JCSE International Journal of Computer Science and Engineering Open Access
Survey Paper Volume-2, Issue-2 E-ISSN: 2347-2693

An Innovational Approach to Security in Cloud Environment

Namrata Thakur[1], Vimmi Pandey[2] and Brejesh Singh[3]

[1*,2]Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India
[3]MPCVV, Rewa, M.P., India

www.ijcaonline.org

Received: 05 Feb 2014 Revised: 12 Feb 2014 Accepted: 22 Feb 2014 Published: 28 Feb 2014

***Abstract*—** The cloud computing platform gives people the opportunity for sharing resources, services and. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. In this paper we have proposed new security architecture for cloud computing platform. This ensures secure communication system and hiding information from others. It aims at meeting all security requirements.

***Index Term*—** *RSA, Trusted Third Party, Security Requirements*

I. INTRODUCTION

Many possible definitions are to be found for cloud computing. Most of them focus on the technology only [9][10]. Research has been done in order to combine all these different definitions to come up with one (proposed) uniform definition [10]. Cloud computing can best be described as a giant pool which contains hardware, software and other services that can be accessed through the “cloud”. All these resources can be accessed whenever necessary. In most cases the provider of the cloud sells his service as pay-per-use. This means that there is high flexibility in the use of these services as extra resources are always available [11].

The definition as described above still leaves a lot of questions about what cloud computing actually is. The giant pool as mentioned earlier refers to the available hardware, software and services as provided by cloud providing organizations. These organizations such as Google and amazon have hardware, software and services running on their own servers at certain fixed locations.

As a recapitulation, cloud computing is stated into different definitions. There are definitions that define a cloud as a some what updated version of utility computing [13]. The other, and broader, side states that anything you can access outside your firewall is cloud computing, even outsourcing. This thesis takes the definition in the middle of these two. In general cloud computing provides hardware and software services that are in the cloud and can be accessed by client as they pay for it. In the “cloud” means that there is no dedicated hardware reserved in a cloud providers’ servers.

To get more into detail about cloud computing, the components will be discussed that are used in the clouds. In general there are three main components in cloud computing, these are the servers, the data centres and the clients [9]. They all connect through the internet with each other and can be seen as a network.

Deployment Models of Cloud Computing

Public cloud –
A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and full responsibilities of installation; management, provisioning, and maintenance are managed by the cloud provider. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud includes Microsoft Azure, Google App Engine. A consumer can develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.

Private cloud –
Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the

Corresponding Author: *Namrata Thakur*

infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems .

Hybrid cloud –
A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services . A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

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, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook.

II. INTRODUCTION TO CLOUD SECURITY

Cloud security is a hot topic and two-factor authentication is one way to mitigate users' well founded concerns. As a result, development and adoption of two-factor authentication systems is proceeding at a rapid pace and should be available for most cloud applications within just a few short years. Though Cloud offers sophisticated storage and access environment, it is not hundred percent reliable; the challenge exists in ensuring the authorized access. Because third parties make the decision regarding our data, security is a big concern. So cloud must ensure that the data accessed is by the trusted users. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. It is a way by which it is verified that someone is who they claim they are. In private and public networks (ie. internet) authentication is commonly done through the use of logon passwords. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a fingerprints, smart card, retina scan, voice recognition, or signature. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password.

III. PROPOSED MODEL

In our proposed model we have worked with the following security algorithms:-

- RSA algorithm for secured communication [1, 2]
- SHA for Secured file encryption [3, 4]
- MD5 hashing for cover the tables from user [6]
- One time password for authentication which will be sent on users valid email id [7].

At present ensuring security in cloud computing platform has become one of the most significant concerns for the researchers. We have undertaken these problems in our research, to provide some solution correlated with security. We have proposed the following security model for cloud computing data storage.

In this model, all the users irrespective of new or existing member, needs to pass through a secured channel which is connected to the main system computer. System server computer has relation with other data storage system. The data storage system can be servers or only storage devices. Here, each of the data storage devices can be thought as one or more servers in number. This means, there are no dedicated servers in cloud computing, rather all are independent servers and can be scaled as necessary.

In the proposed model RSA encryption algorithm is used for making the communication safe. Usually the users' requests are encrypted while sending to the cloud service provider system. RSA algorithm using the system's public key is used for the encryption. Whenever the user requests for a file the system sends it by encrypting it via RSA encryption algorithm using the user's public key. Same process is also applied about the user password requests, while logging in the system later. After receiving an encrypted file from the system the user's browser will decrypt it with RSA algorithm using the user's private key. Similarly when the system receives an encrypted file from the user it will immediately decrypt it using its private key. As a result the communication becomes secured between the user and the system.

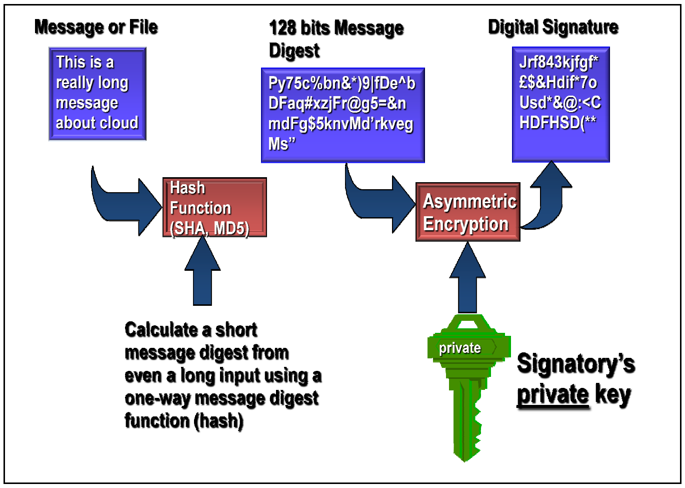
Message or File
This is a really long message about cloud
128 bits Message Digest
Py75c%bn&*)9|fDe^b DFaq#xzjFr@g5=&n mdFg$5knvMd'rkveg Ms"
Digital Signature
Jrf843kjfgf* £$&Hdif*7o Usd*&@:<C HDFHSD(**
Hash Function (SHA, MD5)
Asymmetric Encryption
Calculate a short message digest from even a long input using a one-way message digest function (hash)
private
Signatory's private key

Fig :1 Creating a Digital Sinature

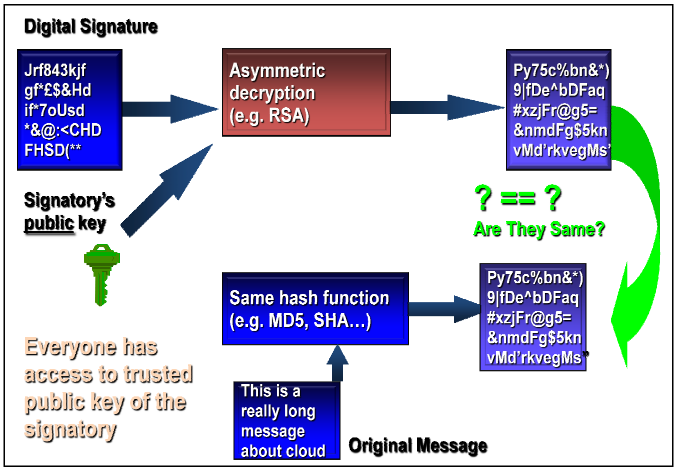
Digital Signature
Jrf843kjf gf*£$&Hd if*7oUsd *&@:<CHD FHSD(**
Asymmetric decryption (e.g. RSA)
Py75c%bn&*) 9|fDe^bDFaq #xzjFr@g5= &nmdFg$5kn vMd'rkvegMs'
Signatory's public key
? == ?
Are They Same?
Everyone has access to trusted public key of the signatory
Same hash function (e.g. MD5, SHA...)
Py75c%bn&*) 9|fDe^bDFaq #xzjFr@g5= &nmdFg$5kn vMd'rkvegMs'
This is a really long message about cloud
Original Message

Fig: 2 Verifying a Digital Signature

Whenever a user login in the system, he/she will be provided with a new password for using it in the next login. This is usually provided by the system itself. This password will be generated randomly. Each time a new password is created for a user, the previous password for that user will be erased from the system. New password will be updated for that particular user. A single password will be used for login only once. The password will be sent to the users authorized mail account. Therefore at a same time a check to determine the validity of the user is also performed. As a result only authorized user with a valid mail account will be able to connect to the cloud system. By this system, existence of unauthorized user or a user with an invalid mail account will be pointed out. The newly generated password is restored in the system after md5 hashing. The main purpose of MD5 hashing is that this method is a one way system and unbreakable. Therefore it will be difficult for an unauthorized or unknown party for retrieving the password for a selected user even if gained access to the system database.

IV. CONCLUSION

Although there are extreme advantages of using cloud based system but still security is a major flaw in front of cloud. This paper focuses how dynamic password technique has overcome the problem of security.

REFERENCES

[1]. R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Laboratory for Computer Science, Massachusetts Institute of Technology, Cam-bridge, November, **1977**

[2]. Burt Kaliski, The Mathematics of the RSA Public-Key Cryptosystem, RSA Laboratories

[3]. Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndael", **1999**

[4]. Joan Daemen, Vincent Rijmen, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication **197**, November **26**, **2001**

[5]. Joshua Holden, Mohammad Musa, Edward Schaefer, and Stephen Wedig, "A Simplified AES Algorithm", January **2010**

[6]. Ronald Rivest, "MD5 Message-Digest Algorithm", rfc 1321, April **1992**

[7]. Neil M.Haller, "THE S/KEY ONE-TIME PASSWORD SYSTEM", **1993.**

[8]. Neil Haller, "A One-Time Password System", October **23, 1995**

[9]. Mell, P., Grance, T., (**2009**). The Nist Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST special publication, 2011 National Institute of standards and technology.

[10]. Vaquero, L.M., Rodero-Merino, L., Caceres, J., Lindner, M. (**2009**). A Break in the Clouds: Towards a Cloud Definition. ACM SIGCOMM Computer Communication Review, **39(1), 50-55**.

[11]. Strickland, J. (**2011**) How cloud computing works. Howstuffworks.com. Available at: computer.howstuffworks.com/cloud-computing.htm

[12]. Vouk, MA. (**2008**) Cloud Computing - Issues, Research and Implementations. Journal of Computing and Information Technology, **16(4), 235-246**.

[13]. Buyya (**2009**), Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems. **25(6) 599-616**.

[14]. Velte, T., Velte, J., Elsenpeter, R. (**2009**). Cloud Computing: A Practical Approach. McGraw-Hill Osborne Media.