Secure Data Sharing For Mobile Cloud Computing Using Data Encryption Standard

Miss. Pratima Bhaurao Wankhede[1],Prof.S.M.Dandage[2], Dr.P.M.Jawandhiya[3]
[1, 2, 3] Dept of Computer Science and Engineering
[1, 2, 3] PankajLaddhad Institute of Technology and Managements Studies, Buldana443002

Abstract- *These days increasingly more information is put away and recovered through Cloud Computing. With progression there emerges a problem in security. This suggests the knowledge are often decrypted effectively and therefore the substance being gotten to by outsiders furthermore, the protection of the knowledge are going to be lost. I've presented a replacement calculation referred to as "Code Attribute Based Encryption Calculation" with symmetric key in our recently proposed light weight information sharing plan for portable distributed computing. Light weight within the sense, information with a genuinely light stockpiling limit like records, brief snippets then on are going to be made sure about hooked in to our proposed idea encoding standard secure data sharing for mobile cloud computing. The info encryption standard secure data sharing for mobile cloud computing structure is adjusted and utilized as an access control in Cipher Attribute Based Encryption (CP-ABE). To decrease the client cost, it presented property depiction fields to actualize lethargic denial which is troublesome in CP-ABE working frameworks. Everything during this activity probably won't be appropriate altogether cell phones on the grounds that the parts are little and adaptableness is a smaller amount. The outcomes from this paper show the problems identified with information protection are settled as a rule for light weight information sharing plan.*

Keywords- Symmetric key, security, privacy, CP-ABE, CSP.

I. INTRODUCTION

With increasing of the cloud storage and more usage of mobile has increased the info sharing model which have been used for the info retroviral and storage. Because the usage of cloud are increased widely, thanks to limitation of mobile storage. The cloud have more amount of storage and resources which is provide by the cloud service provider to store and share the info. The cloud mobile applications such as upload of photos, videos, documents and other files to the cloud and these files are often wont to share with other users.

Management functionality is additionally provided by the cloud service provider, but the private information is vital and it should be not shared in publically. It's important to provide the info privacy and therefore the data security which is that the major concern. The control mechanism provided by the cloud service provider isn't sufficient because it doesn't meet the requirement of the info owner, the primary and much most problem is whenever the user uploads the files on cloud then the cloud service provider may spy on the file for its use which cause the privacy problem later the user want to send the password for the encrypted files to unlock it. To overcome these problem data owner need to divide the info user into different user consistent with the user who want to share their password to the actual group. Password management may be a great issue for the safety.

To take care of specific issues in versatile distributed computing, we have planned a component which can tackle the data encryption standard secure data sharing for mobile cloud computing.

- We have presented CP-ABE calculation procedure which is a code text trait based encryption procedure [4].
- We have utilized an alternate symmetric key method for encryption and decoding. [4]
- Earlier, the information must be controlled by certain soldiers to see and shroud data, yet now extra procedure to safe monitor the data are utilized [2].
- We have plan sluggish encryption method, to meet the denial issue for clients. It keeps up the construction to give diverse administration offices.
- We have reasoned that the code text encryption of ABE issue can be tackle by the model.

II. RELETED WORK

Attribute-based encryption (ABE) is proposed by Sahaiand Waters. Attribute-based encryption (ABE) is a moderately late approach that re-evaluates the idea of public key cryptography. Attribute-based encryption is also referred to as ABE is a sort of public-key encryption wherein the secret key of a person and the cipher-text is established upon attributes.

In an ABE, a person's keys and cipher-texts are labeled with units of descriptive attributes and a symmetric key can decrypt a selected cipher-text only if there's a match between the attributes of the cipher-text and the person's key. It reduces the quantity of key used and hence makes encryption and decryption technique faster.

III. EXISTING SYSTEM

The access control mechanism has stimulated tree structure where Data Owner (DO) uploads the data using Cloud Service Provider (CSP). Data User (DU) will access that file with the help of the trusted authority. There is no data privacy for stored data and no encryption for that content. There is only limited storage available and the computation resources are more in cloud and limited resources are there in mobile devices. Since, essential performances will be slow, more people are starting to use cloud storage for data storing and retrieve purpose.

IV. PROPOSED SYSTEM

The proposed system is a Data encryption standard secure data sharing for mobile cloud computing environment. The main contributions are as follows:

The above problems, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the CSP. 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.

System must offer data owner's 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. The CSP is considered honest and curious, All the sensitive data are encrypted before uploaded to the Cloud, user authorization on certain data is achieved through encryption/decryption key distribution. OTP which will be matched with key in our proposed system data is encrypted before uploading to the cloud. Combination of 3DES algorithm and mobile IMEI no are used for the encryption of the data.

3DES will help to identify the attributes of the data and IMEI will use user authentication. After performing encryption operation, a random key is generated alongside the encrypted data. Data will be send in encrypted format to respective user. To decrypt this data receiver has to enter the One Time Password generated using3DES algorithm.

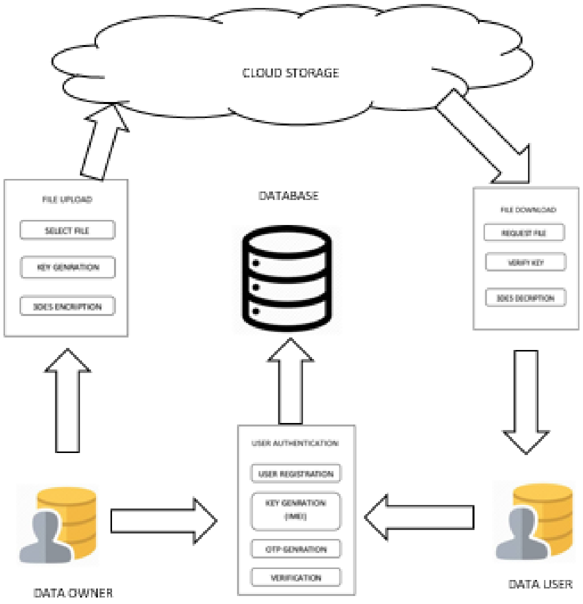

Fig3.1: System Architecture

V. CONCLUSION

In this paper, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. This paper proposes a simple, secure, and privacy-preserving architecture for inter-Cloud data sharing based on an encryption/decryption algorithm which aims to protect the data stored in the cloud from the unauthorized access.

REFERENCES

[1] SunandaNalajala, K Akhil ,VenkatSai, D Chandra Shekhar, Praveen Tumuluru: LIGHT WEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING. in: Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019)

[2] IEEE Xplore Part Number:CFP19OSV-ART; ISBN:978-1-7281-4365-1

[3] Gentry C,Halevi S Implementing Gentrys fully homomorphic encryption scheme in advance in cryptology-EUROCRYPT 2011 Berlin, Heidelberg Spinger press pp 129-145,2011.

[4] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from standard

[5] Adam Skillen and Mohammad Mannan on Implementing deniable storage encryption for mobile device.

[6] Wang W,Li,Z,Owener-R,etal.Secure and efficient access to outsourced data in proceeding often 2009 ACM workshop on Cloud computing security.Chicago,USA.

[7] Kang Yang,XiaohuaJia,KuiRen Attribute based fine grained access control with efficient revocation in cloud storage systems

[8] CRampton J Martin K Wild P on key assignment for hierarchical access control in computer security foundations workshop .

[9] Shri E Bethenout J Chart T H H et al Multi-dimensional range query over encrypted data in proceedings of symposium and privacy

[10] MaheswaraiU,VingralekR,ShaprioW.How to build a trusted database system on untrusted storage in proceedings 4th conference on symposium on OS design & implementation volume-4 usenix association .

[11] Sahai A, Waters B. Fuzzy identity based encryption. in:Proceedings of the Advances in Cryptology. Aarhus, Denmark: Springer-Verlag, pp.457-473, 2005.

[12] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models. Computer, 29(2): 38-47, 1996.

[13] Cong Wang, Kui Ren, Shucheng YU, and Karthik Mahendra RajeUrs.Achieving Usable and Privacy Assured Similarity Search over Outsourced cloud data.IEEE INFOCOM 2012 Orlando,Florida,March 25-30,2012.

[14] SteheleD, Steinfield R.Faster fully homographic encryption in proceedings of 16th International conference on the theory and application of cryptology and information security, singapore springer press pp377-394,2010.

[15] Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable and fine grained data access control in cloud computing INFOCOM 2010 pp534-542,2010.

[16] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities. in: Proceedings of the 4th International Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM press, pp. 276-286, 2009.

[17] Pirretti M, Traynor P, McDaniel P, et al. Secure attribute based systems in: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA:ACM press, pp. 99-112, 2006.

[18] Yu S., Wang C., Ren K., et al. Attribute based data sharing with attribute revocation. in: Proceedings of the 5th International Symposium on Information, Computer and Communications Security (ASIACCS), New York, USA: ACM press pp. 261-270, 2010

[19] D. Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication. in: Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering. Nanjing, China: IEEE, pp. 90-98, 2010

[20] Manekar, A. K., &Pradeepini, G. (2016). Cloud based big data analytics a review. Paper presented at the Proceedings - 2015 International Conference on Computational Intelligence and Communication Networks, CICN 2015,785-788.doi:10.1109/ CICN.2015.160 Retrieved fromwww.scopus.com

[21] SunandaNalajala, PratyushaCh, Meghana A, PhaniMeghana B “Data security using multi prime RSA in cloud” “International Journal of Recent Technology and Engineering” ISSN: 2277-3878, Volume-7,Issue-6S4,April 2019www.scopus.com