© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Cloud Data Sharing Using Cipher Proxy Re-encryption and Ciphertext-Policy Attribute Based Encryption

StanleyRaja S. J.*, Dr R.Subha

Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, TamilNadu, India

ABSTRACT

Due to the rapid growth in networks communication security issue are being a challenging task. In this project deep analysis is to be made in the cyber security using proxy re-encryption and cipher text crypto system. Various algorithm are been proposed for the cipher text encryption and decryption in decentralized mobile networks with mobile user policy. Based on the existing study it is to propose a new algorithm for encryption and decryption. Ciphertext-policy attribute-based encryption scheme delegating attribute revocation process to cloud server by proxy re-encryption. The proposed scheme does not require secret sharing schemes (LSSS) access structure. Proposed scheme is secure against attack by unauthorized users and cloud server. Sharing of the cloud storage has a risk of information leakage caused by service. In order the protect data, the data owner encrypts data shared on the cloud storage so that only authorized users can decrypt the cloud data.

Keywords: Ciphertext, encryption, LSSS, CP-ABE, KP-ABE, Geoghegan

I. INTRODUCTION

Cloud storage is used to store and share the data very easily and low cost, but cloud storage has a risk of data leakage caused by service providers and hackers. In order to protect data, in cloud storage the data owner encrypts data shared on the cloud storage so authorized users can decrypt the data using

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is used for data access control in the cloud storage system. The authority manages the attributes in the cloud storage. The data owner chooses an access structure and encrypts message under the access cloud. The set of attributes assigned to users and create secret key by the data owner. A user is able to decrypt a ciphertext if his secret key satisfies the ciphertext's access structure.

There are user's secret key revocation and grant in CP-ABE. In simple processes of user's secret key revocation, when his secret key is revoked, the data owner re-encrypts the shared data so that user cannot decrypt the data. Then, the authority

Create new secret keys so that other users can decrypt. In simple processes of user's secret key grant, the authority generates a new secret key. These simple processes are concentrated on the data owner and the authority. (Defined by each user's attributes set) is at risk because one's identity is authenticated based on his information for the Purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client's personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers.

Secure Data Sharing in Cloud Computing Cloud Computing is a promising next-generation IT architecture which provides flexible and unlimited resources, including storage, as services to cloud users. In Cloud Computing cloud users and cloud service providers are almost definite to be from different trust domains. A secure user-enforced data access control device must be provided before cloud users have the

liberty to outsource sensitive data to the cloud for storage. In this dissertation, we propose a cryptographic-based data access control mechanism with Attribute Based Encryption enable the data owner to take fully access control over cloud data. Compared to previous work, our scheme provides better scalability when providing fine-grained cloud data access control because the complexity of most system operations in our scheme is linear to the number of attributes rather than the number of users/data files.

In Cloud Computing, cloud servers are very powerful but cloud users could be resource-constrained devices such as mobile phones. To reduce the computation load for cloud users, we combine various computation delegation techniques with ABE and securely offload computation-intensive tasks to powerful cloud servers. For example, we integrate the technique of proxy re-encryption into Attribute Based Encryption and securely mitigate the laborious user revocation task from the data owner to cloud servers. Using another computation delegation technique, we reduce the computation load for data consumers to constant complexity and make it affordable to user devices such as mobile phones. The proposed scheme also significantly saves the computation load for cloud servers by exploiting the technique of lazy re-encryption [14]. Both performance analysis and security proof are provided.

In KP-ABE, ciphertexts are associated with attributes, while user secret keys are defined with access structures on attributes. If only the ciphertext attributes satisfy a user's access structure, can he decrypt. When CP-ABE is applicable in Role-Based Access Control like scenarios, KP-ABE is suitable for applications such as pay-preview TV systems, in which user access privileges are defined over content attributes and could be based on the prices they paid. In these application scenarios, the issue of key revocation also exists. Fig. 2. shows such an example, in which a user currently is allowed to access any series with name "Hero", "Lost", or "Dexter"' provided by channel 4. The system administrator now wants to disable the user's access privilege on series with name "Lost" for some reason (maybe late payment). For this purpose, it is necessary to revoke the corresponding component of the user's secret key. Similar to CP-ABE, the basic construction of current KP-ABE scheme [12] also defines a system master key component t_i for each attribute i. The corresponding public key component is defined as $T_i = g^{ti}$. Encrypting a message with attribute i means including a component T_i^s into the ciphertext, where s is a random number for this ciphertext. In user secret key, the component for attribute i has the form of $g^{\frac{qx(0)}{t_i}}$, where $q_x(\cdot)$ is a polynomial uniquely defined for the user. Therefore, we can revoke a secret key component in the same way as we did for CP-ABE, i.e., the authority redefines the master key component as t'_i and give $\frac{t'_i}{t_i}$ to proxy servers as the proxy re-key. In the same way as our CP-ABE scheme, proxy servers, which are honest by our assumption, will use these proxy re-key's to re-encrypt ciphertexts stored on them and update secret keys for all but the user for revocation. Proof of the new KP-ABE scheme is similar to that of our CP-ABE scheme.

II. METHODS AND MATERIAL

1. Related Work

This section aims to present a summary of existing review articles related to secure data sharing in the Cloud. The review articles and surveys presented in this section do not focus specifically on secure data sharing in the Cloud, rather the main requirements that will enable it. The study of secure data sharing in the Cloud is fairly new and has become increasingly important with the advancements and growing popularity of the Cloud as well as the growing need to share data between people. There have been a number of reviews on security and privacy in the Cloud. Xiao and Xiao identifies the five concerns of Cloud computing; confidentiality, integrity, availability, accountability, and privacy and thoroughly reviews the threats to each of the concerns as well as defines strategies. Chen and Zhao outline the requirements for achieving privacy and security in the Cloud and also briefly outlines the requirements for secure data sharing in the Cloud. Zhou provided a survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security breaches of one's personal data in the Cloud. Wang et al.explored factors that affect managing information security in Cloud computing. It explains the necessary security needs for enterprises to understand the dynamics of information security in the Cloud. Wang carried out a study on the privacy and security compliance of Software-As-A-Service (SaaS) among enterprises through pilot testing privacy/security compliance. They then carry out analysis work on the measurements to check whether SaaS complies with privacy and security standards. ThemethoddoesnothowevertakeintoaccountotherCloudmodelssuchasPlatformAs-A-Service (PaaS) and in

particular Infrastructure-As-A-Service (IaaS), as needed for data sharing. Oza et al. carried out a survey on a number of users to determine the user experience of Cloud computing and found that the main issue of all users was trust and how to choose between different Cloud Service Providers. This is also highlighted in as it states, "Although researchers have identified numerous security threats to the Cloud, malicious insiders still represent a significant concern." There are many examples of insider attacks such as Google Docs containing a flaw that inadvertently shared user documents, MediaMax going out of business in 2008 after losing 45 % of stored client data due to administrator error, Salesforce.com leaking a customer list and falling victim to phishing attacks on a number of occasions. It's clear from many of the reviews, that the Cloud is very susceptible to privacy and security attacks and currently there is on-going research that aims to prevent and/or reduce the likelihood of such attacks.

The importance of data sharing and the need to ensure privacy and security is discussed in a number of existing articles. Saradhy and Muralidhar review the impact of the Internet on data sharing across many different organisations such as government agencies and businesses. They classify data sharing into data dissemination, query restriction, and record matching. They also provide a framework for secure and useful sharing of data on the internet. Butler describes the issues of data sharing on the Internet where sharing information can allow users to infer details about users. This is useful as it raises awareness to organisations that the data they choose to share with the public can still raise privacy issues and does not guarantee the confidentiality of its users. Mitchley describes the benefits of data sharing from a banking perspective and highlights the privacy issues still affecting it. Feldman et al. Discuss the important benefit of data sharing in terms of public health, in particular for education and professional development. Geoghegan discuss a list of organisations that effectively and secure share information via the Cloud. However, it doesn't discuss the methodologies the organisations use to secure data or the downside of these organisations. There is also literature that focus on one aspect of security as well as data sharing; access control. Access control can be used to authorise a subset of users to view confidential data provided they have the right permission. Sahafizadeh and Parsa survey a number of different access control models and evaluates its effectiveness. The survey however, is limited to only software systems and does not take into consideration Cloud systems.

Table shows a summary of the related work. The table categorises the related work in two aspects; Cloud security and Data sharing. The table depicts whether the related work addresses the threats, defense strategies and requirements related to the Cloud or data sharing. The table also depicts whether the related work addresses the impact of the Cloud and/or data sharing in real-world scenarios.

The aim of this paper is to present a comprehensive review of private and secure data sharing in Cloud computing.

2. Privacy Issues in the Cloud

A. Privacy Issues

Privacy has many definitions in literature. Some examples of the different definitions of privacy are "being left alone", "the control we have over information about

Table 1 Summary of related work

	Cloud security	sharing Data	Threats	Defense strategies	Requirements	Impact on society
Xiao an Xiao [14]	Y	N	Y	Y	N	Y
Chen and Zhao [15]	Y	Y	Y	N	Y	Y
Zhou [16]	Y	N	Y	Y	Y	Y
Wang et al. [17]	Y	N	N	Y	Y	Y
Wang [18]	Y	N	N	Y	Y	N
Oza et al. [19]	Y	N	Y	N	Y	Y
Saradhy and Muralidhar [20]	N	Y	Y	Y	Y	Y
Butler [21]	N	Y	Y	N	Y	Y
Mitchley [22]	N	Y	Y	N	N	Y
Feldman et al. [23]	N	Y	N	N	N	Y
Geoghegan [24]	N	Y	N	N	N	Y
Sahafizadeh and Parsa [25]	N	Y	N	N	Y	Y

Y yes, *N* no

Our selves" and also "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is

communicated to others" to name a few. The Organization for Economic Cooperation and Development (OECD) defines it as "any information relating to an identified or identifiable individual (data subject)". The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in the Generally Accepted Privacy Principles (GAPP) standard is "The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information." From these definitions it is clear that a person has some level of control of what they want to disclose about them and want to keep the rest of their information kept secret. Privacy should not be assumed to have the same meaning as confidentiality. Confidentiality is allowing only authorised users to gain access to that information and no-one else. We briefly explain the need of privacy and confidentiality in a number of fields.

Privacy and Confidentiality of data in Healthcare:

In the context of healthcare, patients reveal their health-related information to healthcare professionals in order to diagnose .The Health Insurance Portability and Accountability Act (HIPAA) provides federal protection of an individual's personal health information and gives individual's rights to their information. The HIPAA Privacy Rule provides protection of patient's personal health information and how external entities such as doctors and nurses can gain access to the patient's data with the patient's consent. As argues, since the patient decides to share their data with one or more healthcare professionals, their data is no longer private, but confidential.

Privacy and Confidentiality of data in Social Networking

Social networking has changed the lives of today's generation. There are many social networking sites withmillionsofuserscommunicatingwitheachother.Someexamplesare Facebook, Twitter, Myspace, Blogger, Flickr, dig, YouTube and the list goes on. Internet privacy has been determined as the "right to be left alone". The technology that is built to support social networking does not effectively support privacy and may even sell personal information about the individual to third parties and it is mainly up to the individual to disclose information while maintaining privacy. The individual needs to make sure that they do not unknowingly disclose personal information about themselves. Simply disclosing their age, suburb and nationality is enough for malicious users to identify the person. Facebook had undergone scrutiny in the past for not strengthening its privacy measures on user profiles as private photos could still be viewed by non-private viewers through a friend-of-a-friend by simply having a friend comment on it.

Privacy and Confidentiality of data in Education:

Schools usually collect all students personal and health information. These include name, phone, address, contact details, finance details, medical history and family history to name a few. It is usually strongly implied that schools keep this information confidential and private. Failure to keep student personal information confidential can result in safety consequences for the student.

Privacy and Confidentiality of data in Corporations

Major businesses and organisations also require privacy and confidentiality of their data. Leakage of sensitive information can result in revenue loss for a company even to the point of shutting down.

B. Types of Attacks on the Cloud

There are a number of types of privacy and security attacks in the Cloud. The following contains a summary of the common types of attacks that may occur in the Cloud.

- XMLSignatureWrappingAttacks—UsingdifferentkindsofXMLsignaturewrapping attacks, one can completely take over the administrative rights of the Cloud user and create, delete, modify images as well as create instances.
- Cross site scripting attacks—Attackers can inject a piece of code into web applications to bypass access control mechanisms. Researchers found this possible with Amazon Web Services in November 2011. They were able to gain free access to all customer data, authentication data, and tokens as well as plaintext passwords.
- Flooding Attack Problem —provided a malicious user can send requests to the Cloud, he/she can then easily

overload the server by creating bogus data requests to the Cloud. The attempt is to increase the workload of the Cloud servers by consuming lots of resources needlessly.

- Denial-of-Service Attacks—malicious code is injected into the browser to open many windows and as a result deny legitimate users access to services.
- Law Enforcement Requests—When the FBI or government demand a Cloud Service Provider access to its data, the Cloud Service Provider is least likely to deny them. Hence, an inherent threat to user privacy and confidentiality of data.
- Data Stealing Problem—a term used to describe the stealing of a user account and password by any means such as through brute-force attacks or over the-shoulder techniques. The privacy and confidentiality of user's data will be severely breached. A common mechanism to prevent such attacks is to include an extra value when authenticating. This value can be distributed to the right user by SMS and hence mitigate the likelihood of data confidentiality issues.

C. The Motives of a Malicious User

While there is much literature on what can be done to secure a system against attackers, very little discusses the types of attackers and their motivations for carrying out such attacks. In reality, there are many different types of attackers with different reasons to attack users. The following contains some examples.

- To steal valuable data—Hackers love to steal data as some data stored in the internet are valued millions of dollars. With access to valuable data, they can then generate revenue, for example, WikiLeaks.
- To cause controversy—Some attackers purely love the thrill and excitement of causing chaos and the internet, and similarly the Cloud, is one of the best mediums to target mainly because of the popularity of the internet as well as it being more likely to steal data over the internet in comparison to a personal computer system.
- To get revenge—Former workers who were recently stripped of their position at an organisation may express their dissatisfaction by hacking the organisation's network. When an organisation makes use of the Cloud, this becomes all too easy for the former employee and there have been many cases of this happening in the real-world. For instance, there was the case of a former employee who managed to get access to the Cloud provider's server and deleted an entire season of a children's TV show.
- To help—a hacker, in contrast, may also try to help an organisation by identifying the security flaws in their system. A hacker may be confident enough to bypass the existing security protocol and implant his or her own mechanisms to expose the protocol.
- To prove intellect and gain prestige—Attackers may also want to show off their skills and gain prestige among their social skills if they were able to hack a large organisation with solid security mechanisms. Some hackers make a career out of hacking organisations.
- Are just curious—some hackers are curious to learn something about a company and/or organisation. These kinds of hackers don't usually have malicious intent as they may not be aware of breaking security rules however it does not mean these hackers are less dangerous whatsoever.

D. Examples of Real World Issues

There are many examples of real world privacy and security issues that have affected the Cloud. These issues have provided a barrier to the worldwide adoption of the Cloud. We present these issues as a list.

- In 2007, Salesforce.com leaked customer contact lists after an employee revealed the list toa phisher, and in turn allowed scammer's to target phishing attacks against Salesforce customers.
- Google revealed in June 2011 that hackers from China stole passwords and attempted to break into email accounts to steal information. More than 100 people were affected and included senior government officials. People started to argue whether this, and the Sony incident was start of the downfall of Cloud computing.
- Hotmail and Yahoo Mail users were also targeted in phishing attacks. The attacks involved a user either clicking a malicious link in the email or even viewing the email itself which would then run malicious code and attempt to compromise the user's account.
- Google Docs contained a flaw that inadvertently shared user docs with unauthorised users. Other users could access and edit docs without the Google doc's owner permission.
- There was also the issue of Mega Upload leaving its millions of legitimate users in cyber-limbo. Mega

Upload was a site where people could share files. Unfortunately due to the amount of illegal content such as pirated films and television shows, the site was forced to shut down in early 2012.

- A Distributed Denial-of-Service (DDoS) attack on Amazon Web Services forced many companies to shut down temporarily, such as Bit bucket.
- Facebook was the target of phishing attacks in early 2012 which attempted to steal user accounts and learn financial information. Once accounts were stolen, the user's profile would be locked out and the profile picture would change. In fact, Facebook has been the target of a number of phishing attacks such as Ram nit which affected up to 45,000 users.

Each of these attacks contributes heavily to user suspicion and trust of storing sensitive data in the Cloud. From this list, it is clear why users are apprehensive about storing their most sensitive data in the Cloud and in order to gain trust of using the Cloud to store critical data, mechanisms need to be implemented to guarantee data is kept both confidential and secure from unauthorised users.

E. Recommended Guidelines for Private and Secure Cloud

According to, the above issues may have the following impacts on the Cloud:
Governance Organisations usually have standards, practices, protocols, policies and procedures which employees must abide by and this can cover application development, testing, implementation, monitoring and so on. When an organisation makes use of Cloud services, there is always the possibility that employees bypass these rules, as there is a lack of organisational rules regarding the Cloud.

Compliance Refers to an organisation's responsibility to operate in agreement with established laws, regulations, etc. There are a number of privacy and security laws within different countries, states, and so on and when using the Cloud, one has to consider whether they are likely to breach any privacy or security law as data stored in the Cloud is usually stored in multiple locations around the world, at times without the knowledge of the user.

Trust it is a well-known fact that when a user or organisation chooses to outsource their data to the Cloud, they relinquish full control of their data and provide a high level of trust to the Cloud provider. As discussed in the introduction as well as in the next section, most data privacy and security attacks come from insider attacks. The Cloud provider usually has direct access to data and hence is more likely to steal data for illegal purposes. In terms of trust, there is also the issue of data ownership such as who owns the data, and contracts specifying whether the Cloud has some or no access to parts of its data.

Architecture the architecture of the Cloud needs to be designed in a way to prevent privacy and security attacks. For instance, IaaS Cloud providers can provide Virtual Machine Images to consumers. An organisation which makes use of these images, may store very critical data. An attacker may examine the images to see whether they leak information. An attacker may also supply a corrupted virtual machine image to users and hence steal confidential data. It is important that the architecture of the Cloud is developed such that it ensures privacy and security as attackers are always on the lookout for security holes in Cloud architecture.

Identity and Access Management as data sensitivity and privacy is becoming an ever-increasing issue of organisations, the identity and authorisation framework present in the organisation may not extend into the Cloud and malicious users may be able to gain unwarranted access to data they are not allowed to.

Software Isolation with multi-tenant Cloud computing architectures, computations for different consumers are carried out in isolation even if the software remains in a single software stack. Applications running in the Cloud are susceptible to attack and compromise and hence isolation is needed to prevent such attacks.

Data Protection Data stored in a public cloud usually reside with other data from other organisations. When an organisation places their sensitive data in a public cloud, they must account for the possible privacy and security attacks by ensuring proper access control mechanisms such as encryption. Since data is stored "in the open", this provides a world of opportunities for malicious users to steal data. Similar concerns exist when data is in transit.

Availability as defined in the NIST Security and Privacy Guidelines, availability is the extent to which an organisation's full set of computational resources is accessible and usable. Attacks such as Denial-of-Service attacks, server downtime, and natural disasters affect availability and can affect stored data and more importantly causes downtime which affects an organisation greatly.

Incident Response—an incident response is an organised method of dealing with the consequences a security attack. The Cloud containing many layers such as application, operating system, network, database and so on, and a log is generated of any event as part of its intrusion detection system. Such complexity in its layers means it will take many hours to identify an attack in the Cloud.

III. RESULTS AND DISCUSSION

1. Attribute-Based Encryption

Attribute-Based Encryption (ABE) is one effective and promising technique that is used to provide fine-grained access control to data in the Cloud. Initially, access to data in the Cloud was provided through Access Control Lists (ACLs) however, this was not scalable and only provided coarse-grained access to data . Attribute Based encryption first proposed by Goyal et al. Provides a more scalable and fine-grained access control to data in comparison to ACLs.

Attribute-Based Encryption is an access control mechanism where a user or a piece of data has attributes associated with it. An access control policy is defined and if the attributes satisfy the access control policy the user should be able to get access to the piece of data.

There are two kinds of ABE, which are described as follows.

- Key-Policy ABE (KP-ABE): The access control policy is stored with the user's private key and the encrypted data additionally stores a number of attributes associated with the data. A user can only decrypt the data if the attributes of the data satisfy the access control policy in the user's key. The access control policy is usually defined as an access tree with interior nodes representing threshold gates and leaf nodes representing attributes.
- Ciphertext-Policy ABE (CP-ABE): Essentially the converse of KP-ABE. The access control policy is stored with the data and the attributes are stored in the user's key.

2. ABE for Data Sharing and Collaboration

ABE is also used for data sharing and collaboration works. Tu et al. Made use of CP-ABE in the context of enterprise applications and also developed a revocation share the data with another user, say Bob, she sends the encrypted data to a proxy. The proxy then converts the data encrypted under Alice's public key into data that is encrypted under Bob's public key and sends this to Bob. Bob can now use his private key to decrypt the ciphertext and reveal the contents.

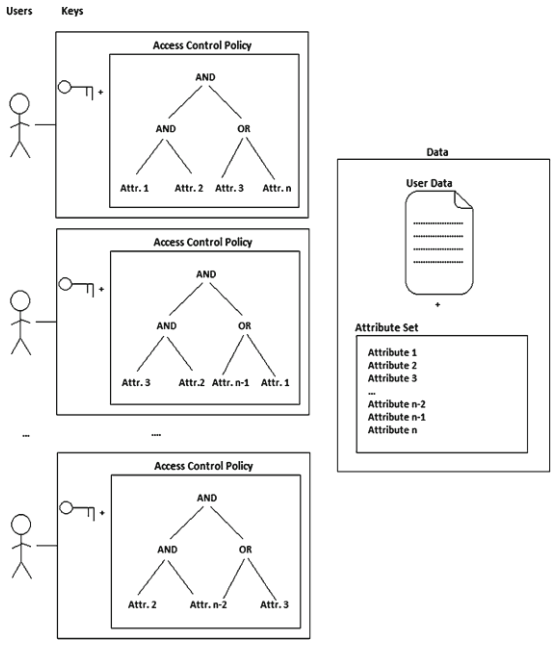

Figure 1. Key-policy attribute-based encryption

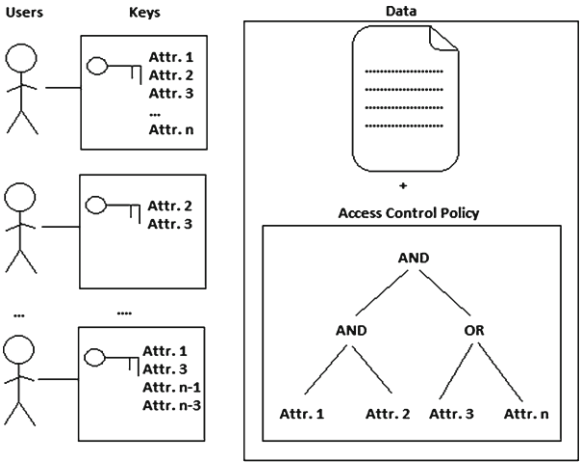

Figure 2. Ciphertext-policy attribute-based encryption

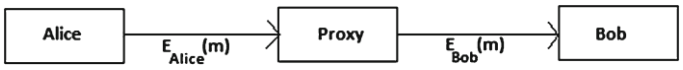

Figure 3. Basic proxy re-encryption scheme

IV. CONCLUSION

Cyber security dominates the entire networks and become a challenging one in crypto systems. In the project we have to analyse the existing algorithms especially for cipher text encryption and decryption. Three approaches are been analysed that the secure data retrieval in decentralized disruption networks, Attribute based Access control with constant size cipher text and finally, a white box traceable cipher text policy attribute based encryption. The above said methods are been analysed and to for proceed to propose a novel cipher text encryption methodology

V. REFERENCES

[1] Mell P, Grance T (2012) The NIST definition of cloud computing. NIST Spec Publ 800:145. National Institute of Standards and Technology, U.S. Department of Commerce. Source: http:// csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Accessed on Oct 2012

[2] Wikipedia definition of Cloud computing (2012). Source: http://en.wikipedia.org/wiki/Cloud_ computing. Accessed on Oct 2012

[3] Healey M (2010) Why IT needs to push data sharing efforts. Information Week. Source: http:// www.informationweek.com/services/integration/why-it-needs-to-push-data-sharing-effort/ 225700544. Accessed on Oct 2012

[4] Gellin A (2012) Facebook's benefits make it worthwhile. Buffalo News.

[5] Riley DA (2010) Using google wave and docs for group collaboration. Library Hi Tech News.

[6] Wu R (2012) Secure sharing of electronic medical records in cloud computing. Arizona StateUniversity, ProQuest Dissertations and Theses

[7] PandeyS,VoorsluysW,NiuS,KhandokerA,BuyyaR (2012)Anautonomiccloudenvironmentfor hosting ECG data analysis services. Future Gener Comput Syst 28(1):147–154 8. Bender D (2012) Privacy and security issues in cloud computing. Comput Internet Lawyer 1–15.

[8] Judith H, Robin B, Marcia K, Fern H (2009) Cloud computing for dummies. For Dummies.

[9] SeongHan S, Kobara K, Imai H (2011) A secure public cloud storage system. Internationalconference on internet technology and secured transactions(ICITST) 2011, pp 103–109.

[10] Zhou M, Zhang R, Xie W, Qian W, Zhou A (2010) Security and privacy in cloud computing: asurvey. Sixth international conferences on emantics knowledge and grid (SKG) 2010:105–112

[11] Rocha F, Abreu S, Correia M (2011) The final Frontier: confidentiality and privacy in the cloud,pp 44–50.

[12] Huang R, Gui X, Yu S, Zhuang W (2011) Research on privacy-preserving cloud storage framework supporting ciphertextretrieval. Internationalconference onnetworkcomputing andinformation security 2011:93–97

[13] Xiao Z, Xiao Y (2012) Security and privacy in cloud computing. IEEE Commun SurveysTutorials 99:1–17

[14] Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. International conference on computer science and electronics, engineering, pp 647–651.

[15] Zhou M (2010) Security and privacy in the cloud: a survey. Sixth international conference onsemantics knowledge and grid (SKG) 2010:105–112

[16] Wang J, Liu C, Lin GTR (2011) How to manage information security in cloud, computing, pp1405–1410.

[17] Wang Y (2011) The role of SaaS privacy and securitycompliance for continued SaaS use. International conference on networked computing and advanced information management (NCM) 2011:303–306

[18] Oza N, Karppinen K, Savola R (2010) User experience and security in the cloud-An empirical study in the finnish cloud consortium. IEEE second international conference on cloud computing technology and science (CloudCom) 2010:621–628

[19] Sarathy R, Muralidhar K (2006) Secure and useful data sharing. Decis Support Syst 204–220. 21. ButlerDDatasharingthreatensprivacy,vol449(7163) . NaturePublishing,Group,pp644–645.