ISSN:0975-9646

Addressing the Security, Privacy and Trust Challenges of Cloud Computing

Rama Krishna Kalluri[#], Dr. C. V. Guru Rao[*]

[#] *Department of Computer Applications, Vasavi college of Engineering, Hyderabad, India*
[*] *Department of Computer Science and Engineering, SR Engineering College, Warangal, India*

***Abstract*— Cloud Computing has emerged as a new paradigm of computing, that builds on the foundations of Distributed Computing, Grid Computing, and Virtualization. Cloud computing is a business model with flexible resource allocation on demand, Internet-accessible, computing on a pay-per-use as utilities. Cloud computing has grown to provide a promising business concept for computing infrastructure, where concerns are beginning to grow about how safe an environment it is. Security is one of the major issues in cloud computing environment. The aim of this paper is, to address the security, privacy and trust challenges of cloud computing, and we proposed some solutions by analyzing the technological, operational and legal issues of cloud computing, taking into consideration of cloud customers.**

***Keywords*- Security, Privacy, Trust, Encryption, Web services**

I. INTRODUCTION

Cloud computing is the latest approach to provide computing infrastructure, with the purpose to shift the location of the computing infrastructure to the network in order to reduce the cost of management and maintenance of hardware and software resources. All these resources are provided as services to customers an as-needed basis. Companies are moving to the cloud according to a study by the Pew Internet & American Life Project, 66 percent of Americans are connected to the Web for some kind of cloud services as online hard drive back up to store files and personal photos, Blogs, wikis and social networks. Defining cloud computing for the purposes of this study, we adopt a definition of cloud computing proposed by the United States National Institute for Standards and Technology (NIST) [1]:

"Cloud computing is 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 service provider interaction".

Cloud computing uses three Service models and three Deployment models [2][3].

Three Service models:

- ***Software as a Service (SaaS)***, where applications are hosted and delivered online via a web browser offering traditional desktop functionality.

Example: Google Docs, Gmail and MySAP.

- ***Platform as a Service (PaaS)***, where the cloud provides the software platform for systems (as opposed to just software).

Example: Google App Engine.

- ***Infrastructure as a Service (IaaS)*,** where a set of virtualized computing resources, such as storage and computing capacity, are hosted in the cloud; customers deploy and run their own software stacks to obtain services.

Example: Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3) and Simple DB.

Three Deployment Models:

- ***Public Cloud*** The cloud infrastructure is available to the general public. The services are offered to individuals and organizations. Public cloud users are by default treated as untrustworthy.
- ***Private Cloud*** The type of the cloud that is available solely for a single organization (provided exclusively to trusted users).
- ***Hybrid Cloud*** This is a cloud infrastructure that is a composition of two or more clouds i.e. private, community or public (Cloud Security Alliance, 2009, p17).

This paper is organized as follows. In section II, we briefly describe the related work. In section III, we describe the Cloud Computing Security, Privacy and Trust Challenges. In section IV, we proposed some solutions to Cloud Computing Security, Privacy and Trust Challenges. In section 5, we conclude.

II. RELATED WORK

Cloud security has become an important issue in industry. Various international conferences and International journals have focused on this subject, such as *International Journal of Cloud Computing*(IJCC), *Journal of Cloud Computing*- a springer Open Journal, *Association of Computer Machinery*(ACM) workshop on *Cloud Computing Security*, the *International conference on Cloud Security Management* and European conference on *SecureCloud* etc.,

Jinwei Hung and David M Nicol [4] have focused on conceptual basis for analysis of trust in cloud by suggesting a framework for integrating various trust mechanisms based on evidence, certification and validation.

Rashmi, Dr.G.Sahoo, and Dr. S. Mehfuz [5] made analysis on existing security challenges in Software as a Service (SaaS) based on a detailed survey and proposed solutions.

The survey paper [6] of "*Security and privacy in Cloud Computing: a Survey",* the security topic was discussed keeping in view Confidentiality, Data Integrity, Availability, and Control and audit properties.

The related work defined above is the basis for our work.

III. CLOUD COMPUTING SECURITY, PRIVACY AND TRUST CHALLENGES

Security, Privacy, [7] and Trust are the three major concerns about cloud computing. In the cloud computing world, the virtual environment lets user access computing power that exceeds that contained within their physical world. To enter this virtual environment a user is required to transfer data throughout the cloud. Consequently several security concerns arise. Before assessing Security concerns of Cloud Computing we will start our discussion by defining the Security, Privacy and trust.

A. Defining security, privacy and trust

• **Security** is all about the maintenance of the confidentiality, availability and integrity of data or information. Security may also include authentication, reliability, non-repudiation

and accountability. The fundamental property of security is the information or data must not be disclosed to any unauthorized person.

• **Privacy** is a fundamental human right which concerns the expression of various legal and non-legal norms regarding the right to private life. Privacy also talks about the protection and appropriate use of the personal data. Organizations manage the privacy using application of laws, polices, standards and processes. The globally accepted privacy principles: consent, purpose restriction, legitimacy, transparency, data security and data subject participation.

• **Trust** can be defined [8] as "*Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another"*. It revolves around 'assurance' and confidence that people, data, entities, information or processes will function or behave in expected ways. Trust may be human to human, machine to machine, human to machine, or machine to human. Trust can be regarded as a consequence of progress towards security or privacy objectives.

B. Security, Privacy and Trust related questions to be answered.

Due to its open nature, Cloud Computing raises strong security, privacy and trust concerns. This approach to delivering computing power and processing has prompted questions about the security and privacy of information in the cloud [8].

- Are data safely stored and handled by Cloud providers?
- How about data privacy?
- Are Cloud providers adhering to rules and regulations?
- Are Cloud providers sufficiently protected against cyber-attacks?

C. Top Threats identified in the Cloud Computing

The Cloud Security Alliance (CSA) has identified the following top threats:

- Abuse and Nefarious use of cloud computing
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Service Hijacking

D. Challenges of Cloud Computing due its Underlying Technologies

By the definition of cloud computing (by NIST), a number of challenges for security, privacy and trust [1] from the underlying technologies (virtualization technology, grid computing, web services, service-orientated architectures, web application frameworks and encryption) of cloud computing are:

Area/ Technology	Security	Privacy	Trust
Virtualization	Integrity	Segregation of personal data on shared infrastructure	Compromised virtual machines/ hypervisors permit loss of trust
Grid technology	Availability		Interoperability
Web services	Integrity and confidentiality	Security and confidentiality	Interoperability
Service-orientated architectures	Integrity		The reliance of distributed systems on different security credentials
Web application frameworks	Integrity and availability		Trust across distributed environments
Encryption in the cloud context	Confidentiality	Security and confidentiality	

Table 1. Challenges of cloud computing

***Challenges identified separately for Security, Privacy and Trust*[9]**

E. Security challenges of Cloud computing:

Cloud computing is not secure by nature. The Security risks depend on the cloud services and deployment model. The security challenges related to Cloud computing are:

Users control over Cloud resources - Cloud users typically have no control over the Cloud resources. There is a risk of data exposure to third parties on the Cloud or the Cloud provider itself. From a security perspective, data containers of the Cloud computing has to ensure that each user can at best enjoy control over its data or information.

Data secrecy & confidentiality - Encrypting data is a common practice to protect secrecy and confidentiality of data. End-users may hold the decryption keys - still poses some technical challenges.

Access control and use of the data - The cloud computing requires the identity and access control management measures. When data are trusted to a third party for handling or storage within a common user environment, precaution must be taken to ensure uninterrupted and full control of the data.

Application & Platform Security - The application, which was developed for internal use, is now being used in cloud computing environment without addressing the risks of new technology. Migration to Cloud computing (the secure development lifecycle of the organization) may need to change to accommodate the Cloud computing risk context.

F. Privacy challenges of Cloud computing:

In the Cloud-computing environment, Cloud providers, can host or store important data, files and records of Cloud users. It is difficult for companies and private users to control the information or data all times they entrust to Cloud suppliers. Some key privacy challenges as particular to the Cloud-computing context are:

Sensitivity of information - Any type of information can be hosted, or managed by the Cloud providers. The information may be highly confidential or extremely valuable as company asset. Then entrusting this information to a Cloud increases the risk because there is a possibility of cloud platform sharing by the competitors.

Users right to access the data - The users of the same Cloud share the premises of data processing and the data storage facilities, they are exposed to the risk of data or information leakage, either by accidental or intentional.

Data transfers to different locations - If the data on the Cloud change the location regularly or reside on multiple locations, it becomes complicated to watch the data flows. Data transfers to other countries require arrangements to be placed. It will be complicated to fulfill these arrangements if data locations are not stable.

Externalization of privacy - Companies engaging in Cloud computing expect that the privacy commitments they have made towards their customers, employees or other third parties will continue to apply by the Cloud computer provider.

G. Trust challenges of Cloud computing:

Trust is critical barrier that must be passed. Cloud customers must trust the cloud providers. Providers must trust customers with access to the services which may leads to security issue. If Cloud providers succeed in providing the solutions to Security and Privacy we can say that they have succeeded in achieving the trustworthy services in cloud computing all most. By this they can enhance user's confidence in the application of Cloud computing and would build market trust in the Cloud service offerings.

Joining the Cloud by users/resources dynamically – In cloud computing environment many users or resources join and leave cloud dynamically. Users, resources and the cloud should establish the trustful relationship among themselves and they should accommodate the change which is happening dynamically.

Different Security policies – The cloud environment consists distributed users and resources from different local systems may have different security policies. In this situation the question arises is how to build a suitable relationship among them?

Continuity and Provider Dependency - The complexity of Cloud architectures and the lack of transparency will increase the security risk. In many Cloud implementations, the centralized management and control introduces several single points of failure. These could threaten the availability of Cloud users' data or computing capabilities indirectly.

Compliance with applicable regulations and good practices - Once the applicable law to a Cloud service is determined, the provider will need to comply with other regulations such as privacy, General civil law and contract law, Consumer protection law, etc.,

Trust enhancement through assurance mechanisms- The Cloud-computing concept cannot guarantee full, continuous and complete control of the Cloud users over their assets. For these reasons, the establishment of appropriate "checks and controls" to ascertain that Cloud providers meet their obligations becomes very relevant for Cloud users.

IV. PROPOSED SOLUTIONS TO CLOUD COMPUTING SECURITY, PRIVACY AND TRUST CHALLENGES:

For the above specified Cloud Computing Security, Privacy and Trust Challenges, the following measures needs to be considered (Some proposed solutions).

A. The steps to be considered when moving to Cloud environment:

Adapting a few guidelines will help protect users on the cloud environment. Cloud security mechanisms can be of two different categories: Partner-based (Security for SaaS, PaaS, IaaS) or User-based (client based).

- **Strategically plan your cloud security -** Considering security during the initial planning phase creates solid foundation. Careful considerations must be taken how corporate workloads should be delivered to end users.
- **Select the Cloud provider –** It is crucial to choose a cloud provider which can protect your sensitive information or data. Before selecting cloud provider check whether they have experience in both IT and security services for their strategic service performance assurances.
- **Find the written document about security measures provided by the cloud provider –** This means getting assurances from the cloud provider written into the contract. The document must include applications, infrastructure, configurations, policies, rules and regulations.
- **Find out who will monitor your data –** Find out who will access to data and why and when they are accessing it.
- **Have a plan for Security issues –** What responsibility the cloud provider is promising, and what actions he will take during and after the security issue must be checked.
- **Verify the access controls being used [3] –** Verify the access controls imposed on the data to ensure that the third parties cannot access the data. It is important to clearly define roles and responsibilities to ensure that even privileged users cannot circumvent auditing, monitoring and testing, unless otherwise authorized.
- **Monitoring system –** Cloud provider must continuously monitor data in the cloud. Establish cloud performance metrics and test regularly.

B. Measures to be taken for the top threats identified in the Cloud Computing

For ***Abuse and Nefarious use of cloud computing***

- Care must be taken in Initial registration and Validation process.
- To use credit card in Cloud computing an Enhanced fraud monitoring system must be implemented.
- Monitoring public blacklists for one's own network blocks.

For ***Insecure Interfaces and APIs***

- Cloud providers interfaces security model must be analyzed properly.
- Strong authentication and access controls must be implemented.
- Understand the dependency chain associated with the APIs.

For ***Malicious Insiders***

- Identify the human resources requirements as a part of legal contracts.
- Information security, management practices requires transparency.
- Decide Security breaches.
- Conduct survey on comprehensive supplier assessment and implement strict supply chain management.

In case of ***Shared Technology issues***

- Best Security practices must be implemented for installation or System configuration.
- Unauthorized activities must be monitored.
- Service level agreements must be enforced.
- Configuration audits and vulnerability scanning must be conducted.
- Strong authentication and access control administrative access.

For ***Data loss or Leakage***

- Implement strong API access control.
- Specify backup and retention mechanisms
- Analyze data protection at both design and run time.
- Necessary measures must be taken for strong key generation, storage, and destruction practices.

With respect to ***Account or Service Hijacking***

- Strong monitory system implementation for to detect unauthorized activity.
- Sharing of account details between users and services must be avoided.
- Read and understand properly cloud security policies.

C. Security requirements need to be considered with respect to service models and cloud deployment models:

The Cloud computing security system has identified six basic and very important Security requirements. And if these security requirements were handled properly we can say that we have succeeded.

A cloud customer needs to check the security state of the cloud model before selecting cloud provider. For this an assessment must be performed in terms of security requirements. The following table 2 gives six security requirements with respect to Cloud Service Models and Cloud Deployment Models [10].

Security Requirements	Cloud Deployment models								
	Public Cloud			Private cloud			Hybrid Cloud		
Identification & Authentication	√	*	√	√	*	√	*	*	√
Authorization	√	√	√	*	*	√	*	*	√
Confidentiality	*	*	√	*	√	√	*	*	√
Integrity	√	*	√	*	√	√	√	√	√
Non-repudiation	*	*	√	*	*	√	*	*	*
Availability	√	√	*	√	√	√	*	*	*
	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS
	Cloud Service Models								

Table 2. Security Requirements

(A Check mark (√) indicates requirement in the Cloud Service Models and Deployment models, while the asterisk (*) indicates optional)

Identification and authentication methods [11] include passwords, smartcards and biometrics. Authorization or access control refers to a set of security polices which defines users' permissions to accesses the resources in the cloud. Depending on the way that the security policies are specified, accesses control can be categorized into different models.

D. Encryption approach:

Encryption is a core mechanism for maintaining the confidentiality of all data, whether it consists of business, personal or sensitive information, and it can also be used to establish the integrity of various transactions, code and data. Encryption will be considered as a security control, on maintaining confidentiality and integrity. The uses of encryption in accessing services in the cloud are similar to data protection as conventional technologies. Many public offered services are provided via an HTTPS-protocol connection to a web service, which works on the concept of Secure Socket Layer (SSL) protection.

V. CONCLUSIONS

Cloud providers have to safeguard the Privacy and Security of personal and confidential data of organizations and users to provide and support trustworthy cloud computing services. We have reviewed many papers related to Cloud security, privacy and trust issues, and discussed the various security challenges faced by the Cloud computing by proposing some solutions. This is not an exhaustive and may not constitute a complete representation with respect to the rapid and dynamic pace of technological change.

REFERENCES

[1] Wayne A. Jansen, NIST "Cloud Hooks: Security and Privacy Issues in Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences – 2011

[2] S. Subashini, V. Kavitha, "A Survey on Security issues in Service delivery models of Cloud computing" available at "Journal of Network and Computer Applications"(2010), doi:10.10.16/j.jnca.2010.07.006 http://www.elsevier.com/locate/jnca

[3] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", grid Computing and Distributed Systems and Software Engineering, The University of Melbourne, Australia.

[4] Jingwei Huang and David M Nicol, "Trust mechanisms for Cloud Computing", Journal of Cloud Computing: Advances, Systems and Applications 2013, 2:9, Springer Open Journal.

[5] Rashmi, Dr.G.Sahoo, Dr.S.Mehfuz, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.4, August 2013.

[6] Zhou M, Zhang R, Xie W, Zhou A (2010) "Security and Privacy in cloud computing: a Survey", In 6th international conference on semantics knowledge and grid(Ningbo, China, 2010), pp 105-112.

[7] Jon Brodkin, "Gartner: Seven Cloud-Computing Security Risks", Available: http://www.infoworld.com, published July 2008, pp. 1-3.

[8] Patrick Callewaert, Erik Luysterborg, "Cloud computing Forecasting change", Security, privacy and trust Consulting - Enterprise Risk Services

[9] Saini Pearson. "Privacy, Security and Trust in Cloud computing", HP Laboratories, appeared as a book Chapter by Springer, UK, 2012.

[10] Ramgovind S, Eloff MM, Smith E(2010), "The Management of Security in cloud computing" Information security for south Africa, Johannesburg, South Africa, pp 1-7.

Lan Zhou, Vijaya Vardharajan and Michael Hitchens, "Cryptogralphic Role-Based Access control for Secure Cloud Data Storage Systems", @ Springer Heidelberg New york Dordrecht London.