OVERVIEW OF CLOUD COMPUTING ARCHITECTURE: SERVICE DELIVERY MODELS, SECURITY& PRIVACY ISSUES AND TRUST

K.V. K Mahesh Kumar

Research Scholar, Department of Computer Science and Engineering, Acharya Nagarjuna University, A.P, India, ***maheshkondraju@gmail.com***

Abstract

This Research paper explores cloud computing architecture, service delivery models, Security & Privacy Issues and Trust Challenges. Evaluates all three service delivery models Software-as-a-Service (Saas), Platform-as-a-Service (PaaS) and Infrastructure-as-a-service (IaaS) and their deployment, requirements and services they provide. In the next section Security & Privacy Issues has been discussed and focus is on potential reasons for them to cause. Also discusses the lack of common cloud security standards with constructive discussion on public cloud providers and on their proprietary security standards. Overview on Challenges with Trust between Cloud provider and cloud user and suggests solutions for inculcating trust among cloud provider and cloud user with the help of trusted thrid party. Solutions and recommendations are suggested to safeguard user Data in the cloud by implementing Data security measures such as use of Crypotography and Trusted platform module (TPM), Data integrity etc. This research paper also focuses on future scope of cloud computing and its evolution in the field of outsourcing and urges on the need of global security standards for mitigating security issues, privacy threats and Trust challenges for wide acceptance of cloud computing in organizations.

Keywords: *Cloud Computing Challenges, Service Delivery Models, Data Security, Security & Privacy Issues, Trust*

----------***----------

1. INTRODUCTION

Now a days Cloud Computing has been center of focus for organizations and software companies for some time but there seems to be no clarity on how effective cloud computing can be due to the factors evolving around Cloud Providers due to the use of their proprietary models and standards [1]. Cloud providers are using different service delivery models which can be differentiated based on the level of virtualization they offer, there are mainly three service delivery models Plaform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service SaaS). These three models together constitute as SPI Model where S stands for Software, P stands for Platform and I stands for Infrastructure [2], [3].

1.1 Software-as-a-Service (SaaS)

In this model Software is provided as a service where cloud user can access the software from his web browser without the concerns of deployment or installation & maintenance. With the advent new & faster HTML 5 standards graphically rich applications can be run smoothly at 60 Frames per second just like running our software on our own personal computers. This service model depicts one to many function as single application running as a service on the server side with many client end users can run it from their web browser simultaneously as they are connected as services [2], [3].

For example let us consider Google Play Store where applications can be purchased on the go and can be run from the web browser, any number of people can purchase and run the application simultaneously but only one instance of the application is running on the server side. This helps in reducing costs on resources and on the customers point of view it is hassle free process service on demand where Cloud user can rent applications without the need of installation and maintenance of the software [2], [3].

1.2 Platform-as-a-Service (PaaS)

This delivery models allows the user to build & develop his own applications using programming languages and tools available on the the cloud provider infrastructure. This kind of service delivery model is useful in situation where the cloud user can deploy his applications on to the cloud with complete control on the applications. But there are few challenges in this service model, where cloud user cant have the control over the machine where it is hosted or deployed, as cloud user cant control or manage cloud infrastructure, operating systems, data storage and network servers. Another challenge in this Platform-as-a-service is where Cloud providers offer pre-defined operating systems and servers to host or deploy applications, So meeting the requirements of software deployment is an issue [3], [7]. For example if an application is compatible with only .Net 4.5 and the operating system deployed by the cloud provider might only Supporting .Net 3.5, So there might be few restriction while deployment of applications

1.3 Infrastructure-as-a-Service (IaaS)

This model delivers basic cloud comuting capabilities such as providing storage systems over the network for rentals or pay as you go. Even this model supports deploying application and software running arbitrary as well as has the control over the operating systems deployed in the cloud by the provider, socloud user here acts as an administrator. So changes to the operating systems, failure & crashes in the operating system and data securityis crucial in this service model [3], [7].

All these service deliverymodels are interconnected to each other or in simple words Infrastructure-as-a-service(Iaas) is the base or foundation of the cloud computing architecture where as Platform-as-a-service (PaaS) is built up on Infrastructure-as-a-service (IaaS) and finally Software-as-a-service (SaaS) is built up on Platform-as-a-service (PaaS) [3], [7].

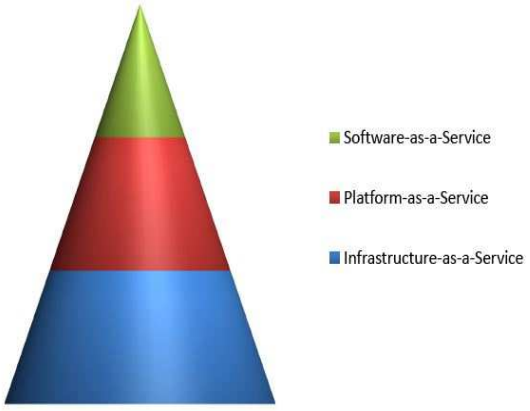


Fig-1: Cloud Computing Stack

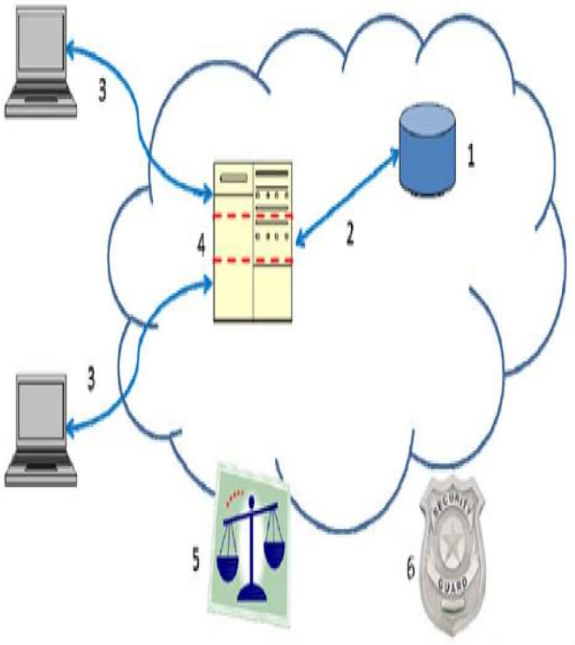
2. SECURITY ISSUES

Cloud computing due to its architectural design and characteristics imposes a number of security benefits such as centralization of security, data and process segmentation, redundancy and high availability. Though many traditional risks are mitigated effeciently, due to its infrastructures singular characteristics many security challenges have arised. Cloud computing has "unique attributes that require risk assessment in areas such as data security, availability reliability issues and data integrity" [7], [10], [11].

2.1 Data Security

In cloud computing securing data of the cloud user is at most important than anything else and it needs to be secured in various transition states between the virtual machines equipped in the cloud to the physical machines used by the end users. There are six key areas where data needs to be secured

- Security of data at rest
- Providing security for the data in transition
- Authentication of Users, Applications and Services
- Data separation between users on the fly
- Legal and regulatory issues
- Generating incident response



Fig– 2: Areas of Security concerns in cloud computing

Data security and confidentiality can be achieved with the use of cryptographic protocols and trusted platform modules (TPM) used for migration of data between virtual machines and physical machines. Technologies such encrypted storage firewalls are useful in ensuring safe data access and storage [13], [14], [15], [16].

2.2 Data Integrity

Data Integrity means protecting data from unauthorized deletion, modification or fabrication. Protecting users admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated or stolen. Data Integrity and system integrity in organizations can be achievedby preventing unauthorized access. Data integrity mechanism"offers the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity"[4], [12].

2.3 Availability

System readily available, accessible and useable to an authorized user even at tough situations where there is a possible chance security breach. This approach of cloud

computing where hardware, software and personal data made available to authorized and loyal cloud users at tough times but this results in congested network for data retrieval and processing and burdens cloud provider with additional costs in acquiring network servers [6], [10].

3. PRIVACY ISSUES

In cloud computing privacy plays a major role in protecting users from their individual rights but in multi domain environments and service oriented architecture it is important to implement multi domain policy integration and secure service composition. There are five key areas where privacy for cloud users is at stake they are

- Authentication and identity management
- Access control and accounting
- Trust management and policy integration
- Secure service management
- Privacy data protection
- Organizational security management [4], [9], [12]

4. TRUST

Trust in cloud computing varies from platform to platform and depends on deployed service delivery model [5].

For example in public cloud, control is reduced only to the infrastructure owner to implement necessary security policy such that appropriate security measures are being planned & performed to mitigate therisk. This delivery model introduces risks and threats, as security is based on trusting the cloud provider[5] [12]. Whereas in private cloud infrastructure is deployed within the premise of the organizations, therefore management and control over the infrastructure is with the organizations and thus it does not introduces any additional security threats as trust remains within the organization but it incurs costs in maintaining the infrastructure as infrastructure owner remains the owner of data and process [5] [12].

Trust plays an important role in cloud computing, Trust in other terms can be stated as reliability on the part of cloud providers. Cloud provider should be reliable and should meet the expectations of the user, So trust can be developed by achieving credibility and being loyal to the user in safeguarding the user data, effectively executing security mechanisms, exhibiting expertise in reducing risk & threats and should acknowledge the users certainty about the cloud provider in providing required services accurately [3] [4][6].

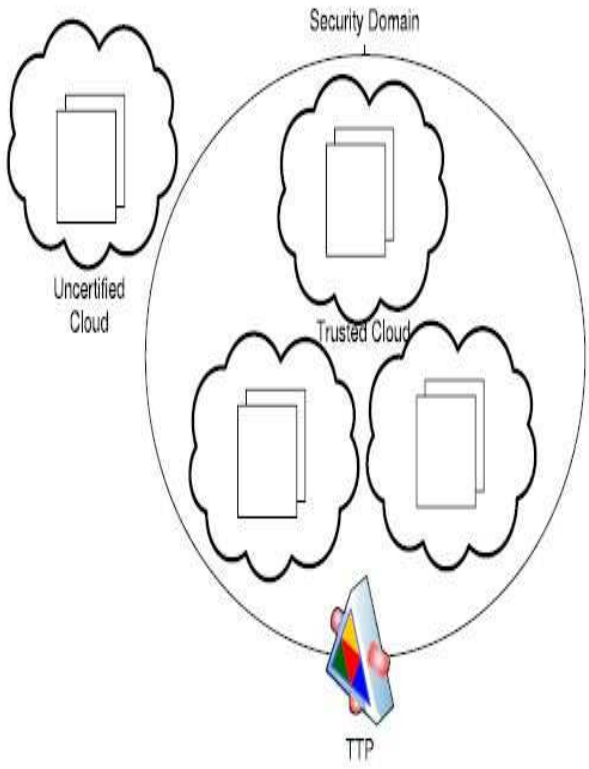


Fig – 3: Trusted Third Party in cloud

Trusted third party (TTP) plays a major role multi-level distributed computing. Trusted third party provides end-to-end security services which are ethical in standard and uses cryptography to ensure confidentiality, integrity and authenticity of data communicated. Trusted third party is an independent ideal security facilitator in cloud computing environment where it provides trusted securitydomains & establishes secure connections and interactions between cloud provider and users[3][6][8].

CONCLUSION

Cloud computing is currently one of the most happening area where organizations are attracted towards it due to its flexibility and cost effective architecture. Though cloud computing is much anticipated there exists many challenges with the architecture and service delivery models used by various cloud providers. Actual problem lies with the lack of global standard in cloud computing and each cloud service providers using their own proprietary models in deploying their infrastructure which indeed leads to Data Security and Privacy issues. At the same time building Trust from cloud users has been a big challenge.Cloud computing looks like a potential contender in the future in areas outsourcing and reducing cost of resources for software companies or Independent software vendors but unless and until all existing cloud provider organizations form into a single large global

group to introduce guidelines and standards for cloud computing, it is tough on the part of software companies or Independent software vendors to trust cloud providers for reducing outsourcing and resource costs.

REFERENCES

[1]. A. Giddens, the Consequences of Modernity, Polity Press, UK, 1991.

[2]. Chen, Y., Paxson, V., & Katz, R.H. (2010). What's New About Cloud Computing Security? Technical Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley, 2010.

[3]. Cloud Security Alliance (CSA)'s Security Guidance for Critical Areas of Focus in Cloud Computing (2009). CSA, April 2009.

[4]. Cloud Security Alliance. Top threats to cloud computing, Cloud SecurityAlliance, 2010.

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

[6]. Everett, C. (2009). Cloud Computing- A Question of Trust.*Computer Fraud & Security*, Vol 2009, Issue 6, pp. 5-7 June 2010.

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

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

[9]. Joshi, J.B.D., Bhatti, R., Bertino, E., &Ghafoor, A. (2004). Access Control Language for Multi-domain Environments.*IEEE Internet Computing*, Vol 8, No 6, pp. 40-50, November 2004.

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

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

[12]. R. Sherman, Distributed systems security, Computers & Security 11 (1) (1992).

[13]. Sen, J. (2010a). An Agent-Based Intrusion Detection System for Local Area Networks.*InternationalJournal of Communication Networks and Information Security (IJCNIS)*, Vol 2, No 2, pp. 128-140,August 2010.

[14]. Sen, J. (2010b). An Intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks. In *Proceedings of the 2nd IEEE International Conference on Intelligence in Communication Systems andNetworks (CICSyN'10)*, pp. 202-207, July, 2010, Liverpool, UK.

[15]. Sen, J. (2010c). A Robust and Fault-Tolerant Distributed Intrusion Detection System.In *Proceedings of the 1st International Conference on Parallel, Distributed and Grid Computing (PDGC'10)*, pp. 123-128,October 2010, Waknaghat, India.

[16]. Trusted Computing Group (TCG)'s White Paper (2010). Cloud Computing and Security- A Natural Match. Available online at: http://www.trustedcomputinggroup.org (Accessed on; January 2013).

BIOGRAPHY

K.V.K Mahesh Kumar holds a B.E. (Bachelor of Engineering) in Computer Science from Osmania University, Graduate Diploma in Professional Computing & Masters in ICT (Information and Communication Technology Management) from University of South Australia and is currently pursuing Ph.D. in Cloud Computing from Department of Computer Science and Engineering at Acharya Nagarjuna University. He has been involved in many diversified research projects and published several papers in international journals in the research areas of HCI (Human Computer Interaction), EHR (Electronic Health Record) systems, E-Business & E-Commerce, Web 2.0 Social Networking, Project Management and Knowledge Management.