International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 5 (2017), pp. 663-672

http://www.ripublication.com

Advanced Security Model for Ensuring Complete Security in Cloud Architecture

Nikhil Kumar Singh

Department of Computer Science and Engineering,
Baba Saheb Bhim Rao Ambedkar University, Lucknow (U.P.), Inida.

Abstract

Cloud computing plays very important part in Internet that is offered to the business environment, educational domain and to individual users. Most of the companies prefer to choose this as compare to others educational institutions. With this concept companies prefer Private Cloud model due to their tight security policies for data and applications. Suppose if there is no confidentiality or security in data then it can be easily stolen out by some unauthorized person. In this paper we focused on the analysis of several security methods applied in Cloud Computing environments and proposed two security models that can be helpful in the safety issues.

Keywords: Cloud Computing, Security, Data privacy, Encryption, Confidentiality.

1. INTRODUCTION

Cloud Computing is a very fast growing technology in the current era it has been used widely in all the fields and especially Public Clouds, have been adopted by individual and academic users and they are growing fast in the business environment because of the well balanced cost to performance ratio compared to privately owned hardware and software platforms. The most important issue why the companies are looking forward to migrate to the Cloud is the confidentiality and data security. Several IT experts focused on finding solutions to these problems and many of them proposed models that are already being used at this moment. In this paper we will discuss some security models that are most appropriate for Cloud systems and introduce a technique that joins client encryption mechanisms with the well known OAuth standard.

2. LITERATURE REVIEW

2.1 The Cloud Computing Concept

In this section a brief literature review of the previous work done in the field of cloud computing has been mentioned. According to the National Institute of Standards and Technology (NIST) the definition for Cloud Computing is given as a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be quickly provisioned and released with minimal management effort or service provider interaction" [1].

This definition includes the basic elements of the concept [1]:

1. The features of cloud computing are resource pooling, broad network access, on demand self service.
2. The cloud service models (software, platform and infrastructure),
3. The deployment models (private, community, public and hybrid) that provide direction to deliver cloud services.

The main features of cloud computing solutions can be summarized as follows [2]:

1. Use of Internet technologies that involve the capacity of on demand resource allocation based on current client requirements, and ubiquitous remote access.
2. Maintenance and security assurance by providers or a combination with the security methods implemented by the client.
3. Highly-redundant, certified security and minimal downtime features that empower the client business at a fraction of private infrastructure costs.

This way, clients can manage their applications whenever they need it, wherever they need it, because we can access the cloud from anywhere where there's an Internet connection. NIST defines three fundamental models for Cloud computing services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [3].

We summarized the services provided by each layer as they are described on NIST website:

1. Infrastructure as a Service (IaaS) is the service model that allows the customers to use computing resources such as servers, storage devices and network infrastructure, often delivered as virtual machines hosted by the service provider and managed remotely. [4]
2. Platform as a Service (PaaS) is the model that provides to the users the capability to build, test and deploy their applications on the cloud infrastructure. This layer offers a collection of programming languages, databases, specialized tools and middleware that are able to host full size applications deployed by the client. [5]
3. Software as a Service (SaaS) is the most popular model, and requires that cloud providers install and operate the complete application stack on their platform and users access these applications remotely through specific client software. In this manner, the customers do not manage the cloud infrastructure

on which their application is running, and are not responsible for maintenance and support. [6]

Desktop as a Service (DaaS) is an integrated approach for the distributed computing, in which a complete VDI (virtual desktop infrastructure) is delivered to the client and completely managed by the service provider [7].

Storage as a Service (StaaS) is more like an auxiliary component of an Internet-based business, which takes backup and data archiving from the client facility and moves it to a high-performance, always-available and secure infrastructure owned by the cloud hosting company [8].

Security as a Service (SECaaS) involves outsourcing the very complex mission of securing the most precious assets of a web-based company: data and applications [9].

2.2 The security on Cloud Computing

Many organizations and institutions used Cloud Computing in order to enhance their business competitively with same-level or lower costs. But adoption reluctance is related to the performance of security methods, so many still expect a model that will give them the necessary confidence in storing and accessing their private data by powerful, secured Public Clouds.

However, more and more enterprises are turning to Cloud Computing environments, because the advantages are becoming more and more attractive. The company management must decide the service level requirements, the need for resources (which can be computing power, memory, bandwidth or business applications licenses).

a. Privacy and Confidentiality– The Cloud service provider must assure that customer data is accessible only to authorized users and that all hosted information will be kept confidential in all circumstances [10].

b. Security and Data Integrity– The Cloud service provider must assure the protection of data by encryption and decryption techniques and implement a mechanism to monitor integrity of the data at the cloud [11].

Some of the data security challenges in the cloud were underlined: [12]

- The need to protect confidential business data on cloud models with multiple enterprises and organizations sharing the same infrastructure.
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive.
- Lack of standards about how Cloud service providers securely recycle disk drives and erase existing data.
- The enterprise IT security and risk management departments lose the control over the data security and operational intelligence activities.

We focused on the first problem, major in our opinion: the lack of an edge that can clearly separate enterprise data and applications in a shared Cloud environment.

There are many possible entry points for an intruder in a Cloud environment, as follows [13]:

a) A customer uses an insecure mobile phone to access the data.
b) A contractor of the network uses a web application that has an embedded vulnerability, a backdoor or one that is not protected.
c) A database administrator of the Cloud provider shares a password with another network customer.

Obviously it becomes more and more difficult to protect a Private Cloud environment having an increased number of users who request access to corporate data and applications with mobile devices or by Internet connections.

3. METHODOLOGY

In several places PKI (Public Key Infrastructure) certificates are released by a trusted organization. Another aspect is the content of a PKI certificate, which involves a pair of public and private keys [14].

We consider that the private key is a secure tool to protect the enterprise data, because it is never transmitted outside.

For SMBs (Small and Medium Businesses), which do not have the required financial and hardware resources to implement a trusted PKI in their own datacenter, the suggestion would be to use the publicly available OAuth standard [15].

3.1 Auth Standard

Due to some business requirements, users need to access several resources in the Cloud and it is very difficult to manage several passwords and authentication methods for each client.

Cloud can solve these problems by implementing a secure SSO (Single Sign On) solution, so each user is granted access to multiple applications after supplying its credentials only once. After validation, the client receives a ticket that enables the access of all the resources.

The next level of authentication and authorization is based on OAuth standard and implies three entities: the user, the client application and the service provider server. OAuth standard enables the user to grant client application/service access to its resources without sharing its username/password with the client application.

3.2 Confidentiality in Clouds by Using Cryptography

As a security purpose encryption doesn't stop attacks, but it minimizes the possibility of being data theft. The message known as plaintext, is encrypted using an encryption algorithm and converted to an unreadable cipher text [16][17]. The opposite process of encryption is called decryption in which the cipher text is converted to plain text.

An authorized party is able to decode the cipher text using a decryption algorithm, which usually requires a secret decryption key.

There are many encryption/decryption methods that use powerful algorithms, classified in three big categories: Symmetric key algorithms, Asymmetric key algorithms and Hashing [18].

In the following part, we will discuss some of the most common encryption methods:

- Symmetric key algorithms use the same key for both encryption and decryption [19]. In Cloud computing DES (Data Encryption Standard), Triple-DES, and AES (Advanced Encryption Standard) algorithms are more frequently used.

DES is the most widely used algorithm and it uses a 64-bit plaintext and same 56 bit cipher key for both encryption and decryption. The encryption process is made of two permutations (P-boxes), and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm [19].

A way of increasing the security is the Triple DES algorithm, which comprises three DES keys, each of 56 bits, applied to one block of 64 bits of data.

AES (Advanced Encryption Standard) encrypts 128-bit blocks with the key size of 128, 192, or 256 bits. AES operates on a 4×4 column-major order matrix of bytes [19].

- Asymmetric-key algorithms use different keys for encryption and decryption: a private key and a public key. Although different, the two parts of this key pair are mathematically linked. The public key is used by the sender for encryption and the private key is used for decryption of data by the receiver [18].

The main advantage of this solution is represented by the mathematical impossibility of deducing the private key from the public key. Everybody can have the public key without any concerns about confidentiality, given that the private key is kept secret and used only by authorized entities.

In Cloud Computing RSA, IKE, Diffie-Hellman Key Exchange asymmetric-key algorithms are used.

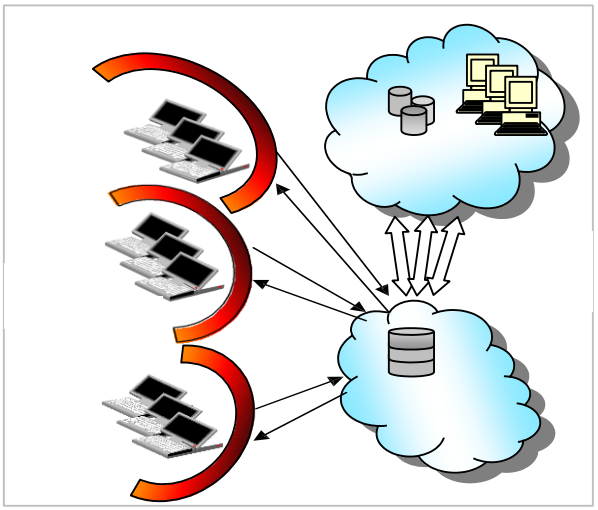
4. PROPOSED METHODOLOGY

The security and encryption fields for Cloud infrastructures have led us to proposing two solutions for ensuring business data confidentiality at the BPaaS level:

Also, for both variants we consider that is necessary to separate the enterprise data in two parts: internal data (data shell) and external data (suppliers, clients, product catalogues etc). By separating data flows in the company datacenter, a symmetric key algorithm is applied which offers the Cloud customer a high level of trust regarding

the security and confidentiality of its critical data as each has a personal encryption key that will never be shared.

This division is as important as choosing the correct application point for the encryption and authorization algorithms, and gives the Cloud users full control of their own data, while the CSP ensures data protection globally for the centralized infrastructure, without knowing the contents of client data. Thus, the first proposed solution (Model 1) is for Public Cloud security and combines OAuth standard authentication methods with encryption algorithms.



A sample use-case may be Google's ecosystem, as it offers business e-mail, calendar, Office apps and storage, but also a powerful platform for running web applications, called Google App Engine. A single account (OAuth) is enough for accessing the infrastructure, and the company can easily manage the user database and access privileges.

The steps to control user's access to the company applications are as follows:

- The user provides its credentials and requests access to the company applications;
- The username and password are redirected to Google Cloud for authentication;
- After validation, user is redirected back to the system with OAuth credentials and now he has the ticket to be granted access to company applications.

Data transmission is made after applying a symmetric-key encryption algorithm, such as DES, Triple-DES or AES.

Solutions to cloud security issues are various, from cryptography and public key infrastructure (PKI) to use of multiple cloud providers.

The second proposed solution (Model 2) involves certificate-based authentication, followed by public key cryptography applied to the confidential business data before storing it in the Cloud.

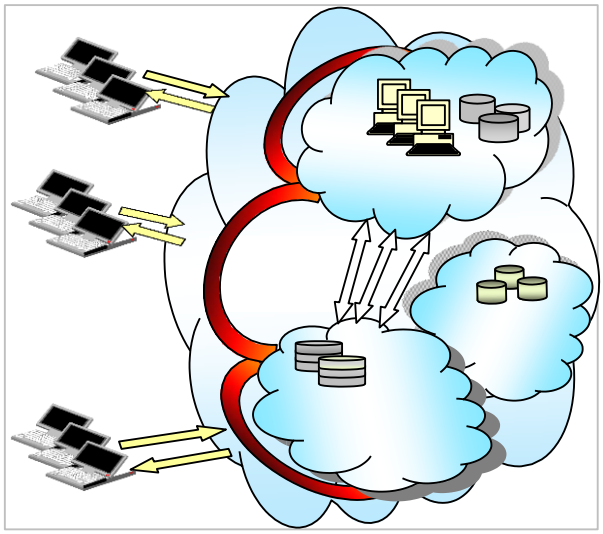
Within a PKI, a certificate authority must create and sign a company's key. Some of the clients found PKIs difficult to use, so the security providers have another variant: public key technologies such as Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), which often required no authentication of the user, but were there simply to authenticate the server and secure transactions.

Also, we consider that using PKI in the Cloud in conjunction with the secure transport mechanism, TLS, is a better solution because it offers a cryptographically strong method of authentication in an unsafe communication environment.

After authentication, private data encryption will ensure the privacy of the data sent from the client devices to the Clouds and back.

The client digitally signs data and sends both the certificate and the signed data across the network. The server uses techniques of public-key cryptography to validate the signature and confirm the validity of the certificate.

Certainly, this is a more secure method than password-based authentication because it is based on Public key cryptography that can verify that a Private Key used to sign some data corresponds to the Public Key in a certificate. The client has the responsibility to keep the private-key password secret.



The SSO model is replacing the password exchange that will normally occur when having different login points. This way, a user will enter its password once and unlock the private key database. Then, a signed certificate will be passed on to the necessary services for authentication.

The main phases for authentication, authorization and protect the confidentiality in this manner are as follows:

- The Cloud maintains a database of the private keys that correspond to the public keys published in any certificates issued for their clients.
- The Client has its private key to digitally sign its data.

- The Client transfer both the user's certificate and data that has been digitally signed using the the network.
- The Cloud server uses the certificate and the evidence to authenticate the Client's identity. The server may perform other authentication tasks, such as checking that the certificate presented by the client is stored in the user's entry in a directory. Also it checks whether the identified user is genuine and permitted to access the requested resource. If all the evaluation results are positive, the Cloud server allows the Client the access the requested resources.

5. CONCLUSION

In this paper based on the studies performed on different Cloud security methods, it is observed that there are many protection models, each with its own advantages and disadvantage, but still there is no perfect solution of this problem which can guarantee that this problem is being solved.

If the customer is from academia, ordinary users or small and medium enterprises, the first proposed model can satisfy their security requirements in low cost and performance conditions. For bigger and privately own companies the security is more important even than the high performance and we recommend the second proposed model because it can be helpful in such a scenario where there is the large need of security.

REFERENCES

[1] Mell, P., Grance, T., (2011), National Institute of Standards and Technology - Definition of Cloud Computing, available on http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html.

[2] Cacciari, C., D'Andria, F., Gonzalo, M., Hagemeier, B. et al., (2010), ElasticLM: A novel approach for software licensing in distributed computing infrastructures, Procedures IEEE 2nd International Conference on Cloud Computing Technology and Science, pp. 67–74.

[3] Final Version of NIST Cloud Computing Definition, NIST Special Publication 800-145, published on October 2011, available on http://www.nist.gov/itl/csd/cloud-102511.cfm

[4] Banica, L., Stefan, C., (2013), From Grid Computing to Cloud Infrastructures, International Journal of Computers & Technology, Vol 12, No.1, pp. 3187-3194

[5] Sreekanth I., (2010), Cloud Deployment and Delivery Models, available on https://www.ibm.com/developerworks/community/blogs/sreek/entry/cloud_4?lang=en

[6] Harding, C. et al., (2011), Cloud Computing for Business, Open Group, http://www.opengroup.org/sites/default/files/contentimages/Press/Excerpts/first_30_pages.pdf, pp.28-31.

[7] Technical White paper VMWare & Symantec, Desktop as a Service with VMware and Symantec (2011), available on: https://www.vmware.com/files/pdf/bdesktop as a service WP en-us 08-11.pdf

[8] Kulkarni, G., Sutar, R., Gambhir, J., (2012), Cloud Computing-Storage as Service, International Journal of Engineering Research and Applications, Vol. 2, Issue 1, pp.945-950

[9] Rashmi, R., Sahoo, G., Mehfuz, S., (2013), Securing Software as a Service Model of Cloud Computing: Issues and Solutions, International Journal on Cloud Computing: Services and Architecture, Vol.3, No.4, DOI: 10.5121/ijccsa.2013.3401

[10] Singla, S., Singh, J., (2013), Cloud Data security using Authentication and Encryption Technique, International Journal of Advanced Research in Computer Engineering & Technology, Vol. 2, Issue 7, pp. 2232-2235.

[11] Singla, S. Singh, J., (2013), Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm, Global Journal of Computer Science and Technology (GJCST), Vol. 13, Issue 5.

[12] Tumulak, D., (2012). Data Security in the Cloud, Computerworld "Cloud Computing" study, http://www.vormetric.com/sites/default/files/wpdata-security-in-the-cloud.pdf

[13] Marx, G., (2013). Can cloud computing be secure? Six ways to reduce risk and protect data, http://www.theguardian.com/medianetwork/ media-network blog/2013/sep/05/cloud computing-security-protect-data

[14] Foster, I., Zhao, Y., Raicu, I., Lu, S., (2008). Cloud Computing and Grid Computing 360-Degree Compared, Grid Computing Environments Workshop, pp. 1 – 10.

[15] Brodkin, K., (2008), Gartner: Seven cloud computing security risks, http://www.networkworld.com/ news/2008/070208-cloud.html.

[16] Krutz, L., R. and Vines, R., D., (2010), Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, Inc. Indianapolis, Indiana 2010.

[17] Goldreich, O., (2004), Foundations of Cryptography: Volume 2, Basic Applications. Vol. 2, Cambridge University Press, 2004.

[18] Nigoti, R., Jhuria, M., Singh, S., (2013), A Survey of Cryptographic Algorithms for Cloud Computing, , International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), volume 4, Issue 2, pp.141-146, available on http://www.iasir.net

[19] Jeeva, A., L., Palanisamy, V., and Kanagaram, K., (2012), Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms, International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp. 3033-3037.