International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

A Secure Information Distributed Scheme for Portable Cloud Computing

MAHANTI SRIRAMULU [1], DODDI SUNIL[2], SIVVALA RAMABABU[3]

[1]**Assistant professor, Dept. of CSE, Lendi Institute of Engineering and Science, Jonnada,Vizianagaram, AP.**

[2]**Assistant professor, Dept. of CSE, Lendi Institute of Engineering and Science, Jonnada,Vizianagaram, AP.**

[3]**Assistant professor, Dept. of CSE, Lendi Institute of Engineering and Science, Jonnada,Vizianagaram, AP.**

Abstract—with the fame of distributed computing, portable devices can store/recover individual information from anyplace whenever. Therefore, the information security issue in portable cloud turns out to be increasingly serious and counteracts further improvement of versatile cloud. There are generous examinations that have been directed to improve the cloud security. Be that as it may, the greater part of them is not material for versatile cloud since portable devices just have restricted figuring assets and power. Arrangements with low computational overhead are in incredible requirement for versatile cloud applications. In this paper, we propose a Lightweight Information Distributed Plan (LIDP) for portable distributed computing. It receives Ciphertext Policy Attribute Based Encryption (CP-ABE) an entrance control innovation utilized in ordinary cloud condition, however changes the structure of access control tree to make it appropriate for portable cloud situations. LIDP moves an enormous bit of the computational serious access control tree change in CP-ABE from portable devices to outside intermediary servers. Besides, to lessen the client renouncement cost, it acquaints property portrayal fields with execute sluggish disavowal, which is a prickly issue in program based CP-ABE frameworks. The trial results demonstrate that LIDP can viably decrease the overhead on the cell phone side when clients are sharing information in portable cloud conditions.

Index Terms—portable cloud computing, data encryption, access control.

1. Introduction

With the advancement of distributed computing and the prevalence of keen portable devices, individuals are bit by bit getting familiar with another period of information sharing model in which the information is put away on the cloud and the portable devices are utilized to store/recover the information from the cloud. Commonly, portable devices just have restricted extra room and registering power. In actuality, the cloud has huge measure of assets. In such a situation, to accomplish the acceptable execution, it is basic to utilize the assets given by the cloud specialist organization (CSO) to store and share the information. These days, different cloud portable applications have been broadly utilized. In these applications, individuals (information proprietors) can transfer their photographs, recordings, reports and different documents to the cloud and offer this information with other individuals (information clients) they like to share. CSOs additionally give information the executive's usefulness to information proprietors. Since individual information records are touchy, information proprietors are permitted to pick whether to make their information documents open or must be imparted to explicit information clients. Unmistakably, information security of the individual delicate information is a major worry for some information proprietors. Obviously, to tackle the above issues, individual delicate information ought to be scrambled before transferred onto the cloud with the goal that the information is secure against the CSO. Nonetheless, the information encryption brings new issues. Instructions to give proficient access control system on ciphertext decoding with the goal that solitary the approved clients can get to the plaintext information is testing. Also, framework must offer information proprietors viable client benefit the board capacity, so they can give/deny information access benefits effectively on the information clients. There have been significant looks into on the issue of information access power over ciphertext. In these looks into, they have the accompanying normal suppositions. To start with, the CSO is viewed as legitimate and inquisitive. Second, all the delicate information are encoded before transferred to the Cloud. Third, client approval on specific information is accomplished

through encryption/unscrambling key circulation. As a rule, we can partition these methodologies into four classes: straightforward ciphertext access control, progressive access control, get to control dependent on completely homophobic encryption and access control dependent on trait based system.

2. METHODLOGY

To address this issue, in this paper, we propose a Lightweight Data Sharing Scheme (LIDP) for portable distributed computing condition. The primary commitments of LIDP are as per the following:

1) We structure a calculation called LIDP-CP-ABE dependent on Attribute-Based Encryption (ABE) technique to offer effective access authority over ciphertext.

(2) We use intermediary servers for encryption and unscrambling tasks. In our methodology, computational serious tasks in ABE are directed on intermediary servers, which extraordinarily lessen the computational overhead on customer side cell phones. In the interim, in LIDP-CP-ABE, so as to keep up information protection, a form ascribe is additionally added to the entrance structure. The unscrambling key organization is changed with the goal that it very well may be sent to the intermediary servers in a safe manner.

(3) We present lethargic re-encryption and depiction field of ascribes to diminish the renouncement overhead when managing the client disavowal issue.

(4) Finally, we execute information sharing model system dependent on LIDP. The investigations demonstrate that LIDP can extraordinarily lessen the overhead on the customer side, which just presents a negligible extra expense on the server side. Such a methodology is valuable to actualize practical information sharing security plot on cell phones. The outcomes likewise demonstrate that LIDP has better execution contrasted with the current ABE based access control conspires over ciphertext.

3. OVERVIEW OF PROPOSED SCHEME

In this segment, we portray the LIDP framework plan. To start with, we give the diagram of LIDP, and after that we present

LIDP-CP-ABE calculation and framework tasks, which are the base of LIDP calculation. At long last, we depict LIDP in detail

(1) Data Owner (DO): DO upload data to the mobile cloud and share it with friends. DO determine the access control policies.

(2) Data User (DU): DU retrieves data from the mobile cloud.

(3) Trust Authority (TA): TA is responsible for generating and distributing attribute keys.

(4) Encryption Service Provider (ESP): ESP provides data encryption operations for DO.

(5) Decryption Service Provider (DSP): DSP provides data decryption operations for DU.

(6) Cloud Specialist Organization (CSO): CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO have stored in the cloud.

As shown in a DO sends data to the cloud. Since the cloud is not credible, data has to be encrypted before it is uploaded. The DO defines access control policy in the form of access control tree on data files to assign which attributes a DU should obtain if he wants to access a certain data file. In LIDP, data files are all encrypted with the symmetric encryption mechanism, and the symmetric key for data encryption is also encrypted using attribute based encryption (ABE). The access control policy is embedded in the ciphertext of the symmetric key. Only a DU who obtains attribute keys that satisfy the access control policy can decrypt the ciphertext and retrieve the symmetric key. As the encryption and decryption are both computationally intensive, they introduce heavy burden for mobile users. To relieve the overhead on the client side mobile devices, encryption service provider (ESP) and decryption service provider (DSP) are used. Both the encryption service provider and the decryption service provider are also semi-trusted. We modify the traditional CP-ABE algorithm and design an LIDP-CP-ABE algorithm to ensure the data privacy when outsourcing computational tasks to ESP and DSP.

4. CONCLUSION

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 because it is computationally intensive and mobile devices only have limited resources. In this paper, we propose LIDP to address this issue. It introduces a novel LIDP-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LIDP can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do ciphertext retrieval over existing data sharing schemes.

5. REFRENCES

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.

MAHANTI SRIRAMULU Assistant Professor.

Area of Interest: Cloud Computing.

DODDI SUNIL, Assistant Professor.

Area of Interest: Cloud Computing and Java Programming.

SIVVALA RAMABABU,

Assistant Professor.

Area of Interest: Networking.