Building Trust In Cloud Using Public Key Infrastructure

A step towards cloud trust

Ms. Heena Kharche
Computer Science and Engineering
IES IPS Academy
Indore India

Mr. Deepak Singh Chouhan
Computer Science and Engineering
IES IPS Academy
Indore India

***Abstract*—Cloud services have grown very quickly over the past couple of years, giving consumers and companies the chance to put services, resources and infrastructures in the hands of a provider. There are big security concerns when using cloud services. With the emergence of cloud computing, Public Key Infrastructure (PKI) technology has undergone a renaissance, enabling computer to computer communications. This study describes use of PKI in cloud computing and provides insights into some of the challenges which cloud-based PKI systems face.**

Keywords- Cloud Computing; Public Key infrastructure; Cryptography.

I. INTRODUCTION

Cloud computing is rapidly emerging as a new paradigm for delivering computing as a utility. It allows leasing of IT capabilities whether they are infrastructure, platform, or software applications as services on subscription oriented services in a pay-as-you-go model.

"Cloud computing" is the next natural step in the evolution of on-demand information technology services and products. To a large extent, cloud computing will be based on virtualized resources.

Cloud Computing is here to stay, as it is proposed to transform the way IT is deployed and managed, promising reduced implementation, maintenance costs and complexity, while accelerating innovation, providing faster time to market, and providing the ability to scale high-performance applications and infrastructures on demand.

This paper will discuss why a cloud customer will trust cloud by using PKI.

This paper is organized in the following sections:

In Section II, we give a background of the technologies to be used. We explore in more detail what are the basic fears from cloud customers to adopt the cloud computing.

In Section III we describe the problems of cloud based PKI.

In Section IV we present our vision, some broad strategies that might be used to mitigate some of the concerns outlined in Sections II and III. Finally in section V we will discuss future work followed by conclusion in section VI.

II. BACKGROUND

A. Cryptography

Now a day, the most effective method of securing the data is by using cryptographic techniques. Cryptography is the method of storing and transmitting data in form that only those it is intended for can read and process [1].Basic terms used in cryptography are;

1. The readable data is referred to as PLAINTEXT
2. The random and unreadable data is referred to as CIPHERTEXT.
3. Process of converting plaintext to cipher text is referred to as ENCRYPTION.
4. Reverse of encryption i.e. Process of converting cipher text to plaintext is known as DECRYPTION.
5. Set of rules dictating how to encrypt and decrypt data are referred to as ALGORITHM.

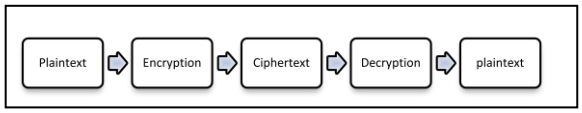

Figure 1. Cryptography process

1) Cryptosystem: The hardware or software implementation of cryptography process is termed as cryptosystem. Following services are provided by cryptosystems [2]:

1. **Confidentiality:** Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.
2. **Integrity:** Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.
3. **Authentication:** Authentication is the process of confirming correctness of the claimed identity.
4. **Authorization:** Authorization is the approval, Permission or empowerment for someone to do something.

5. **Non repudiation:** Non Repudiation is the ability for a system to prove that a specific user and only that user sent a message and it hasn't been modified.

2) Public Key Cryptography: As discussed in RSA data security white paper [3] Cryptography uses mathematical algorithms and processes to convert intelligible plaintext into unintelligible ciphertext, and vice versa. Applications of cryptography include:

- Data encryption for confidentiality
- Digital signatures to provide non-repudiation (accountability) and verify data integrity
- Certificates for authenticating people, applications and services, and for access control (authorization)

The two main kinds of cryptography are shared secret (symmetric key encryption) and public key (Asymmetric key encryption).

3) Symmetric Key Encryption: In symmetric key encryption, encryption key can be calculated from the decryption key and vice versa. With most of the symmetric algorithms, the same key is used for encryption and decryption. The symmetric key is effective only when the key is kept secret by two parties if anyone else discovers the key in any way; it affects both Confidentiality and Authentication. A person with unauthorized symmetric key not only can decrypt messages sent with key but can encrypt new messages and send them on behalf of the legitimate parties using the key.

4) Asymmetric Key Encryption: Public key encryption also called as Asymmetric Encryption involves a pair of keys, a public key and a private key, associates with an entity. Each public key is published, and the corresponding private key is kept secret. Data encrypted with public key can be decrypted only with corresponding private key.

B. Public Key Infrastructure

PKI consists of programs, data formats, procedures, communication protocols, security policies and public key cryptographic mechanisms working in a comprehensive manner to enable a wide range of dispersed people to communicate in a secure and predictable fashion. PKI provides authentication, confidentiality, non-repudiation, and integrity of the messages exchanged. PKI is hybrid system of symmetric and asymmetric key algorithms and methods [1-3].

A public-key infrastructure (PKI) is a framework that provides security services to an organization using public-key cryptography. These services are generally implemented across a networked environment, work in conjunction with client-side software, and can be customized by the organization implementing them. An added bonus is that all security services are provided transparently— users do not need to know about public keys, private keys, certificates, or Certification Authorities in order to take advantage of the services provided by a PKI [4].

1) Components of PKI: As discussed in paper [5] there are five components in PKI:

a. End Entity: End Entity is a generic term used to denote end-users, devices (e.g., servers, routers), or any other entity that can be identified in the subject field of a public key certificate. End entities typically consume and/or support PKI-related services.

b. Certification Authority (CA): an entity which issues certificates. One or more in-house servers, or a trusted third party such as VeriSign or GTE, can provide the CA function

c. Registration Authority (RA): The RA is an optional component that can assume a number of administrative functions from the CA. The RA is often associated with the End Entity registration process, but can assist in a number of other areas as well.

d. Repository: A repository is a generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by End Entities.

e. CRL Issuer: The CRL Issuer is an optional component that a CA can delegate to publish CRLs.

2) PKI and the Aims Of Secure Internet Communication:

The four aims of secure communication on the Internet are as stated earlier: confidentiality, integrity, authentication and non-repudiation. Authentication is the procedure to verify the identity of a user. There are three different factors authentication can be based on. These factors are something the user knows, something the user possesses and something the user is. Something the user knows could be a password that is a shared secret between the user and the verifying party. This is the weakest form of authentication since the password can be stolen through, for example, a dictionary attack or sniffing the network. Something the user possesses could be a physical token like a credit card, a passport or something digital and secret like a private key. This authentication form is usually combined with something the user knows to form a two-factor authentication. For instance, a credit card and a PIN are something possessed and something known. Something the user is could be something biometric like a fingerprint, DNA or a retinal scan which is unique for the user.

C. Cloud Computing

Cloud computing ('cloud') is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver those [6]. Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction [7].

1) Cloud services exhibit five essential characteristics [6-7] that demonstrate their relation to, and differences from, traditional computing approaches:

i. *On-demand self-service:* Computing capabilities are available on demand without any interference of third party.

ii. *Broad network access:* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud based software services.

iii. *Resource pooling:* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization.

iv. *Rapid elasticity:* Capabilities can be rapidly and elastically provisioned, in some cases automatically to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

v. *Measured service:* Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the service.

NIST Visual Model of Cloud Computing Definition gives the overall perspective and definition of what cloud computing is [8]:

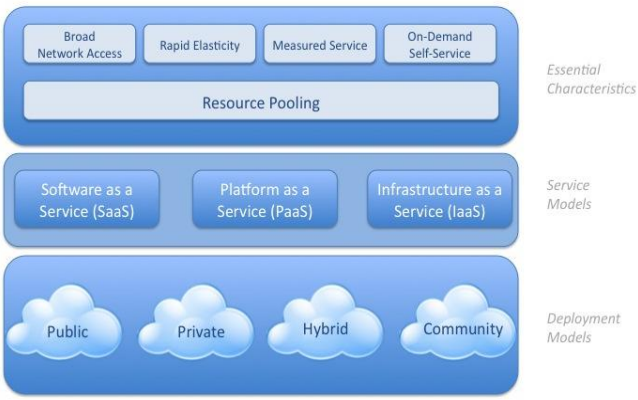

Figure 2. NIST Visual Model of Cloud Computing

a. Service Models: Cloud computing can be classified by the model of service it offers into one of three different groups.

i. **IaaS (Infrastructure as a Service):** The capability provided to the customer of IaaS is raw storage space, computing, or network resources with which the customer can run and execute an operating system, applications, or any software that they choose.

ii. **PaaS (Platform as a Service):** The cloud provider not only provides the hardware, but they also provide a toolkit and a number of supported programming languages to build higher level services (i.e. software applications that are made available as part of a specific platform).

iii. **SaaS (Software as a Service):** The SaaS customer is an end-user of complete applications running on a cloud infrastructure and offered on a platform on-demand. The applications are typically accessible through a thin client interface, such as a web browser.

b. Deployment Models: Clouds can also be classified based upon the underlying infrastructure deployment model as Public, Private, Community, or Hybrid clouds.

i. Public Cloud: A public cloud's physical infrastructure is owned by a cloud service provider. Such a cloud runs applications from different customers who share this infrastructure and pay for their resource utilization on a utility computing basis.

ii. Private Cloud: A pure private cloud is built for the exclusive use of one customer, who owns and fully controls this cloud.

iii. Community Cloud: When several customers have similar requirements, they can share an infrastructure and might share the configuration and management of the cloud. This management might be done by themselves or by third parties.

iv. Hybrid Cloud: Any composition of clouds, be they private or public could form a hybrid cloud and be manage a single entity, provided that there is sufficient commonality between the standards used by the constituent clouds.

2) Complications in cloud:

There are some concerns that should not be taken lightly when moving to a cloud service. Once the data has been moved to a cloud provider, control over it has been lost. The user cannot tell where the data resides physically and cannot be fully confident the data is handled with care in a secure manner. Furthermore, when the data has been moved to or created in the cloud, there are concerns about who really owns the data. For instance, if the subscription to the cloud service is cancelled, the customer cannot be fully confidant the data is removed. Also, if the customer wishes to switch cloud provider, there are concerns about if it is even possible as the provider might lock in the customer with various methods. Providers are very much aware of the complications and concerns of their services and works constantly to improve the quality and security of their services. Among others things they usually employ IT-security staff 24 hours a day every day to cope with any upcoming problems.

Benefits of cloud Computing: According to Mike Klein [12] there are six strong benefits that a cloud user gets:

i. *Lower Costs:* Cloud computing pools all of the computing resources that can be distributed to applications as needed – optimizing the use of the sum of the computing resources and delivering better efficiency and utilization of the entire shared infrastructure.

ii. *Cap-Ex Free Computing:* Whether you go with a public cloud or outsourced private cloud computing option, cloud computing delivers a better cash flow by eliminating the capital expense associated with building the server infrastructure.

iii. *Deploy Projects Faster:* Because servers can be brought up & destroyed in a matter of minutes, the time to deploy a new application drops dramatically with cloud computing. Rather than installing and networking a new hardware server, the new server can be dialed up and imaged in through a self-serve control console.

iv. *Scale as Needed:* As your applications grow, you can add storage, RAM and CPU capacity as needed. This means you can buy "just enough" and scale as the application demands grow. This benefit includes elasticity of the resources.

v. *Lower Maintenance Costs***:** Driven by 2 factors: Less hardware and outsourced, shared IT staff. Because cloud computing uses less physical resources, there is less hardware to power and maintain. With an outsourced cloud, you don't need to keep server, storage, network, and virtualization experts on staff full time.

vi. *Resiliency and Redundancy:* One of the benefits of a private cloud deployment is that you can get automatic failover between hardware platforms and disaster recovery services to bring up your server set in a separate data center should your primary data center experience an outage.

D. Transport layer Security:

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL) [9].

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide endpoint authentication and secure communications over any transport. TLS is normally associated with Internet communication but can be applied to any transport layer, including sockets and HTTP. TLS allows for two levels of security: Server Authentication and Mutual Authentication [10].

Server Authentication: Server Authentication authenticates the server to the client. When server authentication is used, the end user, or client, verifies that the server they are communicating with is actually who it says that it is. In the Internet world, your browser is the client, and a website such as Amazon™ is the server. Millions of clients need to be able to prove that the site to which they are giving financial information is really Amazon.

Mutual Authentication: Mutual Authentication authenticates the server to the client, and the client to the server. When Mutual Authentication is used, both the client and the server provide and validate certificates in order to verify each other's identity.

The TLS protocol is made up of two layers [11].

- The TLS record protocol is designed to protect confidentiality by using symmetric data encryption.
- The TLS handshake protocol allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

Need of TLS: Sending unencrypted messages increases the risk that messages can be intercepted or altered. TLS security technology automatically encrypts e-mail messages between servers thereby reducing the risk of eavesdropping, interception, and alteration.

III. ISSUES IN CLOUD BASED PKI

According to us there can be three issues that can complicate the implementation of PKI on cloud:

A. Storing Private Keys In Scalable And Mobile Systems:

The three factors to consider when designing the system are scalability, mobility and automation. A solution must be able to add more CAs on demand, be relatively consistent in required time to sign certificates and always be available. Hence, the solution must support the CA operations being movable to another less strained server if the number of requested signatures increases beyond the limit of the Hardware Security Module or the service unexpectedly fails. To able to move all CA operations to another server, all data regarding that CA must be moved between databases and the private key has to be moved or be the same at the new location. However, there exists no sufficiently secure procedure to move private keys between HSMs autonomously. Therefore, the same private keys must be predefined in HSMs at all available locations of that CA. The ability to move the CA to another location and to bind private keys on demand provides scalability in the number of signatures the system can handle. The scalability of the number CAs at one location is relative to the number of keys the Hardware Security Module is able to store.

B. Certificate Authority Separation:

One essential requirement of a cloud based PKI is that one customer should only be able to see and use its own CAs. Consequently, there must be separation between CAs and customers.

C. Providing Secure Authentication And Authorization:

Only a number of predefined CAs can issue certificates to administrators due to the trust store in the application server. Other CAs issuing administrator certificates can be added but that requires restarting of the application server. The purpose of this is to give each customer a dedicated CA to issue certificates to its administrators.

IV. Proposed Solution

In order to build complete trust over CA we must use the model suggested in RSA Conference Europe 2011 [12]. Studying the model we can establish trust of cloud consumer in cloud.

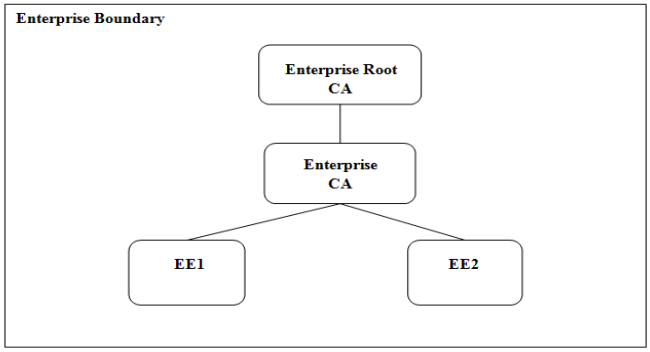

Figure 3. Enterprise root CA and Enterprise CA

An Enterprise Certificate Authority (CA) is a CA which generates certificates for a restricted community such as for an organization. The enterprise CA is selected by the mutual understanding of the enterprises and participating enterprises should trust the enterprise CA and Enterprise root CA.

The above model has following advantages:

1) Trust points (Root CA and CA certificates) are inside the enterprise boundary: All the enterprisess now can trust the root CA and CA as they are inside their boundary and the data kept on the cloud will not pass through the enterprise boundary.

2) Full control of security properties of PKI: In this model we will get the full functionalities of the Public Key Infrastructure that is the management of keys and the trust boundary will not be beyond the enterprise boundary.

3) On demand certificate and certificate revocation issuing: As both the enterprise CA and root CA are in the enterprise boundary any enterprise can easily revocate or issue a new certificate without have to wait for a long procedure and time.

The limitation of the mentioned model is, only few browsers will support the certificates issued by Enterprise root CA. The above limitation can be ignored as enterprise group can use a common browser to interact with each other.

Following aspects are considered while using the system:

a. Browser to be used: As the root CA is the enterprise CA therefore, the Certificates issued by the root CA will be supported only by few browsers. In order to interact with the cloud the enterprise should be aware of which browser is to be used.

b. Selection of Enterprise root CA and CA: Both the enterprise root CA and CA must be selected mutually by all the enterprises. A set of rules must be abided by the enterprises while choosing the and CA.

c. Switching cloud outside enterprise boundary: If any of the enterprise, at any time wants to switch the data from the enterprise boundary to outside world it can do so by mutually signed agreements and set of rules.

V. Future Work

A. Cross-Certification And Building Additional Certification Paths Dynamically

As it is a cloud service, it has the ability to cross certify the email authentication CAs from different customers under one central root email CA. In this scenario every customer that satisfies the criteria of the email certification will be offered to have the email CA certified and join the group of trusted email CAs. The implication would be that all customers in a group could send secure emails to each other and have access to the certificates and revocation information. The scenario relies on dynamically adding the certification path without having to reissue the certificates, which may or may not be possible.

B. Caching

Online Certificate Status Protocol (OCSP) is a very simple request/reply protocol that allows clients to ask an "OCSP responder" about the revocation status of one or more certificates. The OCSP responder returns digitally signed responses regarding the status of the certificates identified in the request. OCSP is designed to return real time responses to client queries, and can provide an efficient method for returning certificate status on demand.

To minimize the workload of the OCSP responder, caching of the result for some time could be used. However, OCSP use POST to send data which should not, in contrary to GET, be cached according to RFC 2616. Hence, further studies in the field of caching an OCSP response are required.

VI. Conclusion

PKI is enabling computer to computer communications in The Cloud because it offers a cryptographically strong method of authentication which can be tied to the secure transport mechanism, TLS [12].

The security of any system is not a question of if the system is secure or not, it is a question of how secure it is or in other words, to what extent it is secure. Every system has flaws, either in the design or in the nature of the system, thus absolute security cannot be guaranteed for any system. Technologies and incentives to access or destroy systems emerge as technology moves forward and the value of the system increases. Hence, a system can only be classified secure to an extent or not secure at all.

One critical factor in security is cost. To limit the incentives to break the system, the cost of breaking the system should be higher or equal to the value of the information the system is protecting. The paper has discussed a model to build trust in Cloud using public key Infrastructure. Despite of the limitation of browser support it can be widely used by

enterprises. The application of the above model can be the different plants and branch offices that want to share same data can create a public cloud and define their own Root CA and CA to ensure confidentiality and integrity of the data.

While working on future scope we can easily make a cloud consumer trust that their data is safe on cloud that too within their own enterprise boundary.

REFERENCES

[1] Shon Harris, CISSP All-in-One Exam Guide, Fifth Edition.

[2] Glossary of terms in SANS reading room available at: http://www.sans.org/security-resources/glossary-of-terms/

[3] Understanding Public Key Infrastructure (PKI) An RSA Data Security White Paper available at: ftp://ftp.rsa.com/pub/pdfs/understanding_pki.pdf

[4] Article from Entrust.com available at: http://www.entrust.com/resources/pdf/whatsapki.pdf

[5] Shashi kiran, Patricia Lareau, Steve Lloyd PKI Basics - A Technical Perspective available at: http://www.oasis-pki.org/pdfs/PKI_Basics-A_technical_perspective.pdf

[6] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 available at: https://cloudsecurityalliance.org/csaguide.pdf

[7] Guidelines on Security and Privacy in Public Cloud Computing Wayne Jansen Timothy Grance Draft Special Publication 800-144 available at: http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[8] cloud computing architectural framework in CSA found at https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_Framework

[9] Blog by Mikko Nieminen available at: http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS

[10] VMware vCenter Configuration Manager Transport Layer Security Implementation WHITE PAPER available at: http://www.vmware.com/files/pdf/techpaper/vcenter-configuration-manager-transport-security-layer-tls-guide.pdf

[11] Transport Layer FAQ available at: http://www.bnymellon.com/security/tlsencryption.pdf

[12] PKI reborn in cloud by Jaimee Brown and Peter Robinson RSA, The Security Division of EMC found at: http://365.rsaconference.com/servlet/JiveServlet/previewBody/3037-102-1-4074/NMS-301%20-%20PKI%20Reborn%20in%20the%20Cloud.pdf

AUTHORS PROFILE

Ms. Heena Kharche
Pursuing Masters of engineering 2nd year
Computer Science and Engineering
Institute of Engineering and science Indore professional Studies Academy Indore India
heenak.28@gmail.com

Mr. Deepak Singh Chouhan
Working in Computer Science and Engineering department,
Institute of Engineering and science Indore professional Studies Academy Indore India.
deepak.ur@gmail.com