Security Issues in Cloud Computing

Pardeep Sharma[1], Sandeep K. Sood[2], and Sumeet Kaur[1]

[1] Computer Science & Engineering Guru Kashi Campus,
Punjabi University, Talwandi Sabo, India
shah4ash@yahoo.co.in, purbasumeet@yahoo.co.in
[2] Department of Computer Science & Engineering,
Guru Nanak Dev University, Regional Campus, Gurdaspur, India
san1198@gmail.com

Abstract. The cloud is next generation platform that provides dynamic resource pooling, virtualization and high resource availability. It is one of today's most enticing technology areas due to its advantages like cost efficiency and flexibility. There are significant or persistent concerns about the cloud computing those are impeding momentum and will compromise the vision of cloud computing as a new information technology procurement model. A general understanding of cloud computing refers to the concept of grid computing, utility computing, software as a service, storage in cloud and virtualization. It enables the virtual organization to share geographically distributed resources as they pursue common goals, assuming the absence of central location, omniscience and an existing trust relationship. This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.

Keywords: Cloud Computing, Hypervisor, Privacy, Security and Virtualization.

1 Introduction

Cloud computing is a dream of computing as a utility. It makes software more attractive as a service and shaping the way as information technology hardware is designed and purchased. Cloud computing is defined as applications delivered as services over the Internet, hardware and system software in the datacenters that provides services. These services are called software as a service (SAAS). The datacenter hardware and software is known as a cloud .The foundation of cloud concept is based on the lease manner. The idea of cloud computing was very popular in the late 1960s when researchers thought about the utility computing. But in the mid-1970s this idea was attenuated when it became clear that companies of the day were unable to sustain such a futuristic computing model. However, with the increasing demand of computation resources, the concept has been revitalized. With the growth in Internet technology concepts such as search engines, the term cloud computing began to emerge in technology circles [1- 3]. The concept of cloud computing becomes more understandable when enterprises begins to think about what modern information technology environments always require. Modern information technology environments always like to increase capacity or add capabilities to their infrastructure dynamically, without

A. Mantri et al. (Eds.): HPAGC 2011, CCIS 169, pp. 36–45, 2011.

investing in new infrastructure. Given a solution to the aforementionedneeds, cloud computing models encompass a subscription-based or pay-per-use paradigm [4].It provides a service that can be used over the Internet and extends an information technology shop's existing capabilities. This approach provides a return on investment that companies are aiming for since decade. The tremendous growth of the Web over the last decade has given rise to a new class of web scaling problems and challenges such as supporting thousands of concurrent e-commerce transactions or millions of searchqueries in a minute. It has become a large and growing market because of its value propositions of low costs, increased flexibility, and shorter time to market.Security issues in cloud computing are hampering the interest of perspective organizations. There have been a lot of proven security attacks on different cloud computing providers such as Google (Gmail, App Engine), Amazon Web Services (Amazon S3), Salesforce.com (Salesforce.com) **etc.** Security is one of the main concerns in cloud computing environment [5].

This paper is organized as follows. In Section 2, we introduce the literature review which is classified as different types of effort done in security aspects with their advantages and disadvantages. In Section 3, we describe the challenges of the cloud. In Section 4, we describe the different service models. We describe Deployment models in Section 5. In Section 6, we show the comparison of deployment models in terms of security requirements. In Section 7, we propose future research directions and Section 8 concludes the paper.

2 Literature Review

In 2000, Yamaguchi and Hashiyama [6] proposed concept of Reconfigurable Computing technique for encryption processing. Reconfigurable Computing (RC) is capable of accelerating the information processing using dynamic reconfiguration of Field Programmable Gate Arrays (FPGAs). Dividing the target problems into hardware and software processing appropriately, the computation time will be less. It is one of the aims of researchers to have fast and flexible encryption technique in the Internet. Encryption technique generally consumes more computational power and needs specific hardware for feasible implementation. Moreover, these techniques are computational intensive. They implemented RC system onto FPGA board. In this technique, they developed application specific IC (ASIC) but this process has a problem of scaling. It is suitable for real time problems only.

In 2009, Yuefa et al. [7] suggested the concept of hadoop distributed file system (HDFC) architecture for the data security requirement of cloud computing. They use the same file system as the Google uses named as Google file system (GFS). This model works only in open system.

In 2010, Tribhuwan et al. [8] proposed a method to enhance the security of data stored in the cloud by utilizing the concept of homomorphic tokens and distributed verification of erasure coded data. This method attains the integration of storage correctness insurance and data error locations. They introduces a new two way handshake scheme which is based on the token management method but this method does not work properly for maintaining the integrity and confidentiality of data.

In 2010, Brandic and Dustdar [9] proposed a novel approach for compliance management in clouds, termed as Compliant Cloud Computing (C3). They used novel languages for specifying compliance requirements which concernedabout security issues, privacy and trust, by leveraging domain specific languages and compliance level agreements. They proposed C3 middleware architecture. In this, the middleware is responsible for the deployment of certifiable and auditable applications, for provider selection with the user requirements.

In 2010, Ramgovind et **al. [10]** purposed overall security perspective for cloud computing with the aim to highlight the security concerns. They tried to address the cloud computing concerns and also remained successful to some extend to realize the full potential of Cloud computing. Some of the most important issues in Cloud computing are like data storage and data localization in the cloud. They also addressed problems like how the organization will deal with new and current cloud compliance risks. It helps for cloud computing implementation. It deals with the potential impact of cloud computing on the business concerning governance and legislation. They discussed how cloud computing may affect the organization in terms of its business intelligence and intellectual property by potentially influencing its market differentiation.

In 2010, Almulla and Yeun [11] **discussed** challenges regarding information security concerns as confidentiality, integrity and availability. Most of the organizations are very much concerned about the security issues and the ownership of the data. However, they have not addressed security challenges for cloud computing including Identity and Access Management (IAM). They presented the current state authentication, authorization and auditing of users by accessing the cloud along with the emerging IAM protocols and standards.

In 2010, Somani et al. [12] suggested the cloud storage and data security in the cloud by implementation of digital signature with RSA algorithm. In Digital Signature, software will crunch down the data, document into just a few lines by a using hashing algorithm. They also suggested cloud challenges and responsibilities. They proposed algorithms for implementing digital signature with RSA algorithm. This technique crunch the document using hash functions, encrypt the message digest with private key then uses RSA algorithm.

In 2010 Sato et al. [13] suggested that one of security concern for cloud can be summarized as social insecurity. It is classified into the multiple stakeholder problems, the open space security problem and the mission critical data handling problem. As a solution of those problems, they proposed a new cloud trust model. They consider both internal trusts model and contracted trust that controls cloud service providers. They present a model named as *"*Security Aware Cloud.*"* In a security aware cloud, internal trust must be established as the firm base of trust. By implementing security such as identity management and key management on internal trust, they obtain a firm trust model.

3 Challenges of the Cloud

Ultra large-scale: Larger is the cloud, faster is the cloud. The cloud providers have a large network of servers, which are to give services to users or consumers. The cloud

of Google has owned more than one million servers. Even in Amazon, IBM, Microsoft, Yahoo, they have more than hundreds of thousands servers. There are hundreds of servers in an enterprise **[10, 12].**

Virtualization: Cloud computing makes user to get service anywhere, through any kind of terminal. It is applied to memory, networks, storage, hardware and operating system .You can do all you want through net service using a notebook computer or a mobile phone [10]. Users can attain or share it safely through an easy way, anytime, anywhere. Virtualization has characteristics like Partitioning (many applications and operating systems are supported in a single physical system by partitioning or separating the available resources) and Isolation (each virtual machine is isolated from its host physical system and other virtualized machine. **therefore if one virtual machine crashes, it doesn't affect the other virtual machines)** [12]. In addition, data is not shared between one virtual container and another. It also provides Encapsulation (a virtual machine can be represented as a single file, so you can identify it easily based on the service it provides. In essence, the encapsulated process could be a business service. The encapsulated virtual machines can be presented to an application as a complete entity. Therefore, it can protect each application so that it does not interfere with another application) **[14, 15].**

High reliability: Cloud uses data multi transcript fault tolerant. It replicates the same data at different location or at different machines that ensure high reliability. Chances of data crash become less. It supports the integrity and transaction constraints as well [14].

Versatility: Cloud computing can produce various applications supported by cloud and one cloud can support different applications running on it, at the same time. It may be for same problem or for different problems [16].

High extendibility: The scale of cloud can extend dynamically to meet the increasingly requirement. This application brings up hundreds of virtual servers on-demand, runs a parallel computation on them. By using an open source distributed processing framework called Hadoop, then shuts down all the virtual servers. Releasing all bound resources back to the cloud with low programming effort and at a very reasonable cost for the caller **[16, 17].**

On demand service: **Cloud** is a large resource pool that you can buy according to your need. Cloud is just like running water, Electric, and gas that can be charged by the amount that you used. It works like pay-as-you go manner, simply as in homes we pay for electricity bills as how much we used. Similar in cloud, we pay as we use the resources of cloud provider. This is also known as utility computing.

Extremely inexpensive: **The** centered management of cloud make the enterprise need not undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully enjoy the low cost advantage [17].

4 Service Models

Cloud computing provides three service models that provides different levels of control and security are described ahead.

Software as a service (SAAS): The services provided over the Internet is referred as software as a service. It includes the capabilities which are provided to the consumers to use the provider's applications, that running on a cloud infrastructure. Applications accessible from various client devices through a thin client interface such as a Web browser (e.g., web-based email) [4]. The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. The traditional model of software distribution is the software purchased and installed on personal computers, is sometimes referred to as Software-as-a-Product [18].It is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. Software as a service is becoming an increasingly dominant delivery model as underlying technologies that support web services and service-oriented architecture (SOA) **[1] [19].**

Platform as a service (PAAS): Platform as a service provides capabilities to the consumers to deploy onto the cloud infrastructure. Various consumers created applications use programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems and storage. The consumer has control over the deployed applications and possibly application hosting environment configurations. Cloud computing has acquired to includes the platform for building and running custom web-based applications, this concept known as Platform-as-a-Service. PAAS is an outgrowth of the SAAS applications delivery model. The PAAS model has aim to support the complete life cycle of building, delivering web applications and services entirely available from the Internet. Adverse to IAAS model, where developers may create a specific operating system instance with homegrown applications, PAAS developers are concerned only with web based development and generally do not care which operating system is used[4]. Its services allow users to focus on innovation rather than complex infrastructure. Organizations can redirect a significant portion of their budgets for creating applications that provide real business values instead of worrying about all the infrastructure issues. The PAAS model is thus driving a new era of mass innovation. Now, developers around the world can access unlimited computing power. Anyone with an Internet connection can build powerful applications and easily deploy them to users globally **[1] [17] [19].**

Infrastructure as a service (IAAS): Infrastructure as a service provides control over the storage and resources. It provides the consumer to rent processing, storage, networks, and other fundamental computing resources. Where the consumer is able to deploy and run arbitrary software, or control the underlying cloud infrastructure. The consumer has less control over operating systems, storage, deployed applications, and possibly selects networking components (e.g., firewalls, load balancers). IAAS is the

delivery of computer infrastructure (typically a platform virtualization environment) as a service. It leverages significant technology, services, and data center investments to deliver information technology (IT) as a service to customers [19]. IAAS is established on a model of service delivery that provisions a predefined and standardized infrastructure that is specifically optimized for the customer's applications. An IAAS provider handles the transition and hosting of selected applications on their infrastructure. Customers maintain ownership and management of their applications while off-loading hosting operations and infrastructure management to the IAAS providers [1].

5 Deployment Models

Private Cloud: In private clouds the physical infrastructure may be owned by or physically located in the organization's datacenters. These are managed by third party or own personnel with on or off-premise. They provide a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity, accountability and utility model of Cloud. The consumers of the service are called trusted. Trusted consumers of service are those who are considered part of an organization's legal/contractual umbrella including employees, contractors and business partners. It is easier to align with security, compliance and regulatory requirements and provide more enterprise control over development and use. All cloud resources and applications managed by the organization itself. Utilization on the private cloud can be much more secure than that of the public cloud because of its internal control or exposure. Only the organization and stake holders may have access to operate on a private cloud [15] [19].

Public Cloud: **Public** Clouds are provided by designated service providers. Theyoffer either a single-tenant (dedicated) or multi-tenant (shared) operating environment with the benefits and functionality of elasticity, accountability and utility model of Cloud. In public cloud the physical infrastructure is generally owned by and managed by the designated service provider which is located within the provider's datacenters (off-premise.) Consumers of Public Cloud services are called untrusted. Untrusted consumers are those that may be authorized to consume some **or** all services but are not logical extensions of the organization. These types of cloud are stand alone or proprietary, run by third party companies such as Google, Amazon etc.

Managed Cloud: **These types of clouds are established where various organizations have same requirements.** They offer both **single-tenants** (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity, accountability and utility model of Cloud [20]. The physical infrastructure is owned by and/or physically located in the organization's datacenters with an extension of management and security control planes controlled by the designated service provider. Consumers of Managed Clouds may be trusted or untrusted.

Hybrid Cloud: **Hybrid** Clouds are a combination of public and private cloud. It offers transitive information exchange and possibly application compatibility and

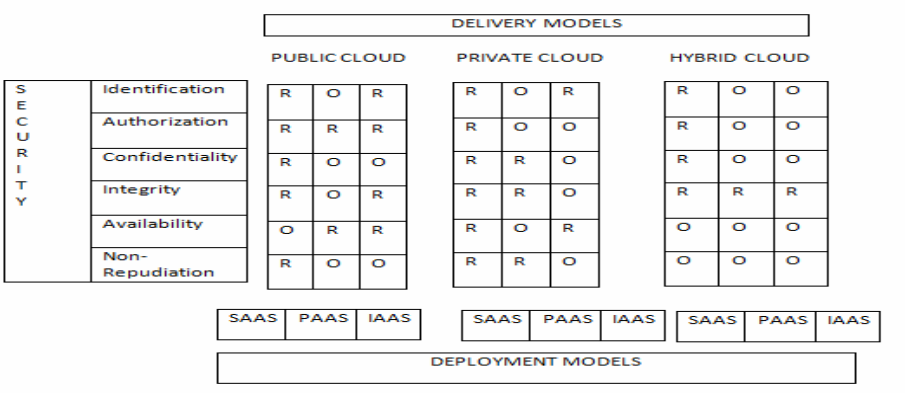
portability. Cloud service offerings and provides utilizing standard or proprietary methodologies regardless of ownership or location. This model provides an extension of management and security control planes. Consumers of hybrid Clouds are trusted or untrusted [20, 21].

Table 1. Cloud Computing Services Models and Their Providers [11]

	SERVICES	PROVIDERS
SAAS	• Support running multiple instances on it. • Develop software that run in cloud	• Google Docs • Mobile Me • Zoho
PAAS	• Platform which allow developers to create programs that run in the cloud. • It Include several applications services which allow easy development	• Microsoft Azure • Force.com • Google App Engine
IAAS	• Consist of database servers and storage • Highly scaled and shared computing infrastructure	• Amazon S3 • Sun's Cloud Service

6 Comparison Analysis

We have already described different delivery models of cloud by which different types of services are delivered to the end user. The three delivery models are the SAAS, PAAS and IAAS which provide infrastructure resources, application platform and software as services to the consumer. These service models also place a different level of security requirement in the cloud environment. IAAS is the foundation of all cloud services, with PAAS built upon it and SAAS in turn built upon it. Just as capabilities are inherited, so are the information security issues and risks. There are significant trade-offs to each model in terms of integrated features, complexity, extensibility and security. If the cloud service provider takes care of the security at the lower part of the security architecture of cloud, then the consumers become more responsible for implementing and managing the security capabilities. This paper presents information of the services and providers of services. Comparative analysis on different cloud delivery and deployment models is presented along with security concern [22]. Parameters in security are identification, authorization, confidentiality, integrity, non-repudiation and availability in terms of deployment models**.** Figure.1 shows that security is required at higher extent in public cloud. This is one the main area of researchers to improve security in public cloud. Especially authorization and integrity in public cloud require great attention of researchers to fulfill the dream of implementation of cloud [17].



R = Required, O = Optional

Fig. 1. Comparison of Security Parameters in Different Delivery Models

7 Future Direction

One of the thrust and major area of research is to find technical solutions for the interoperability among the cloud. Cloud enterprises want to assure that there will be exit or a migration strategy across multiple clouds thereby avoiding the perils of vendor lock-in. Second is the enabler ecosystem. There are various complex domains within a cloud data center infrastructure. Some examples of these domains are computing, network, storage, security, software applications and service management. In those domains, there are several areas of complexity including integration, interoperability, operation, scalability, and compliance. Because of this enterprises start adopting private clouds, they would need a healthy ecosystem of cloud solution providers. It would ease the burden of the above mentioned complexitiesof cloud computing. The main area for research in cloud computing is its security. It is great obstacle in implementation of cloud. Different solutions to security have been suggested. These solutions include reconfigurable computing, cryptography, identity access management and various cloud computing models as well. Still, efficient solutions are required for different domains of clouds.

8 Conclusion

Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However one must be very careful to understand the limitations and security risks posed in utilizing these technologies. Cloud computing is no exception. In this paper challenges, deployment models and key security issues which are currently faced by cloud computing are highlighted. We mentioned the requirement of security at different service models

which easily give the view where we require more security and concentrate our focus to under developed areas. By following this paper, the insecurities of cloud may be easily expelled, saving business owner time and investment. This service can be easily integrated by different organizations such as banking, search engines and enterprise applications.

References

1. Julisch, K., Hall, M.: Security and Control in the Cloud. Information Security Journal: A Global Perspective 19(6), 299–309 (2010)
2. Balachandra, R.K., Ramakrishna, P.V., Rakshit, K.: Cloud Security Issues. In: IEEE International Conference on Services Computing, pp. 517–520 (2009)
3. Cheng, G., Jin, H., Zou, D., Zhang, X.: "Building Dynamic and Transparent Integrity Measurement and Protection for Virtualized Platform in Cloud Computing. Concurrency and Computation: Practice and Experience 22, 1893–1910 (2010)
4. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, L., Lee, G.: Above the clouds: A Berkeley View of Cloud Computing. University of California, Berkeley, Tech. Rep. USB-EECS-2009, vol. 28, pp. 23-29 (2009)
5. Zissis, D., Lekkas, D.: Addressing Cloud Computing Security Issues. Future Generation Computer System (2010) Article in Press, http://dx.doi.org/10.1016/j.future.2010.12.006
6. Yamaguchi, T., Hashiyama, T., Okuma, S.: A Study on Reconfigurable Computing System Cryptography. In: IEEE International Conference on Cloud Computing, vol. 4, pp. 2965–2968 (2000)
7. Yuefa, D., Bo, W., Yaqiang, G., Quan, Z.: Data Security Model for Cloud Computing. In: International Workshop on Information Security and Applications, pp. 141–144 (2009)
8. Tribhuwan, M.R., Bhuyar, V.A., Pirzade, S.: Ensuring Data Storage Security in Cloud Computing Through Two Way Handshake Based on Token Management. In: International Conference on Advances in Recent Technology in Communication and Computing, pp. 386–389 (2010)
9. Brandic, I., Dustdar, S., Anstett, T., Schumm, D., Leymann, F.: Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds. In: IEEE International Conference on Cloud Computing, pp. 244–251 (2010)
10. Ramgovind, S., Eloff, M., Smith, E.: The Management of Security in Cloud Computing. In: IEEE International Conference on Service Computing, pp. 126–130 (2010)
11. Almulla, S.A., Yeun, C.Y.: Cloud Computing Security Management. In: IEEE International Conference on Service Computing, pp. 121–126 (2010)
12. Somani, U., Lakhani, K., Mundra, M.: Implementing Digital Signature with RSA Encryption Algorithm to Enhance Data Security of Cloud in Cloud Computing. In: IEEE International Conference on Parallel, Distributed and Grid Computing, pp. 85–94 (2010)
13. Sato, H., Kanai, A., Tanimoto, S.: A Cloud Trust Model in a Security Aware Cloud. In: IEEE International symposium on Applications and the Internet, pp. 121–124 (2010)
14. Kaufman, L.M.: Data Security in the World of Cloud Computing. IEEE Security and Privacy 7(4) (2009)
15. Amazon Web Services (AWS), http://aws.amazon.com
16. Shen, Y., Li, K., Yang, L.T.: Advanced Topics in Cloud Computing. Journal of Network and Computer Applications 12, 301–310 (2010)

17. Subashini, S., Kavitha, V.: A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Network and Computer Applications 34, 1–11 (2010)
18. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J.: Controlling Data in the Cloud Outsourcing Computation without Outsourcing Control. In: CCSW, Chicago, Illinois, USA (2009)
19. Lombardi, F., Pietro, R.D.: Secure Virtualization for Cloud Computing. Journal of Network and Computer 12, 407–412 (2010)
20. Google App Engine, `http://code.google.com/appengine`
21. Caslo, V., Rak, M., Vilano, U.: Identity Federation in Cloud Computing. In: IEEE International Conference on Information Assurance and Security, pp. 253–259 (2010)
22. Casola, V., Mazzeo, A., Mazzocca, N., Victoriana, V.: A Security Metric for Public key Infrastructures. Journal of Computer Security 15(2), 78–85 (2007)