International Journal of Management, IT & Engineering
(ISSN: 2249-0558)

CONTENTS

Editorial Board

Mr. SANJAY ASATI
Dept of ME, M. Patel Institute of Engg. & Tech., GONDIA(M.S.)

Mr. G. Y. KUDALE
N.M.D. College of Management and Research, GONDIA(M.S.)

Editorial Advisory Board

Title

PRIVACY AND TRUST MANAGEMENT IN CLOUD COMPUTING

Author(s)

Mahesh A. Sale
MTech Computer
VJTI, Matunga, Mumbai
Maharashtra, India

Pramila M. Chawan
Associate Professor
Computer Department
VJTI, Matunga, Mumbai
Maharashtra, India

Abstract:

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is. The purpose of the paper is to focus on various privacy and trust issues in Cloud Computing with the aim to suggest solutions on them. To address the privacy and trust challenges in Cloud Computing, a Client-based Privacy Manager is proposed in this paper. We proposed Client-based Privacy Manager that allows establishing privacy and trust in cloud environment. The design is totally user-centric. Most of the operations involved in granting data accesses are done at the client-side. This minimizes the load over the Cloud Service Provider.

Keywords: CSP (Cloud Service Provider), Pseudonyms, shared-key, personae, Obfuscation, Privacy, Security

Introduction:

It is difficult to come up with a precise definition of cloud computing. In general terms, it's the idea that your computer's applications run somewhere in the "cloud", that is to say, on someone else's server accessed via the Internet. Instead of running program applications or storing data on your own computer, these functions are performed at remote servers which are connected to your computer through the internet [1].

In telecommunications, a "cloud" is the unpredictable part of any network through which data passes between two end points. In cloud computing, the term refers generally to any computer network or system through which personal information is transmitted, processed, and stored, and

over which individuals have little direct knowledge, involvement, control. With more reliable, affordable broadband access, the Internet no longer functions solely as a communications network. It has become a platform for computing. Rather than running software on your own computer or server, Internet users reach to the "cloud" to combine software applications, data storage, and massive computing power. When users store their data with programs hosted on someone else's hardware, they lose a degree of control over their sensitive information. The responsibility for protecting that information from hackers and internal data breaches then falls into the hands of the hosting company rather than the individual user. Government investigators trying to subpoena information could approach that company without informing the data's owners. Some companies could even willingly share sensitive data with marketing firms. So there is a privacy risk in putting your data in someone else's hands. Obviously, the safest approach is to maintain your data under your own control. The concept of handing sensitive data to another company worries many people. Is data held somewhere in the cloud as secure as data protected in user-controlled computers and networks? Privacy and security can only be as good as its weakest link. Cloud computing increases the risk that a security breach may occur.

The remainder of this paper is structured as follows: Section 2 introduces the privacy and trust issues in Cloud Computing. Section 3 describes Recommended Privacy Practices. Section 4 presents a client-based privacy manager which helps to reduce the risk of data leakage and loss of privacy.

Literature survey:

Privacy and Trust Issues in Cloud Computing:

Privacy

The Privacy Act [2] regulates 'information privacy'. The type of privacy covered by the Privacy Act is the protection of people's personal information. Personal information is information that identifies you or could identify you. There are some obvious examples of personal information,

such as your name or address. Personal information can also include medical records, bank account details, photos, videos, and even information about what you like, your opinions and where you work - basically, any information where you are reasonably identifiable.

Privacy Issues in Cloud Computing:

Cloud Computing allows users to collectively share information, data, and apps online, access data and applications wherever they can connect online and to use various mobile devices to access their data and information. Of course there are legitimate privacy concerns with so much user information stored on several virtual servers.

Current privacy laws require implementation of varied security measures depending on the nature of the information. For example medical information, social security numbers, and tax information require a higher degree of security protection to prevent breaches. Considering the recent Twitter breach of information stored on Google Apps, there is concern about whether information stored on the "Cloud" can be adequately protected. If companies that utilize Cloud Computing do not put adequate security measures in place, they are exposing themselves to significant liability. Cloud Computing Service Providers should make it a standard practice to implement the same type of security measures in place as required for private networks. Here are a few tips on adequate security measures for Cloud Computing Service Providers and Consumers.

Service Providers should:

- Require all persons having access to sensitive information sign non-disclosure/confidentiality agreements,
- Implement multiple level password protection for those having access to sensitive data.
- Require those having access to use code words,
- Restrict the amount of people having access to the personal information,

Ensure the levels of security measures implemented are consistent with current privacy laws.

Consumers should:

Read privacy policies thoroughly before using a Cloud Computing Service. Specifically consumers should thoroughly understand:

- What type of personal information is collected,
- What type of technology is used to collect the information,
- What specific measures are in place to protect the personal information,
- Where is the information stored.

Cloud Computing is definitely the future and here to stay. However, the industry needs to tighten up their security measures in order to thrive.

Trust:

Trust means an act of faith; confidence and reliance in something that's expected to behave or deliver as promised [3][4]. It's a belief in the competence and expertise of others, such that you feel you can reasonably rely on them to care for your valuable assets [5].

We trust a system less if it gives us insufficient information about its expertise. Mere claims such as "secure cloud" or "trust me" don't help much to boost the trust level of consumers unless sufficient information is presented with the services [6].

Trust Issues in Cloud Computing:

The various trust issues in cloud computing are as follows:

Control

The trust on a system is less when we don't have much control over our assets. The more control consumer shave over the data consigned to a cloud, the more they'll trust the system.

Ownership

When enterprises consign their data to cloud computing (data representing both their own interests and those of their clients), it creates two folds of complex relationship. First, the enterprise must trust the cloud provider. Second, the enterprise must ascertain that its clients have enough reasons to trust the same provider [8].

Prevention

For most of the enterprises, the security breach of data is irreparable. No amount of money can guarantee to restore the lost data or the enterprise's reputation. The cloud computing trust model thus should focus more on preventing failure than on post-failure compensation [8].

Security:

Cloud service providers need to secure the virtual environment, which enables them to run services for multiple clients and offer separate services for different clients. In the context of virtualization, the key security issues include identity management, data leakage (caused by multiple tenants sharing physical resources), access control, virtual machine (VM) protection, persistent client-data security, and the prevention of cross-VM side-channel attacks.

Recommended Privacy Practices:

Some recommended privacy practices for cloud computing designers are as follows:

- Keep the personal information sent and stored in the cloud at minimum
- Protect personal information in the cloud
- Enhance user control on the data
- Mention and restrict the purpose of data usage
- Give feedback

It is to be noted that these privacy practices do not cover all the privacy requirements of cloud, but these are the minimum one that should be implemented in order to ensure privacy in

cloud to an acceptable extent. We now consider in more detail how these guidelines might be achieved in real practice.

Keep the personal information sent and stored in the cloud at minimum:

Analyse the system to find the amount of personal information that needs to be protected. Thus access how only the minimal amount of personal information necessary can be collected and stored. By minimizing the personal information stored in cloud it may not be necessary to protect data as strongly during storage and processing. Also, whenever possible, try to anonymyse the important and sensitive data by obfuscation or encryption techniques. One approach would be to encrypt or obfuscate information on the client machine before it is sent to the cloud for processing, so that only information is revealed that is necessary for the operation of the service [7].

Protect personal information in the cloud:

To protect the personal information in the cloud security safeguards should be used. These security safeguards prevent unauthorized access, disclosure, copying, use or modification of personal information. Personal information can be protected by setting up access controls governing access to it.

Enhance user control on the data:

The lack of control in cloud computing leads to user distrust. Giving someone control over the personal information of the user creates the problem of trust for that user. One possible solution for this is to permit users to state preferences for the management of their personal information. Users should be able to view, modify and correct their personal information in the cloud. Another approach can be to provide auditing mechanism for the user.

Mention and restrict the purpose of data usage:

The user should specify the preferences or the conditions about how the personal information in the cloud be treated in order to ensure that it cannot be compromised. For example, the

personal information of user is only to be for particular purposes, by certain people or that the user must be contacted before it is used. Every information should be adhered to these constraints whenever it is going to be processed. In particular, data usage has to be limited to the purpose for which it was collected.

Give feedback:

Design processes, applications and services to provide feedback, i.e. Supply users with information to allow them to make informed decisions in terms of privacy and to provide notice. An important aspect is the potential for providing assurance to end users about the honesty of the cloud service provision and its capability to carry out both its business and its privacy promises, in order to help users trust the service.

Client-based privacy manager:

In this section, we describe a client-based privacy manager. Some of the features of Client-based privacy manager require the co-operation from Cloud Service Provider. The main goal for designing the client-side privacy manager is to provide a user-centric privacy model. It helps users to control their private and sensitive information, provided that the Cloud Service Provider co-operated with the cloud user.

Architecture of Client-Based Privacy Manager:

The overall architecture of the client-based privacy manager is shown in figure 1. This privacy manager on the client side ensures the privacy to the personal data of cloud-user. One of the main features of the privacy manager is to encrypt the most sensitive information to be sent on the cloud. This minimizes the amount of sensitive information held within the cloud. In addition, the privacy manager ensures the user to check the integrity of his data, to remotely express privacy preferences about the treatment of the data, use multiple personae, access the data with greater trust using user-centric design of privacy manager etc.

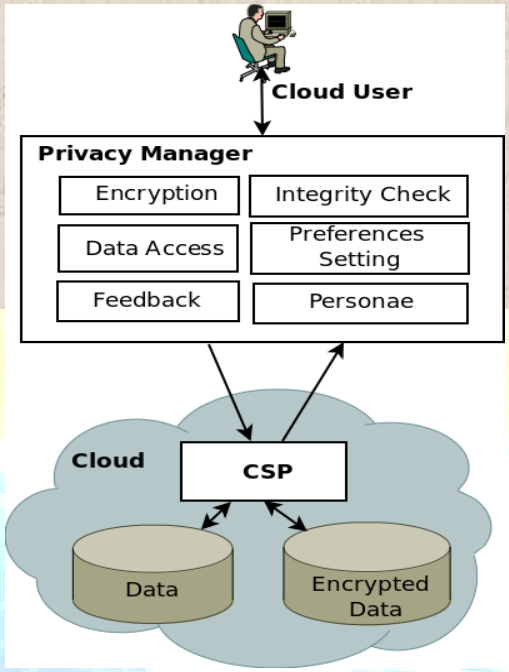

Fig 1: Client-based Privacy Manager

Privacy Manager:

In this section we describe the Privacy Manager in more detail.

Encryption

The main feature of Encryption module in Privacy Manager is to provide encryption and decryption of the data. This feature can automatically encrypt and decrypt some or all of the fields in the data structure. This is done before the data is sent on to the cloud and when the data is accessed from the cloud by the user. The encryption and decryption of the fields in data structure is done by using a secret key. The secret key is known only to the user of the cloud, and it is unknown for the Cloud Service Provider. This assures that no one, except the user, can access the user-protected data. User encrypts those fields in the data structure which he finds more confidential. Since the encryption is controlled by the user, it is more user-centric.

In general, the more fields the user encrypts smaller will be the set of applications that can run using the encrypted user data. It is not always required to encrypt all the fields in the data structure. The data items that are not encrypted may be used by cloud services for personalisation of user content and targeting of advertising.

Preference Setting

The Preference Setting feature of Privacy Manager allows cloud users to set different preferences about the management and handling of their personal and sensitive data and also the data being stored in encrypted form. These preference settings can be associated with the data being stored in cloud. This association of policies can be done by cryptographically bounding the policies to the data (the policy and the data can be encrypted by using a shared-key between the sender and receiver) [6]. For ensuring the privacy and security in encrypting policies and data using the shared-key we can use the key exchange methods of Leighton and Micali [12]. The specifications involved in preference setting could be checked before accesses were granted and it could involve the purpose of using the personal data within the cloud.

Data Integrity Check

The Privacy Manager contains a module that allows users to check the integrity of their data. This module works following the Encryption module. This module allows cloud user to see what is being held about them and to check its accuracy. This is actually an auditing mechanism which will detect privacy violations once they have happened, rather than a mechanism to prevent violations from happening in the first place.

In this module, user attaches a checksum script to the data and sends it to the cloud along with that data. The script follows the data, wherever it goes. The script is get stored in the database at CSP. As mentioned in Preference setting module, the script can be encrypted by the user using a key shared by the sender and receiver [12].

If someone accesses the data of the user or violates its integrity, script will identify that violation. The script will then inform the Alerting Module at the CSP. It's the responsibility of Alerting Module to alert the user about the access or integrity violations.

The Alerting Module can be configured by Cloud user so as to send the alert by E-mail, SMS or the other communication mechanisms provided by CSP.

Data Access

This section introduces the Trust implementation in cloud data access. The design shown in figure 2 is totally user-centric. Most of the operations involved in granting data accesses are done at client-side.

The cloud-user and the CSP negotiate by sharing a shared-key, which can be generated either by CSP or the user. The cloud-user generates a key that is large enough. This key is termed as the original-key. The user then divides the key equally. The first halve of the key is termed as user-key and the second halve is termed as the CSP-key. The user sends this CSP-key to the CSP by encrypting it with the shared-key. The CSP can then decrypt the CSP-key using the same shared key. We can the method of exchanging the keys given by Leighton and Micali [12] for key distribution.

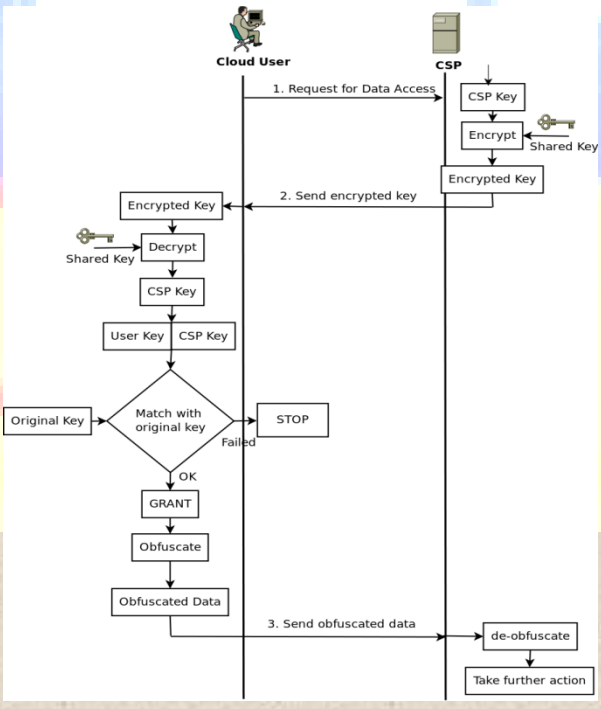

Fig 2: The process of granting access to data in Cloud

After the secure distribution of keys the process of granting access to a user starts. After receiving the request from a user for access to the cloud data, the CSP encrypts his CSP-key with the shared key and sends that encrypted key to the user. The user decrypt the key received from CSP, using the shared key and append it to his user-key to form a larger key for comparison. The resultant key is then compared with the original key previously generated by the user. If the two keys matched, the user will generate the specific order like GRANT, DENY etc. otherwise the process will stop.

The order generated by the user is then obfuscated by the obfuscate unit and the resultant obfuscated order is then send to the CSP. The CSP then de-obfuscate the order and takes the further action. That is if, after de-obfuscation, the order received from the user is GRANT; the CSP will grant the access to that particular user otherwise it will simply deny the access.

The Process of Obfuscation

This feature automatically obfuscate the order generated by the user before it is sent off to the CSP for processing, and translate the same to de-obfuscated form at CSP-side [6]. Here, the obfuscation feature obfuscates the user-generated orders GRANT, DENY etc. into pseudonyms. The obfuscation software will generate new pseudonym maps for each new user. The pseudonym maps may be implemented by association tables or by a deterministic symmetric encryption function.

Feedback

The system proposed by Miranda Mowbray and Siani Pearson [6] describes a feedback method that manages and displays feedback to the user regarding usage of his personal information, including notification of data usage in the cloud. The same logic could be integrated with our system. As suggested by Miranda Mowbray and Siani Pearson this module could monitor personal data that is transferred from the platform. This could involve location information, usage tracking, behavioural analysis, etc. The Preferences Setting feature would allow the user to control such collection.

Personae

The Personae module of Client-Based Privacy Manager allows the user to choose between number of sessions of cloud access. In some sessions, for example, a user might not want to reveal any personal information and just act in an anonymous manner, whereas in other contexts he might wish for partial or full disclosure of identity [12]. The choice of user about a personae will decide the strength of encryption. For example, certain data items would be encrypted in one personae whereas the same data items might not be encrypted in another one.

CONCLUSION:

We proposed Client-based Privacy Manager that allows establishing privacy and trust in cloud environment. The design is totally user-centric. Most of the operations involved in granting data accesses are done at the client-side. This minimizes the load over the CSP. Also, here the user is proving his identity and not the CSP. Thus, its hard for a malicious user to prove his identity to CSP for granting access to the data. The CSP-key is known to the user (user himself has generated it), still the CSP needs to send his key to the cloud-user. This approach is for avoiding the MITM (Man In The Middle) attack and DOS (Denial of Service) attack. An intruder can act as a CSP to user, but the intruder can succeed only if he knows both the CSP-key and the shared key. And its hard for an intruder to get both the keys of CSP. As both the CSP-key and the user-key are decided by the user, it greatly ensures the "Trust" factor in data access. That is no one other than the user, is allowed to grant the access to the cloud-data. Even CSP has to grant or deny access according to user's order. Even if a hacker succeeded in getting the shared key, that will be useful for him only if he knows the CSP-key also.

REFERENCES:

- http://www.privacyrights.org/ar/cloud-computing.htm
- http://www.privacy.gov.au/law/act

- C. Costa and K. Bijlsma-Frankema, "Trust and Control Interrelations," Group and Organization Management, vol. 32, no. 4, 2007, pp. 392–406.
- M. Lund and B. Solhaug, "Evolution in Relation to Risk and Trust Management," Computer, May 2010, pp. 49–55.
- D. Gambetta, "Can We Trust Trust?" Trust: Making and Breaking Cooperative Relations, Basil Blackwell, 1988, pp. 213–237.
- Miranda Mowbray and Siani Pearson, HP Labs, Long Down Avenue, Stoke Gofford Bristol, UK, "A Client-Based Privacy Manager for Cloud Computing", COMSWARE'09, June 16-19,2009, Dublin, Ireland. Digital Object Identifier, http:dx.doi.org/10.4108/ICST.COMSWARE2009.6493.
- Kai Hwang, University of Southern California, Deyi Li, Tsinghua University, China, "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE INTERNET COMPUTING, 2010 IEEE.
- Siani Pearson, HP Labs, Bristol, UK, "Taking Account of Privacy when Designing Cloud Computing Services", CLOUD'09, May 23, 2009, IEEE.
- Bret Michael Associate Editor in Chief, "In Clouds Shall We Trust?", IEEE Computer and Reliability Society, SEPTEMBER/OCTOBER 2009, pp. 03.
- Lori M. Kaufman BAE Systems, "Can a Trusted Environment Provide Security?", IEEE Computer and Reliability Society, JANUARY/FEBRUARY 2010, pp. 50-52.
- Erel Geron, Avishai Wool, Tel Aviv University, "CRUST: Cryptographic Remote Untrusted Storage without Public Keys", Fourth International IEEE Security In Storage Workshop, 2007, IEEE.
- F.T. Leighton and S. Micali. Secret-key agreement without public-key cryptography. In Proc. of CRYPTO, volume 773 of Lecture Notes in Computer Science, pages 456–479. Springer, 1993.