International Journal of Engineering Inventions
ISSN: 2278-7461, www.ijeijournal.com
Volume 1, Issue 5 (September2012) PP: 41-46

Implementing Trust in Cloud Using Public Key Infrastructure

Heena Kharche[1], Prof.Deepak Singh Chouhan[2]
[1] *Student at Computer Science and Engineering, IES IPS Academy, Indore India*
[2]*Faculty at Computer Science and Engineering, IES IPS Academy, Indore India*

Abstract— Cloud is not a destination. It is an approach. Cloud service providers, along with cloud technology vendors, today are working towards developing a cloud ecosystem. The main area of concern in cloud ecosystem is security and trust. As Public Key Infrastructure (PKI) technology has undergone a renaissance, enabling computer to computer communications this paper will describe the ways to implement trust models using Microsoft Windows Azure. This paper will provide implementations to the trust model used to enable trust in Cloud.

Keywords — Azure; Cloud Computing; Cryptography; Public Key infrastructure; Windows

I. INTRODUCTION

Cloud computing is rapidly emerging as a new paradigm for delivering computing as a utility. While enterprises in India are apprehensive about public clouds, they would still like to avail themselves benefits that cloud computing have to offer. The idea behind any cloud computing proposal is for you to pay only for what you use, scaling up or down according to business needs. Vendors supporting cloud computing can interpret this statement differently, providing varying levels of services to achieve this result. The industry is now on its way towards cloud computing and virtualization is the infrastructure on which it is being built. The cloud model will see a rapid adoption in India, as business will appreciate how technology enables them to easily expand scalability and enhance elasticity [1].
This paper is organized in the following sections:

In Section II, we give a background of the technologies and trust model to be used. In Section III we describe the implementation methodologies of cloud based PKI. In Section IV we will discuss Conclusion and future work.

II. BACKGROUND

A. 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 [2-4]. 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 [5].

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.

B. Cloud Computing

Gartner defines cloud computing as Scalable, IT related capabilities provided as a service on Internet. The term cloud computing implies access to remote computing services offered by third parties via a TCP/IP connection to the public Internet. The cloud symbol in a network diagram, which initially represented any type of multiuser network, came to be associated specifically with the public Internet in the mid-1990s[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:

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

b) *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.

c) *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.

d) *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.

e) *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 [7]:

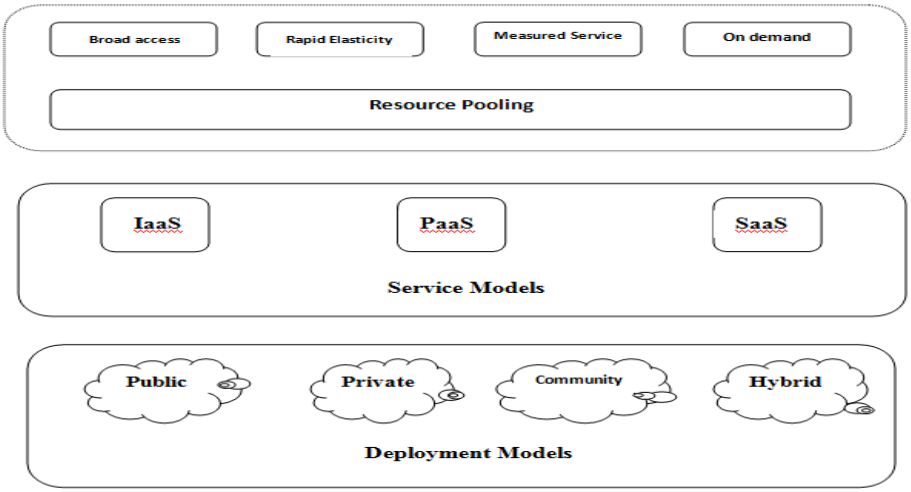

Fig. II.B NIST Visual Model of Cloud Computing

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.

C. Windows Azure

Windows Azure platform consists of a highly scalable (elastic) cloud operating system, data storage fabric and related services delivered by physical or logical (virtualized) Windows Server 2008 instances. The Windows Azure Software

Development Kit (SDK) provides a development version of the cloud-based services, as well as the tools and APIs needed to develop, deploy, and manage scalable services in Windows Azure.
According to Microsoft, the primary uses for Azure are to

i. Add web service capabilities to existing packaged applications
ii. Build, modify, and distribute applications to the Web with minimal on-premises resources
iii. Perform services, such as large-volume storage, batch processing, intense or high-volume computations, and so on, off premises
iv. Create, test, debug, and distribute web services quickly and inexpensively
v. Reduce costs and risks of building and extending on-premises resources
vi. Reduce the effort and costs of IT management
vii. The Windows Azure Platform supports three types of scalable persistent storage:
viii. unstructured data (blobs)
ix. structured data (tables)
x. messages between applications, services, or both (queues)

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) [8].

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. 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.

E. Trust Models

Enterprise Boundary[5] consists of a group of enterprises that wish to form a group to implement a common procedure of security.

1) Public Root CA and Public CA

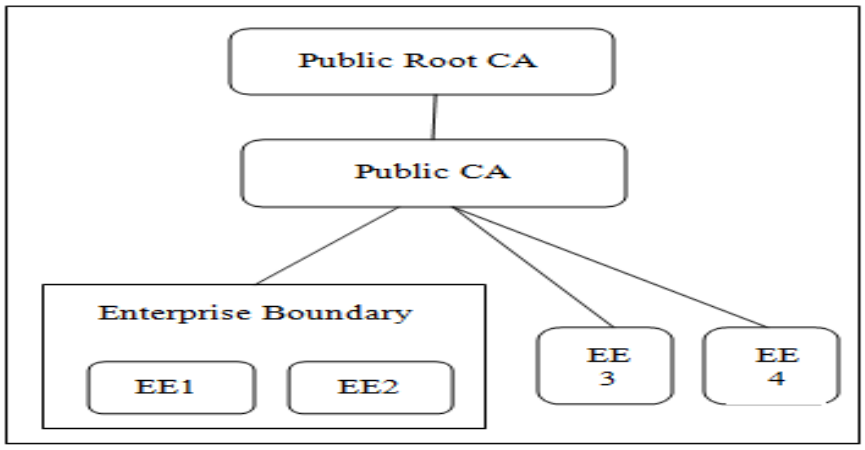

Fig. II.E.1 Public root CA and public CA

Above model consists of a public root CA and the Public CA which are connected by some enterprises in enterprise boundary that share same rules of security and some individually connected by public CA's.

Advantage of above model is that all web browsers trust the root CA certificate, and hence all certificates generated in the hierarchy.

i. This model lacks in following:
ii. Trust point (CA certificate) is outside the enterprise boundary and issues certificates to other parties.
iii. No control of security properties of PKI
iv. Key Strength: 3072 bit RSA rather than 1024 bit RSA.
v. Certificate extensions: Key usage.
vi. Inability to issue certificate and certificate revocation information on demand.
vii. High implementation cost.

2) Public root CA and Enterprise CA

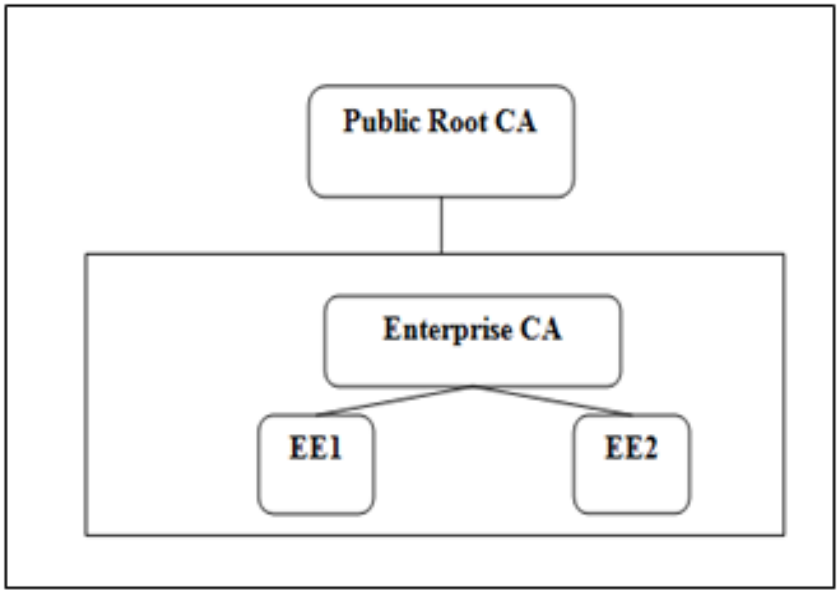

Fig. II.E.2 Public Root CA and Enterprise CA

Above model consists of a public root CA and an enterprise CA which rules the secure communication between various enterprises and the root CA.

Advantages of the above model are:

i. Trust point (CA certificate) is inside the enterprise boundary.
ii. On demand certificate and certificate revocation issuing.
iii. Web browsers trust the root CA certificate, and hence all certificates generated in the hierarchy.

Disadvantages of the above model that is supports Limited control of security properties of PKI and the implementation cost is too high.

3) Enterprise root CA and Enterprise CA

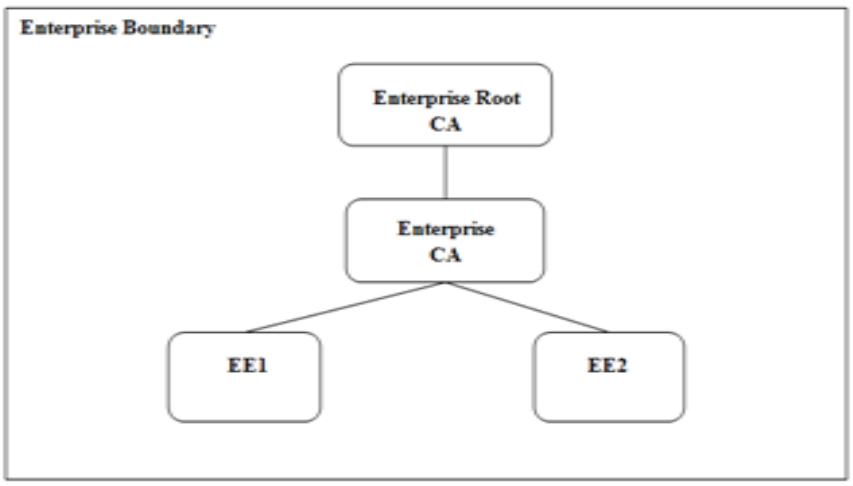

Fig. II.E.3 Enterprise root CA and enterprise CA

Above model operates completely in enterprise boundary which means complete trust is established between the enterprises communication and remote access.

Advantages of above model are:

i. Trust points (Root CA and CA certificates) are inside the enterprise boundary.
ii. Full control of security properties of PKI.
iii. On demand certificate and certificate revocation issuing.

The only disadvantage of the above model is Web browsers do not trust the root CA certificate, and hence all certificates generated in the hierarchy.

III. IMPLEMENTATION METHODOLOGIES

Above trust models can be implemented by following methodologies in a sequence for reducing risks in cloud computing and develops trust of cloud customer in cloud.

Summary of the protocols and algorithms to be used in following methodologies are:

Transport Layer Security is used as secure protocol. Advanced Encryption Standard is used for cipher algorithm with secure hash Algorithm and RSA as key exchange.

F. Public root CA and Public CA

In this model only thing we have to look around is the secure communication using TLS and secure data transmission using Advanced Encryption standard.

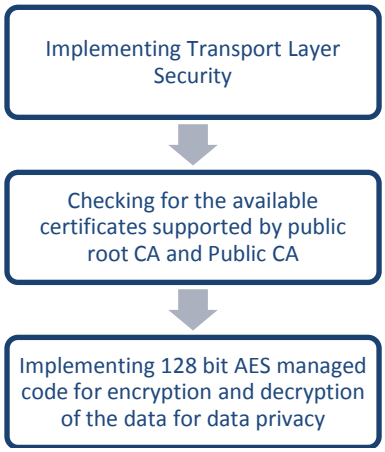

Fig. III.A Methodology for model 1

G. Public Root CA and Enterprise CA

In this model only thing we have to look around is the secure communication using TLS then we create self signed certificate which makes enterprise CA, we import the certificates in the browser and secure data transmission using 128 bit Advanced Encryption standard.

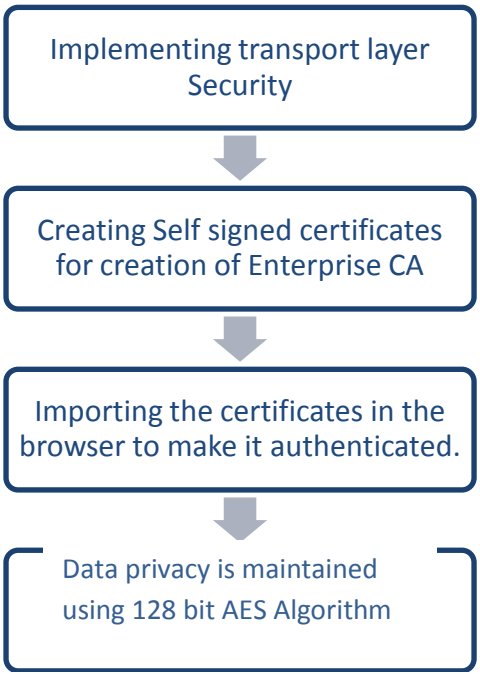

Fig. 3.B. Methodology for model 2

H. Enterprise Root CA and Enterprise CA

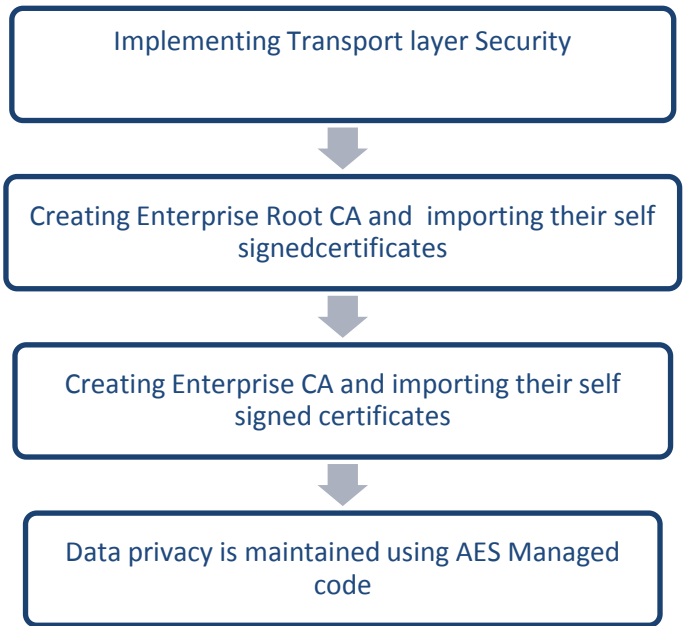

Fig.3.C Methodology for model 3

IV. CONCLUSION AND FUTURE WORK

In this model the methodology that is implemented is quite complicated in this we have to create both the CA and have to maintain it across the enterprises which lie in enterprise boundary. The table below shows the comparison between three models on various parameters which have been calculated logically:

Parameters	Public Root CA and Public CA	Public Root CA and Enterprise CA	Enterprise Root CA and Enterprise CA
Secure	Less	Medium	More
Privacy	Less	Medium	More
Trust	Medium	Medium	High
Cost	High	High	High
Feasibility	High	Medium	low
Performance	High	Low	Low

Table IV Comparative Analysis

By implementing the above model we can easily avail the trust within the enterprise boundary using Microsoft platform .By creating Root CA and Enterprise CA with the decision of all the enterprises may build the complete trust in the cloud. 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. In future these algorithms can be expanded with the new forthcoming algorithms to eliminate the disadvantages of the existing system. Various performance factors can be improved in the cloud for the use of cloud with full trust.

REFERENCES

1. Wayne Jansen Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing
2. Understanding Public Key Infrastructure (PKI) An RSA Data Security White Paper
3. Article from Entrust.com
4. Shashi kiran, Patricia Lareau, Steve Lloyd PKI Basics - A Technical Perspective
5. Heena kharche,Deepak Singh Chouhan : Building Trust In Cloud Using Public Key Infrastructure, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012,Pg(26-31)
6. Roger Jennings: Cloud Computing with the Windows Azure Platform,2010 ,pp11-12
7. VMware vCenter Configuration Manager Transport Layer Security Implementation WHITE PAPER
8. The bank of New York Mellon, Transport Layer FAQ ,