**Cloud Computing Security**

Om Lohakare

B. E. III

ACPCE

**Abstract:**

The recent emergence of cloud computing has drastically altered everyone’s perception of infrastructure architectures, software delivery and development models. Projecting as an evolutionary step, following the transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapid transition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. From a security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. As a result the aim of this paper is twofold; firstly to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.

**Keywords:** Cloud Computing; Security; Trusted Computing; Data integrity and confidentiality; Survey;

**Introduction:**

Cloud Computing is becoming a popular option for renting of computing and storage infrastructure services, for remote platform building and customization for business processes; and for renting of business applications as a whole. The cloud infrastructure has been further sub-divided into public cloud - where the infrastructure resides totally outside of the tenant / enterprise firewall; hybrid cloud - where the infrastructure and business processes reside partly within the enterprise and partly consumed from third party and private cloud - where IT services are mounted on top of large-scale conglomerated and virtualized infrastructure within enterprise firewall and consumed in “per transaction” basis. Technology consulting firm Gartner had an estimated market size of $149 billion in 2014 for Public and Hybrid cloud. However, real and perceived security concerns remain one of the greatest inhibitors for adoption of Cloud Computing. The primary concerns for cloud security are around cloud infrastructure, software platform and user data; as well as access control and identity management. Researchers also include broader issues like data integrity and compliance under security. Additionally, physical data center security and processes play an important role.

There is a growing body of work dealing with various cloud computing security issues. Authors have mostly discussed about singular aspects of cloud security such as vulnerabilities in platform layer (virtualization, network, or common software stacks); vulnerabilities with co-located user data and multi – tenancy; access control; identity management and so on. Recently, a draft report by NIST discusses some security challenges and considerations that organizations planning to utilize public cloud environment should be aware of. However, barring a few, there has not been a holistic treatment on cloud security issues and state of research in each of these issues.