A SECURE RAW DATA FILE SHARINGN MECHANISM IN CLOUD COMPUTING

G. Praveen Kumar Associate Professor, Department of CSE, Narayana Engineering College Gudur, SPSR Nellore, AP
Ch.Divya ,A.Akhila, J.Ruchitha UG Scholar, Department of CSE, Narayana Engineering College Gudur (Autonomous), SPSR Nellore, AP

ABSTRACT

With the recognition of cloud computing, mobile devices will store/retrieve personal knowledge from anyplace at any time. Consequently, the info security downside in mobile cloud becomes additional and additional severe and prevents any development of mobile cloud. There square measure substantial studies that are conducted to enhance the cloud security. However, most of them don't seem to be applicable for mobile cloud since mobile devices solely have restricted computing resources and power. Solutions with low machine overhead square measure in nice want for mobile cloud applications. during this paper, we tend to propose a light-weight knowledge sharing theme (LDSS) for mobile cloud computing. It adopts CP-ABE, AN access management technology employed in traditional cloud atmosphere, however changes the structure of access management tree to create it appropriate for mobile cloud environments. LDSS moves an outsized portion of the machine intensive access management tree transformation in CP-ABE from mobile devices to external proxy servers.
what is more, to cut back the user revocation price, it introduces attribute description fields to implement lazy-revocation, that could be a thorny issue in program based mostly CP-ABE systems. The experimental results show that LDSS will effectively cut back the overhead on the mobile device aspect once users square measure sharing knowledge in mobile cloud environments.

INTRODUCTION

Cloud computing is that the use of computing resources (hardware and software) that area unit delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped image as Associate in Nursing abstraction for the advanced infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's knowledge, software system and computation. Cloud computing consists of hardware and software system resources created on the market on the net as managed third-party services. These services usually give access to advanced software system applications and high-end networks of service.

The goal of cloud computing is to use ancient supercomputing, or superior computing power, usually employed by military and analysis facilities, to perform tens of trillions of computations per second, in consumer-oriented applications like monetary portfolios, to deliver personalised data, to produce knowledge storage or to power massive, immersive laptop games.The cloud computing uses networks of enormous teams of servers usually running inexpensive shopper laptop technology with specialised connections to unfold data-processing chores across them. This shared IT infrastructure contains massive pools of systems that area unit joined along. Often, virtualization techniques area unit wont to maximize the facility of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing supported the definitions provided by the National Institute of Standards and nomenclature (NIST) area unit printed below:

On-demand self-service: A shopper will unilaterally provision computing capabilities, like server time and network storage, PRN mechanically while not requiring human interaction with every service's supplier.

Broad network access: Capabilities area unit on the market over the network and accessed through customary mechanisms that promote use by heterogeneous skinny or thick consumer platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling: The provider's computing resources area unit pooled to serve multiple shoppers employing a multi-tenant model, with totally different physical and virtual resources dynamically assigned and reassigned in step with shopper demand. there's a way of location-independence therein the client usually has no management or data over the precise location of the provided resources however could also be ready to specify location at a better level of abstraction (e.g., country, state, or knowledge center). samples of resources embody storage, processing, memory, network information measure, and virtual machines.

Rapid elasticity: Capabilities may be speedily and elastically provisioned, in some cases mechanically, to quickly scale out and speedily discharged to quickly scale in. To the patron, the capabilities on the market for provisioning usually seem to be unlimited and might be purchased in any amount at any time.

Measured service: Cloud systems mechanically management and optimize resource use by leverage a metering capability at some level of abstraction acceptable to the kind of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage may be managed, controlled, and according providing transparency for each the supplier and shopper of the utilised service.

Services Models:

Cloud Computing contains 3 totally different service models, particularly Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The 3 service models or layer area unit completed by Associate in Nursing user layer that encapsulates the top user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, as an example, she will be able to run her own applications on the resources of a cloud infrastructure and stay chargeable for the support, maintenance, and security of those applications herself. If she accesses a service on the applying layer, these tasks area unit usually taken care of by the cloud service supplier

LITERATURE SURVEY

With the fast development of the net of issue (IoT), numerous IoT devices square measure utilized in several applications [1], like sensible grid [2], vehicle network [3], body space network [4]. These IoT devices extremely facilitate existence, however, information privacy [5] [6] issues ought to be addressed since the {information} from IoT devices contains the sensitive information [7].In past decades, k-anonymity [8] [9] and differential pri- vacy [10] square measure wide researched to ensure privacy once information is revealed. Specifically, k-anonymity guarantees that every person can't be distinguished from a minimum of alternative k 1 people by modifying corresponding attributes, meanwhile, differential privacy adds noise to the revealed information to avoid the speech act of personal info records.

However, each k-anonymity and differential privacy square measure accustomed shield the privacy of {the information|the info|the information} that has been col- lected and hold on in data center, in fact, it's below the idea that {the information|the info|the information} center is absolutely trustworthy since it owns or is aware of all hold on data. However, the idea that an information center or edge nodes connecting to IoT devices square measure absolutely trustworthy isn't sensible. Therefore, the sting nodes and information center mustn't directly get information from IoT devices, instead, the information collected with IoT devices ought to be disguised before it's sent to alternative nodes. 2 necessities squaremeasure necessary, specifically information privacy and utility.

Data aggregation permits an information center to get the typical, most or minimum {of information|of knowledge|of information} in a locality while not knowing individual data [11]. However, in some applica- tion eventualities, the typical, most or minimum of information cannot meet

the requirements, a spread of fine-grained information is needed. Recently, a privacy-preserving computing perform library is meant supported Intel code Guard Exten- sions (SGX) [12]. However, Intel SGX might suffer from attack like side-channel attack [13]. For information utilization, n- supply obscurity could be a possible answer by delinking information and its supply wherever a chunk of information is shielded from associate degree n-member cluster and at the same time the rawness of information is ensured. Current n-source obscurity primarily based information assortment schemes primarily use virtual rings a trustworthy third party (TTP) and shuffling to order slots for loading information. However, the sensitive information of associate degree IoT device in virtual rings are often derived thanks to the collusion attack of its upstream and downstream devices. additionally, it's arduous to deploy a TTP in observe. Hence, shuffle is employed to switch the role of TTP, and at the same time to confirm the rawness and unlinkability. sadly, once n IoT devices construct a gaggle for masking their information, in every IoT device of virtual ring reserves n/2 slots on the average, and in n slots square measure reserved. As a consequence, the significant storage value is dropped at every IoT device once n is giant.

RELATED WORK

In general, we are able to divide these approaches into four categories: easy ciphertext access management, hierarchical access management, access management supported totally homomorphic secret writing and access management supported attribute-based secret writing (ABE). of these proposals square measure designed for non-mobile cloud surroundings

Tysowski et al. thought of a particular cloud computing surroundings wherever information square measure accessed by resource-constrained mobile devices, and projected novel modifications to ABE, that allotted the upper process overhead of cryptanalytic operations to the cloud supplier and lowered the entire communication price for the mobile user.

Drawbacks

1.Data privacy of the non-public sensitive information may be a huge concern for several information homeowners.

2.The progressive privilege management/access management mechanisms provided by the CSP square measure either not comfortable or not terribly convenient.

3.They cannot meet all the necessities of information homeowners.They consume great deal of storage and computation resources, that aren't on the market for mobile devices Current solutions don’t solve the user privilege modification drawback okay. Such associate degree operation may lead to terribly high revocation price. this is often not applicable for mobile devices further. Clearly, there's no correct answer which might effectively solve the secure information sharing drawback in mobile cloud.

PROPOSED SYSTEM

We propose a light-weight information Sharing theme (LDSS) for mobile cloud computing surroundings.The main contributions of LDSS square measure as follows:

We style associate degree rule known as LDSS-CP-ABE supported Attribute-Based secret writing (ABE) technique to supply economical access management over ciphertext.

We use proxy servers for secret writing and secret writing operations. In our approach, process intensive operations in ABE square measure conducted on proxy servers, that greatly cut back the process overhead on shopper aspect mobile devices. Meanwhile, in LDSS-CP-ABE, so as to take care of information privacy, a version attribute is additionally other to the access structure. The secret writing key format is changed so it will be sent to the proxy servers during a secure means.

Advantages

1. We introduce lazy re-encryption and outline field of attributes to scale back the revocation overhead once managing the user revocation drawback.

2.Finally, we have a tendency to implement a knowledge sharing epitome framework supported LDSS.
3.The experiments show that LDSS will greatly cut back the overhead on the shopper aspect, that solely introduces a nominal further price on the server aspect.
4.Such associate degree approach is helpful to implement a sensible information sharing security theme on mobile devices.
5.The results additionally show that LDSS has higher performance compared to the present ABE based mostly access management schemes over ciphertext.
6.Multiple revocation operations square measure united into one, reducing the overhead In LDSS, the storage overhead required for access management is incredibly little compared to information files.

METHODOLOGY

MODULES

1 System Framework
2 Data Owner
3 Data User
4 Trusted Authority
5 Cloud Service supplier

System Framework

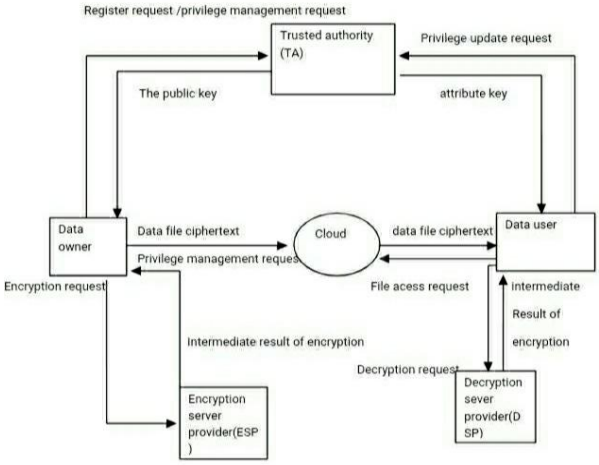
The development of cloud computing and therefore the quality of sensible mobile devices, folks area unit step by step obtaining aware of a brand new era of information sharing model during which the information is hold on on the cloud and therefore the mobile devices area unit wont to store/retrieve the information from the cloud.In these applications, folks (dataowners) will transfer their documents andother files to the cloud and share these information with otherpeople (data users) they prefer to share. CSPs conjointly provide data management practicality for information house owners. Sincepersonal information files area unit sensitive, information house owners area unit allowedto opt for whether or not to form their information files public or canonly be shared with specific information users. Clearly, informationprivacy of the private sensitive
information may be a huge concern formany data house owners.We propose LDSS, a framework of light-weight datasharing theme in mobile cloud. it's thefollowing six parts. (1)Data Owner (DO) (2) information User (DU) (3) Trust Authority (TA) (4) cryptography Service supplier (ESP) (5) decipherment Service supplier (DSP) (6) Cloud Service supplier (CSP).

Data Owner (DO)

When the information owner (DO) registers on metal, metal runs the algorithmic rule Setup() to get a public key PK and a passe-partout MK. PK is shipped to try to to whereas MK is unbroken on metal itself. DO defines its own attribute set and assignsattributes to its contacts. of these info are going to be sent to metal and therefore the cloud.TA and therefore the cloud receive the knowledge and storeit.DO uploads information to the mobilecloud and share it with friends. DO determines the accesscontrol
policies.DO sends information to the cloud. Sincethe cloud isn't credible, information has got to be encrypted before it's uploaded. The DO defines access management policy within the sort of access management tree on files to assign that attributes a DU shouldobtain if he desires to access a particular information file.

Data User (DU):

DU logins onto the system and sends, AN authorization request to metal. The authorization request includes attribute keys (AK) that DU already has.TA accepts the authorization request and checks the request and a generate attribute keys (AK)for DU.DU sends letter of invitation for information to the cloud.Cloud receives the request and checks if the DU meets the access demand. DU receives the ciphertext, that includesciphertext of information files and ciphertext of the parallel key. DU decipher the ciphertext of the parallel key with the help of



DSP. DU uses the parallel key to decipher the ciphertext of information files.

Trusted Authority:

To make LDSS possible in follow, a trustedauthority (TA) is introduced. it's accountable ofgenerating public and personal keys, and distributingattribute keys to users. With this mechanism, users will share and access information while not being conscious of the cryptography and decipherment operations. we tend to assume metal is entirely credible, and a trusty channel exists between the metal and each user. the very fact that a trusty channel exists doesn't mean that the information is shared through the trusty channel, for the information is in a very great deal. metal is barely wont to transfer keys (in atiny low amount) firmly between users. additionally, it's requested that metal is on-line all the time as a result of information users could access information at any time and wish metal to update attribute keys.

Cloud Service Provider:

CSP stores the information for DO. It dependably executes the operations requested by DO, whereas it should peek over information that DO has hold on within the cloud.DU sends letter of invitation for information to the cloud. Cloud receives the request and checks if the DU meets the access demand. If DU can't meet the necessity, it refuses therequest; otherwise it sends the ciphertext to DU. CSP manages the Uploaded Files.

CONCLUSION

In this work, a new notion of lightweight data sharing scheme(LDSS-CPAB)is introduced to support keyword searching and data sharing. A concrete LDSS-CPAB scheme has been constructed in this paper and we prove its LDSS security in the random oracle model. The proposed scheme is demonstrated efficient and practical in the performance and property comparison. This paper provides an affirmative answer to the open challenging problem pointed out in the prior work, which is to design an attribute based encryption with keyword searching and data sharing without the PKG during the sharing phase. Furthermore, our work motivates interesting open problems as well including designing LDSS-CPAB scheme without random oracles or proposing a new scheme to support more expressive keyword search

REFERENCES

[1] A. Zaslavsky, C. Perera, and D. Georgakopoulos, "Estimating age privacy leakage in online social networks," in *proc. of ACC*, 2012, pp. 21–29.

[2] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Pérez- González, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 75–86, 2013.

[3] Y. Liu, S. Lv, M. Xie, Z. Chen, and P. Wang, "Dynamic anonymous identity authentication (daia) scheme for vanet," *International Jour- nal of Communication Systems*, vol. 32, no. 5, p. e3892, 2019.

[4] M. Rabbi, S. Ali, T. Choudhury, and E. Berke, "Passive and in- situ assessment of mental and physical well-being using mobile sensors," in *proc. of UBIC*, 2011, pp. 385–394.

[5] X. Li, Y. Zhu, J. Wang, Z. Liu, Y. Liu, and M. Zhang, "On the soundness and security of privacy-preserving svm for outsourcing data classification," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 906–912, 2018.
[6] Y. Zhu, Y. Zhang, X. Li, H. Yan, and J. Li, "Improved collusion- resisting secure nearest neighbor query over encrypted data in cloud," Concurrency and Computation: Practice and Experience, p. e4681, 2018.
[7] Bhargava, M.G., Vidyullatha, P., Venkateswara Rao, P., Sucharita, V. A study on potential of big visual data analytics in construction Arena International Journal of Engineering and Technology(UAE), 2018, 7(2.7 Special Issue 7), pp. 652–656
[8] Y. Zhang, Q. Chen, and S. Zhong, "Privacy-preserving data aggre- gation in mobile phone sensing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 980–992, 2016.
[9] M. Badra and S. Zeadally, "Design and performance analysis of a virtual ring architecture for smart grid privacy," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 321–329, 2014.
[10] Y. Liu, Y. Wang, X. Wang, Z. Xia, and J. Xu, "Privacy-preserving raw data collection without a trusted authority for iot," *Computer Networks*, vol. 148, pp. 340 – 348, 2019.
[11] A. Shamir, "How to share a secret," *Communications of the ACM*,vol. 22, no. 11, pp. 612–613, 1979.
[12] J. C. Benaloh, "Secret sharing homomorphisms: keeping shares of a secret secret (extended abstract)," in *proc. of EUROCRYPT*, 1987, pp. 251–260.
[13] Y. Liu and Q. Zhao, "E-voting scheme using secret sharing and k-anonymity," *World Wide Web*, vol. 22, no. 4, pp. 1657–1667, 2019.