A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

[1]Prof. Kanchan Umavane, [2]Miss. Nidhi Sharma, [3]Miss. Vrushali Gadhari , [4]Miss.Vedangi Pawar
[5]Mr. S Mohd Huzaifa
[1]Asst.Professor,[2,3,4,5]UG Student,[1,2,3,4,5]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharashtra, India. [1]kanchanumavane2020@gmail.com, [2]nssharma11m@gmail.com, [3]vrushaligadhari8@gmail.com, [4]Pawarveda07@gmail.com, [5]huzaifasayyed66@gmail.com

Abstract: the widespread cloud computing technology, smart phones may now store and access personal information from any location at any time. Consequently, the database security issue in mobile cloud is becoming increasingly serious, impeding the mobile phone usage is increasing cloud. There have been numerous studies undertaken to increase cloud security. However, because mobile devices have very limited processing abilities and power, the majority of them are not appropriate for mobile cloud. For mobile cloud apps, applications with low computing overhead are in high demand. It propose a simple data sharing strategy (LDSS) to mobile cloud computing in this paper . It utilizes CP-ABE, a common authorization technique in cloud environments, but modifications the structure of the access control tree to make it fit for cloud network. environments. LDSS CP-ABE offloads a major chunk of the computationally demanding access control tree translation to external proxies. It also includes attribute descriptive fields to enable carefree, which is a tricky issue in program-based CP-ABE systems, to lower the cost of user revocation. The Experiments reveal that when users share data in portable cloud environments, LDSS can efficiently reduce the latency on the smartphone side.

Keywords—mobile cloud computing ,data authentication methods, encryption, and remote access, user revocation.

I. INTRODUCTION

The utilisation of computer power (hardware and software) offered as a service through a network is known as cloud computing (typically the internet). The name stems from the widespread use of an internet symbol in system diagrams as an abstract for the complicated architecture it encompasses. all data, software, and processing of a user are trusted to remote services in cloud computing.. Cloud-computing is a term referring to using of managed third-party services to make hardware & system capabilities available over the internet. Typically, services provide

-access to powerful software applications server computer networks. How Cloud Computing Works? The Cloud computing's purpose is to is to use traditional high performance computing supercomputing power, which is typically used by army and research centers to perform hundreds Cloud computing's aim is to for every second in consumer-oriented applications like financial portfolios, personalised information, data storage, and the power to Computer games that are big and immersive. Cloud computing distributes data-processing tasks across a network of huge computers that often run reduced consumer PC technologies with specialised connectivity. Typically, services provide access to powerful software applications . high server computer networks.

II. AIMS AND OBJECTIVE

a) Aim

The aim of the scholarly article is a simple, secure data-sharing mechanism for mobile using cloud computing.

b) Objective

- On the cheap, globalise your workforce. all around the world can use the cloud if they have a Connection to the internet.
- Processes should be streamlined. With less, you get more things faster time.1
- There is a drop in employee training needed. It On the cloud, it takes fewer workers to do more work, and there is a low learning curve for hardware and software concerns.

III. LITERATURE SURVEY

Paper 1: In cloud storage systems, essential element perfectly alright authentication and authorization with efficient revocation.

 DOI : 10.35291/2454-9150.2022.0163

A cloud service enables data owners to offload private details to the cloud and offer users with access to it. The semi-trusted cloud service cannot be depended on to implement the access policy since the cloud provider and the data provider are not in that trust domain. Traditional solutions for dealing with this issue typically involve the end user to decrypt data and provide decryption keys to authorised users. These solutions, on the contrary, usually include complex key management and a great amount of overhead for data owners. This present a solution in this paper fine-grained access management structure for cloud services based on an adapted. Ciphertext-Policy, Attribute-based Approach to encryption . An efficient property revocation approach is proposed in the proposed strategy to deal with dynamic changes in users' authorized access in complex networks.

Paper 2: Creating a likeness that is both usable and private Search for data on the cloud that has been outsourced.

This research paper adopts the issue is difficult to solve because of the significant number of the on data users and massive number of outsourced data in the cloud, since it is highly difficult to meet the practical criteria of efficiency, system usability, and greater user searching experiences. The challenge of efficient and secure similarity search across cloud data that has been outsourced investigated in this study. Consistency search is a basic and powerful tool for retrieving plaintext information, but it has yet to be fully revealed in the encrypted information realm. With distance measure as a metric of resemblance, our mechanism design initially uses a suppression technique to build space similarity word sets from the a given document collection. then create a private substring searching index based on it, and display it correctly.

Paper 3: **Various sub with delegation capabilities based on the attributes**

ABPRE (attribute-based proxy re-encryption scheme) is a novel cryptographic primitive that extends classic usually re (public key or identity-based cryptosystem) to the attribute-based equivalent, allowing users to delegate access control authority. users could freely nominate a proxy, defined by qualities, who could re-encrypt a ciphertext associated with one access structure to another with a different entry policy. Without random oracles, the suggested method is shown to be selective-structure selected text secured and master key secure. In addition, in our scheme, are working on a new product type of key delegation capacity and examine certain related topics, such as a greater security architecture and applications.

IV. EXISTING SYSTEM

This existing system , For propose a new kind of key delegation capability and examine various relevant topics such as a better security model and applications. The system that has been proposed has as been proven to just be secure using a selective-structure chosen plaintext and it provides the secure data .

V. COMPARATIVE STUDY

SR NO.	PAPER TITLE	AUTHOR NAME	TECHNOLOGY	ADVANTAGE	PURPOSE
1.	Attribute-based fine-grained access control with Efficient revocation in cloud storage systems	KanYang, Xiaohua Jia, Kui Ren	Cloud Storage	Model produce small size so can be implemented on server1s and mobile devices.	the data owner to encrypt the data and deliver decryption keys to authorized users.
2.	Achieving Usable and Privacy- similarity ensured Search for data on the cloud that has been outsourced.	Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje	Attribute Revocation	Easy to implement	Allow secrecy utilisation procedures for outsourced cloud data using plaintext keyword search is so critical.
3.	Re-encryption of a proxy based on attributes with delegating capabilities	Liang Xiaohui, Cao Zhenfu, Lin Huang	CP-ABE Algorithm	Useful for multi-class classification	a novel cryptographic primitive that builds on the Proxy protocol.

VI. PROBLEM STATEMENT

To provide security for mobile devices in the context of cloud computing in a lightweight manner.

- To have a revocation policy that isn't too heavy. Using a secret key, the encrypted and decryption data should be secure

 DOI : 10.35291/2454-9150.2022.0163

.● The file should only be shared with authorised users that have access privileges.

● There should also be the option of lowering the expense of the cryptography standard algorithm and researching low-overhead security solutions overhead.

VII. PROPOSED SYSTEM

For mobile cloud computing, they propose the any kind of Scheme (LDSS). The following are the significant contributions of LDSS: To provide efficient network access over ciphertext, we developed the LDSS-CP-ABE algorithm, on the basis of the Attribute-Based Encryption (ABE) approach. Encryption and decryption processes are handled by proxy servers. In this technique, ABE's Operations that are computationally expensive are carried out on proxy servers, reducing the computational burden on client-side mobile devices significantly. Meanwhile, in LDSS-CP-ABE, a version property is introduced to the structure providing access to guarantee data privacy. The decrypt key form is changed so it can be securely supplied to proxy servers. To the measures of the file, introduce sluggish re-encryption and a description field in the attributes. To When coping with user revocation problem, lower the revocation overhead. Finally, this construct an LDSS-based data sharing prototype system.

VIII. ALGORITHM

Step-1: Start.
Step-2: taking the user's points into two c, d.
Step-3: The Attribute-Based Encryption process gets the data attributes from the users' formats.
Step-4: These Attributes are being used to create a different figure Key and identify the type of data to be scrambled using the BRE algorithm.
Step-5: The information is divided into an equivalent number of blocks, and also the N x N matrices is constructed from these blocks.
Step-6: A pools of thread will be formed according to the block size.
Step-7: To produce encrypted data inside a a small number of time, run the threads on a multi-core CPU.
Step-8: To open an encrypted file that is saved in the cloud, a hidden key is created.
Step-9: The user receives the secret key by email or text message. The selected file will be unencrypted in its original state using the authorised user's key number. The encrypted file will be decrypted using this key.
Step-10: Integity Ver (P) → (true, false). After getting the proof P , CMS computes L ¼ Pc i¼1sigg ðhðRiÞ⊕H1ðti‖viÞ and verifies whether the following equation holds.
Step-11: The file's algebraic signature block composed of strings s0,s1, …,s n − 1 is defined as sig g ðs0;s1;…; s n − 1Þ¼Pn − 1in the block.
Step-12: The computation overhead of DR is mainly in data sharing phase. DR downloads F′ and computes CK0 ¼ eðC0 ;KÞ V ¼θs . Then DR gets K=C/CK′ and recovers the plaintext F=H2(K) ⊕ F′. Therefore, the computation overhead of DR side is Pair + X or + 2Div.
Then the implementation for encrypted and upload to the file on a server.
Step-13: Exit.

$$L\ (X_i, Y_i) = -\sum_{j=1}^{C} y_{ij} * \log(p_{ij}) \qquad (3)$$

$$y_{ij} = \begin{cases} 1, & if\ i_{th}\ \text{element is in class } j \\ 0, & if\ i_{th}\ \text{element is not in class } j \end{cases}$$

IX. MATHEMATICAL MODEL

• Assumption of Discrete Logarithm (DL). Assume g is just a cyclical number associative group G generator of prime order q. On input y ∈ G, Zero probability exponential time exists procedure that generates the value x∈ Z ω q such that g x =y with non- negligible probability.

• Computational Diffie-Hellman (CDH) Assumption. Assume the letter g is a cyclic nonlinear group G generator of prime order q. On input g x; g y ∈ G, there Probabilistic polynomia does not exist. time-based algorithm that produces g x y ∈ G with non-negligible probability.

• Access Structure. Suppose P= {P1, P2, …, P n} is a group of people. A collection of W ⊆ 2P is monotone if ∀B,C : B ∈ W and B ⊆ C then C ∈ W. An access

• structure is the collection W with non-empty sub- sets of P, i.e., W ⊆ 2P\{∅}. The groups in W are given as follows sets that aren't approved, and sets that aren't They are referred to as the unapproved in W Sets g. It also manually checks the accuracy and decreases learning rate after some successful epochs in order to arrive at the global minima.

The calculation for output can be define by

$$\hat{y} = a = w1x1 + w1x1 + w1x1 \qquad (1)$$

This function can be seen :

$$L\left(\hat{y}^{(i)}, y^{i}\right) = \frac{1}{2}\left(\hat{y}^{(i)}, y^{i}\right)^2 \qquad (2)$$

The model output vector is closer to the true class. (3)

X. SYSTEM ARCHITECTURE

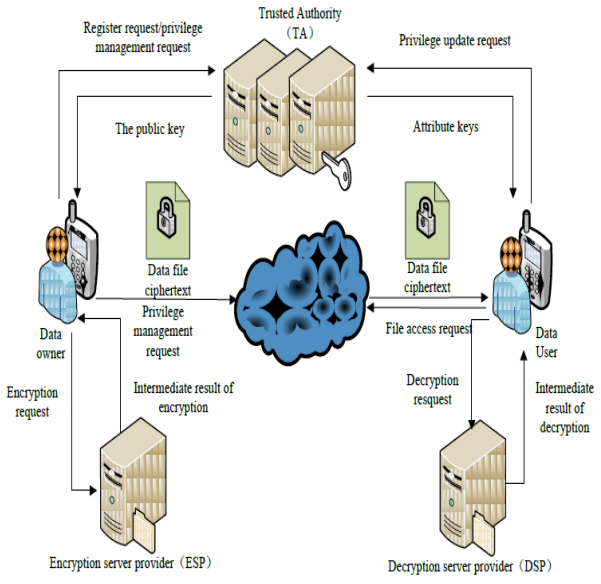

Fig 1. Cloud computing System Architecture

Description:

People are fastest being accustomed to a new era of data sharing in which data is take in the cloud and viewed with

 DOI : 10.35291/2454-9150.2022.0163

the others and mobile devices are used to store/retrieve data from the cloud, due to the rise of cloud computing and the popularity of smart phones. Users (data owners) can use these applications to upload their documents and other files to the cloud and share it with other people (data users) they want to share them with. CSPs also give data owners the ability to leave this data. Sensitive nature of personal data files, data owners have the option to make their files public or just sharing them with specific data users.

XI. ADVANTAGES

- Price**:** Pay for only the resources used.
- Security: To improve security, cloud instances are networked separately from other instances.
- Performance**:** For enhanced performance instance can be added instantaneously. Clients have unlimited access to all resources Scalability: When needed, auto-deploy cloud instances.

XII. DESIGN DETAILS

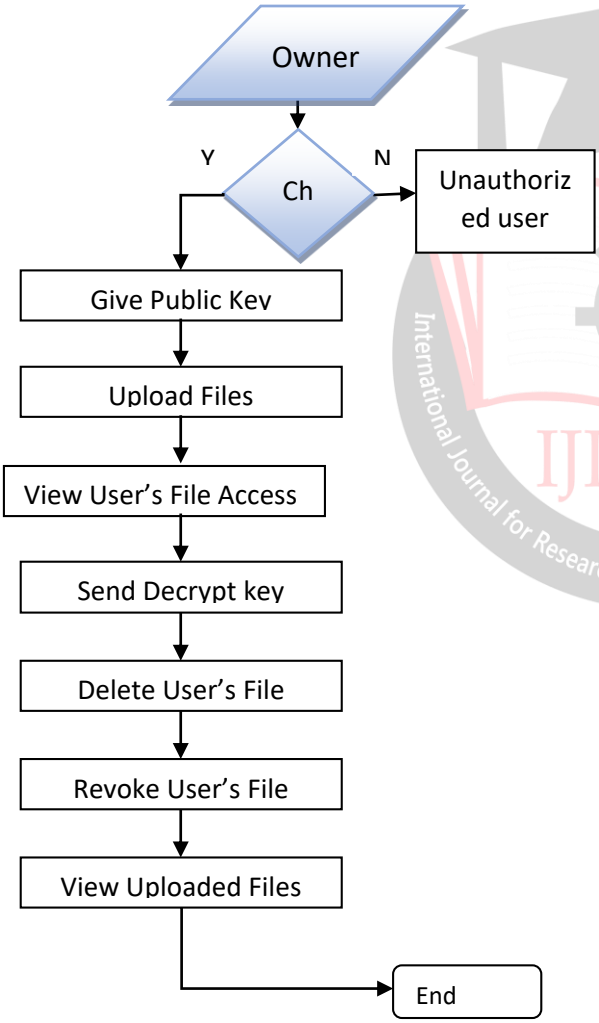

Fig 2. Flowchart for owner.

The bubble chart is also another term for the DFD It's a simple graphical formalism for a system's given data, processing, and output data. One of the most important tools is the data flow diagram (DFD). It's used to portray the system's many components.

These an external entity at which the system interacts process, the data used by the process an external entity with which the system interacts and the information flows in the system.

XIII. CONCLUSION

Thus, In this we have attempt to implement the paper of Author "Tian X , Wang X L, Zhou A Y. In DaaS, DSP RE-Encryption is a flexible tactic to control access control enforcement. in Proceedings of IEEE International Conference on Cloud Computing. IEEE press, pp.25-32, 2009. is incompatible with mobile cloud. because it takes a lot of time to compute and Only a few features are available on mobile devices resources. It suggest in this study To overcome this problem, the LDSS was created. presents a new book T migrate, use the LDSS-CP-ABE algorithm. Major computation overhead from mobile It can therefore resolve the issue of safe data exchange by directing devices to proxy servers We'll also look into how to accomplish it using a mobile cloud ciphertext retrieval of previously shared data scheme.

REFERENCE

[1] Tian X , Wang X L, Zhou A Y. DSP RE-Encryption: A flexible mechanism for access control enforcement management in DaaS. in: Proceedings of IEEE International Conference on Cloud Computing. IEEE press, pp.25-32, 2009.

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

[4] Shamir A. How to share a secret. Communications of the ACM,1979, 22 (11): 612-613.

[5] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. in: Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, pp. 213−229, 2001.

[6] Benjamin Livshits, Jaeyeon Jung. Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications. USENIX Security, pp.113-130, Aug. 2013.

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

[8] 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.

 DOI : 10.35291/2454-9150.2022.0163