International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3395-3400 www.ijaem.net ISSN: 2395-5252

Lightweight Data Sharing in Mobile Cloud Computing

[1]Vivek Vardhan Vadapalli, [2]B.Vineela Rani, [3]R.Alekya, [4]K.Satyavathi, [5]G.S.Pavan Kumar

[2]*Assistant Professor, Raghu Institute Of Technology, Visakhapatnam*

[1,3,4,5]*Student, Raghu Institute Of Technology, Visakhapatnam*

Submitted: 15-07-2021 Revised: 29-07-2021 Accepted: 31-07-2021

ABSTRACT:
With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud.
There are substantial studies that have been conducted to improve the cloud security.
However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications.
Here we implemented a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments

I. INTRODUCTION:

With the development of cloud computing and popularity of mobile devices,people are highly accustomed to a new era of data sharing in which the data is stored on the cloud and the mobile devices are used to store or retrieve data from the cloud.

It is essential to use resources provided by cloud service provider(CSP)to store and share the data.
Here, the data owners can upload their photos, videos and documents and other files to the cloud and share this data with the other people (data users).

II. LITERATURE SURVEY:

S.no	Author	Year	Title	Technique
1	Zhang et.al	2017	Efficient privacy-preserving decentralized ABE supporting expressive access structures.	ABE Algorithm
2	Raipurkaret.al	2016	Improve data security in cloud environment by using LDAP and two-way encryption algorithm.	Two-way encryption algorithm
3	Wang et.al	2016	Achieving secure, scalable, and fine-grained data access control in cloud computing.	Attribute policy

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3395-3400 www.ijaem.net ISSN: 2395-5252

4	Y.Sunandet.al	2016	Scalable hierarchical access control in secure group communications.	Integrated key graph
5	Bonehet.al	2011	Functional encryption: Definitions and challenges.	Ciphertext security in the random oracle model
6	G.Atenieseet.al	2007	Provable data possession at untrusted stores in cloud.	Privacy preserving cryptographic technique

Problem Definition:

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud environment because it is computationally intensive and mobile devices only have limited resources.

It has less security, high storage space and high revocation cost, and non-efficiency.

Here, we designed an algorithm called LDSS-CP-ABE based on attribute based encryption (ABE) method to offer efficient access control over cipher text which provides high security

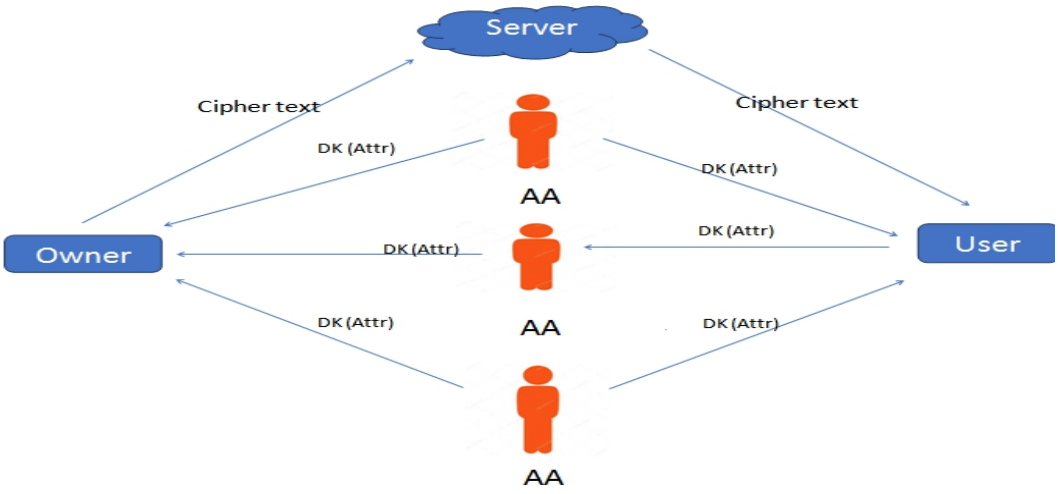
Existing system:

Many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud environment because it is computationally intensive and mobile devices only have limited resources.ABE has been adopted to protect outsourced data. However there are some security issues.Firstly, the user's attributes information is leaked to the authorities and secondly,the access structure being sent along with ciphertext violates its privacy.In current cloud servers ,all the data can be viewed and accessed by anyone who is having an account in the cloud.

Disadvantages:

- Data privacy of the personal sensitive data is a big concern for many data owners.
- The state-of-the-art privilege management/access control mechanisms provided by the CSP are either not sufficient or not very convenient.
- They cannot meet all the requirements of data owners.
- They consume large amount of storage and computation resources, which are not available for mobile devices

Existing system architecture:



Algorithm used in existing system:

In existing system, Diffie-Hellman algorithm is used. The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel. The point is to

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3395-3400 www.ijaem.net ISSN: 2395-5252

agree on a key that two parties can use for a symmetric encryption. Diffie-Hellman key exchange is a specific method of securely exchanging cryptographic keys over a public channel. Traditionally, secure encrypted communication between two parties requires that they first exchange keys by some secure physical channel. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. At the end of the communication both sender and receiver have the same key.

The steps in the algorithm are

1. Alice and Bob agree on a prime number p and a base g.
2. Alice chooses a secret number a, and sends Bob (g a mod p).
3. Bob chooses a secret number b, and sends Alice (g b mod p).
4. Alice computes ((g b mod p) a mod p).
5. Bob computes ((g a mod p) b mod p). Both Alice and Bob can use this number as their key. Notice that p and g need not be protected.

Proposed system:

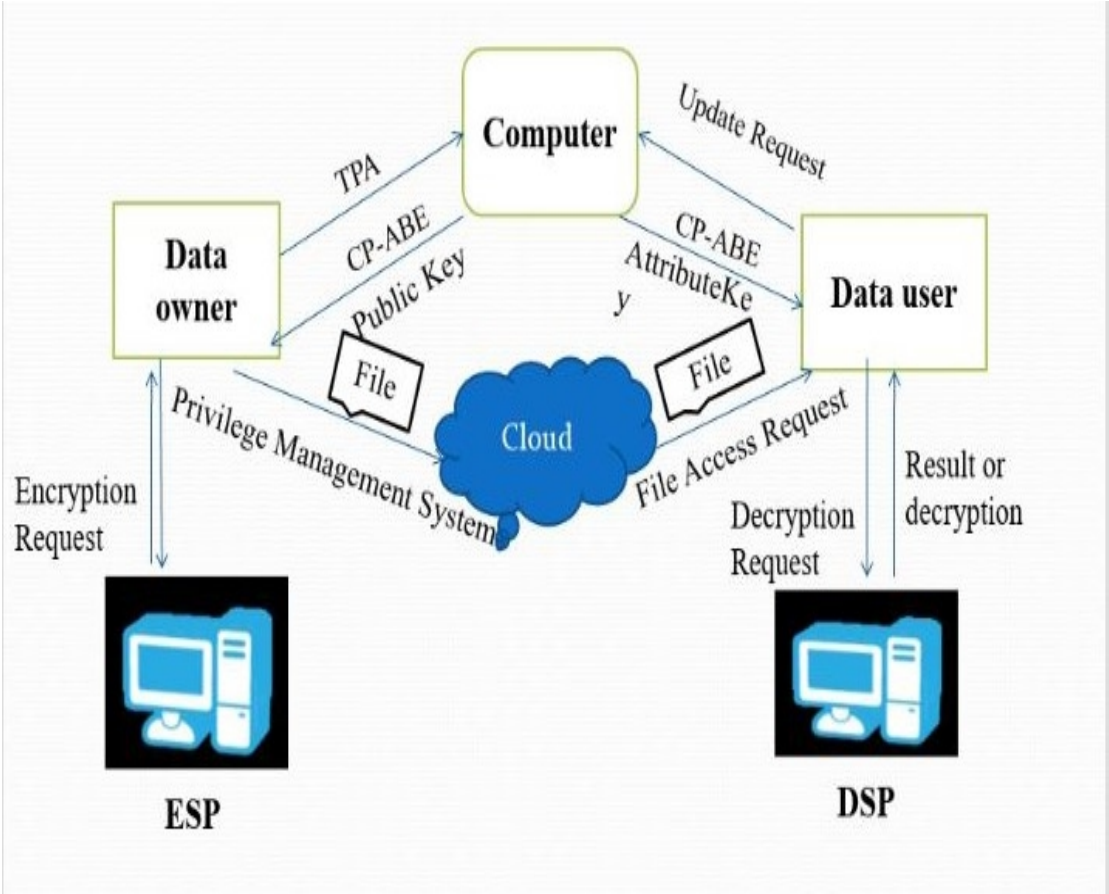
Proposed system architecture.

We implemented a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment.We design an algorithm called LDSS-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over cipher text.We use proxy servers for encryption and decryption operations. In our approach, computationalintensive operations in ABE are conducted on proxy servers, which greatly reduce the computational overhead on client side mobile devices.

Advantages:

- The experiments show that LDSS can greatly reduce the overhead on the client side, which only introduces a minimal additional cost on the server side.
- Such an approach is beneficial to implement a realistic data sharing security scheme on mobile devices.
- The results also show that LDSS has better performance compared to the existing ABE based access control schemes over ciphertext.
- Multiple revocation operations are merged into one, reducing the overall overhead.
- In LDSS, the storage overhead needed for access control is very small compared to data files.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3395-3400 www.ijaem.net ISSN: 2395-5252



Algorithm used in proposed system:

The blowfish algorithm is used in proposed system. It is applied to encrypt and decrypt data and to generate keys. Blowfish is a symmetric encryption algorithm. It consists of a single key that is used for both encryption and decryption process. This blowfish encryption scheme's secret key ranges from 32 to 448 bits. If the range of key is 448 bits, then it needs 2448 groupings to define all the entire keys. Furthermore, this key has a fixed 64-bit block size with variable-length key block cipher. The cipher is a 16-round Feistel network, which uses password-dependent S-boxes to develop the structure by which the encryption and decryption process has taken place. This cipher divides messages into 64 bits blocks and then encrypts them separately. The algorithm possesses two main sub-key groups, namely, the 18-entry P-boxes (permutation boxes) to perform bit-shuffling and four 256-entry S-boxes (substitution boxes).

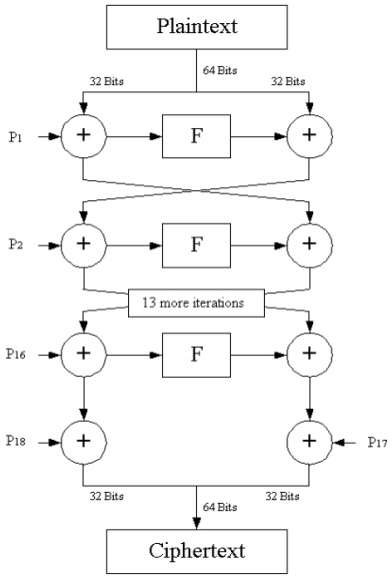
Key generation

The p-array consists of 18, 32-bit subkeys
P1,P2,…….,P18
Four 32-bit S-Boxes consists of 256 entries each
S1,0, S1,1,……. S1,255
S2,0, S2,1,…….. S2,255
S3,0, S3,1,…….. S3,255
S4,0, S4,1,……... S4,255

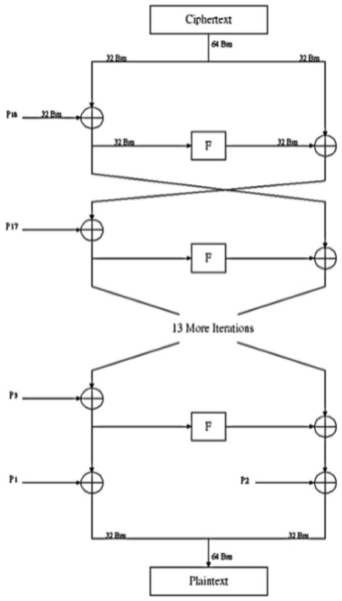
Blowfish Encryption Algorithm

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time.
It will follows the feistel network and this algorithm is divided into two parts. Key expansion and data encryption. Here, the rounds are used in p1,p2….p18 order.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3395-3400 www.ijaem.net ISSN: 2395-5252



Blowfish Decryption Algorithm
Decryption is exactly the same as encryption, except that P1, P2 ..... P18 are used in the reverse order.



Required Resources:
Hardware:
Hardware is the collection of physical parts of a computer system. The hardware requirements used are

(i) System : Pentium IV 2.4 GHz.
(ii) Hard Disk : 40 GB.
(iii) Floppy Drive : 1.44 Mb.
(iv) Monitor : 15 VGA Colour.
(v) Mouse : Logitech.
(vi) Ram : 512 Mb.

Software:
System requirements are the configuration that a system must have in order for a hardware or software application to run smoothly and efficiently. The software requirements are:
(i) Operating system: Windows XP.
(ii) Coding Language: J2EE
(iii) Data Base: MYSQL
(iv) Tool : NetBeans 7.1.1

Implementation:

In proposed system, we develop the architecture of LDSS by using following six components. The six components are:

(1) Data Owner (DO)
(2) Data User (DU)
(3) Trust Party Authority (TPA)
(4) Encryption Service Provider (ESP)
(5) Decryption Service Provider (DSP)
(6) Cloud Service Provider (CSP)

III. CONCLUSION:

The studies in access control in cloud are based on attribute-based encryption algorithm (ABE).

We design an algorithm called LDSS-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over cipher text.

We use proxy servers for encryption and decryption operations which greatly reduce the computational overhead on client side mobile devices.

Thus, it can solve the secure data sharing problem in cloud

IV. FUTURE SCOPE:

There are numerous cryptographic techniques and algorithms are available to provide the data security and privacy to mobile users data for firmly stored on public cloud storage servers. Three cryptographic techniques will be used to improve the security of confidential data.CTR modes of block based cryptographic technique, Blowfish symmetric cryptographic algorithm and MAC will be applying for proposed Data Security Frameworks. For future work there will be the opportunities for researchers to present the secure sharing schemes for sharing the essential data among authorized users. The files must be shared among users according to access privileges assigned by data owner to specific authorized users. There will be additional opportunity to decrease the overhead of cryptographic standard algorithms and research the schemes to afford same security with low overhead as provided by standard cryptographic algorithms.

REFERENCES:

[1]. Zhang, L., Li, H., Zhang, Y., & Khan, F. (2017, May). Efficient privacy-preserving decentralized ABE supporting expressive access structures. In 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 547-552). IEEE.

[2]. Raipurkar, K. V., &Deorankar, A. V. (2016, March). Improve data security in cloud environment by using LDAP and two way encryption algorithm. In 2016 Symposium on Colossal Data Analysis and Networking (CDAN) (pp. 1-4). IEEE.

[3]. Yu, S., Wang, C., Ren, K., & Lou, W. (2016, March). Achieving secure, scalable, and fine-grained data access control in cloud computing. In 2016 Proceedings IEEE INFOCOM (pp. 1-9). Ieee

[4]. Sun, Y., & Liu, K. R. (2016, March). Scalable hierarchical access control in secure group communications. In IEEE INFOCOM 2016 (Vol. 2, pp. 1296-1306). IEEE.

[5]. Boneh, D., Sahai, A., & Waters, B. (2011, March). Functional encryption: Definitions and challenges. In Theory of Cryptography Conference (pp. 253-273). Springer, Berlin, Heidelberg.

[6]. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007, October). Provable data possession at untrusted stores in cloud. In Proceedings of the 14th ACM conference on Computer and communications security(pp. 598-609). Acm.