



International Journal of Engineering, Business and Enterprise Applications (IJEBA)

www.iasir.net

SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

Dr.G.N.K.Suresh Babu¹ and Dr.S.K.Srivatsa²

¹Associate Professor, Department of Computer Applications, GKMCE, Chennai, Tamil Nadu, India

²Sr.Professor, St. Joseph College of Engineering, Chennai, Tamil Nadu, India

Abstract: Cloud computing is an emerging computing paradigm where computing resources are provided as services over Internet. Even though it enables us to dynamically provide servers with the ability to address a wide range of needs, this paradigm brings forth many new challenges for the data security and access control as users outsource their sensitive data to clouds, which are beyond the same trusted domain as data owners. The range of services provided under Cloud Computing covers the entire information technology spectrum and includes infrastructure (e.g. processing power, storage), platforms and software. With Cloud Computing, as with many new technologies and services, information security and data protection issues are intensely debated. In this paper we describe about the cloud computing concepts and security and privacy issues in cloud computing.

Keywords: Cloud Computing, IAAS, PAAS, SAAS, Data Security

1 INTRODUCTION

Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. The market research and analysis firm IDC suggests that the market for Cloud Computing services was \$16billion in 2008 and will rise to \$62billion/year by 2015. It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications. Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services.

II. TYPES OF CLOUDS

A. Public Clouds

A public cloud encompasses the traditional concept of cloud computing, having the opportunity to use computing resources from anywhere in the world.

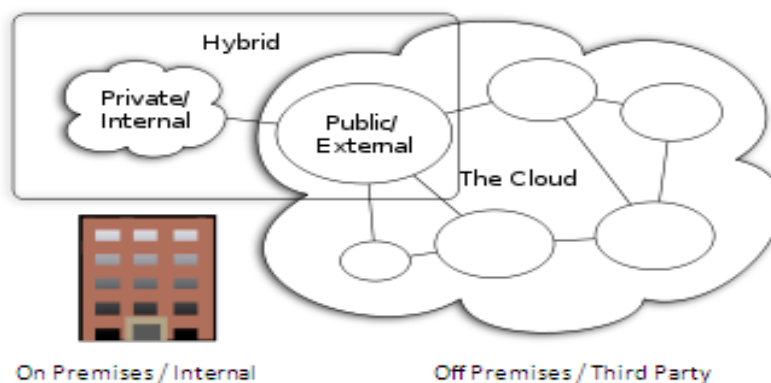
B. Private Clouds

Private clouds are normally datacenters that are used in a private network and can therefore restrict the unwanted public to access the data that is used by the company. It is obvious that this way has a more secure background than the traditional public clouds. However, managers still have to worry about the purchase, building and maintenance of the system.

C. Hybrid Clouds

As the name already reveals, a hybrid cloud is a mixture of both a private and public cloud. This can involve work load being processed by an enterprise data center while other activities are provided by the public cloud.

Figure 1: Represents the Cloud Computing types.



III. TYPES OF SERVICES

Cloud Computing encompasses different types of services. There are 3 classes of technology capabilities that are being offered as a service and which will be introduced in the following:

A. Infrastructure as a Service

Statistically proven figures show that 80% of the computing power is not efficiently used, neither is 65% of the storage of servers. Hence there is a huge potential to share resources in order to use them in a cost efficient way rather than underutilizing them.

B. Platform as a Service

Platform as a service provides the facility to support the development lifecycle from design, implementation, debugging, testing, deployment, operation and support of rich internet applications (RIA) and online services. Here mostly the internet browser will be used for the development).

C. Software as a Service

Companies can use software that is made available online on a rental or usage basis rather than buying the whole software package locally without being sure whether or not the investment will pay off on a long-term basis. No maintenance or updates are involved; this will all be handled by the software provider.

IV. CLOUD COMPUTING AND DATA SECURITY

As we described in this paper, because of the pay as you go method, most of the enterprises tend to move to Cloud Computing to save cost. The enterprises move to cloud and get the space for data storage. This data storage is certainly cheaper for them if compared to the in-house data storage but the question is, if this data storage in cloud is also secured and beneficial for enterprises. Hence, one of the most impending tasks for enterprises is the security of data storage. The IDC survey in June 2013 has shown that security is the most serious concern for the enterprises subscribed to Cloud Computing. Mostly the security issues which arise in Cloud Computing are the result of users/enterprises lack of control on the physical infrastructure. Enterprises mostly don't know where their data is physically stored and which security mechanisms are in place to protect data i.e. whether the data is encrypted or not and if yes, which encryption method is applied also if the connection used for data to travel in the cloud is encrypted and how the encryption keys are managed. Browser Security is also an important issue in Cloud Computing as in a cloud most of the computation is done on remote servers and the client PC is only used for I/O, and authorization of commands to cloud. Hence, standard web browser was a need of situation to send I/O and this was utilized by different names: web applications, web 2.0 or Software as Services (SaaS). However, the use of web browser raised the question of security. TLS (Transport Layer Security) is important in this matter as it is used for host authentication and data encryption. XML signature or XML encryption cannot be used by browser directly as data can be only encrypted through TLS and signatures are only used with the TLS handshake. As stated above, understanding the relationships and dependencies among Cloud Computing models is critical for understanding the security risks of it. For all the cloud services IaaS is the foundation and PaaS is build on it, while SaaS is build on PaaS and IaaS as described in the cloud reference model diagram (Fig.2)

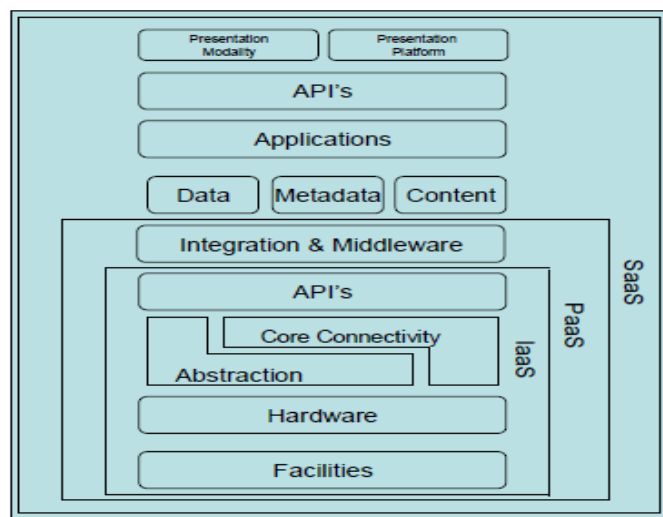


Figure 2: Cloud Reference Model

Security controls in Cloud Computing are not different than security controls in IT environment. However, as Cloud Computing deploys different service models, operation models and technologies, so it presents different

risks to an organization. The enterprise security is implemented on one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), and all the way to the information and applications (application security). The security responsibilities of provider and consumer are dependent on cloud models.

V. SECURITY AND PRIVACY ISSUES

Shared infrastructure scares many enterprise customers. Placing enterprise data in a public cloud is a serious concern and companies wary about their sensitive data logically question the ability of public cloud computing providers to provide the same level of security as their own datacenters. Depending on the type of cloud computing used (IaaS or PaaS) and the level of abstraction (OS-level vs. platform vs. application level) different security issues arise in public clouds. The cloud provider is responsible for the physical security of the machines, for ensuring that VM instances are running isolated from one another (i.e. crashes and software exploits of one system do not affect the others) as well as for setting up firewalls to protect the VM machines from the network. However, higher level cloud services such as Google AppEngine and platforms like Azure are also responsible for their application-level security and clients have less control controlling it. In addition, downtimes, outright data losses in storage services and risks of cloud provider malfeasance are further threats to be weighted when a company considers public cloud services usage.

Two main issues exist with security and privacy aspects of Cloud Computing:

1. Loss of control over data and
2. Dependence on the Cloud Computing provider.

These two issues can lead to a number of legal and security concerns related to infrastructure, identity management, access control, risk management, regulatory and legislative compliance, auditing and logging, integrity control as well as Cloud Computing provider dependent risks.

A. Loss of Control over Data

1. Most customers are aware of the danger of letting data control out of their hands and storing data with an outside Cloud Computing provider. Data could be compromised by the Cloud Computing provider itself or other competitive enterprises which are customers with the same Cloud Computing provider.
2. Many Cloud Computing providers are technically able to perform data mining techniques to analyse user data. This is a very sensitive function and even more so, as users are often storing and processing sensitive data when using Cloud Computing services. This holds especially true for social media applications that encourage users to share much of their private life e.g. private photos.
3. Mobile devices, in particular with their limited storage and computing capabilities are drivers for having services provided by Cloud Computing instead of using software on individual computers. Even data that are only to be transferred from one mobile device to another (local) device, are often transferred via the cloud, when cloud oriented applications on the mobile devices are involved. Therefore users often put themselves at risk without noticing this, as they assume that the data is transferred locally.
4. Since Cloud Computing is a service, it has to be accessed remotely. The connection between the Cloud Computing provider and customer is not always adequately protected. Security risks that threaten the transfer line include eavesdropping, DNS spoofing, and Denial-of-Service attacks.
5. As all technical control is given to the Cloud Computing provider, customers often want to have an external audit of this provider. Therefore logging and auditing information has to be stored and protected in order to enable verification. Appropriate logging could provide the possibility for forensic investigation in cases of incident.
6. Concerns also exist with regard to deletion of data: It is difficult to delete all copies of electronic material because it is difficult to find all copies. It is impossible to guarantee complete deletion of all copies of data. Therefore it is difficult to enforce mandatory deletion of data. However, mandatory deletion of data should be included into any forthcoming regulation of Cloud Computing services, but still it should not be relied on too much: the age of a "Guaranteed complete deletion of data", if it ever existed has passed. This needs to be considered, when data are gathered and stored.

B. Dependence on the Cloud Computing provider

1. A major concern regarding dependence on a specific Cloud Computing provider is availability. If the Cloud Computing provider were to go bankrupt and stopped providing services, the customer could experience problems in accessing data and therefore potentially in business continuity.
2. Some widely used Cloud Computing services (e.g. GoogleDocs) do not include any contract between the customer and Cloud Computing provider. Therefore a customer does not have anything to refer to if incidents occur or any problems arise.
3. Cloud Computing is a service similar to other more "traditional" services and utilities. Both Cloud Computing services and traditional services and utilities tend to be offered by large providers dealing with smaller

customers. Therefore the customers usually depend on the providers because it is difficult to change providers if it is possible at all.

VI. RECOMMENDED SUGGESTIONS

1. Risk management and (legal) compliance issues must be well defined in the contract between Cloud Computing provider and customer and should enable transparency with regard to the processing and storage of data, e.g. the physical location of data storage. In this way the trust between the Cloud Computing provider and customer can be strengthened.
2. The service provided shall be compliant with the regulation and legislation that the customer needs to follow, and also customers should be enabled to be compliant with the respective regulation and legislation.
3. The problems and risks that affect data protection rules in Europe must be considered properly when Cloud Computing platforms are located on servers in non-European countries.
4. The communication line between the Cloud Computing provider and the customer has to be adequately protected to ensure confidentiality, integrity, authentication control and further to minimise the risk of denial-of-service attacks. An open and clear specification of the measurements taken to ensure the security of the communication line should be obligatory for any Cloud Computing provider and should be based on open and transparent standards and technologies.
5. The Cloud Computing providers should be obliged to ensure data confidentiality.

VII. SECURITY BENEFITS OF CLOUD COMPUTING

Cloud Computing has a lot of potential to improve security for enterprises and the ways it can improve security is described below.

A. Benefits of Scale

It is a fact that all types of security measures which are implemented on a larger scale are cheaper. Hence by adopting Cloud Computing enterprises gets better protection with same amount of money. The security includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances, human resources and their management and vetting, hardware and software redundancy, strong authentication, efficient role-based access control and federated identity management solutions by default, which also improves the network effects of collaboration among various partners involved in defense. Along with these benefits, other benefits include:

B. Multiple Locations

The cloud providers by default have economic resources to replicate content and this increases the redundancy and independence from failure. Hence, it provides the disaster recovery.

C. Edge Networks

Cloud Computing provides reliability, quality increase and less local network problems for enterprises by having storage, processing and delivery closer to the network edge.

D. Improved Timelines of Response

Cloud providers have larger to incidents or well-run-larger-scale systems. These systems help in improved timelines of response e.g. because of the early detection of new malware deployments, it can develop more effective and efficient incident response.

VIII. SUMMARY

In a nutshell we can say that cost and security are the important factors for any enterprise to adapt Cloud Computing. Enterprises tend to choose the payment methods for paying Cloud Computing providers. Most common payment method for enterprises and the cloud providers is “pay as you go”. This is one of the novel feature of Cloud Computing, which is cheaper in a longer term than having own data center. However, Cloud Computing is cheaper for small and medium sized enterprises than large enterprises. Elasticity is another factor for enterprises to adapt Cloud Computing as they can use their resources dynamically. Amazon S3 provides services in a bundle of high durability, high availability and fast access however most enterprises don’t need all but some of them. Hence, cloud providers should work on it to give enterprises more benefit. The administrative costs are lessened with the adoption of Cloud Computing for enterprises. Security of data is the most serious concern of enterprises adapting Cloud Computing. Most security issues are due to lack of control of enterprise over physical infrastructure. Web services and web browsers are also a concern regarding Cloud Computing as most of the cloud services are accessed through web. In this paper we describe along with security concerns there are also some benefits of Cloud Computing with respect to security. These benefits include benefit of scale with multiple locations, edge networks, improvised time line of response and we have given some recommended suggestions also.

REFERENCES

- [1] Alstom (2010). About Us. Alstom Homepage. Available at: <http://www.alstom.com/>.
- [2] Amazon (2009). About Amazon Web Services. Amazon Web Services Homepage. Available at: <http://aws.amazon.com/>.
- [3] Borko Furht. Handbook of Cloud Computing. Springer, New York, September 2010. ISBN 9781441965233.

- [4] Craig-Wood, K. (2009). The Differences Between IT Outsourcing and Cloud Computing. Thoughts on British ICT, energy & environment. Available at:<http://www.katescomment.com/difference-it-outsourcing-cloudcomputing/>.
- [5] Cloud Security Alliance. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing.
- [6] Fellowes, W. (2008). Partly Cloudy, Blue-Sky Thinking About Cloud Computing.
- [7] Gartner (2008). <http://www.gartner.com/it/page.jsp?id=707508>.
- [8] Hobson, D. (2009). Into the Cloud We Go... Cloud Computing Journal Vol. 2, Issue 3, pp8-9.
- [9] A. Iosup, R. Prodan, D.Epema, "IaaS cloud benchmarking: approaches, challenges, and experience," 5th IEEE Workshop on Many-Task Computing on Grids and Supercomputers, 2012.
- [10] Kondo, D., Javadi, B., Malecot, P., Cappello, F., Anderson, D., (2009). Cost-Benefit Analysis of Cloud Computing versus Desktop Grids. INRIA, France, UC Berkeley, USA.
- [11] Murphy, M., Abraham, L., Fenn, M., & Goasguen, S. (2009). Autonomic Clouds on the Grid. Journal of Grid Computing, 1-18.
- [12] NIST (2009). The NIST Definition of Cloud Computing. from <http://csrc.nist.gov/groups/SNS/cloud-computing/>.
- [13] D. Huang, D. Ye, Q. He, J. Chen, K. Ye, "Virt-LM: a benchmark for live migration of virtual machine," ACM/SPEC International Conference on Performance Engineering, pp.307-316, 2011.
- [14] G. Fowler, B. Worthen, The Internet Industry is on a Cloud – Whatever That May Mean, The Wall Street Journal, March 26, 2009
- [15] S. Gajek, M. Jensen, L. Liao, and J. Schwenk, Analysis of Signature Wrapping Attacks and Countermeasures, IEEE International Conference on Web Services, Los Angeles, CA, July 2009
- [16] D. Jacobs, S. Aulbach, Ruminations on Multi-Tenant Databases, Fachtagung für Datenbanksysteme in Business, Technologie und Web, March 2007, <http://www.btw2007.de/paper/p514.pdf>
- [17] W. Jansen, Directions in Security Metrics Research, Interagency Report 7564, National Institute of Standards and Technology (NIST), April 2009
- [18] M. Jensen, J. Schwenk, N. Gruschka, L. L. Iacono, On Technical Security Issues in Cloud Computing, IEEE International Conference on Cloud Computing, Bangalore, India, September 21-25, 2009