seoud, S. A., & Taj-Eddin, I. A. (2019). A case study of the impact of denial of service attacks in cloud applications. Journal of Communications, 14(2), 153-158. Web.

[9]Gai, K., Qiu, M., Zhao, H., & Xiong, J. (2016). Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing. 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). Web.

[10]Kalaiprasath, R., Elankavi, R., & Udayakumar, D. R. (2017). Cloud. security and compliance-A semantic approach in end to end security. International Journal Of Mechanical Engineering And Technology (Ijmet), 8(5), 482-494. Web.

[11]Krancher, O., Luther, P., & Jost, M. (2018). Key affordances of platform-as-a-service: Selforganization and continuous feedback. Journal of Management Information Systems, 35(3), 776-812. Web.

[12]Madni, S. H. H., Latiff, M. S. A., Coulibaly, Y., & Abdulhamid, S. M. (2016). Resource scheduling for infrastructure as a service (IaaS) in cloud computing: Challenges and opportunities. Journal of Network and Computer Applications, 68(2), 173–200. Web. 12

[13]Ahmed, M., & Litchfield, A. T. (2016). Taxonomy for Identification of Security Issues in Cloud Computing Environments. Journal of Computer Information Systems, 58(1), 79–88. Web.

[14]Alani, M. M. (2016). General cloud security recommendations. In Elements of cloud computing security 51-54. Springer, Cham. Web. [15]Abdul Muttalib Khan , Dr. Shish Ahmad , Mohd. Haroon, A Comparative Study of Trends in Security in Cloud Computing, 2015 Fifth International Conference on Communication Systems and Network Technologies, IEEE 201

 DOI: 10.36893.DRSR.2023.V13I0.0189-0194