ISSN:0975-9646

Secure Cloud – A Survey

I Jaffar Ali[1], N Shareefa Rabiya[2]
[1,2] *Assistant Professor,*
Department of Computer Science and Engineering,
PET Engineering College, Vallioor, Tamil Nadu, India

Abstract - Cloud computing is an emerging technology where the data is outsourced to the Cloud. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel control, Cloud moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. The major security challenge with Clouds is that the owner of the data may not have control of where the data is placed. So, proper access control mechanisms should be employed to protect the data from the security attacks. In this survey, the various security issues and access control mechanisms have been listed for awareness.

Keywords - Cloud, Outsourcing, Data Center.

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, On-demand network access to a shared pool of configurable computing resources (e.g., Networks, Servers, Storage, Application and Services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Providing Security is a challenging issue in Cloud.

In Cloud computing, the available service models are

- *Infrastructure as a Service (IaaS)*
  This model allows users to use virtualized IT resources for computing, storage and networking.
  The users can deploy and run their applications over the chosen OS environment [2].
  When security is concerned, *IaaS* only provides basic security such as perimeter firewall, load balancing etc., but applications moving into the Cloud will need higher levels of security provided at the host [3].
- *Platform as a Service (PaaS)*
  To be able to develop, deploy, and manage the execution of applications using provisioned resources demands a Cloud platform with the proper software environment. Such a platform includes Operating System and run time library support. This has triggered the creation of the *PaaS* model to develop and deploy their user applications [2].
  When security is concerned, maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental [3].
- *Software as a Service (SaaS)*
  The *SaaS* model provides software applications as a service. On the customer side, there is no investment in servers and software licensing [2].
  SaaS applications are accessed using web browsers over the Internet, so web browser security is vitally important [3].

The deployment models in Cloud are

- *Public Cloud*
  A public Cloud is built over the Internet and can be accessed by any user who has paid for the service. Public Clouds are owned by service providers and are accessible through a subscription.
- *Private Cloud*
  A private Cloud is built within the domain of an intranet owned by a single organization. It may exist on-premise or off-premise.
- *Hybrid Cloud*
  A hybrid Cloud is built with both public and private Clouds. Private Clouds can also support a hybrid Cloud model by supplementing local infrastructure with computing capacity from an external public Cloud.
- *Community Cloud*
  The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.
  When security is concerned hybrid Cloud is more secure than public and private Cloud. Private cloud is more secure then public Cloud. Public Cloud is the least secure model [3].

II. SECURITY ISSUES IN CLOUD

Security issues in Cloud computing has a major role which is to be addressed first. The major security challenge with Clouds is that the owner of the data may not have control of where the data is placed. Measuring the quality of security is difficult, because the infrastructure will not be exposed.

The seven Security Issues that need to be addressed are:

Privileged User Access, Regulatory Compliance, Data Location, Data Segregation, Recovery, Investigative Support and Long-term viability [4].

The network that interconnects the systems in a Cloud has to be secure. Mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. Resource allocation and memory management algorithms have to be secure [5].

When moving to a Cloud, the data is stored away from the customer's local machine and the data is moving from a single-tenant to a multi-tenant environment. Data leakage can be prevented using Data Leakage Prevention (DLP) applications [6].

A few security attacks in Cloud are discussed as follows:

- *Malware Injection Attack*
  Malware Injection Attack is a Web-based attack, in which hackers exploit vulnerabilities of a web application and embed malicious codes into it that changes the course of its normal execution [7].
- *Wrapping Attack*
  During the translation of SOAP messages between a legitimate user and the web server, the hacker hacks the user's account and password, and embeds the wrapper into the message structure, moves the original message body under the wrapper, replaces the content of the message with malicious code, and then sends the message to the server. Since the original body is still valid, server authorizes the message that has actually been compromised. As a result the hacker is able to gain unauthorized access to protected resources [7].
- *DDoS Attack*
  When a *DDoS* attack is launched, it sends a heavy flood of packets to a Web server from multiple sources. Most network countermeasures cannot protect against *DDoS* attacks as they cannot differentiate between good traffic and bad traffic. So, Cloud providers can add more resources to protect themselves from such attacks [6].

III. ACCESS CONTROL MECHANISMS IN CLOUD

3.1 Data Coloring Method

The advantages of secured Cloud storage and software watermarking through data coloring and trust negotiation is combined.

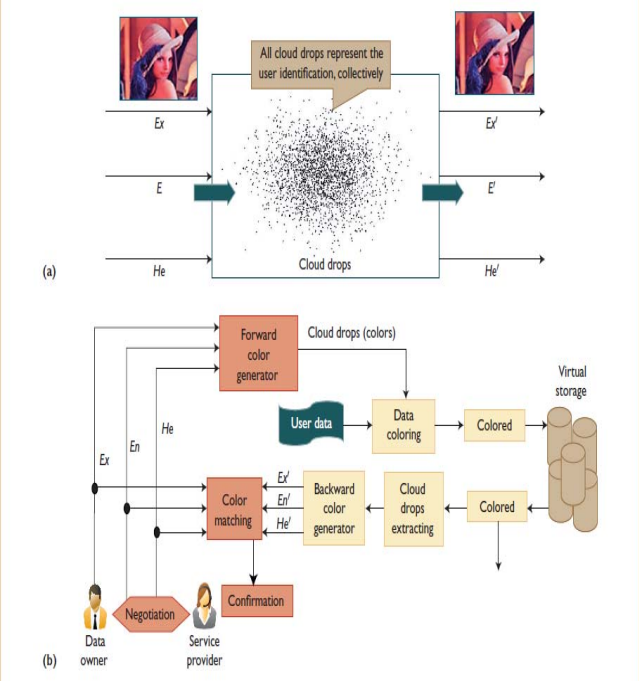

Fig 1 Data Coloring Method

The Cloud drops (data colors) are added into the input photo and the colors are removed to restore the original photo. The coloring process uses three data characteristics to generate the color: the expected value (*Ex*) depends on the data content, entropy (*En*) and hyper entropy (*He*), add randomness or uncertainty, which are independent of the data content and are known only to the data owner. These three functions generate a unique color that cannot be detected.

The computational complexity of the three data characteristics is much lower than the conventional encryption and decryption calculations in PKI services. The *En* and *He* functions guarantee data owner privacy [9].

3.2 Combination of KP-ABE, PRE and Lazy Re-encryption

To achieve secure, scalable and fine-grained access control on outsourced data in the Cloud, three advanced cryptographic techniques: KP-ABE, PRE and lazy re-encryption are combined. KP-ABE technique is utilized to escort data encryption keys of data files. If this technique is used alone, it introduces heavy computation overhead for the data owner. PRE technique is combined with KP-ABE so that the computation intensive operations are done by the Cloud Servers. Data confidentiality is also achieved since Cloud Servers cannot learn the plain text of the data file. Lazy re-encryption technique is also used to allow Cloud Servers to aggregate computation tasks of multiple system operations.

The computation complexity on Cloud Servers is either proportional to the number of system attributes or linear to the size of the user access tree, which is independent to the number of users in the system. Thus scalability is achieved. This method protects user access privilege information against Cloud Servers [11].

3.3 Third Party Secure Data Publication applied to Cloud

Since many of the documents are on the web, the data is represented as an XML document. Users must possess the credentials to access XML documents. The model has a untrusted third party publisher.

The owner of a document specifies the access control policies for the users. Users get the policies from the owner when they subscribe to the document. The owner sends the document to the publisher.

When the user requests for a document, the publisher applies the policies and gives portions of documents to the user. Since the publisher is not trusted, the owner encrypts the combinations of documents and policies with the private key. Thus the user can verify the authenticity and completeness of the document [5].

3.4 A Hierarchical Model for Cloud

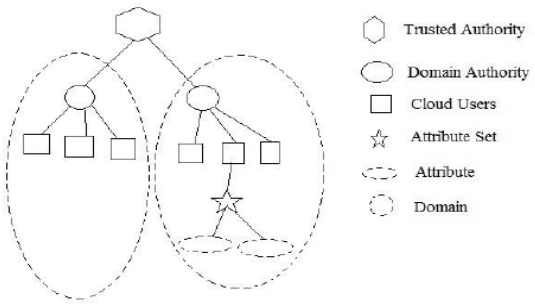

Fig 2 Hierarchical Model

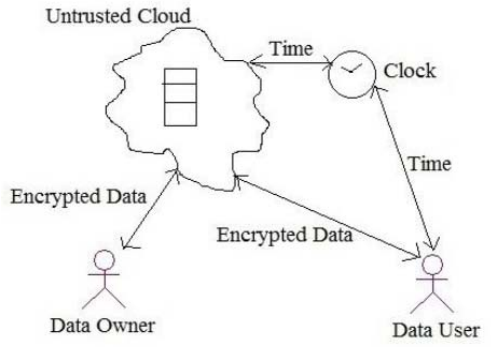

Fig 3 System Design

The trusted authority is the root and it authorizes the top level domain authorities. The domain authorities authorize the Cloud users. For each Cloud user, an attribute set is maintained.

The data owner encrypts the file and uploads to the Cloud. When a data user needs the file, a request is sent to the Cloud which is then forwarded to the owner. The owner checks the attribute set of the user and if it is valid, the key is sent to decrypt the file. Meanwhile a clock is set, and within the time limit, the file should be accessed [10].

3.5 Multiple Biometric Security

Biometrics refers to the use of unique physiological characteristics to identify an individual.

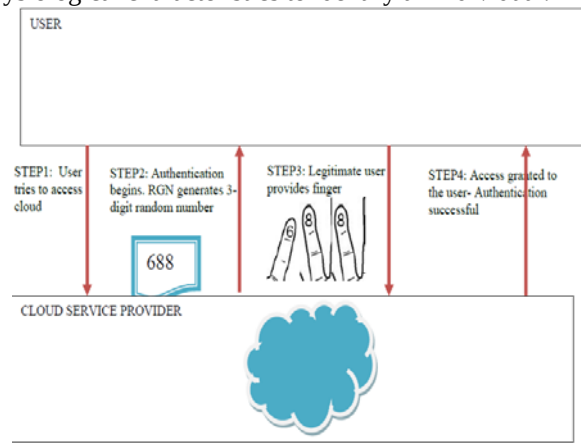

Fig 4 Multiple Biometric Security

Multi finger security model is a technique where users can register with three fingers of their choice and assign a single digit number for each of these three fingers. These recorded images are encrypted using Elliptical algorithm and stored at the service provider's end. RSA algorithm is used for numbers and mappings.

For authentication purpose, a Random Number Generator is used, which generates a three digit number that are chosen by the user during registration. User provides the finger prints in the order of the generated random numbers and thus he can access the Cloud.

Even if the stored template is hacked, the hacker cannot access because of the random number that is generated. After three consecutive wrong attempts the access will be denied [8].

IV. CONCLUSION

Although Cloud computing can be seen as a new technology which revolutionizes the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate with the potential of making human lives easier. However, one must be very careful to understand the security risks and challenges in utilizing these technologies. Cloud computing is no exception. In this paper the security challenges and various access control mechanisms in the Cloud computing are highlighted.

REFERENCES

[1] P.Mell, "The NIST Definition of Cloud Computing" , U.S. Department of Commerce: Special Publication 800-145.
[2] Rajkumar Buyya, Christian Vecchiola, S.Tamarai Selvi, 'Mastering Cloud Computing", TMGH,2013.
[3] Kuyoro S.O., Ibikunle F., Awodele O., "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks, Volume(3): Issue (5): 2011.
[4] J.Brodkin. (2008, Jun.). " Gartner: Seven Cloud Computing security risks." Infoworld, Available: < http://www.infoworld.com/d/security-central/gartner-seven-Cloudcomputing-security-risks-853?page=0,1> [Mar.13, 2009].
[5] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2),39-51, April-June 2010.
[6] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE, 2011.
[7] Te-Shun Chou, " Security threats on Cloud Computing vulnerabilities", IJCSIT, Vol 5, No 3, June 2013.
[8] D.Pugazhenthi, B.Sree Vidya, "Multiple Biometric Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, 3(4),April-2013,pp.620-624.
[9] Kai Hwang, Deyi Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE,2010.
[10] Bibin K Onankunju, " Access Control in Cloud Computing", IJSRP, Volume 3, Issue 9, September 2013.
[11] Shucheng Yu, Cong wang, Kui Ren, and Wejing Lou, " Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE, 2010.