Security Challenges in IaaS-based Cloud Computing

Kamal Kant Jaiswal[1] Dr. A.K.Dua[2]
[2]Professor

Abstract— The security of our assets in digital form has been challenging to us day by day. As the threats are constantly evolving, the security have been in continuous change from well explained boundary to an elastic borders. This paper clearly mentions the complicated threats the world of IaaS is facing in the present scenario. It also identifies few of the technologies and concerns on the perpective of the identified users as well as it give future remedies for the security research and development to help enhance the security structure of the present technology.
Key words: Cloud Computing, SaaS, IaaS

I. INTRODUCTION

The "cloud" has been defined as many things to many people and it will be constantly evolving day by day. For the present, the scope will be limited to IaaS. So, the main meaning of IaaS is the to give consumers the computational facilities through the Virtual machines, who then try to access those resources assigned to them through Any internet resources such as Wan. The cloud system consumers are granted complete control of any resources assigned to them (e.g., VMs or storage volumes), but have no control of the underlying virtualization or partitioning layer, the physical host(s) on which it executes, or the mapping of virtual resources to physical devices. While the security concerns for this realm are largely applicable to any external handling and processing of an individual or organization's digital assets, we will focus on security concerns for computational cloud computing from the perspectives of cloud service users, cloud service providers, and general security practitioners in both the technical and legal realms.

The dependency on the technology and its high paced evolution has made a challenge for us to secure our digital assets. In older times, computer systems were placed in physical perimeter and data centric approach was made to secure the data stored in the computer. Due to the continuous evolvement of the technology, and f the course the seamless increase of the communication and internet, it became nearly difficult of the people to get their data secured. It became necessary to secure the endpoints rather than data centric protection or physical security. It can be accomplished through the means of various mechanisms including firewalls, changing settings, and other measures. Due to the enhancement of connectivity, the security focus shifted to an overhead of even protecting the applications which are connected to the network. So, it began to increase the demand for making the application layer more secure for those applications and newer areas of tension emerged that included request and provide data, and virtual workstations.

The new evolution towards cloud computing, both IaaS-based and (as data and services are "outsourced" to the cloud) Software as a Service (SaaS)-based and again demands a reconsideration of methods used to provide security. The new critical point is that the changing perimeter that extends further into realms that are controlled by others. The concern is how to secure data which is in transition and also in storage, moreover how to ensure that resources are protected from the service providers. The playable roles of the stakeholders in a system are ever-changing, so the distinguished difference between insider and outsider has become largely blurred [1].

II. TECHNICALITIES AND CHALLENGES.

IaaS-based cloud computing brings many advantages but this model also raises significant technical security considerations and questions. Among those the issues needed to be considered are operational trust modes, sharing of resources, new strategies of attacks and digital forensics. These are important areas of consideration moreover they are further complicated by the issues associated with giving up control in any environment. [6] Due to increase reliance on others to provide functionality, you correspondingly give them control. As this control is given to someone who most likely does not share your vested interest or your corporate mission, it becomes a concern. When you relinquish control, you lose access to information and so, give up the ability to answer some of the important questions regarding technical and jurisdictional issues. In other cases, the information required to make informed security decisions will no longer be available. The data that is available will not be trustworthy because it would be in a system on which you have complete control. Hence, it is vital that the security implications of a cloud computing be carefully considered and factored into a decision about the appropriateness of a cloud-based solution for a given set of IT requirements.

In cloud computing scenario, the cloud resource provider maintains sole access to the underlying physical components of the system, and provides the cloud consumer with full control over some portion of it. In practice, this means that the provider has access to all of the consumer's operations and data in the cloud environment. Among the approaches to that can be used reduce the required level of trust in the cloud provider are:

- *Encryption in Channels for storing Cloud:* From encrypting cloud which is used only to store data, it allows a cloud storage consumer to encrypt the information prior to the process of being inserted in the cloud, hen decrypting it after moving it back to their personal systems. It should be observed, that such purpose cryptographic algorithms are not that effective enough if the data is intended for use *within* the cloud. But it does not mean that information cannot be inferred from careful observation even if it is encrypted. It can be done through carefully observing the data stream.[4]
- *Computation on Encrypted Data:* There are some cases in which it is possible to work on the encrypted data and certain mechanisms allow doing these sorts of methods. They are known as homomorphic schemes. They do not expose the inputs and give the results. This is an area of active

All rights reserved by *www.ijsrd.com*

study in which current results are to be applicable to fairly less amount of operations [2, 3]. Even in this type of operation, a malicious service provider may be able to infer useful information, then the characteristics of the encrypted inputs and results.

A. Sharing of resources

In the current model, resources like storage and hosts are to be used exclusively by a corporate entity. But, in the cloud model it is entirely reasonable that when a resource is allocated to one corporation, it may be used on some physical infrastructure which also hosts resources allocated to other corporate users. As an example, a virtual machine may be started on a physical server which is hosting several VM's; each VM may be allocated to a different corporation. It is quite possible that if there are two competitors, then they may be allocated resources on the same physical infrastructure. Security policies and procedures must consider the possibility that data may leak between competing corporations, or that the actions of one corporation could impact the ability of a competitor to conduct business. Some work has already demonstrated that this can occur [5].

B. Strategies of new attacks

The cloud model has a property to make new attack strategies possible. The new attacking strategies must not be neglected when it is attempted to secure cloud computing resources. There is an example of such a strategy which is the ability of an attacker to co-locate resources with the resources of target [5]. As the attacker has gained such a command, frequent and subsequent attacks may be possible, by using current attacks, by attacking the virtualization layer or physical hardware directly.

III. SOLUTIONS

There is a potential solution that would be for the consumers to tag their resources in a way that would symbolize which components have to be shifted and the whereabouts in certain conditions. This will help into making decisions by a cloud provider about shift of data, not only on the available resources, but also on the necessities of the consumers, indicated by the tags. This would help to simplify the legal problems, particularly for the consumers. It would also limit the provider's ability to manage their resources efficiently which would result in a model which looks far more like the traditional one than the flexible cloud.

IV. CONCLUSION

Though IaaS-based security challenges may not sound that dangerous, it needs to be investigated so that our digital assets could be secured. There should be sound understanding of cloud computing and stakeholders related to it. There should be more research done in the legal and technical issues faced in the world of IaaS-based cloud so that the future threats could be stopped. It needs research related to cloud so that technical and technological issues could be identified which includes trust modes, attack strategies, and sharing of resources. Moreover, legal issues should be concentrated in resource-based cloud research and its implementation and development.

REFERENCES

[1] Bishop, M. and Gates, C. 2008. Defining the insider threat. In Proceedings of the 4th Annual Workshop on Cyber Security and information intelligence Research: Developing Strategies to Meet the Cyber Security and information intelligence Challenges Ahead (Oak Ridge, Tennessee, May 12 - 14, 2008). F. Sheldon, A. Krings, R. Abercrombie, and A. Mili, Eds. CSIIRW '08, vol. 288. ACM, New York, NY, 1-3. DOI= ttp://doi.acm.org/10.1145/1413140.1413158

[2] Change, C, and S. Tsu. Arithmetic operations on encrypted data. International Journal of Computer Mathematics. International Journal of Computer Mathematics, Volume 56, Issue 1 & 2 1995, pages 1 - 10

[3] Micciancio, D. 2010. A first glimpse of cryptography's Holy Grail. Commun. ACM 53, 3 (Mar. 2010), 96-96.DOI= http://doi.acm.org/10.1145/1666420.1666445

[4] [Chen, S, R. Wang, X. Wang, and K. Zhang. Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow. Retrieved June 11, 2010 from http://www.informatics.indiana.edu/xw7/WebAppSide Channel-final.pdf

[5] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. 2009. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM Conference on Computer and communications Security (Chicago, Illinois, USA, November 09 - 13, 2009). CCS '09. ACM, New York, NY, 199-212. DOI= http://doi.acm.org/10.1145/1653662.1653687

[6] Brewer, D.F.C., and M. Nash. "The Chinese Wall Security Policy," pp. 206, 1989 IEEE Symposium on Security and Priv0061cy, 1989.

All rights reserved by *www.ijsrd.com*