Security Concerns In Cloud Computing

Shekhar S. Kausalye[1], Miss. Rina S. Patil[2], Kapil B. Pawar[3]
[1, 2] Department of Information Technology
[3] Department of Computer Technology
[1, 2, 3] Sanjivani College of Engineering

Abstract- *Now a day's infrastructure architecture, development models and software service has a new perspective due to cloud computing technology. Cloud computing follows development of mainframe computers to client server model, and deployment of the model. It takes advantages of grid computing, cluster computing, utility computing and has an innovative deployment architecture with various services. Though this new innovation in cloud has a enormous options and services various critical issues must be considered depending on information, communication system and data security. There are number of risks and challenges have been introduced in this new technology affecting traditional security mechanism. This paper focus on evaluation of cloud security by highlighting effective security requirement and trying to propose possible solution for those threats. The solution uses cryptography (PKI) in concern with LDAP & SSO. This ensures integrity, confidentiality & authentication of data.*

Keywords- Cloud Computing Security, Trust, PKI, and Third Party.

I. INTRODUCTION

From beginning of computer history various techniques like time sharing, network computing, and grid computing, virtual computing are evolved which try to abstract the computer hardware & its need. These attempts are becoming real and efficient now a days as cloud computing is becoming popular in commercial as well as academic areas. Cloud computing is new architecture which has completely changed the whole perspective & concept of Operating System, services, client server architecture and browser. It relaxes

user form hardware requirement & its complexity.

As cloud computing is becoming popular, security issues are raised while adopting this new architecture. There is need of reconsideration of effectiveness of traditional security mechanism as cloud computing has improved and different architecture than traditional. This paper addresses security challenges in cloud environment and its security perspectives. This paper proposed security solution which reduces burden of user, this is achieved by Third Party whose task is to assure various security characteristics in cloud environment.

One of the main advantage of Grid computing is to solve complex calculations and data-intensive scientific applications easily. This is possible because in Grid high performance computers and servers are connected using fast data communication links. Grid computing provides consistent & cost efficient high end computational capabilities. Cloud computing can be considered as improved version of Grid Computing with some very efficient added capabilities and services [1]. It is an architecture which provides efficient on demand services to shared pool of computing resources like network, storage, application, platform, services, servers, etc. which are configurable according to need of user & which can be easily managed form central location [3]. Cloud computing takes advantage of Virtualization Technology which is mainly developed for mainframe computers. Virtualization provides essential cloud characteristics like elasticity, resource pooling & location independence. Heart of virtualization is hypervisor which creates virtual machine & this virtual machine simulates physical computers which are capable to run any application to operating system without any problem [4].

Datacenters consists of number of physical devices form processor, HDD, network devices are located independent of geographical locations and these data centers full fill storage and processing needs. Above this hardware there are Software, Virtualization & management layers which allows effective management of servers. Management layer's work is monitoring traffic and according to requirement create and destroy servers & also monitors security of the cloud. Challenges of grid computing are overcome with virtualization which separating logical & physical concept [5]. One of the main difference and advantage of cloud virtualization server is it achieves high utilization by allowing one server to process several tasks concurrently where as in grid this task is done by multiple servers [6].

A deployment model defines the purpose of the cloud and the nature of how the cloud is located.

1) Public cloud: The public cloud infrastructure is available for public use alternatively for a large industry group and is owned by an organization selling cloud services.

2) Private cloud: The private cloud infrastructure is operated for the exclusive use of an organization & managed by that organization or a third party.
3) Hybrid cloud: A hybrid cloud combines multiple clouds (private, community of public) where those clouds retain their unique identities, but are bound together as a unit.
4) Community cloud: A community cloud is one where the cloud has been organized to serve a common function or purpose. A community cloud is similar to a public cloud except that its access is limited to a specific community of cloud consumers

Following are various service models of Cloud computing:

1) Infrastructure as a Service (IaaS): IaaS provides virtual machines, virtual storage, virtual infrastructure, and other hardware assets as resources that clients can provision. The IaaS service provider manages all the infrastructure, while the client is responsible for all other aspects like operating system, applications, and user interactions with the system.
2) Platform as a Service: PaaS provides virtual machines, operating systems, applications, services, development frameworks, transactions, and control structures. The service provider manages the cloud infrastructure, the operating systems, and the enabling software. The client is responsible for installing and managing the application that it is deploying.
3) Software as a Service: SaaS is a complete operating environment with applications, management, and the user interface. In the SaaS model, the application is provided to the client through a thin client interface (a browser, usually), and the customer's responsibility begins and ends with entering and managing its data and user interaction.

Various key characteristics of cloud computing [7] are:

1) On-demand self-service: Service without interaction of Service Provider.
2) Resource pooling: A cloud service provider creates resources that are pooled together in a system that supports multi-tenant usage.
3) Rapid elasticity: Resources can be rapidly and elastically provided. Aromatic or manual scalu up and scale out of resources.
4) Measured service: The use of cloud system resources is measured, audited, and reported to the customer based on a metered system.
5) Multitenancy: enables sharing of resources and costs across a large pool of users thus allowing for: centralization of infrastructure in locations with lower costs
6) Quality of Service: The Quality of Service (QoS) is obtain through agreement from vendor.
7) Reliability: The scale of cloud computing networks and their ability to provide load balancing and failover makes them highly reliable.
8) Simplified maintenance and upgrade: As system is centralized patches and upgrades can be easily applied [8].

II. SECURITY

A. Trust in Cloud Computing

Trust was used in the process of convincing observers that a system (model, design or implementation) was correct and secure [9]. Trust between two parties can be described as: ‘‘A party A is considered to trust another party B when party A believes that party B will behave exactly as expected and required’’ [10]. The concept described above can be termed as reliability, which is nothing but quality of a person or entity that is trust worthy. Trust in the IT has various grounds, based on calculus, on knowledge or on social reasons [11]. The concept of trust in an organization could be defined as the customer’s certainty that the organization is capable of providing the required services accurately and infallibly.

The concept of security in cloud is to a given circumstances where all possible risks are either eliminated or brought to an absolute minimum [12]. In cloud environment trust depends on the particular deployment model. In old-style architectures, trust was imposed by an efficient security policy, which addressed constraints on functions and flow among them. In a cloud deployment, this view is totally hidden. In Public or Community clouds control is given to the organization which owns infrastructure.

Differentiation between deployment models is vital as a private cloud, where infrastructure is managed by a private organization, and it does not introduce distinctive security challenges because trust remains within the organization. In such a situation the infrastructures owner remains the data and process owner. Cloud environment weakens the awareness of perimeter security as it us a set of physical and programmatic security policies which protects abstract border form remote malicious activity. In a cloud computing model, the border becomes uncertain, weakening the effectiveness of security control. According to perimeter security, the cloud seems outside trust border and must be viewed with misgiving, but this adversely leads to not trusting essential business processes and services that have been

outsourced. The ability to clearly identify, authenticate, authorize and monitor what or who is accessing the resources of an organization is important to protect an information system from threats and exposures. Separation is the key ingredient of any secure system, and is based on the ability to create boundaries between those entities that must be protected and those which cannot be trusted [13].

This paper proposes Trusted Third Party within a cloud environment by supporting trust and using cryptography to safeguard the confidentiality, integrity and authenticity of data and communications. The relying party trust the TTP for the security it is supposed to offer in all communications [14]. The TTP provides end-to-end security services, which are scalable, based on standards and useful through different domains, geographical areas. Using TTP address the loss of the traditional security periphery by producing trusted security domains and enabling support between these. A TTP is essentially a Trusted Authority delegated with the responsibility of addressing a number of security issues in a multilevel distributed environment.

B. Identification of Threats

Information System security involves recognizing distinctive threats which need to be addressed by implementing the appropriate countermeasures. To effectively incorporate security controls in information systems functional requirements, operational requirement & other relevant system requirements selected security controls are introduced to the standard systems engineering process [15]. Cloud computing imposes various security benefits some of them are security centralization, data and process segmentation, redundancy and high availability. Cloud computing has ‘‘unique attributes that require risk assessment in areas such as availability and reliability issues, data integrity, recovery, and privacy and auditing [16]. These important aspects of security are used for all categories of assets which must be secured i.e. data, software and hardware resources.

Unique security challenges or cloud infrastructure are:

1) Confidentiality and privacy: Confidentiality is that only approved parties or systems has ability to access protected data. Data compromise is an issue in cloud, due to the increased number of parties, devices and applications involved, that increase number of sources of access. Multitenancy is the cloud characteristic of resource sharing. Several features of the IS are shared like, memory, programs, networks and data. In Cloud computing resources are shared at network, host, and application level. Users are isolated at virtual level but hardware is not isolated. With a multitenant architecture, a software application is designed to virtually partition its data and configuration so that each client organization works with a customized virtual application instance. Due to virtual isolation of logical drives & lack of hardware separation between multiple users on a single infrastructure, data eminence may lead to the reluctant disclosure of private data. Weak authentication can lead to unauthorized access to users account on a cloud, result in privacy breach. Software confidentiality is defined as trusting specific applications or processes that maintain and handle the user’s confidential data in a secure manner. Software applications interacting with the user’s data must not introduce confidentiality and privacy risks. Unauthorized access can become possible through the exploitation of an application vulnerability or lack of strong identification, bringing up issues of data confidentiality and privacy. Privacy is willingness of a party to control the expose of personal information. The cloud has various challenges of privacy issues of data which is stored at remote locations in the cloud, which could be in Russia, America, or anywhere else.

2) Integrity: Also called as accountability refers that data can be modified only by authorized users or in authorized ways. By avoiding unauthorized access, organizations can achieve better confidence in data and system integrity. This also used determining who or what have altered data or system information, which affects integrity. As there are more number of entities and access rights in cloud authorization plays vital role in deciding that only authorized entities can interact with data. Software Integrity protection of software from unauthorized deletion, modification, access; which may be internal of external of organization. That’s why Cloud computing has an APIs which are designed for customer for managing and interacting with cloud services.

3) Availability: It means that system is accessible and usable whenever demanded by an authorized person or entity. System must work regardless of any security breach. Its cloud owner’s responsibility that information and system must be available to user whenever demanded by the user. System availability includes a systems ability to carry on operations even when some authorities misbehave. Services in cloud computing are dependent on resource infrastructure and network availability at any time

III. TRUSTED THIRD PARTY

Trusted Third Party in cloud ensures necessary trust level and delivers solution for preserving confidentiality,

authenticity & integrity [17] for all data communication in the cloud as shown in fig 1.

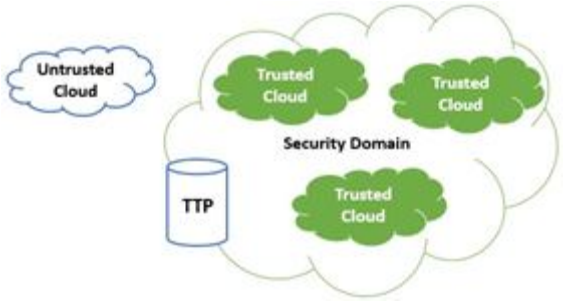

Figure 1. TTP Cloud Infrastructure of federation

In cryptography TTP allows secure interaction between two parties who trust TTP. It has responsibility to provide end-to-end security which is based on security standards across different geographical sectors. Using fraudulent digital content TTP analyses all communication between users.

TTP services are provided and guaranteed by technical as well as by legal, financial, and structural means. It is connected through certificate paths to provide a web of trust forming the notion of a Public Key Infrastructure (PKI). Public Key Infrastructure provides technically sound and legally acceptable means to implement:

1) Strong Authentication
2) Authorization
3) Data Confidentiality
4) Data Integrity
5) Non-Repudiation

LDAP is important protocol in support of PKIs directory services for certificates and certificate revocation lists (CRLs). It is also used by other web services for authentication. A directory combined with PKI can be used for distributing:

1) Certificates, for applications such as e-mail.
2) Certificate status information, such as certificate revocation lists (CRLs).
3) Private keys, in case users do not use the same machine each day.

The trusted third party can be relied upon [1] Low and High level confidentiality, Server and Client Authentication, Creation of Security Domains, Cryptographic Separation of Data, Certificate-Based Authorization.

A. Confidentiality Level

Data travelling through network is hard to secure and is complex process. And in cloud this complexity increases as there is lack to traditional physical connection also due to virtual environment which has abstraction property. PKI implements IPSec or SSL for secure communications. IPSec is an protocol which work on IP layer to enables sending and receiving of encrypted i.e. protected packets of any kind like TCP, UDP, ICMP, etc. without any modification. IPSec provides two cryptographic services viz. confidentiality and authenticity. SSL protocol allows end-to end encryption by interfacing between applications and the TCPIP protocols to provide client–server authentication and an encrypted communications channel between client–server.

According to security requirement IPSec or SSL can be selected. IPSec is compatible with any application but requires an IPSec client to be installed on each remote device to add the encryption. In contrast, SSL is built into every browser, so no special client software is required.

Cloud services are mostly retrieved through browsers, SSL has many benefits for client to host communications. On the other hand, IPSec supports using compression making it a more efficient choice for host-to-host communications [1]. This paper proposes implementing IPSec for encrypting communications for host-to-host communications and SSL for Client-to Cloud communications

B. Creation of Security Domain

To have the efficient trust relationship between different entities in cloud the federation in association with PKI and LDAP technology must be implemented. As everyone knows federation is a group of legal entities that share a predefined set of agreed policies and rules for accessing online resources [18]. Federation provides structured and legal framework which enables authentication and authorization. Cloud infrastructures can be organized in unique security domains enabling ‘‘Federated clouds’’ [1]. Federated Clouds are a collection of clouds which appears as a single Clouds that can interchange data and computing resources through agreed policies. According to basic federation principles, in a Federation of Clouds each single Cloud remains independent, but can interoperate with other Clouds in the federation through standardized interfaces.

C. Cryptographic Data Parting

In this processes, computations and data are cloaked in such a way that they appear imperceptible to strangers [19]. Confidentiality and integrity & privacy of data can be protected through encryption. Using a combination of

asymmetric and symmetric cryptographic which is nothing but hybrid cryptography can offer the efficiency of symmetric cryptography while maintaining the security of asymmetric cryptography [1].

D. Certificate based Authorization

Cloud environment is very versatile having several independent domains in which relationship between user and resource (service) is ad hoc and dynamic. Resources and users are in different domain. In cloud users are recognized by their characteristics or attributes instead of identity. Hence, traditional identity based access control models are not effective, and access decisions has to be made using attributes [1]. Certificates issued by a PKI facility can be used for enforcing access control in the Web environment. These certificates are issued by a certification authority that acts as a trust center in the global Web environment. It contain an attribute–value pair and the principal to whom it applies. Attribute based access control, provides flexibility and scalability that are vital cloud.

IV. ASSESSMENT

This paper try to suggest a security solution for challenges in a cloud environment, which reduces security burden of the client by trusting TTP. Trust works in top down flow as shown in figure 2.

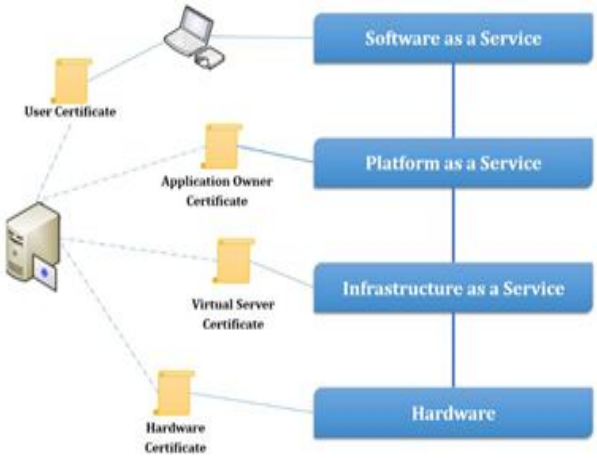

Figure 2. Trust operates in a top-down flow, every layer is required to trust the layer immediately below it.

Trust essentially operates in a top-down way. Every layer needs to trust the layer immediately below it, and requires a security guarantee at an operational, technical, procedural and legal level to enable secure communications with it (Fig. 2). A trusted certificate serves as a reliable "e-passport'' that creates an entity's identity, credentials and responsibilities.

Trust is provided by the process called as certificate process in which set of policies and requirement has to be confirm by the party who require certification. TTP provides security facility between two unknown parties who want secure communication in the distributed cloud environment. End user has to validate his access rights to a required resource. This certificate is used in combination with the service provider's certificate (PaS or IaS level). This helps to establish secure SSL connection between them, thus encrypting exchanged data and guaranteeing their security through the cloud infrastructure (Fig. 3) [2].

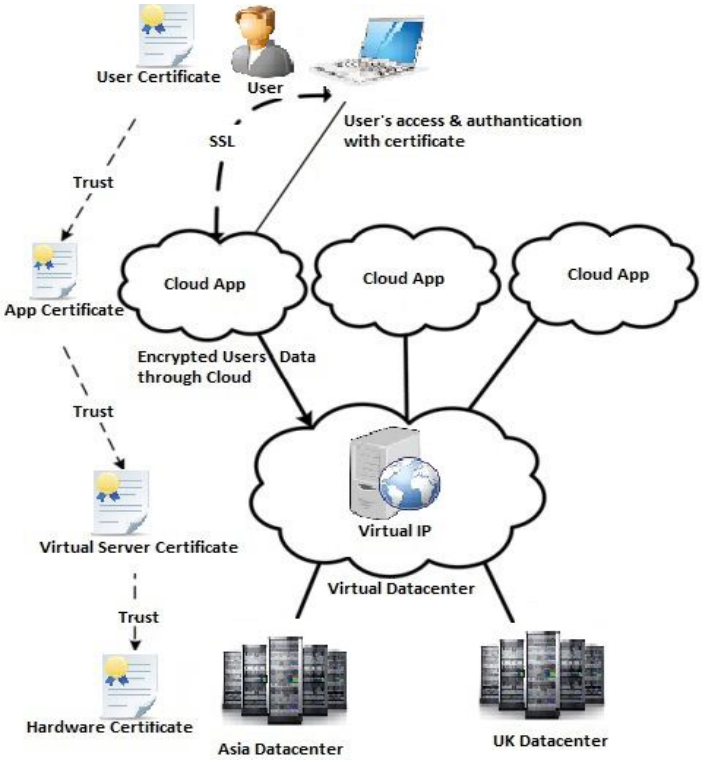

Figure 3. A user authentication with cloud service using his personal certificate which further used with the service provider certificate to secure and encrypt all communications.

The user is able to encrypt all personal data stored on the cloud to reduce confidentiality risks. Application provider use its own certificate to authenticate itself in cloud communications and also use this certificate encryption & decryption of application data. At hardware layer owner makes use of a digital certificate for secure communication and also for authentication. Encryption Key management is important issue, as the virtualization of services complicates identification of physical location of key stored, which weakens or sometimes disable traditional protection mechanisms. Keys are stored and protected at a hardware infrastructure level.

The proposed solution demands cryptography, especially Public Key Infrastructure, to ensure the

authentication, integrity and confidentiality. In federation of clouds TTP plays a role for assuring particular security characteristics in cloud environment, and it also confirms trust between entities. The solution, has horizontal level of service for all concerned entities. This solution's approach uses combination of Public Key Cryptography and LDAP directories authentication and identification of entities. The model adheres advantage of each technology used with its deficiencies.

The TTP can be depend on Low and High level confidentiality, Server and Client Authentication, Generating Security Domains, Cryptographic Separation of Data, Certificate-Based Authorization.

PKI efficiently alter security problems into key management issues. Main key feature of this proposed solution depends on controlling access to private key.

As the performance depends on network availability is important in cloud. Quality of Service is a key issue, also in host-to-host communication. Continuous encryption/decryption process consumes high bandwidth and may effect performance of network along with additional process. Cloud infrastructure rigidity of on demand CPU can reduces this burden or system overhead and speed up encryption/decryption.

V. CONCLUSION

Certainly cloud computing will support additional characteristics of IS. Weakness of traditional IS cand be addressed by deployment model or architecture of Cloud computing. This paper identified general design principles of a cloud environment which tries to control vulnerabilities and threats. To do so, software engineering and IS design approaches were adopted. Security in a cloud environment can be built on trust, mitigating protection to a TTP. A combination of PKI, LDAP can identify most of the cloud computing threats which are related with integrity, confidentiality, authenticity and availability of data and communications. The proposed solution offers horizontal level of service, available for all concerned entities which require security in federations (cloud computing federation), in which critical trust can be maintained.

REFERENCES

[1] Dimitrios Zissis , Dimitrios Lekkas, Addressing cloud computing security issues, Elsevier, Future Generation Computer Systems 28 (2012) 583–592 2012.

[2] K. Stanoevska-Slabeva, T. Wozniak, Grid and Cloud Computing-A Business Perspective on Technology and Applications, Springer-Verlag, Berlin, Heidelberg, 2010.

[3] National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.

[4] E. Naone, Technology overview, conjuring clouds, MIT Technology Review, July–August, 2009.

[5] Merrill Lynch, The cloud wars: $100+ billion at stake, Merrill Lynch, 2008.

[6] D. Harris, Why 'grid' doesn't sell, 2008

[7] G. Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, in: Theory in Practice, O'Reilly Media, 2009

[8] B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems (2009).

[9] A. Nagarajan, V. Varadharajan, Dynamic trust enhanced security model for trusted platform based, Future Generation Computer Systems (2010) doi:10.1016/j.future.2010.10.008.

[10] International Telecommunication Union, X-509 | ISO/IEC 9594-8, The directory: Public-key and attribute certificate frameworks, ITU, X-Series, 2001.

[11] D. Lekkas, Establishing and managing trust within the public key infrastructure, Computer Communications 26 (16) (2003).

[12] A. Giddens, The Consequences of Modernity, Polity Press, UK, 1991.

[13] R. Sherman, Distributed systems security, Computers & Security (1) (1992).

[14] D. Lekkas, S. Gritzalis, S. Katsikas, Quality assured trusted third parties for deploying secure Internet-based healthcare applications, International Journal of Medical Informatics (2002).

[15] National Institute of Standards and Technology. Guide for mapping types of information and information systems to security categories, NIST 800-60, 2008.

[16] Gartner. Assessing the security risks of cloud computing, Gartner, 2008.

[17] D. Polemi, Trusted third party services for health care in Europe, Future Generation Computer Systems 14 (1998) 51–59.

[18] UK Federation Information Centre, UK federation information Centre, 2007

[19] C.P. Pfleeger, S.L. Pfleeger, Security in Computing, Prentice Hall, 2002.