ISSN (e): 2250 – 3005 || Vol, 04 || Issue, 6 || June – 2014 ||
International Journal of Computational Engineering Research (IJCER)

Security Issues in Cloud Computing and Risk Assessment

Darshan R, Smitha G R
Department of Information Science and Engineering, RV College of Engineering. Bangalore-560059

Abstract-
Nowadays organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). In this paper we speak about the number of security issues/concerns associated with cloud computing. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. This paper also speaks about the Risks involved in cloud computing when implementing in different organisation considering three scenarios and how it affects the system and also about the risk assessment process where the level of risks are estimated on the basis of the likelihood of an incident scenario when compared against the estimated impact. Finally it concludes by discussing about some of the problems to be solved such as standardised format for the SLA (Service level agreement) and about the encryption process which is computationally expensive.

Keywords- *Cloud Computing, Security issues and Risk Assessment.*

I. INTRODUCTION

Cloud computing becomes more and more familiar to industry crowd, and its wide range of application areas becomes more and more wide. Building a secure computer cloud computing environments becomes one of the hot research topics. In this paper, we discuss the definition of clouding computing, its development status, and analysis part of the security problems. Along with all these some ideas about security and its effect on Cloud computing and at last we propose in this paper about the combination of reducing encryption cost and enhancing SLA strength will be a promising direction of the future cloud security researches.

II. EVOLUTION OF CLOUD COMPUTING

Cloud Computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to give users the pleasure to take most of the advantages from all the technologies, even without much need of shear knowledge about each one of them. The cloud aims to reduce costs, and help the wide range of users to focus on the core business instead of being worried about different IT obstacles. The main enabling technology for cloud computing is virtualization. With the help of virtualization we can generalizes the physical infrastructure of cloud computing, which is the most important and the most rigid component, and convert it as a soft component which will be easy to use and manage it. Doing so, virtualization provides the wide range of agility property required to speed up the IT business and operations, also reduces the cost by massively increasing infrastructure utilization. And also, autonomic computing initiates the automating the process with which the user can provision resources on-demand. In this way, by minimizing user involvement, the process of automation speeds up the process and reduces the possibility of human errors [4].Users face difficult business problems every day. Cloud computing inherits ideas from Service-oriented Architecture (SOA) that can help the user minimize these problems into services that can be integrated to provide a solution. Cloud computing offers all of its resources as a services, and uses all the well-established rules, standards and best practices proposed in the field of SOA to allow vast global and easier access to cloud services in a standard way as shown in Fig 1.

Cloud computing also uses concepts from utility computing with the intention to provide metrics for the services used. All those metrics are at the core of the public cloud models [2]. Along with this, measured services are a necessary part of the feedback loop in autonomic computing, which allows services to measure on-demand and to initiate automatic failure recovery.Cloud computing is also a kind of grid computing, it has evolved by addressing the Quality of Service and reliability problems. It also provides all the necessary technologies and tools to build data and also to compute intensive applications with much lesser prices compared to traditional computing techniques.

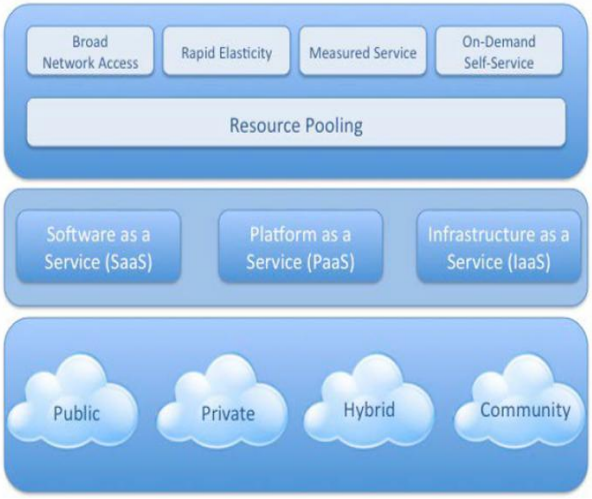

Fig 1: Visual model of Cloud Computing

Advantages

Cloud systems are very economical and useful for all kind of businesses. Cloud computing is a new technology which benefits the user in huge manner and the benefits are:

1. Flexibility.
2. Reliability and Security.
3. Portability.
4. Enhanced Collaboration.
5. Simpler devices.
6. Unlimited Storage and Speed.

III. SECURITY ISSUES

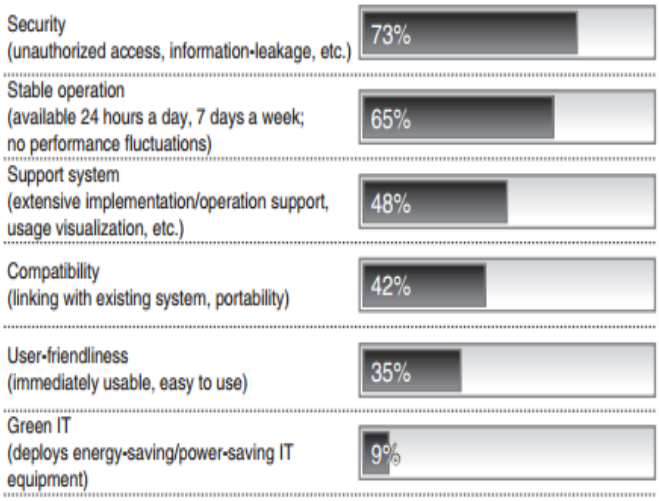

Fig 2: Concerns in Cloud Computing

As shown in the Fig 2, the security element accounts for huge mark of concern in cloud computing. The security issues affecting Cloud Computing Systems are [1]:

- Data security
- Trust
- Network traffic
- Multiple cloud tenants
- Need for access control and identity management

A. Data Security:

About using of cloud computing services, users are not aware of the hosting server location of their data and which particular server manages these data. Based on this, the cloud users and cloud service providers are very important to avoiding data loss and theft. Therefore the following will state the security of cloud computing from data privacy and data isolation [1].

• Data privacy. Data storage in the cloud are shared, that is not to open a separate storage area for the user. So the data has potentially dangerous. And compared with the traditional software, data in cloud computing are maintained by the third party, and due to the characteristics of cloud computing architecture, these data may be stored in scattered locations, and are stored in plain text form. Although the firewall can protect malicious alien attack in some degree of protection, this architecture makes some critical data might be leaked.

• Data isolation. At present in the network users share the data in data encryption ways, but in the cloud computing environment, if they can separate their own data from other user data, they can more effectively ensure data security. Because all customer data will be stored in only one instance of the software system, so it is urgent to develop additional data isolation mechanism to ensure the confidentiality of the data of every customer and provide disaster recovery plan.

B. Trust:

Trust is not easily defined, but most people agree that when it comes to cloud computing, trust can be explained better in terms of transparency. Businesses must be able to see cloud service providers are complying with agreed data security standards and practices. The standards must include controls about access to data, staff security, and the technologies and processes to segregate, backup and delete data. Vendors of cloud technologies and services are quick to claim that cloud computing is well equipped to provide the necessary controls. While Virtualization is viewed with suspicion and fear by many IT directors, suppliers like RSA, IBM and other say that the technology enables organizations to build security into the infrastructure and automate security processes, to surpass traditional data protection levels.

C. Lack of visibility into network traffic:

Many security organizations monitor network traffic to identify and block malicious traffic. The Vendors have delivered appliances that perform monitoring to ease the problems of installation and configuration. All these appliances can be installed on the network just like a normal server, also they can be up and running for longer duration. This appliance approach has simplified security practices and has been an enormous gift to hard-pressed IT and security groups.

There's one problem in the approach, virtual machines on the server communicate through the hypervisor's internal networking, where no packets crossing the physical network and also where the security appliance sits ready to stop them. Of course, if the virtual machines (VMs) are placed on different servers, traffic internal to VMs will run across the network and be available for inspection. To enhance the performance, the virtual machines associated with the same application (example, an application's database server and Web server) are always on the same physical server. Virtualization vendors have provided hooks into their hypervisors that network vendors such as Cisco and Arista have used to integrate with virtual switches that, in turn, enable traffic inspection. Hence this problem is not insurmountable, even though it requires an upgrade to the current method of network switching and the use of security products integrated with the new model. We can translate this as a need for more financial investment.

D. Need for better access control and identity management:

The cloud by nature is highly virtualized, and you need an approach to maintain control and manage identities across your cloud and other ' clouds," says Alan Boehme, who is the senior vice president of IT strategy and architecture at financial services firm 'ING'.

E. Risk of multiple cloud tenants:

As we know cloud services make much use of virtualization technology, the amount of risks associated with multiple organizations' data located on a single hypervisor platform occurs, and that will continue to unless specific segmentation measures are enacted, says Dave Shackle ford, director of security assessments and risk & compliance at Sword & Shield Enterprise Security, and a member of the faculty of research firm IANS [5].

IV. RISK ASSESSMENT

A. USE-CASE SCENARIOS

For the purposes of this risk assessment of cloud computing, we have three use-case scenarios [3]:

i) An SME perspective on Cloud Computing

ii) The Impact of Cloud Computing on service resilience.

iii) Cloud Computing and eGovernment.

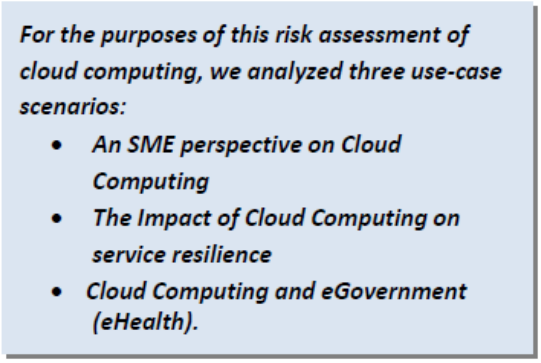

Fig 3: Use case scenarios.

As shown in the Fig 3, the selection was based on the rationale that in Europe the cloud market is foreseen to have a great impact on new businesses and new start-up companies, and also on the way new business models will evolve. Since EU industry is mainly composed by SMEs (99% of companies according to EU sources- (9)) it makes sense to spotlight on SMEs. We have included several risks and recommendations which apply specifically to governments and larger enterprises. The SME scenario is based on the results of the survey: An SME perspective on Cloud Computing and it is NOT meant to be a road map for companies considering, planning or running cloud computing projects and investments. A medium-sized company was used as a use-case to guarantee to the assessment a high enough level of IT, legal and business difficulties. The main aim of this was to expose all the possible security risks. Some of those risks are specific to medium-sized businesses, others are general risks that micro or small enterprises are also likely to face when migrating to a cloud computing approach.The second scenario explores how the use of cloud computing affects the resilience of services in the face of,sudden increases in customer demand (e.g., in periods of financial crisis),denial of service attacks,localised natural disasters, misuse of the infrastructure as an attack platform, data leaks (malicious or careless insider or broken process).The third scenario explores the use of cloud computing by large government bodies which have to satisfy strict regulatory requirements and are very sensitive to negative public perception. A key consideration when using cloud services will be a public perception that there has potentially been a lack of consideration of security or privacy issues. This would be especially true should ‘public’ cloud services be used.

European Health represents a large government health service in Europe but does not describe any specific national health service. European Health is composed of public organisations and private suppliers providing e Health services. It is a very large organisation spread across several sites and it caters to 60 million citizens. Prior to using any kind of cloud infrastructure, it has over 20 IT service providers and more than 50 data centres.

V. RISK ASSESSMENT PROCESS

The level of risk is estimated on the basis of the likelihood of an incident scenario when compared against the estimated impact. The possibility of an incident approach is given by a threat exploiting vulnerability with a given likelihood [3]. The possibility of each incident scenario and the business impact was determined in consultation with the expert group after contributing, obtaining on their collective experience on this report. Whenever the cases where it was judged not possible to provide a well founded estimation of the possibility of an occurrence, then the value will be N/A. In most of the cases the estimate of possibility depends heavily on the cloud model or architecture under consideration. The following shows the risk level as a function of the business impact and possibility of the incident scenario, refer Fig 4. The resulting risk which is measured on a scale of 0 to 8 will be evaluated against risk acceptance criteria. And this risk scale can also be mapped to a simple overall risk rating:

- Low risk: 0-2
- Medium Risk: 3-5
- High Risk: 6-8

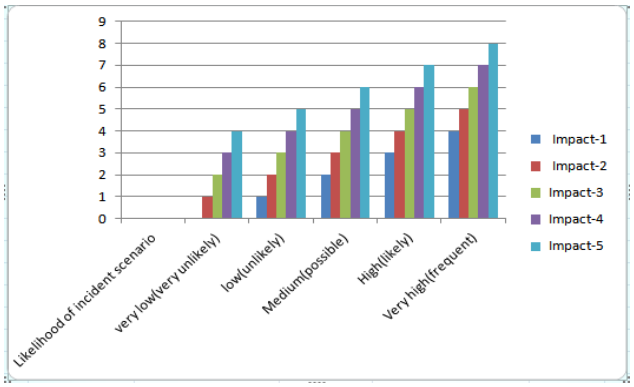

Fig 4: Risk Assessment report

VI. CONCLUSION

Cloud Computing offers some incredibly huge benefits such as unlimited storage, quick processing power and also the ability to easily share the information and process it; however, it also have several issues, and most of them are security issues. Cloud systems must overcome many difficulties before it becomes widely adopted and popular, although it can be utilized right now with some compromises and in the right conditions. Organization can enjoy all the benefits of cloud computing if we can address the very real security concerns that comes along with storing sensitive information in databases scattered around the internet.We have discussed several security issues that currently affect cloud systems; even after all that, there may be many undiscovered and unmentioned security problems. So many research work are currently being done on the different unknown issues faced by cloud systems and possible solutions for these issues, there is still a need for better solutions if cloud systems are to be widely adopted.One of the main problems that need to be addressed is coming up with a clear and standardized format for the Service Level Agreement (SLA) [5], a format that fully documents all of the services, the services and processes that would be provided by the service provider to back up its assurances. In the situations where the customers have the right amount of expectations and all the insecurities concerns are deemed manageable, cloud computing as a whole will keep ground and take firm hold as usable technology.
Another major issue cloud systems face is Encryption. There are many methods like Encryption, which is the main method of ensuring security of data stored in the cloud; Encryption is computationally expensive. Encryption methods specific to Cloud Databases has been developed and more research is currently being done on Encryption mechanisms for cloud systems, more efficient methods are still needed to help accelerate the adoption of cloud systems.

VIII. ACKNOWLEDGMENT

I would like to thank my guide Mrs. Smitha G R for guiding me in all aspects in the process of preparing this paper.

REFERENCES

[1] Liu Xiao-hui, Song Xin-fang. Analysis on cloud computing and its security. Computer science and education(ICCSE), 8th international conference on digital object identifier, 2013, pp:839-842.

[2] O.Mirkovic. Security Evaluation in cloud. Information and communication Technology electronics and microelectronics(MIPRO), 36th International Convention.2013,pp-1088-1093.

[3] ENISA, "Cloud computing:Benefits,risks and recommendations for information security.

[4] Yushi Shen; Jie Yang; Keskin,T. The Evolution of IT towards Cloud computing in china and U.S.Computational Problem solving(ICCP), International Conference on digital object identifier, 2012. Pp:224-235.

[5] Behl,A;Behl,K; An analysis of Cloud Computing security issues. Information and communication Technologies(WICT), World congress on digital object identifier,2012,pp-109-114.

[6] Yang Jian, Wang Haihang, Wang Jian, Yu Dingguo. Survey on Some Security Issues of Cloud Computing. Journal of Chinese Computer Systems. 2012(3):473-476

[7] Wu Jiyi, Shen Qianli, Zhang Jianlin, Shen Zhonghua, Ping Lingdi. Cloud Computing:Cloud Security to Trusted Cloud. Journal of Computer Research and Development. 2011(48 suppl):230-231.

[8] Tian Ming, Zhang Yongsheng. Analysis on cloud computing and its security. Information technology in medicine and education (ITME), International symposium on digital object identifier, 2012, pp:379-381.

[9] Shaikh, F.B.Haider. Security threats in cloud computing. Internet technology and secured transactions(ICITST), International Conference, 2011, pp:214-219.