Privacy Preserving Mobile Data Cloud With Sandboxing

E. Arun[*1], J. Rajeesh[2], R. Krshnan Thampi[3]

[1]Professor, Department of Computer Science and Engineering
[2]Professor, Department of Electronics and Communication Engineering
[3]Dean, Department of Computer Science and Engineering Department
Ponjesly College of Engineering, Tamil Nadu, 629 162, India
arunsedly@yahoo.com, arunres2005@gmail.com

Abstract: Managing data on the cloud raises many complications. In mobile cloud computing, as the name itself suggests, data that would traditionally be accessible only to the mobile device's owner, would now be stored on, accessible to, shared with external devices or users. The issue here is the unauthorized access by malicious programs found over net or by hacker. This can be addressed by Sandboxing the files into secure specific locations on cloud. In a mobile cloud, user's geographical locations are not fixed, and bandwidth must be conserved because of data access costs. This problem can be resolved by providing a mobile application that can upload / download files over internet using compression to the cloud server. One of the key concerns for people about using a mobile cloud is that their personal data on mobile device could be stored on, or accessed by the cloud. The access privilege for each user is set through ACL (Access Control Lists) provided by the cloud server.

[E. Arun, J. Rajeesh, R. Krshnan Thampi. **Privacy Preserving Mobile Data Cloud With Sandboxing.** *Life Sci J* 2013;10(7s):1019-1023] (ISSN:1097-8135). http://www.lifesciencesite.com. 164

Keywords: privacy, sandboxing, ACL, security, cloud, storage**.**

1. Introduction

After dotcom boom the technologists are touting cloud computing as the big thing in the world of internet. But the potential of cloud computing is not limited to only internet based pc applications. this is the era of mobility and almost each and every pc based application is now has a mobile version available. Mobile cloud computing is an technique or model in which mobile applications are built, powered and hosted using cloud computing technology.

A mobile cloud approach enables developers to build applications designed specifically for mobile users without being bound by the mobile operating system and the computing or memory capacity of the smart phone. Mobile cloud computing centered are generally accessed via a mobile browser from a remote web server, typically without the need for installing a client application on the recipient phone.

Smart phones, tablets, and cloud computing are converging in the new, rapidly growing field of mobile cloud computing. in less than four years, there will be 1 trillion cloud-ready devices. learn about the devices (smart phones, tablets, wi-fi sensors), the trends (more flexible application development, changing work patterns), the issues (device resource poverty, latency/bandwidth, security), and the enabling technologies that come along with a more mobile, device-loving cloud environment. mobile cloud computing aims to empower the mobile user by providing a seamless and rich functionality, regardless of the resource limitations of mobile devices. here consider one problem issue as operational issue and provide some technologies to overcome the existing problems.

Managing data on the cloud raises many complications. in mobile cloud computing, as the name itself suggests, data that would traditionally be accessible only to the mobile device's owner, would now be stored on, accessible to, shared with external devices or users. for many mobile users, this raises privacy and security questions. computations in a mobile cloud would be spread across a distributed file system, where multiple devices may need to access and modify files. the issue here is the unauthorized access by malicious programs found over net or by hacker. this can be addressed by sandboxing the files into secure specific locations on cloud.

2. Literature Review

Cloud computing is an emerging concept combining many fields of computing. The foundation of cloud computing is the delivery of services, software and processing capacity over the Internet, reducing cost, increasing storage, automating systems, decoupling of service delivery from underlying technology, and providing flexibility and mobility of information.

Motivation: the need for a mobile cloud The case for mobile cloud computing can be argued by considering the unique advantages of empowered mobile computing, and a wide range of potential mobile cloud applications have been recognized in the literature. These applications fall into different areas such as image processing, natural language processing, sharing GPS, sharing Internet access, sensor data applications, querying, crowd computing and multimedia search. However, as explained in [4], applications that involve distributed computation do have certain common characteristics, such as having data with easily detectable segment boundaries, and the time to recombine partial results into a complete result must also be small. An example is string matching/manipulation such as grep and word frequency counters

However, the actual realization of these benefits is far from being achieved for mobile applications and arises many new research questions. In order to better understand how to facilitate the building of mobile cloud-based applications, we have surveyed existing work in mobile computing through the prism of cloud computing principles.

Cloud storage services enable users to remotely access data in a cloud anytime and anywhere, using any device, in a pay-as-you-go manner. Moving data into a cloud offers great convenience to users since they do not have to care about the large capital investment in both the deployment and management of the hardware infra structures. However, allowing a Cloud Service Provider (CSP), whose purpose is mainly for making a profit, to take the custody of sensitive data, raises underlying security and privacy issues. To keep user data confidential against an untrusted CSP, a natural way is to apply cryptographic approaches, by disclosing the data decryption key only to authorized users.

In this paper, investigate the characteristics of cloud storage services and propose a Secure and Privacy Preserving Keyword Searching (SPKS) scheme[3], which allows the CSP to participate in the decipherment, and to return only files containing certain keywords specified by the users, so as to reduce both the computational and communication overhead in decryption for users, on the condition of preserving user data privacy and user querying privacy. Performance analysis shows that the SPKS scheme is applicable to a cloud environment.

The biggest hurdle to the adoption of cloud storage (and cloud computing in general) is concern over the confidentiality and integrity of data. While, so far, consumers have been willing to trade privacy for the convenience of software services (e.g., for web-based email, calendars, pictures etc), this is not the case for enterprises and government organizations.

This reluctance can be attributed to several factors that range from a desire to protect mission-critical data to regulatory obligations to preserve the confidentiality and integrity of data. The latter can occur when the customer is responsible for keeping personally identifiable information (PII), or medical and financial records. To address the concerns outlined above and increase the adoption of cloud storage, we argue for designing a virtual private storage service based on recently developed cryptographic techniques. Such a service should aim to achieve the best of both worlds by providing the security of a private cloud and the functionality and cost savings of a public cloud.

3. Material and Methods

The currently available applications on server can use and download the resources with a simple authenticity verification by the server end. The authenticated server user can use the files without the classification of authorized / unauthorized files which may not be classified to any users. This leads to privacy breaching of access over files on server.

The proposed system will strictly have privacy preserving techniques to identify the users and the resource authenticity. The unauthorized access by the other server users are limited by the Access Control Lists provided carefully by the Cloud Server with prompt access privileges. Each user on upload of resources to the cloud will be scrutinized and categorized by the server. Then the grouped resources are given privileges and ACL is provided.

Upon request by the Mobile client applications, the user rights are identified and requested resource access will be given or denied. The proposed system will have strong sandboxing techniques to put the resources on the cloud in order to get it accessible by the clients with at most security. The grouping and locating can be done at server end with a detailed Access Control Specification. The client can get the access right of the cloud server resources after the access control authenticity verification and processing.

3.1 Working Principle

The area of interest is mobile cloud computing**.** Mobile devices allow users to run powerful applications that take advantage of the growing availability of built-in sensing and better data exchange capabilities of mobile devices. As a result, mobile applications seamlessly integrate with real-time data streams and Web 2.0 applications, such as mash ups, open collaboration, social networking and mobile commerce.

In a mobile cloud, user’s geographical locations are not fixed, and bandwidth must be conserved because of data access costs. This problem can be resolved by providing a mobile application that can upload / download files over internet using compression to the cloud server.

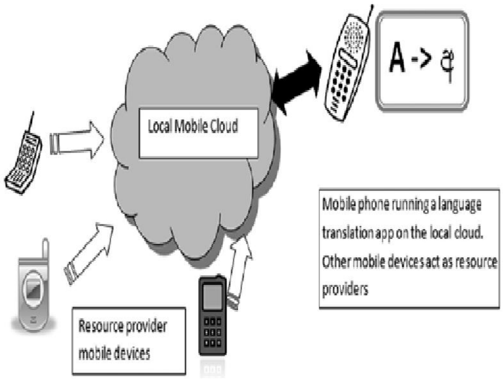
Local Mobile Cloud
A -> क
Mobile phone running a language translation app on the local cloud. Other mobile devices act as resource providers
Resource provider mobile devices

Figure 1. A virtual resource cloud made of mobile devices in the vicinity

One of the key concerns for people about using a mobile cloud is that their personal data on mobile device could be stored on, or accessed by the cloud. The access privilege for each user is set through ACL (Access Control Lists) provided by the cloud server.

Modules:

User authentication

- Storage ACL
- Upload/download through desktop
- Remote view through Android device

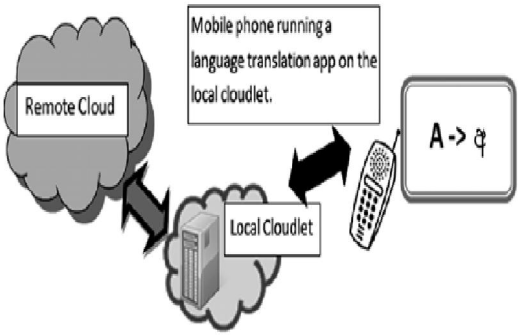
Remote Cloud
Mobile phone running a language translation app on the local cloudlet.
Local Cloudlet
A -> क

Figure 2. A cloudlet enabling mobile devices to bypass latency and bandwidth issues while benefitting from its resources.

User authentication

- ✓ Register a client through desktop application
- ✓ Android mapping/unmapping.
- ✓ Login verification through desktop.
- ✓ Login verification through android application

Storage and ACL

- ✓ Creating a remote storage.
- ✓ Location content remote storage
- ✓ Set ACL list for remote content

Upload/download through desktop.

- ✓ Upload local content to cloud storage.
- ✓ Download local content from cloud storage.

Remote view through Android device

- ✓ User authentication with remote server
- ✓ Getting storage list to view an android

3.2 Algorithm

One of the emerging concept in mobile data protection is k-anonymity, which has been recently proposed as a property that captures the protection of mobile data with respect to possible re-identification of the respondents to which the data refer. k-anonymity demands that every files in the mobile data list released be indistinguishably related to no fewer than k respondents. One of the interesting aspect of k-anonymity is its association with protection techniques that preserve the truthfulness of the data. In this chapter we discuss the concept of k-anonymity, from its original proposal illustrating its enforcement via generalization and suppression. We also discuss different ways to, introduce a taxonomy of k-anonymity solutions.

The goal of this section is to provide a formal framework for constructing and evaluating algorithms and systems that release information such that the released information limits what can be revealed about properties of the entities that are to be protected. For convenience, I focus on client-server system, so the entities are clients, and the property to be protected is the identity of the clients whose information is contained in the data. However, other properties could also be protected. The methods provided in this paper include the k-anonymity protection model.

Making such a determination directly can be an extremely difficult task for the systems to release information about data to be stored. Although I can assume the system knows which data can also appear externally, and therefore what constitutes a quasi-identifier, the specific values contained in external data cannot be assumed. I therefore seek to protect the information in this work by satisfying a slightly different constraint on released data, termed the k-anonymity requirement. This is a special case of k-map protection where k is enforced on the released data.

3.2.1 *Definition: k-anonymity*

Let RT(A1,...,An) be a table and QIRT be the quasi-identifier associated with it. RT is said to satisfy k-anonymity if and only if each sequence of values in RT[QIRT] appears with at least k occurrences in RT[QIRT]. I have presented the k-anonymity protection model, explored related attacks and provided ways in which these attacks can be thwarted.

3.2.2 *The l-diversity Method*

The k-anonymity is an attractive technique because of the simplicity of the definition and the numerous algorithms available to perform the anonymization. Nevertheless the technique is susceptible to many kinds of attacks especially when background knowledge is available to the attacker. Some kinds of such attacks are as follows:

3.2.3 *Homogeneity Attack*

In this attack, all the values for a sensitive attribute within a group of k records are the same. Therefore, even though the data is k-anonymized, the value of the sensitive attribute for that group of k records can be predicted exactly.

3.2.4 *Background Knowledge Attack*

In this attack, the adversary can use an association between one or more quasi-identifier attributes with the sensitive data in order to narrow down possible values of the sensitive field further.

Clearly, while k-anonymity is effective in preventing identification of a record, it may not always be effective in preventing inference of the sensitive values of data of that record. Therefore, the technique of l-diversity was proposed which not only maintains the minimum group size of k, but also focuses on maintaining the diversity of the sensitive files storage. Therefore, the l-diversity model for privacy is defined as follows:

3.3 The t-closeness Model

The t-closeness model is a further enhancement on the concept of l-diversity. One characteristic of the l-diversity model is that it treats all values of a given attribute in a similar way irrespective of its distribution in the data. This is rarely the case for real data sets, since the attribute values may be very skewed. This may make it more difficult to create feasible l-diverse representations. Often, an adversary may use background knowledge of the global distribution in order to make inferences about sensitive values in the data. Furthermore, not all values of an attribute are equally sensitive.

Furthermore, the t-closeness approach tends to be more effective than many other privacy preserving data methods for the case of storing a files.

Privacy-preserving data finds numerous applications in surveillance which are naturally supposed to be "privacy-violating" applications. The key is to design methods which continue to be effective, without compromising security. Most methods for privacy computations use some form of transformation on the data in order to perform the privacy preservation. Typically, such methods reduce the granularity of representation in order to reduce the privacy. This reduction in granularity results in some loss of effectiveness of data management or mining algorithms. This is the natural trade-off between information loss and privacy. Some examples of such techniques are as follows:

3.4 The k-anonymity model and l-diversity

The k-anonymity model was developed because of the possibility of indirect identification of records from public databases. This is because combinations of record attributes can be used to exactly identify individual records. In the k-anonymity method, we reduce the granularity of data representation with the use of techniques such as generalization and suppression. This granularity is reduced sufficiently that any given record maps onto at least k other records in the data. The l-diversity model was designed to handle some weaknesses in the k-anonymity model since protecting identities to the level of k-individuals is not the same as protecting the corresponding sensitive values, especially when there is homogeneity of sensitive values within a group. To do so, the concept of intra-group diversity of sensitive values is promoted within the anonymization scheme.

3.5 Privacy Quantification

The quantity used to measure privacy should indicate how closely the original value of an attribute can be estimated. The work in uses a measure that defines privacy as follows: If the original value can be estimated with c% confidence to lie in the interval [α1, α2], then the interval width (α2 − α1) defines the amount of privacy at c% confidence level. For example, if the perturbing additive is uniformly distributed in an interval of width 2α, then α is the amount of privacy at confidence level 50% and 2α is the amount of privacy at confidence level 100%. However, this simple method of determining privacy can be subtly incomplete in some situations. This can be best explained by the following example.

Example: Consider an attribute X with the density function fX(x) given
by:
fX(x) = 0.5 0<=x<=1
0.5 4 <=x<=5
0 otherwise

Assume that the perturbing additive Y is distributed uniformly between [−1, 1]. Then according to the measure proposed in [2], the amount of privacy is 2 at confidence level 100%.

4. Results

This paper tells the importance of protecting the individuals on cloud storage and their privacy in access of the resources. This paper provides an important privacy preserving technique with security known as k-anonymity and we strongly explained it with its functional details.

The combination of cloud computing, wireless communication infrastructure, portable computing devices, location-based services, mobile Web, etc., has laid the foundation for a novel computing model, called mobile cloud computing, which allows users an online access to unlimited computing power and storage space. Taking the cloud computing features in the mobile domain, the application software can be created.

Mobile cloud computing is a model for transparent elastic augmentation of mobile device capabilities via ubiquitous wireless access to cloud storage and computing resources, with context-aware dynamic adjusting of offloading in respect to change in operating conditions, while preserving available sensing and interactivity capabilities of mobile devices."

Cloud computing is an emerging concept combining many fields of computing. The foundation of cloud computing is the delivery of services, software and processing capacity over the Internet, reducing cost, increasing storage, automating systems, decoupling of service delivery from underlying technology, and providing flexibility and mobility of information.

However, the actual realization of these benefits is far from being achieved for mobile applications and arises many new research questions. In order to better understand how to facilitate the building of mobile cloud-based applications, we have surveyed existing work in mobile computing through the prism of cloud computing principles.

We have argued that it is imperative to use privacy preserving techniques in cloud storages that may share personal data such as mobile resources and personal data files. We have achieved good results in subscriber authentication, confidentiality and integrity protection for subscription and publication, and integrity verifying for storage data.

5. Discussions

The Privacy Preserving Mobile Cloud is advantageous in using cloud storage on authenticated access. The much challenging resource identification system on the cloud store by the client application is performed by the smart phone application with effective ACL (Access Control Lists) prepared on the uploading time itself.

The authenticity of mobile users is checked and confirmed by the cloud server on demand basis to provide secure environment in data handling and sharing. The protected data are kept in secured from the malicious accesses by the unauthorized client users. The shared data are distributed to the client mobiles upon request by the client after validating their identity and access rights in the ACL.

Thus argue that it is imperative to use privacy preserving techniques in cloud storages that may share personal data such as mobile resources and personal data files. We have achieved good results in subscriber authentication, confidentiality and integrity protection for subscription and publication, and integrity verifying for storage data.

References

1. Dinh H.T, Lee C, Niyato D, Wang P. A survey of mobile cloud computing: architecture, applications, and approaches: IEEE transactions on Wireless Communications and Mobile Computing, 2011; 48:123-153.
2. Nam. Y.J, Park Y.K, Lee J.T, Ishengoma F,Cost-aware virtual usb drive: providing cost-effective block I/O management commercial cloud storage for mobile devices, IEEE transactions on Computational Science and Engineering, 2010;12: 427–432.
3. Takashi Yoshino, Tomohiro Muta and Jun Munemori. A Survey on Privacy in Mobile Participatory Sensing Applications:", IEEE transactions on security of sensitive customer data in the cloud, 2009; 48: pp. 37-46.
4. Kossmann D, Kraska T, Loesing S. (), An evaluation of Alternative Architectures for Transaction Processing in the Cloud: proceedings on management of data in cloud computing, 2010; 12: 579–590.
5. Satyanarayanan M, Bahl P, Caceres R, and Davies N. The case for VM-based cloudlets in mobile computing, IEEE pervasive comput. 2009; 8(4):14–23
6. Ng W.S, Kirchberg M, Bressan S, Tan K.L, Towards a privacy-aware stream data management system for cloud applications: International Journal of Web and Grid Services, 2011;7: 246–267.
7. Rajendra Prasad M, Jayadev Gyani, Murti P. R. K, Mobile Cloud Computing: Implication and challenges,Journal of information engineering and application, 2012; 2(7): 1-15.
8. Perez S, Mobile cloud computing:$9.5 billionby 2004, http://explanet.eu/catalog.php, 2010.

6/24/2013