Effective Service Security Schemes In Cloud Computing

[1,]K.Sravani, [2,] K.L.A.Nivedita
[1,2,]Assistant Professor Department of CSE Swarna Bharathi College of Engineering
Khammam, Andhra Pradesh

Abstract

The cloud computing is the fastest growing concept in IT industry. The IT companies have realized that the cloud computing is going to be the hottest topic in the field of IT. Cloud Computing reduces cost by sharing computing and storage resources, merged with an on demand provisioning mechanism relying on a pay-per use business model. Due to varied degree of security features and management schemes within the cloud entities security in the cloud is challenging. Security issues ranging from system misconfiguration, lack of proper updates, or unwise user behaviour from remote data storage that can expose user‘s private data and information to unwanted access can plague a Cloud Computing. The intent of this paper is to investigate the security related issues and challenges in Cloud computing environment. We also proposed a security scheme for protecting services keeping in view the issues and challenges faced by cloud computing.

Keywords— Cloud Computing, Data Protection, Security, Application Program Interface, Average Revenue Per user.

1. Introduction

The basic principle of cloud computing is to make the computing be assigned in a large number of computers, rather than local computer or remote server. The cloud computing is extension of grid computing, distributed computing and parallel computing [3]. In cloud computing the recourses are shared via internet. Cloud computing provides the fast, quick and convenient data storage and other computing services via internet. The cloud computing system is like your virtual computer that is a virtual location of your resources. The user can access their resources those are placed on a cloud as on their real system resources. The user can install applications, store data etc. and can access through internet anywhere. The user do not need to buy or install any hardware to upgrade his machine. They can do it via internet. In future we may need only notebook PC or a mobile phone to access our powerful computer and our resources anywhere.Security aspects of cloud computing are gaining interests of researchers as there are still numerous unresolved issues which needed to be addressed before large scale exploitation take place. Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time -shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications [2].

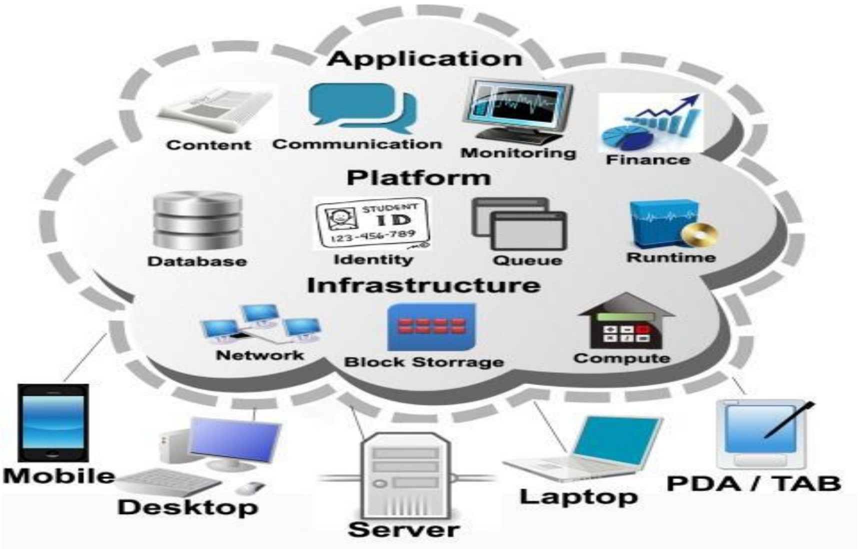

Figure1:The Cloud

The basic idea of cloud computing is that it describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. The attractive feature of Cloud computing is that it has made access to computing resources a lot easier, but with that convenience has come a whole new universe of threats and vulnerabilities. In this paper, we explore the security issues and challenges for next generation CC and discuss the crucial parameters that require extensive investigations. Basically the major challenge for employing any efficient security scheme in CC is created by taking some of the important characteristics into considerations such as Shared Infrastructure, Dynamic Provisioning, Network Access and Managed Metering.

2. Cloud Computing Security Issues

Security issues are the most concerned challenges in cloud computing [3]. Cloud is expected to offer the capabilities like encryption strategies to ensure safe data storage environment, strict access control, secure and stable backup of user data. However, cloud allows users to achieve the power of computing which beats their own physical domain. It leads to many security problems. We will discuss the major security concerns in the following:

2.1. Identification and Authentication:

The multi tenancy in cloud computing allows a single instance of the software to be accessed by more than one users [3]. This will cause identification and authentication problem because different users use different tokens and protocols , that may cause interpretability problems.

2.2. Access control:

Confidential data can be illegally accessed due to lenient access control.If adequate security mechanisms are not applied then unauthorized access may exist. As data exists for a long time in a cloud, the higher the risk of illegal access [3].

2.3. Data Seizure:

The company providing service may violate the law. There is a risk of data seizure by the some foreign government.

2.4. Encryption/ Decryption:

There is an issue of the Encryption/ Decryption key that are provided. The keys should be provided by the customer itself.

2.5. Policy Integration: Different cloud servers can use different tools to ensure the security of client data. So integration policy is one of the major concerns of security.

2.6. Audit: In cloud computing the Cloud Service Provider (CSP) controls the data being processed. CSP may use data while being processed [3]. So the process must be audited. The all user activities must be traceable. The amount of data in Cloud Computing may be very large. So it is not possible to audit everything.

2.7. Availability: Availability is the major concern in the cloud computing. When the client data is virtualized, clients have no control on the physical data [3]. If in the cloud, the data or service is not available, it is rigid to fetch the data.

2.8 Network Consideration

Cloud computing is a technique of resource sharing where servers and storage in multiple locations are connected by networks to create a pool of resources. When applications are run, resources are allocated from this pool and connected to the user as needed. The missions of connecting the resources (servers and storage) into a resource pool and then connecting users to the correct resources create the network's mission in cloud computing. For many cloud computing applications, network performance will be the key to cloud computing performance.

2.9. Virtualization Paradigm

In order to process a user request in CC environment, a service provider can draw the necessary resources on demand, perform a specific job and then relinquish the unneeded resources and often dispose them after the job is done. Contrary to traditional computing paradigms, in a cloud computing environment, data and the application is controlled by the service provider. This leads to a natural concern about data safety and also its protection from internal as well as external threats. Usually, in a cloud computing paradigm, data storage and computation are performed in a single data enter that may led to the development of various security related failure.

2.10. Mapping machines

Cloud computing offers a means to decouple the application activities from the physical resources required. This has enabled consolidation of multiple applications onto a lesser number of physical servers resulting in an increase in server utilization. Such decoupling of resources is facilitated by the concept of a virtual machine which encapsulates an application with a specific set of functionalities. Physical resources are made available to the virtual machine by a guest operating system running on each physical machine. The virtual machine runs over this guest operating system which also provides facilities for creation, destruction and migration of virtual machines. The different security parameters are required to facilitate these functions in cloud computing.

2.11 Secure Data Management

As data is an important tool of CC the some aspects of the secure cloud, namely aspects of the cloud storage and data layers. In particular the security issues ranging from ways of efficiently store the data in foreign machines to querying encrypted data, as much of the data on the cloud may be encrypted is a critical challenge for implementing security schemes in Cloud Computing [8].

2.12 Resource Allocation

With the cloud model, we lose control over physical security. In a public cloud, we are sharing computing resources with other companies. In a shared pool outside the enterprise, we don't have any knowledge or control of where the resources run. Exposing our data in an

environment shared with other companies could give the government "reasonable cause" to seize your assets because another company has violated the law. Simply because we share the environment in the cloud, may put your data at risk of seizure. Storage services provided by

one cloud vendor may be incompatible with another vendor's services should decide to move from one to the other. Thus to secure the resources in a cloud demand highly encrypted schemes.

3. Challenges Of Security Schemes

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Basically the major challenge for employing any efficient security scheme in CC is created by the tasks expected from the clouds. Security schemes look like a defense tool which every organization needs. However there are some challenges the organizations face while deploying a security system in Cloud computing. Some of them are:

3.1 Abuse and Nefarious Use of Cloud Computing

Providers offer their customers the illusion of unlimited computer, network, and storage capacity often coupled with a friction less registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity.

3.2 Insecure Interfaces and APIs

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency.

3.3 Malicious Insiders

Another important challenge regarding implementing security schemes is the threat of a malicious insider. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance (e.g. [7], [1]). To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

3. 4 Shared Technology Issues

Vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defence in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's
actual or residual data, network traffic etc.

3.5 Data Loss or Leakage

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example [6]. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.

4.PROPOSED SECURITY FRAMEWORK

In the recent years, CC security has been able to attract the attentions of a no. of researchers around the world [4]. In this section we proposed a security scheme taking regarding issues and challenges keeping in mind. Our aim is to design and develop a security proposal that would be accurate, secure data in shared pool, secure for unexpected intrusions, adaptive and be of real time. The proposed secure model provides the security of cloud services by the following ways:

4.1 Secure Cloud service

The cloud service providers with the highest margins, highest ARPU, lowest operating costs, and lowest churn will have a significant competitive advantage in the long run. To achieve this advantage, they will need a comprehensive cloud service delivery platform and the cost of developing such a platform with security parameter is a factor they will need to take into account. Not all cloud service providers are the same. While some are giants with multiple data centers worldwide, some, in particular niche service providers. That is not all bad computing still is their business, which means they invest all their operating and capital budgets in IT operations. And even the largest providers are not immune to security problems as the hacking of the Sony network and the major crash of Amazon's infrastructures- a-service installation demonstrated. The security of service provider managed by:

- ➢ Check out its security staff.
- ➢ Ask where its data centres are, how many it has, and what its security parameters and proposals are.
- ➢ Separating the company data from company operations has many security advantages.
- ➢ Stricter initial registration and validation processes for customers.
- ➢ To enhanced credit card fraud monitoring and coordination.
- ➢ Comprehensive introspection of customer network traffic.
- ➢ Monitoring public blacklists for one's own network blocks.

4.2 Secure Web Platform

Cloud platform services deliver a computing platform and solution stack as a service often consuming cloud applications [5]. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. The security of the web platform is to securing all content and data traffic - including email, web and identity traffic - moving between an organization and the Cloud. Some schemes that protect the data and its travels within or outside the organization to the Cloud are:

i. Analyze the security model of cloud provider interfaces.
ii. Ensure strong authentication and access controls in concert with encrypted transmission.
iii. Understand the dependency chain associated with the API.

4.3 Secure Cloud Infrastructure

Cloud infrastructure is a platform which holds the development environments and within it one would find managed hosting environment where various applications are built. To secure this Using a secure password management service that protects user ID and password data and can flag users that repeat passwords across various systems. For secure cloud Infrastructure we have used:

- LDAP controls and administering credentials that keep access information from being scattered around.
- Running scripts to remove access when employees leave the organization are also proposed for identity management security.
- Determine security breach notification processes.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations [3].
- Conduct vulnerability scanning and configuration audits.

4.4 Secure Cloud Data Pool

- When enterprises adopt cloud computing and deploy databases in virtual environments, they run the risk of exposing highly-sensitive data to a broad base of internal and external attacks [3]. Here, we enlist strategies to help enterprises protect their data when implementing a database security strategy in cloud or virtualized environments.
- Multi-tenancy: To be used for single backup system to protect multiple business units or customers and to allocate resources to them dynamically on-demand. Therefore, every storage pool needs to be kept secure and fully independent from the others.
- Chargeback systems: For data protection resources allocated by end-user needs, storage providers need to track this usage by a wide range of criteria for both chargeback and billing purposes and for infrastructure optimization purposes.
- Robust Reporting: CC environment need an accurate way to forecast their capacity and processing needs for budgeting purposes. It also needs to analyze usage to optimize available system resources for better efficiencies. Thus detailed reporting and analytics not only helps in managing the current environment but also enables trending and modelling for planning future investments.
- Quality of Service delivery: Storage pooling enables CC environment to set replication priorities for each pool so that the most mission critical data is replicated before less important data. This QoS orientation can be set to specific backup policies with different retention periods for a particular storage pool.
- Storage Tiering: Storage tiering is the mechanism to allocate disk drives to a storage pool according to the capacity or performance requirements for a specific set of data under protection.
- Global Deduplication: De duplication is a critical part of an effective data protection environment. It is not only necessary for cost-effective optimization of the overall storage capacity but also provides a cost effective WAN implementation for replication and movement of data to a remote location for disaster recovery.

5. Conclusion

The proposed secure model has to ensure security of each service by applying the various security schemes on each cloud architectural component. While most of the risk against security in Cloud computing are caused by the involvement of computing in different plate forms. For defending the threats, developing the secure system that will be efficient is a great research challenge. Again, ensuring each component secure is a major research issue. Many of today’s security schemes based on specific component mode but there is a lack of combined effort to take a common model to ensure security of each architectural component, in future though the security mechanism become well - established for each individual component, combining all the mechanism together for making them work in collaboration with each other will incur a hard research challenge.

References

[1] P.F. da Silva and C.B. Westp hall, “Improvements in the Model for Interoperability of Intrusion Detection Responses Compatible with the IDWG Model” Int’l J. Network Management, vol. 17, no. 4, 2011, pp. 287–294.

[2] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong , “Characteristics of cloud computing” , 39th International Conference on Parallel Processing Workshops ,2012

[3] ZiyuanWang , “Security and privacy issues within the Cloud Computing” ,International Conference on Computational and Information Sciences , 2011

[4] Shuai Zhang, ShufenZhang, Xuebin Chen and XiuzhenHuo , “The Comparison Between Cloud Computing and Grid Computing” , International Conference on Computer Application and System Modeling (ICCASM 2010),2010

[5] Siani Pearson and AzzedineBenameur , “Privacy , Security and Trust Issues Arising from Cloud Computing”,2nd IEEE International Conference on Cloud Computing Technology and Science

[6] ZhidongShen and QiangTong ,“The Security of Cloud Computing System enabled by Trusted Computing Technology”, 2nd International Conference on Signal Processing Systems (ICSPS) , 2010

[7] Shuai Zhang , Shufen Zhang , Xuebin Chen and XiuzhenHuo , “Cloud Computing Research and Development Trend” , Second International Conference on Future Networks , 2010

[8] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, “The Eucalyptus open source cloud-computing system” in Proceedings of the 9thIEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID 09), May 2011, pp. 124–131.

[9] Q. Wang, K. Ren, W. Lou, and Y. Zhang, “Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance” Proc. of IEEE INFOCOM, 2010.

[10] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey , you, get off of my cloud: exploring information leakage in third-party compute clouds,” in CCS 09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2011, pp. 199–212.

[11] K.hamlin, M. Kantarcioglu, L. Khan and B. Thuraisingham "Security Issues for Cloud Computing" Journal of Information Security and Privacy,vol. 4, no. 2, pp. 39–51, April-June 2010.