Analysis of Security Issues in Cloud Computing

Ms.N.Kalanivani[1] Mr.M.Karthik[2] Ms.J.Valarmathi[3]
[1,3]ResearchScholar [2]Associate Professor
[1,2,3]Department of Computer Science
[1,2,3]D. B. Jain (Autonomous) Chennai-97, Tamil Nadu

Abstract— Nowadays, Cloud computing is booming in most of the IT industry. Cloud Computing represents a new computing model that poses many demanding security issues at all levels, e.g., network, host, application, and data levels. Cloud computing can be used by a prospective Cloud service for analyzing the data security risk before putting the confidential data into a cloud computing environment. The global computing infrastructure is rapidly moving towards cloud based architecture. The improvement of the cloud technology also increases the security issues twice. So we need to solve the security issues in the cloud technology. This paper presents a survey on Security in Cloud Computing.

Key words: Cloud Computing, SaaS, PaaS, IaaS

I. INTRODUCTION

A. Cloud Computing

Cloud computing is defined as provision of resources, application and information as a service over the cloud on demand. It supports the high storage capabilities and computational power. Today small and medium size companies are moving to Cloud due to various reason like reduced hardware, maintenance cost, pay-for use scalability, accessible location independent, on-demand security controls, fast deployment, flexibility and the highly automated process i.e. he customer need not worry about software up-gradation[22].

The cloud computing model allows access to information and computer resources from anywhere that a network connection is available.

II. CLOUD SERVICE MODELS

The Cloud computing services can be delivered to customer in many different ways. The cloud computing delivery models offering a various types of services like, Software as a service (SaaS), Platform as a service (PaaS) and infrastructure as a service (IaaS).

A. Infrastructure as a Service

It refers to sharing of hardware resources for executing services using virtualization technology.

The resources will be scaled up based on demand. The charges will be based on pay-per use. The following resources are offered like hardware, data storage, networking and bandwidth.

B. Platform as a Service

It provides a higher-level software infrastructure where customers can build and deploy particular application and services using the tools and programming languages supported by the provider. Platform services are aimed at specific domains, such as the development of web applications, and are dependent on the programming language. Customers get a separated environment to test and develop or to permanently deploy their applications. It allows you to deploy applications without having to spend the money to buy the server [13].

C. Application as a Service

The customer can manage or control the underlying infrastructure and application platform. It refers complete application is hosted on internet, it eliminate the need to install in local computer and user can use them. Customers rent software hosted by the vendor. Popular software services are the Google Apps. It include web based email, calendar, contacts and chat appliances, Google Docs package allows access and sharing of documents, spreadsheets and presentations.

D. Cloud service deployment model is divided into four ways

1) Public Cloud

Cloud infrastructure is hosted, operated and managed by a third party [20]. The infrastructure is available to all enterprise of all users. The service is offered to multiple customers over a common infrastructure. The services will be provided over the internet by the third party provider who shares the resources and pay what they used.

2) Private Cloud

Cloud infrastructure is made available to specific customer and managed by organization or third party service provider [20]. Its good option to deal with data protection and service-level issues. Its owned by a single customer who controls which applications run, and where.

3) Hybrid Cloud

It's a combination of public and private cloud models.

4) Community Cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether its managed by them or third part service provider [2].

E. Five Essential Characteristic of Cloud Computing

On-demand self-service. Individuals can set themselves up without human interaction with a service provider.

Broad network access Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (mobile phones, Laptops and PDA).

Location independence Resource pooling the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically signed and reassigned according to consumer demand.

Cloud computing is virtualized environment. The users can get the services at any place with any API. The demanded resources are from Cloud, is virtualized.

Rapid elasticity. It means users can rapidly increase and decrease their computing resources as needed, as well as release. Measured service Users can pay for only the

resources they actually use. Resource usage can be monitored, controlled and reported.

F. Advantage of Cloud Computing

- Virtualization
- Flexibility to choose vendor
- Elasticity and Cost Reduction

III. SECURITY IN CLOUD

There are four layers of security which can be implemented in cloud [9].

1) Physical security
2) Operating System / Database Security
3) Network security
4) Application Security

A. Physical Security

Physical Security can be implemented by appointing a security guard on the premises where our servers and sensitive data is present. He will take care and will be responsible of all kind of accesses and entry for that premises and a record can be maintained either in hard copy or in softcopy of the persons entering or leaving the premises with their names, address, phone number, purpose, time of entry and exit, so that the person responsible for any kind of future damage can be tracked down.

B. Operating System / Database Security

Next level of security is the operating system and database security. The need for operating system based security is that any system can be globally accessible through a set of vast inter and intra-network connections [9]. Another reason is transition motivated by the need to work remotely, convenience in accessing personal records. Convenience and efficiency will increase security risks. The most important reason is that even a single security loophole in the OS design known to a malicious attacker could do serious damage [9]. For implementing operating system based security in azure "Windows Live Id" is provided. There are Security Descriptors that represent access rights of a logged-in user. There is Object Manager that reads the security descriptors and passes on the information to the Security Reference Monitor (SRM). SRM determines whether a user's action is legal or illegal. We can encrypt file system for providing security.

C. Network Security

Next level of security is network security where we can do the setup of a firewall which is going to monitor the incoming and outgoing traffic in our network. Now the question arises, that can be set up a firewall in azure? The answer is yes.

1) Controlling Access To Your Data With The Firewall In Azure

The source IP address is checked against a list of allowed sources before an incoming connection. If the source address is not in this list, the connection is denied. There are no other rules supported, just the list of allowed addresses. The list isstored in the master database for your SQL Azure database server [4]. To manage your firewall rules through code, you can create a connection to the master database with your administrator account and use the provided stored procedures: sp_set_firewall_rule will create a firewall rule, andsp_delete_firewall_rule will remove a rule [4].

D. Application Security

The final level of security is application security in which the application can only be accessed by providing some kind of credentials only and by providing the type of credentials we can further divide the application security in four types

1) Identity based access
2) Role based access
3) Key based access
4) Claim based access

1) Identity Based Access

In identity based access a username and password is provided by the user and if they matches with the records in the database then only the access is provided otherwise the access is denied. Now the username can be of many types for example, name, email address, id proofs like driving license number, pan card number, ssn number in America, Uid number in India etc which will uniquely identify that person. In case of email id we have got additional advantage that in case of lost password we the issuing authority can send the new password to that email id. We can also enjoy the advantage of email id with other identity types if we take email id as an input at the time of registering.

2) Role Based Access

In role based identity a role is associated with the user like administrator, developer etc and the application changes the view according to the role of that user. Other credentials are also stored while issuing the role based identity to that user for security purpose.

3) Key Based Access

In key based identity the end user is provided a key and by using that key only the end user can access the services. This key is also stored in the database for verification. This key is encrypted and is generally very long such that no one can guess it. The level of security is very high with key based identity. It is generally associated with a time stamp and the services can only be enjoyed generally for certain amount of time only like 1 day or 6 hours, 1month etc.

4) Claim Based Access

In claim based identity a live id is created for a particular brand and all other services provided by that particular brand are accessed by that id. This is done because the end user or customer does not want to or does not prefer to create a new id and remembering the credentials each time for using the different services of that particular brand. The end user never likes filling the form each time for different services of that particular brand. So in order to attract customer to use their services without any pain and at the same time not compromising with the security claim based identity has been introduced and efforts and cost for maintain the data also reduce to great extent and at the same time we can track the data that how many services and what type of the services has been accessed by a particular type of person and this data can be used for data warehousing purpose. The example of claim based identity is Google id which is same for Gmail, Google+, Blogspot, Google search etc. Similarly Windows live id which is common for downloading all kinds of software provided for Windows. Similarly facebook id which is not only accepted by

facebook but also accepted by websites of other brands also like Scribd as an additional type for login purpose.

IV. SECURITY PRINCIPLES

The fundamental basis for developing secure cloud environment is based on various security principles:

- Confidentiality**:** The prevention of unauthorized disclosure of information that may be intentionally or unintentionally refers to the confidentiality.
- Integrity: The concept of cloud information integrity is based on two principles Prevention of modification of data from unauthorized users and preventing the unauthorized modification of data by authorised user.
- Availability: This Principle ensures the availability of cloud data and computing resources when needed**.**
- Authentication: It refers to the process of testing the user's identity and ensures that users are who they claim to be.
- Authorization: It refers to the privileges that are granted to individual or process for enabling them to access any authorized data and computing resources.
- Accountability: This is related to the concept of non-repudiation where the person cannot deny from the performance of an action. It determines the action and behavior of single individual within cloud system.

V. CONCLUSION

We conclude with that we can implement security in cloud by providing a shared access token. We have also talked about different types of security available in cloud. We have also given the answer for implementing firewall in network level security in cloud. We have talked about some principles that should be kept in mind while proposing a solution for security in cloud. A deeper study on current security approaches to deal with different security issue related to the cloud should be the focused of future work.

REFERENCES

[1] Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines.
[2] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal, "A Survey on Security Issues in Cloud Computing,"2011 CoRR, VOL- abs/1109.538.
[3] The Cloud: Understanding the Security, Privacy and Trust Challenges, Neil Robinson, Lorenzo Valeri, Jonathan Cave & Tony Starkey (RAND Europe) Hans Graux (time.lex) Sadie Creese & Paul Hopkins (University of Warwick)
[4] Azure in Action, , Chris Hey, Brain H Prince
[5] Jon Marler, "Securing the Cloud: Addressing Cloud Computing Security Concerns with Private Cloud," Rackspace KnowledgeCentre, March 27, 2011, ArticleId:1638. http://www.rackspace.com/knowledge_center/private-cloud/securing-the-cloud-addressingcloud-computing-security-concerns-with-private-cloud.
[6] Fourth International ICST Conference on Communication System software and middleware . June 2009. R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate," 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.
[7] By " Secure Connectivity for Intra-Cloud and Inter-Cloud Communication**"** Shiping Chen and Surya Nepal, Information Laboratory, CSIRO ICT Centre, Sydney, Australia.
[8] "Inter Cloud Security" By William Strickland, COP 6938 Fall 2012, University of Central Florida, 10/08/2012. [5] "A Comprehensive Overview of Secure Cloud Computing" By Dr. Bhavani Thuraisingham , November, 2012. **[6] "**Cloud Computing: Strategies for Cloud Computing Adoption" By Faith ShimbaDublin Institute of Technology, faith.shimba@gmail.com.
[9] Windows Azure™ Security Overview Charlie Kaufman and Ramanathan Venkatapathy.
[10] Joint, A., Baker, E. and Eccles, E. (2009). Hey, you, get off of that cloud? Computer Law & Security Review, 25, 270–274. doi:10.1016/j.clsr.2009.03.001
[11] Jorissen, K., Villa, F.D. and Rehr, J.J. (2012). A high performance scientific cloud computing environment for materials simulations. Computer Physics Communications, 183, 1911–1919.doi:10.1016/ j.cpc.2012.04.010
[12] Khorshed, T.M., Ali, A.B.M.S. and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation ComputerSystems, 28,833–851. doi:10.1016/j.future.2012.01.006.
[13] Nathan Mcfeters, "Recent CNN Distributed Denial of Service Attack Explained". http://www.zdnet.com/blog/security/recent-cnndistributed-denial-of-service-ddos-attack-explained/1054.
[14] Kim, J. and Hong, S. (2012). A Consolidated Authentication Model in Cloud Computing Environments. International Journal of Multimedia and Ubiquitous Engineering, 7(3), 151-160.
[15] Kim, W. (2009). Cloud Computing: Today and Tomorrow. Journal of Object technology, 8(1), 65-72.
[16] King, N.J. and Raja, V.T. (2012).Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Reviews, 28, 308-319.
[17] Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computingand Services Science, 1(2), 53-58.
[18] Kuyoro, S.O., Ibikunle, F. and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks, 3(5), 247-255.
[19] Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.
[20] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
[21] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011).Cloud computing — The business perspective. Decision Support Systems, 51, 176– .doi:10.1016/j.dss.2010.12.006

[22] Miranda Mowbray, Siani Pearson. A Client-Based Privacy Manager for Cloud Computing. COMSWARE '09: Proceedings of the Fourth International ICST Conference on Communication System software and middleware. June 2009.

