International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

To Improve the Data Security of Cloud in Cloud Computing by using Digital Signature with RSA Encryption Algorithms

K.Praveen Kumar [1]& Gali Swetha [2]

[1] ASSISTANT PROFESSOR, Dept of CSE, MLR Institute of Technology, Hyderabad, Telangana
[2] PG Scholar ,Dept of CSE, MLR Institute of Technology, Hyderabad, Telangana

ABSTRACT

Cloud computing has showed up as a popular design in managing world to back up managing large volumetric details using cluster of commodity computer systems. It is the newest effort in offering and managing computing as a service. Cloud Computing has become a boon for an IT industry nowadays. It is like a next stage platform in the evolution of Internet. It provides a platform with an enhanced and efficient way to store data in the cloud i.e. server with different range of capabilities and application. It provides an easy way of accessing one's personal file or data and use application without installing it on machines by just having Internet access. We can have efficient computing by centralized data storage, processing and bandwidth. Example: Yahoo, Gmail, Amazon etc. are good cloud service providers. So all we need is to have Internet access then we can send mail and can access our account from any part of the world. The server and the email management software is installed on the cloud and managed by service providers. Providing an easy access to work and business still it has a major problem and threat i.e. "DATA SECURITY". In this Research Paper, we have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm.

Keywords: Security; RSA; digital signature and Cloud Technology

I. INTRODUCTION

Cloud computing has become a necessity today when the company plans to increase capacity "or capabilities on the fly without getting to invest new infrastructure, training new individual purchase new license application, etc. based service encompasses any subscription or pay per use which extends the existing IT capabilities of the company, current time through Online.

By introducing cloud, the days of keeping all your documents, photos, music files etc. on your computer's hardware are gradually coming to a close. Today, the cloud storage is fulfilling the need for more storage space to hold all of your digital data. Cloud storage providers operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualizes the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects [1]. Physically, the resource may span across multiple servers.

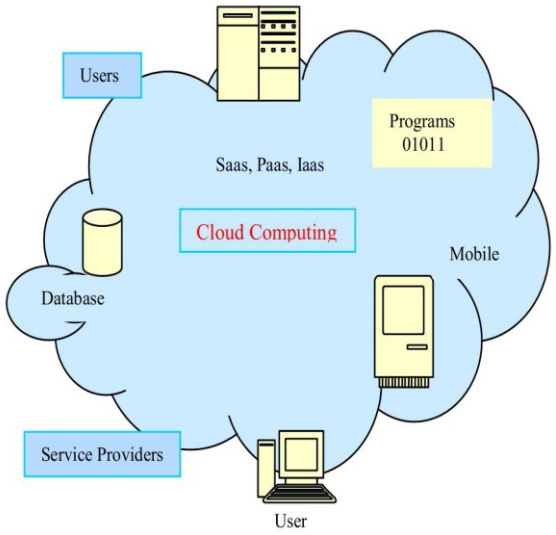
Cloud computing interconnects the large-scale computing resources to integrate, and provide resources as a service to users. Users are allowed on demand access to virtual computers, without the need to consider the complexities of the underlying hardware implementation and its management, greatly reducing the user's investment. The cloud computing applications and research continue to advance the development of cloud facing many critical issues, and bear the brunt of security issues and, the growing popularity of cloud computing but the security issues have restricted its importance in development.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

Cloud Computing Service Model

In the cloud computing, the available service models are:

- Infrastructure as a Service (IaaS): This model allows user to rent processing, storage, network and other resources. The user can deploy and run the guest OS and application [5]. The user does not manage of control the underlying cloud infrastructure but has control over only OS, storage and deployed application and possibly selected networking components. Examples include Amazon Elastic Computer Cloud (EC2), Microsoft Windows Azure[3].



- Platform as a Service (PaaS): Provides the consumer with the capability to deploy onto the cloud infrastructure, consumer created or acquired applications, produced using programming languages and tools supported by the provider [2]. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Examples include Google's Apps Engine, Microsoft- Windows Live. Open shift, etc.
- Software as a Service (SaaS): Provide the user with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various consumer devices, through a thin client interface, such as a web browser. The consumer does not manage or control the underlying cloud infrastructure various resources. Examples include Salesforce.com, VoIP from Skype and Vonage, Google's Gmail and Apps, instant messaging from Yahoo and AOL

II. RELATED WORK

Deployment models have been identified for cloud computing architecture solution:

- **Private cloud**: The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.
- **Community cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.[4]
- **Public cloud:** A public or external cloud is a general-purpose cloud computing environment managed by a cloud provider.[8] The cloud provider could be external provider, such as Amazon EC2, Google Apps [6], Salesforce, etc. that leases third-party cloud resource to the consumer. However, a cloud could be public even when third party cloud resources are not used; the most important aspect of a public cloud is its content.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

Challenges faced in Cloud computing:

Several security models have been developed to address the data security issues in cloud computing. The data security model using Two-Way handshake is a method which utilizes the homomorphic token with distributed verification of erasure-coded data and achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server

1 Ultra large-scale: The scale of cloud is large. The cloud of Google has owned more than one million servers. Even in Amazon, IBM, Microsoft, Yahoo, they have more than hundreds of thousands servers. There are hundreds of servers in an enterprise [6][7].

2. Virtualization: Cloud computing makes user to get service anywhere, through any kind of terminal. You can complete all you want through net service using a notebook PC or a mobile phone. Users can attain or share it safely through an easy way, anytime, anywhere. Users can complete a task that can't be completed in a single computer.

3. High reliability: Cloud uses data multi transcript fault tolerant, the computation node isomorphism exchangeable and so on to ensure the high reliability of the service. Using cloud computing is more reliable than local computer.

4 Versatility: Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.

5. High extendibility: The scale of cloud can extend dynamically to meet the increasingly requirement.

6. On demand service: Cloud is a large resource pool that you can buy according to your need; cloud is just like running water, electric, and gas that can be charged by the amount that you used.

7. Extremely inexpensive: The centered management of cloud makes the enterprise needn't undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully enjoy the low cost advantage. Various applications and advantages of cloud computing is listed below:

1. Cloud computing do not need high quality equipment for user, and it is easy to use.
2. Cloud computing provides dependable and secure data storage center. You don't worry the problems such as data loss or virus.
3. Cloud computing can realize data sharing between different equipments.

4 Cloud provides nearly infinite possibility for users to use internet.

III. PROPOSED SYSTEM

In this section, we provide an example of our approach along with digital signature and RSA algorithms. In order to achieve secure and efficient data access control in cloud computing, we uniquely combine capability based access control technique with cryptography [13][15].

a. Digital signature:

For security assurance to the user's data, we propose step 1: Data security model that uses Elliptic curve cryptosystem for digital signature. Step 2: The message digest is encrypted with private key to produce digital signature.

Step 3: Using Elliptic curve Algorithm, digitally signed signature is encrypted with receiver's public key.

Step 4: Receiver will decrypt the digital signature into message digest using sender's public key and the cipher text to plain text with his private key Digital signatures are important to detect forgery and tampering.

b. RSA: Ron Rivest, Adi Shamir and Leonard Adleman described the RSA algorithm in 1978. The letter RSA is abbreviating form by initials of their surname. RSA algorithm involves three steps algorithm key generation, encryption and decryption. In this RSA algorithm, m is known as the modulus, "E" is known as the encryption exponent or public key exponent and "D" is known

as the decryption exponent or private key exponent. **Algorithm:**

1. Choose two large prime P & Q
2. Calculate N = P * Q
3. Select the public key (i.e. encryption key) E such that it is not a factor of (P - 1) and (Q - 1).
4. Select the private key (i.e. decryption key) D such that following equation is true:
(D * E) mod (P - 1) * (Q - 1) = 1
5. For encryption calculate cipher text CT from the plain text PT as follows:
CT = PTE mod N
6. Send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text PT from the cipher text CT as follows:

PT = CTD mod N

IV Conclusion:

Cloud Computing is the phenomenon of separating applications from hardware and providing an easy way to deploy on demanded server. Service models: Application, Platform and Infrastructure. The functioning of Cloud Computing is greatly affected by issues such as that of data security, integrity, theft, loss and presence of infected applications. To solve these issues various algorithms such as ECC, RSA, RC4 and El-Gamal have been suggested. In future we can optimize efficiency of system by reducing size of key for encryption and check the performance with the proposed algorithms.

REFERENCES

[1]Gartner survey feb 2013: from http://www.slideshare.net/GaldeMerkline/pwc-zloudenabledtelcoopportunitiespdf

[2] Peter Mell, and Tim Grance, Draft NIST Working Definition of Cloud Computing, 2009: from http://csrc.nist.gov/groups/SNS/cloud-computing/

[3] R. Buyya, C. S. Yeo, and S. Venugopal, Market oriented cloud computing: vision, hype, and reality, for delivering IT services as computing utilities, *Proc.* 10th IEEE International Conference on High Performance Computing and Communications,Dalian, China, Sept 2008.

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the clouds: A berkeley view of cloud computing, University of California, Berkeley, Tech Rep USB-EECS-2009-28, Feb 2009.

[5] David Chappell, Introducing the Azure Service Platform, White paper, Oct 2008.

[6] Amazon EC2 and S3, Online at http://aws.amazon.com/

[7] Google App Engine, Online at : http://code.google.com/appengine/

[8] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, A Data Outsourcing Architecture Combining Cryptography and Access Control, *Proc.* ACM Workshop on Computer Security Architecture (CSAW'07), Nov 2007, USA.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, *Proc.* IEEE INFOCOM 2010, San Diego, CA, pp. 1-9.

[10] W. Wang, Z. Li, R. Owens, and B. Bhargava, Secure and efficient access to outsourced data, *Proc.* ACM Cloud Computing Security Workshop 2009, Chicago, Illinois, USA, 2009, pp. 55-65.

[11] S. Kamara, and K. Lauter, Cryptographic Cloud Storage, *Proc.* Financial Cryptography: Workshop on real life cryptographic protocols and standardization, 2010: from http://research.microsoft.com/pubs/112576/cryptocloud. pdf

[12] Z. Dai, and Q. Zhou, A PKI-based Mechanism for Secure and Efficient Access to Outsourced Data, *Proc.* International Conference on Networking and Digital Society, Wenzhou, China, 2010, pp. 640-643.

[13] J. Anderson, Computer Security Technology Planning Study, Air Force Electronic Systems Division, report ESD-TR-73-51, 1972: from http://seclab.cs.ucdavis.edu/projects/history/

[14] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage, ACM Transactions on Information and System Security, Vol. 9, No. 1, Feb 2006, pp. 1-30.

[15] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, Over-encryption: Management of access control evolution on outsourced data, *Proc.* 33rd International Conference on Very Large Databases (VLDB'07), Vienna, Austria, 2007, pp. 123-134.