International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Secure Data Sharing in Cloud and Solution for DDos Attack on Cloud

Ms. Sathayabama[1], Vaibhav P Pawde[2], Nrusinha Prasad[3], N Sachin[4]

[1]Asst Professor, Dept of IT, SRM IST Chennai
[2,3,4]Student, Dept of IT, SRM IST Chennai

Abstract: Cloud computing is one of the developing technologies in which a huge amount of storage, data and services are offered over the internet. Data sharing is an important operation in cloud storage. In this paper, we show how to securely, proficiently, and amenably share data with others in cloud storage. We describe a brand-new public-key cryptosystem that produces fixed-size ciphertexts such that effective delegation of decryption rights for any set of ciphertexts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can issue a fixed-size aggregate key for flexible choices of ciphertext set in cloud storage, but the other encrypted files outside the set remain restricted. This compact aggregate key can be suitably sent to others or be stored in a smart card with very limited secure storage. Cloud services are distributed so that they can be accessed by countless users. Due to this, the cloud environment has several security challenges. Distributed Denial of Service (DDoS) is most foremost security attack in cloud computing. DDOS is the greatest threat which can influence the availability of cloud services as it has a multi-tenant architecture. We will discuss the solutions for the DDOS attack in the paper.

1. Introduction:

Security or Cybersecurity is always considered a weak factor in cloud computing. In the earlier days data was not as much as it is today, and that's the reason people were not interested in storing data in cloud. Now many methods are used to secure the data. Key plays a very important role in cloud. So, every user has his/her own key to access the cloud. The main aim of our project is to share the data in cloud without having to give access to the receiver or having the sender download and send it. In this paper, we show how to securely, efficiently and flexibly share scalable data with others in cloud storage. For that we propose Key-Aggregate Cryptosystem which produces cipher text of constant size such that decryption rights can be assigned on them. By combining a set of secret keys, we can make a compact single key. Then, by using this compact key, we can send data to others or can store data in a very limited secure storage. First, the owner of the data sets up the public system. Next, the KeyGen algorithm generates a public or master/secret key. By using this key, users can convert plain text to cipher text. Next user will give input as master secret key by Extract function; it will produce output as aggregate decryption key.

2. Literature Survey

1) Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing

This paper addresses this puzzling open issue by outlining and imposing access policies based on data attribute and, on the other hand, permitting the data owner to delegate most of the computation tasks concerned in fine-grained data access control to untrusted cloud servers while not disclosing the underlying data contents. We achieve this goal by manipulating and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has prominent properties of user access privilege, confidentiality and user secret key accountability.

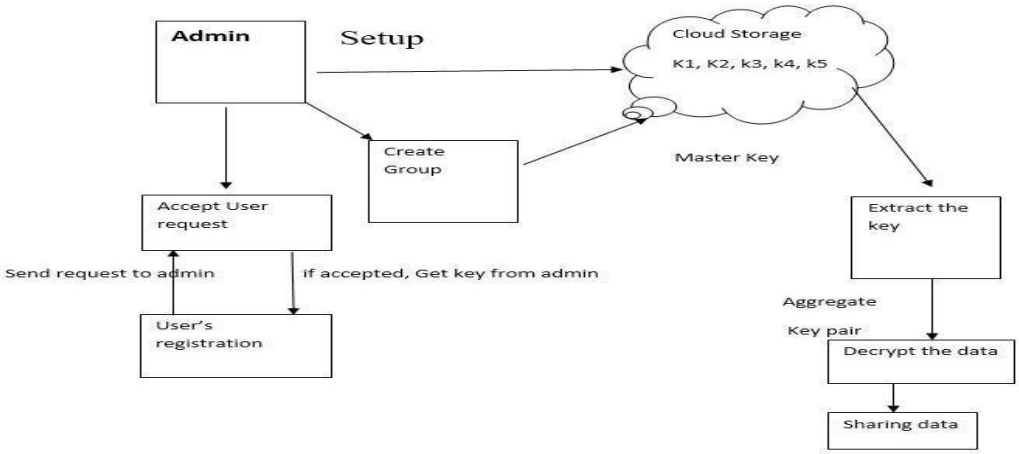
2) Plutus: Scalable secure file sharing on untrusted storage

This paper has introduced fresh uses of cryptographic primitives applied to the problem of secure storage in the presence of untrusted servers and a desire for owner-managed key distribution. Eliminating most necessities for server trust (we still need servers to not destroy data – though we are able to identify if they do) and keeping key distribution (and therefore access control) in the hands of individual data owners provides a foundation for a secure storage system that can protect and share data at very large scales and across trust boundaries.

3) Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

This paper presents more sensitive data is shared and stored by third -party sites on the internet, there will be a need to encrypt the data that is stored at these sites. One disadvantage of encrypting information is that it is by selection shared solely at a coarse-grained level (i.e., giving another party your private key). We develop a brand-new cryptosystem for fine-grained sharing of encrypted information that we like to call Key-Policy Attribute-Based cryptography (KP-ABE). In our cryptosystem, ciphertexts are unit tagged with sets of attributes and private keys are linked with access structures that regulate which ciphertexts an user is allowed to decrypt.

3. System Architecture



Admin:

Admin is a component of the system which is accessed only by the administrator. This component is used to create groups, to add users to the groups and revoke users from said groups. User account is only created by the admin. Users don't have permission to create their own account.

User registration:

User credentials are stored using this component of system. After this process the users gets their credentials through auto-generated email.

Create group:

Groups are created using this component of system. It is done only by the admin.

Cloud Storage:

In this all the users' data and their files are stored.

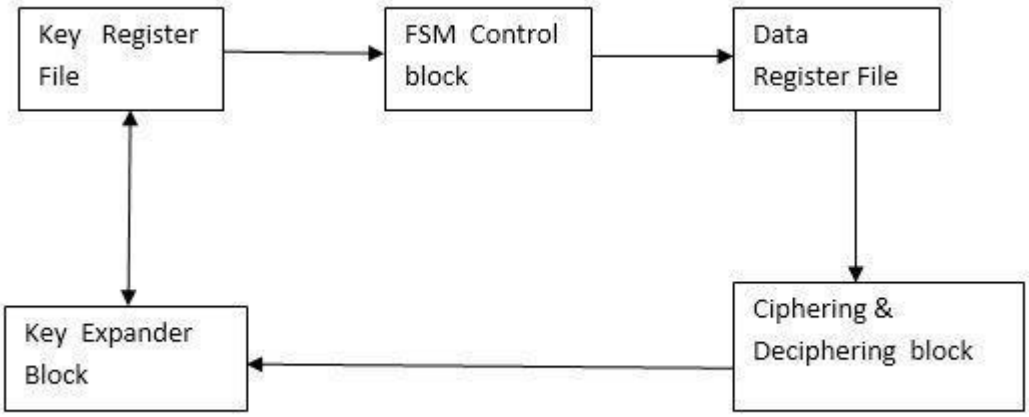
Encryption and Decryption:

Using encryption method data is encrypted and stored in cloud. It has master key to extract the data. No one will be able to see the data unless and until he/she has the access to the portal.

4. Methodologies:

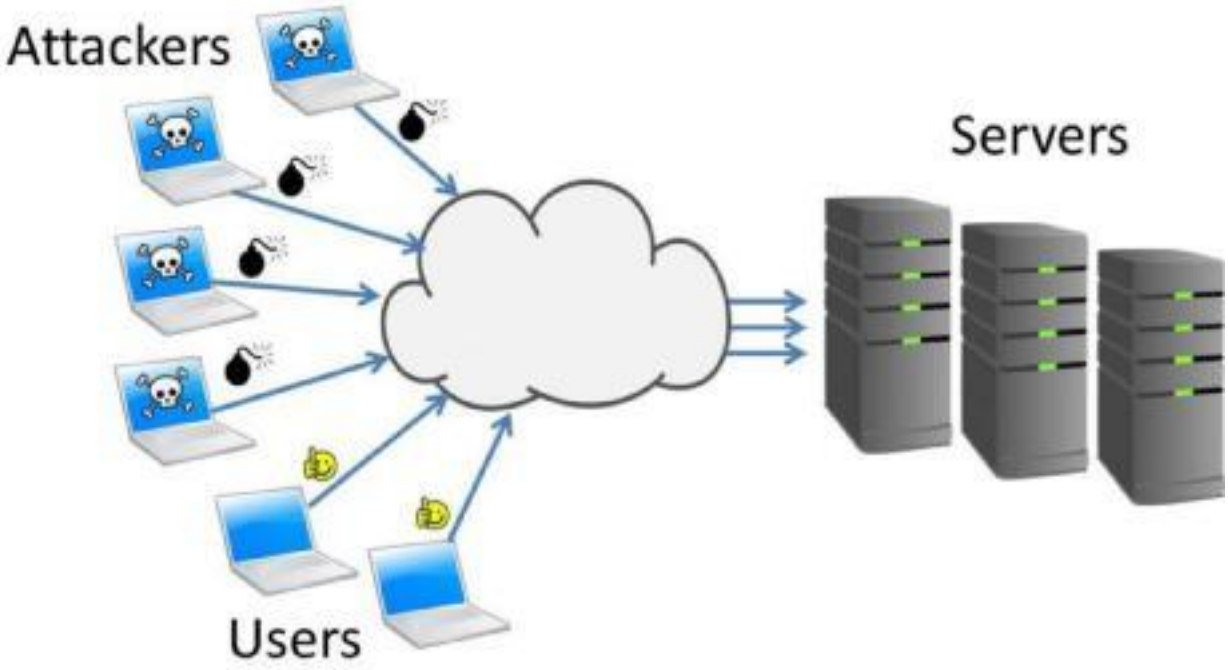
Advanced Encryption Standard (AES):

The Advanced Encryption Standard (AES) is an encryption algorithm for electronic data that was established by the US National Institute of Standards and Technology which got common in the US in the 2002 and may eventually become the de facto encryption standard for commercial transactions in the private sector.



Distributed Denial of Service (DDOS) Attack on Cloud:

We all know that most of the DDOS attacks that we hear or face have little to none intentions of killing a service entirely but rather impair the customers significantly by crippling the service for a certain period. Hence having a reliable DDOS protection is very much important for good and sound business, else attackers can easily pull off a successful DDOS attack under the radar leaving the provider and the customers none the wiser. The most prominent feature of a reliable DDOS protection is the ability to distinguish legitimate traffic from the spam ones.



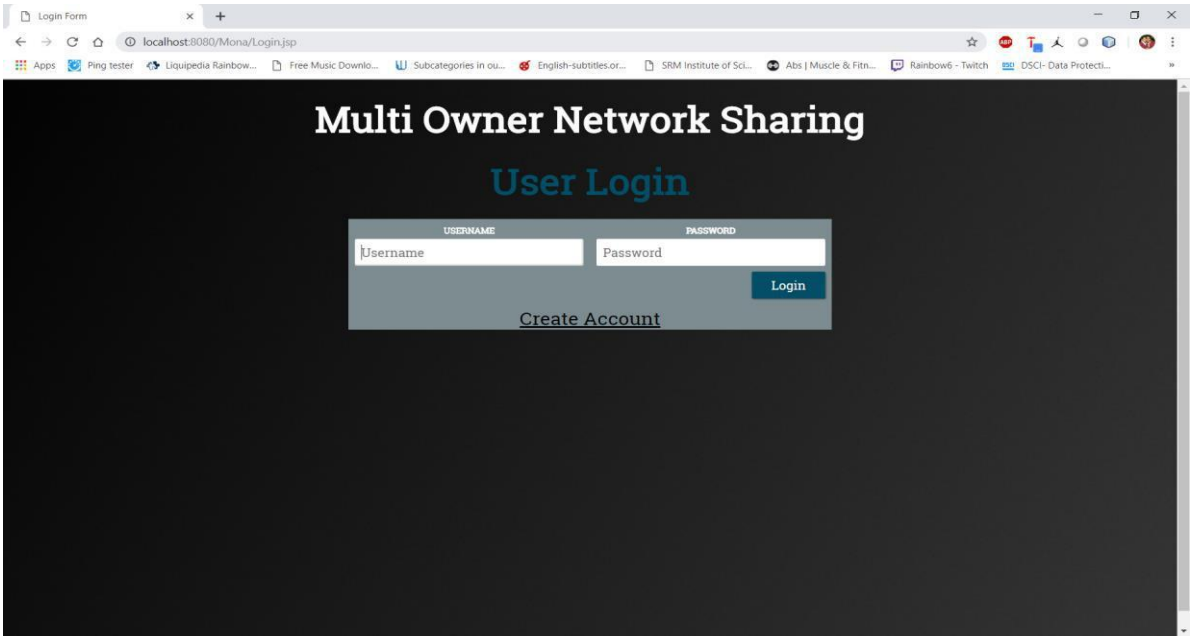
The above image picturises the DDOS attack in the simplest manner understood by any Layman. The attacker(s) basically send in multiple requests from multiple systems. That may be done by a group of hackers or; the simplest and effective way, due to the unawareness of people about cyber security, is to use a botnet of hacked systems to send those requests. This way the hacker's identity even stays hidden behind those legitimate IP addresses. The number of requests will need to be more than the traffic the cloud server can usually handle, which not a big ask for a hacker with a botnet at his/her disposal. This will cause the servers to become unresponsive to legitimate traffic if they do not have routines in place to isolate fake requests from the legitimate ones, thus crippling the sole purpose of the cloud servers.

5. Process

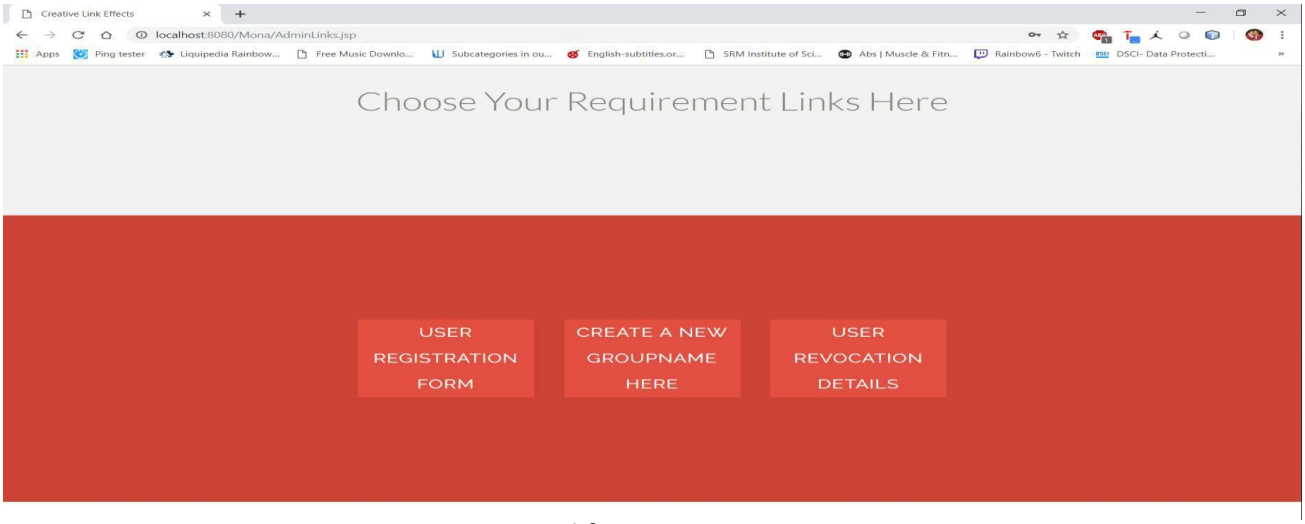
Our project focuses on the scalable data sharing over cloud platform securely. For this, we have created a cloud platform using jsp and java in NetBeans IDE. The webpage opens to a login page where the registered users can login using the username and group's generated key provided by the admin. There is also an create account option below. But accounts

can only be created by the admin. Thus, on clicking the create option an admin login page comes up. After the admin logs in there are three options presented; user registration, create groups and revoke users.

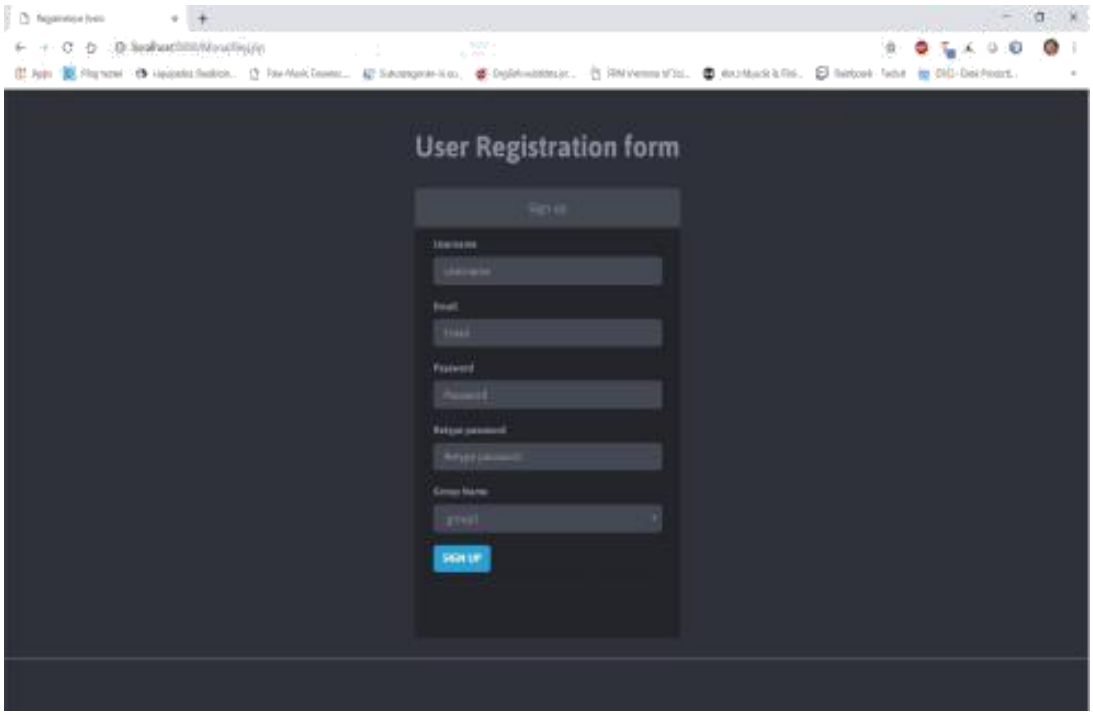
In the user registration page, the admin has to fill up a form which includes the users' email id. This email is then used to send the group name and its corresponding key through a pre-programmed computer-generated email after the admin has registered the user. The group creation page just has two text fields to be filled i.e., group name and key for that group. The third page is the user revocation page that is to revoke a certain user's access to the cloud platform. For this the admin has to just select the group and the username from a drop-down list and the user will be revoked. Now coming to the point of data sharing, once any document is uploaded in to the group anyone in the same group can decrypt and download it. But if you want to download a file from another group you will need to get the permission from someone of that group. The requested file will show up in the group approval box. Once someone from the group gives the permission the person who requested can download the file. This way the owner doesn't have download and share or give access to his/her cloud but just give permission. Tad more effective than what we see today.



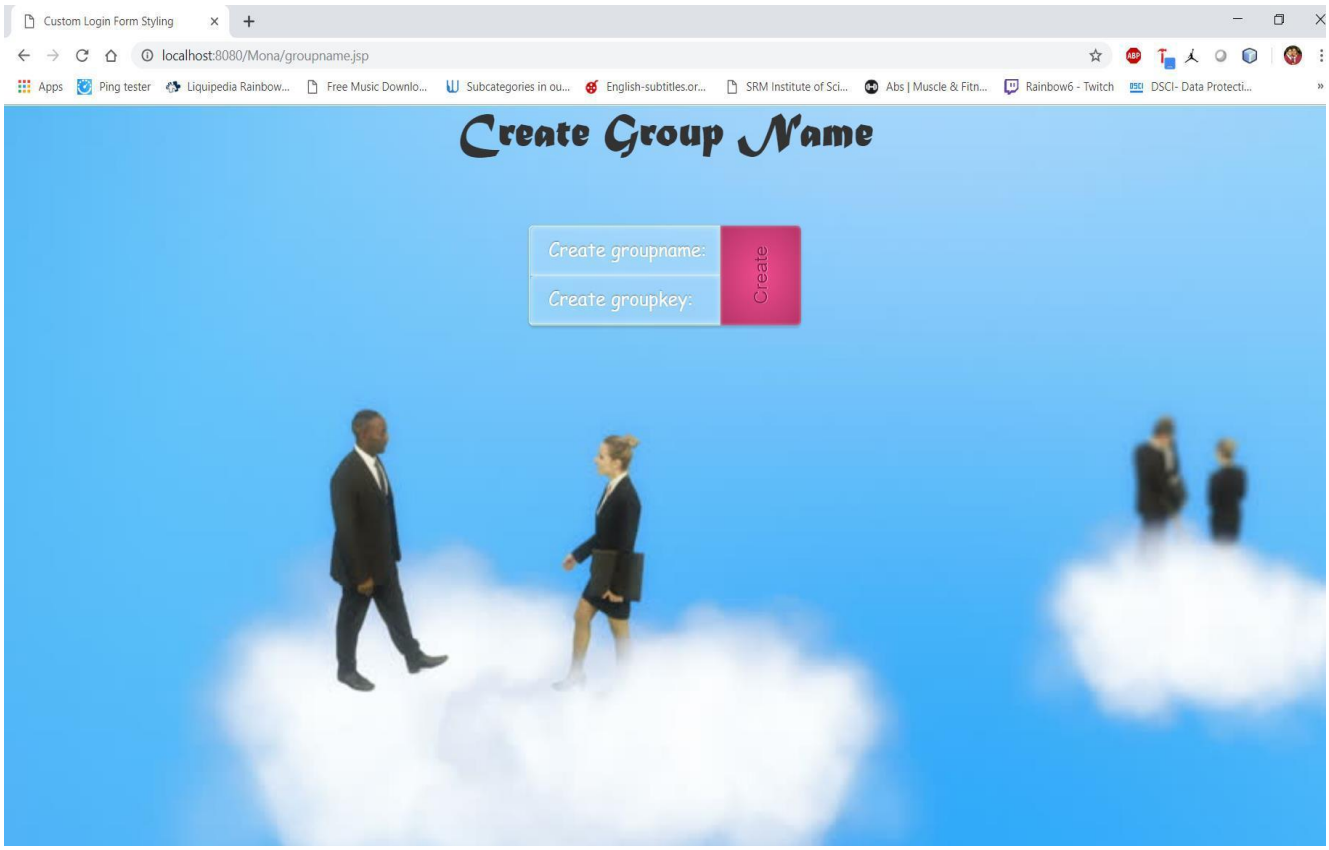
Login page



Admin actions



User registration



Group creation

User revocation

6. Conclusion

Cloud undoubtedly helps IT organizations use different technologies to achieve and cost-effective application performance. The installed applications are based on a strange networking software, the operating system, in a virtual machine. In a virtual environment. The virtual device reduces some enterprise-level management issues because most of the maintenance, software updates, configuration tasks, and other management tasks are responsible for the organization. However, this proposed approach for the decentralization of access and access is being carried out at all times and places data, opportunities and offers a series of new challenges and security issues that need to be considered before the data is transferred to the cloud. In addition, this does not mean that software running on a virtual machine can perform well in the cloud. Then, in the cloud, there are hidden risks and costs in managing cloud compliance. The key to the success of cloud computing projects is to achieve a balance between business benefits and potentially hidden risks that impact on effectiveness. Cloud providers Different servers are often a strong source for users to compromise the same services and clouds with other internet-based technologies. On the other hand, they can be attacked, such as powerful DDoS attacks, such as other internet-based technologies. As a solution, cloud providers can protect more resources from attack, but unfortunately there is no defence against their powerful DDoS that there are partial attacks. The issues discussed in this article are the main reason why many companies have converted the cloud to the west of the cloud with non-sensitive data and important data stored on their local engines. Finally, although cloud computing is widespread? Attractive technology introduced in the computer industry; This does not mean that all IT companies need to move to the cloud. Additionally, a move to cloud computing must consider a number of parameters and the most important is security.

7. References:

1. S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2009.

2. J Brodkin. (2008). Gartner Seven cloud-computing security risks. Available: http://www.networkworld.com/news/200S!07020S-cloud.html

3. D. L. Ponemon, "Security of Cloud Computing Users," 2010.

4. S. K. Tim Mather, and Shahed Latif, Cloud Security and Privacy: O'Reilly Media, Inc , 2009.

5. In the era of cloud computing."C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009