International Journal of Science Engineering and Advance Technology

A New LDSS for Mobile Cloud Computing

[1]D.V.SubbaRaju, [2] D.ChandraMouli
[1]Assistant Professor,Dept. of CSE, Srinivasa Institute of Engineering & Tech., Cheyyeru, Amalapuram, E.G.Dt,AP, India
[2]Assistant Professor ,Dept. of CSE, Vignan Institute of Information Techonolgy., Duvvada, Visakhapatnam,AP, India

ABSTRACT:
We suggest a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control innovation utilized as a part of ordinary cloud condition, yet changes the structure of access control tree to make it appropriate for portable cloud situations. LDSS moves a huge part of the computational serious access control tree change in CP-ABE from cell phones to outer intermediary servers. Moreover, to decrease the client repudiation cost, it acquaints trait portrayal fields with actualize languid renouncement, which is a prickly issue in program based CP-ABE frameworks.

KEYWORDS: Data encryption, access control, user revocation

INTRODUCTION:
The best in class benefit administration/get to control systems gave by the CSP are either not adequate or not exceptionally advantageous. They can't meet every one of the necessities of information proprietors. To start with, when individuals transfer their information documents onto the cloud, they are leaving the information in a place where is out of their control, and the CSP may keep an eye on client information for its business advantages as well as different reasons. Second, individuals need to send watchword to every datum client in the event that they just need to share the encoded information with specific clients, which is extremely unwieldy. To improve the benefit administration, the information proprietor can isolate information clients into various gatherings and send secret key to the gatherings which they need to share the information. In any case, this approach requires fine-grained get to control. In the two cases, secret word administration is a major issue.

LITERATURE SURVEY:
[1]THE AUTHOR, Jia W, Zhu H **(ET .AL), AIM**we project a secure mobile user-based data service mechanism (SDSM) to give secrecy and fine-grained get to control for information put away in the cloud. This system empowers the versatile clients to appreciate a safe outsourced information administrations at a limited security administration overhead. The core thought of SDSM is that SDSM outsources the information as well as the security administration to the portable cloud in a trust way. Our investigation demonstrates that the proposed instrument has many focal points over the current conventional strategies, for example, bring down overhead and advantageous refresh, which could better cook the necessities in versatile distributed computing situations.

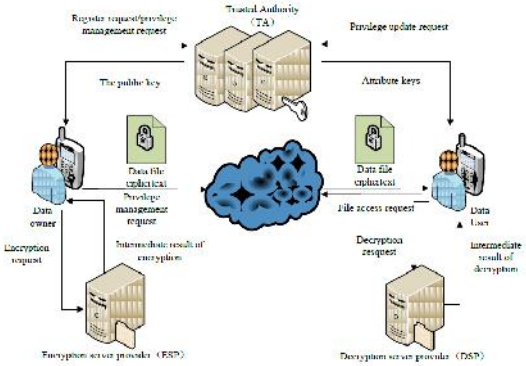
[2]THE AUTHOR, Zhou Z, **(ET .AL), AIM** we show a far reaching security information request system for portable distributed computing. Our answer concentrates on the accompanying two research headings: First, we present a novel Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) to protect sensing data. Using PP-CP-ABE, light-weight devices can securely outsource heavy encryption and decryption operations to cloud service providers, without revealing the data content. Second, we propose an Attribute Based Data Storage (ABDS) system as a cryptographic group-based access control mechanism.

PROBLEM DEFINITION:
With the advancement of distributed computing and the prevalence of brilliant cell phones, individuals are steadily getting acclimated to another time of information sharing model in which the information is put away on the cloud and the cell phones are utilized to store/recover the information from the cloud. Commonly, cell phones just have restricted storage room and figuring power. Unexpectedly, the cloud has huge measure of assets. In such a situation, to accomplish the acceptable execution, it is basic to utilize the assets gave by the cloud specialist organization to store and offer the information.

PROPOSED APPROACH:
Obviously, to take care of the above issues, individual touchy information ought to be scrambled before transferred onto the cloud with the goal that the information is secure against the CSP. Be that as it may, the information encryption brings new issues. Step by step instructions to give proficient access control system on figure content

unscrambling with the goal that exclusive the approved clients can get to the plaintext information is testing. Likewise, framework must offer information proprietors successful client benefit administration ability, so they can allow/disavow information get to benefits effortlessly on the information clients. There have been considerable examines on the issue of information get to control over figure content.

SYSTEM ARCHITECTURE:



PROPOSED METHODOLOGY:

1. **Text Encryption and Decryption**

User encrypted the plain text to encrypted format and uploaded to the cloud. The encryption is done by using a password. Only using this password only anyone can decrypt the text. The user upload the password also include with encrypted data. The trusted authority id responsible for passing the password to the requested user

2. **Image Encryption and decryption**

Like the same as the image encryption is also done. And the encrypted images and password will also be uploaded to the cloud. The trusted authority id responsible for passing the password to the requested user

3. **Text request**

Any user can view the file uploaded in the server. All the files are in encrypted format. User cant view the files without know the password. For view the file first user need to request the password to Trusted Authority TheAuthority check the user and provide the password for valid user.

4. **Image request**

Image request is also same as the Text Request. The list of images can view in the application. But user can only view the images after getting the password from trusted authority

5. **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 password for the requested user.

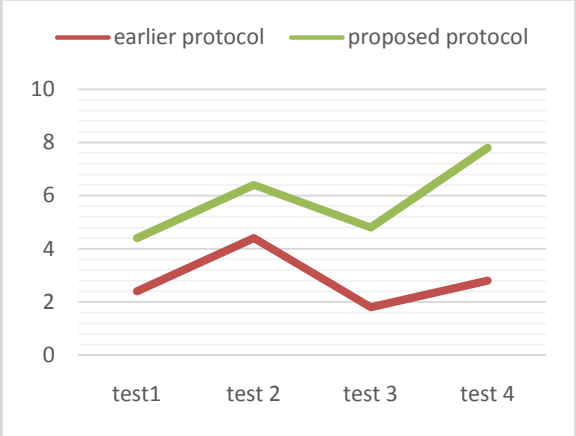
6. **View user request**

After user view the encrypted data they can request the password for encrypted data. This user request can be view in the Trusted authority

7. **Provide password**

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

RESULTS:



The results are conveyed in java. Finally the proposed reasoning exhibits capable execution to the extent security and correspondence and also count overhead appeared differently in relation to before framework.

CONCLUSION:

We propose LDSS to address this issue. It presents a novel LDSS-CP-ABE algorithm to move significant calculation overhead from cell phones onto intermediary servers, consequently it can take care of the protected information sharing issue in versatile cloud. The exploratory outcomes demonstrate that LDSS can guarantee information security in portable cloud and decrease the overhead on clients' side in versatile cloud. Later on work, we will plan new ways to deal with guarantee information 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 16th ACM 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 20th Annual 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] Kan Yang, XiaohuaJia, KuiRen: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.

[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] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350- 364

[10] Cong Wang, KuiRen, Shucheng Yu, and KarthikMahendraRajeUrs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[11] 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

[12] Kan Yang, XiaohuaJia, KuiRen, Bo Zhang, RuitaoXie: DAC- MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[13] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.

[14] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure key- policy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute- based encryption. in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.