Evaluation of The faults of Data Security and Privacy in the Cloud Computing

AL-Museelem Waleed[1,a], Li Chunlin[2,b]

[1, 2]School of Computer Science, Wuhan University of Technology, Wuhan, CHINA

[a]waleed_aboanas@hotmail.com, [b]waleedalmuseelem@gmail.c

Keywords: Cloud computing, Data Security, Data Privacy, Ubuntu Cloud Simulation, CloudSim, SQL injection ,Attacks, Encryption.

Abstract. Recently the topic of Cloud Computing use is considered to be a burning issue as this notion is rather new and still not studied enough. Therefore, its advantages and disadvantages are currently discussed by the specialists. According to the definition, Cloud Computing is "a model for delivering information technology services in which resources are retrieved from the internet through web-based tools and applications, rather than a direct connection to a server. Data and software packages are stored in servers. However, cloud computing structure allows access to information as long as an electronic device has access to the web. The vital requirements include networking infrastructure that is physically available. The internet and the evolution that has taken place in the internet are also recognized as a major source and driving force behind the growth of cloud computing. End devices that are constantly evolving e.g. mobile, laptops, desktops are also recognized as essential in the support of cloud computing as a service. The problem is mainly the security and storage of client's data. In the paper the faults on security of their data storage and it's privacy is reviewed. It also includes in it conducted experiment and statistical analysis using ubuntu simulation. and CloudSim The paper identifies and evaluation the faults and proposes solutions to combat the identified problems.

Introduction

Cloud computing is a flexible delivery platform for business or consumer services provided over the internet. Public cloud computing delivers better services under pressure. The concept of cloud computing was initiated in the early 1960's and initially was used basically by telecommunication companies. By the year 2008 Gartner highlighted the characteristics for customer and service providers [3]. The paper outlines awareness of cloud computing power in the entire IT industry through addressing of global challenges and arising issues in implementation of the public cloud infrastructure.

In spite of all the possible security and privacy risks, Cloud Computing is believed to be beneficial for the public and private IT organizations. According to the latest researches, this phenomenon is proved to have six main advantages that make it attractive for the potential users. There is a brief summary of these peculiarities:

1. Economy of cost (Cloud technology is usually paid incrementally, thus saving money for the company);
2. High level of automatism (this software product has the update function and IT personnel can escape this task);
3. Increase of Storage capacity (more data can be stored as compared to the private computer systems);
4. Flexibility (more flexible in comparison with the previous computing methods);
5. Mobility (the employees are able of accessing the information from the place of their location);
6. Freedom of actions to the organization (the company has the possibility to shift the focus and concentrate better on the innovations than on the constant server updates).

The principle of the Cloud Computing is related to the searching for the connection between the main layers of the structure. It usually consists of five layers: client, application, platform,

infrastructure and server. Correspondingly, each of them has its own characteristics and is considered to play important role in the process of Cloud Computing. Consequently, this trend is very interesting and useful to investigate as it may become a basis of the future IT structure for the organizations.
In the collection of information and statistics, experiments were conducted and analysis done using ubuntu simulation. With a review of cloud computing data storage, addressing the security faults and challenges faced in implementation of public cloud service, including mitigation steps [4].

Literature Review

The literature identifies the major broad service models used in cloud computing. The most recognizable model of cloud computing to many consumers is the public cloud model, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet [6]. To some extent they can be defined in contrast to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform to which only a single organization has access. Public clouds, however, provide services to multiple clients using the same-shared infrastructure.
The most salient examples of cloud computing tend to fall into the public cloud model because they are, by definition, publicly available. Software as a Service (SaaS) [7] offerings such as cloud storage and online office applications are perhaps the most familiar, but widely available Infrastructure as a Service (IaaS) [8] and Platform as a Service (PaaS) [9] offerings, including cloud based web hosting and development environments, can follow the model as well (although all can also exist within private clouds). Public clouds are used extensively in offerings for private individuals who are less likely to need the level of infrastructure and security offered by private clouds. However, enterprise can still utilize public clouds to make their operations significantly more efficient, for example, with the storage of non-sensitive content, online document and webmail [10].
The public model offers the following features and benefits:
A. Ultimate scalability
Cloud resources are available on demand from the public clouds' vast pools of resource so that the applications that run on them can respond seamlessly to fluctuations in activity
Cost effective; public clouds bring together greater levels of resource and so can benefit from the largest economies of scale. The centralized operation and management of the underlying resources is shared across all of the subsequent cloud services whilst components, such as servers, require less bespoke configuration. Some mass-market propositions can even be free to the client, relying on advertising for their revenue.
B. Utility style costing
Public cloud services often employ a pay-as-you-go charging model whereby the consumer will be able to access the resource they need, when they need it, and then only pay for what they use; therefore avoiding wasted capacity.
C. Reliability
The sheer number of servers and networks involved in creating a public cloud and the redundancy configurations mean that should one physical component fail, the cloud service would still run unaffected on the remaining components. In some cases, where clouds draw resource from multiple data centers, an entire data centre could go offline and individual cloud services would suffer no ill effect. There is, in other words, no single point of failure which would make a public cloud service vulnerable [11].
D. Flexibility
There are a myriad of IaaS, PaaS and SaaS services available on the market which follow the public cloud model and that are ready to be accessed as a service from any internet enabled device. These services can fulfill most computing requirements and can deliver their benefits to private and enterprise clients alike. Businesses can even integrate their public cloud services with private clouds, where they need to perform sensitive business functions, to create hybrid clouds [12].

E. Location independence

The availability of public cloud services through an internet connection ensures that the services are available wherever the client is located. This provides invaluable opportunities to enterprise such as remote access to IT infrastructure [13] or online document collaboration from multiple locations. The most recognizable model of cloud computing to many consumers is the public cloud model, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet. To some extent they can be defined in contrast to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform to which only a single organization has access. Public clouds, however, provide services to multiple clients using the same shared infrastructure.

Problem statement

The capacitance of cloud computing that is to be used b y an information and technology organization. Giving inspirations for the implementation of cloud computing. The section is based on security issues of cloud computing, with results of a research conducted on cloud computing security.

A. Research Results on Cloud Computing Security

B. Security Issues In Cloud Computing

Cloud computing is a use of diverse computer resources like software and hardware introduced as a service within the certain network, especially Internet. Basically, there exist three kinds of cloud computing: service platform, infrastructure as a service and software service. The information flow is usually provided within the network and by means of central and remote servers.

This way, computer owners can track the work done and secure operational systems on remote computers. Virtualization is an aspect of cloud computing where virtual versions of operating systems, hardware platforms, network resources or storage devices are created. The main purpose of virtualization is to centralize administrative tasks, improving overall hardware-resource utilization. The ability to run two operating systems in parallel mode allows reducing overhead costs due to running the same programs within the same operating systems.

Both cloud computing and virtualization can have numerous benefits and drawbacks. First of all, let us speak about cloud computing. Cloud computing is favorable in terms of ability to achieve economies of scale. It allows increasing production output with fewer people. Respectively, the cost of projects is also slightly reduced because of that. Furthermore, cloud computing give an opportunity to globalize workforce for cheap. It means that everyone from everywhere can access the computer cloud via Internet. Cloud computing also reduces spending on technology infrastructure: minimal upfront spending is worth unlimited access to information.

Virtualization also has both benefits and drawbacks. Let us initially focus upon its benefits. The major benefit of virtualization is the amount of hardware required for all software applications. And this is a cost-saving factor. Additionally, application virtualization offers a flexible opportunity to run applications with various configuration settings. Virtualization eliminates the need to run numerous separate servers. This way, hardware is seen to be used efficiently. Living in the globalized world, we are always linked to computers. Virtualization support enables many organizations to outsource practically all their computing requirements.

Operational security concerns include business continuity, disaster recovery, incident response, encryption, vulnerability assessment, identity access management and virtualization [15].

The cloud plays a critical role in helping organizations capitalize on the efficiency, flexibility and ease of operation. Companies must invest in people with the technical skills necessary to assess their readiness for implementing different cloud architectures that help move data in and out of public/private clouds and understand the security risks associated with changes related to cloud architecture.

In the SAAS model control lies on the cloud service provider hands.

It is risk as delicate and sensitive information might be accessed someone else. Providing guidelines for the process.

1. Protection of transferred data.
2. Service provider giving clients security policies.
3. Back up Availability.
4. Lack of availably of data backups.
5. Multi-Tenancy.

A future of SAAS that allows a single program running in multiple machines It increases vulnerability.

Proposed solution

The authenticity and confidentiality of data are based on data encryption method. Encryption of data.The simulation tool is distributed file base system, which is downloadable in the Ubuntu and other operating systems. There is a critical need in information security, and one of the most crucial ways to localize possible threats is simulation and modeling. The simulation is the process of designing the real cyber-attacks models. This process is targeted to satisfy the expectations at the end. The simulation models can be continuous and discrete, depending on time characteristics. Constructing models, we test our system in the virtual world and want to shape our company strategy. Here it is obvious that the simulation model is effective as it depicts all the processes that are planned to happen in succession. Though each process is connected to the other one, they are supposed to be supported by the respective managers. The methods of modeling and simulation should be immediately introduced to every company that is interested in getting high incomes.In terms of analysis and simulation models it is proposed to give priority to team or group work and profound brainstorming. In terms of management processes it is suggested to implement the innovative software within each department that is recommended to be used only by the professional managers, who can bring positive results. As for the types of attacks performed in the system, they are as follows: Mandatory attacks, SQL injection attacks, and directory traversal attacks.

Indisputably, every particular organization is prone to threats, because in all times the competing companies are targeted to drive their rivals out of the market, gaining the competitive advantage over them.Basically, it is crucial for the business organization to establish correct information security policy in order to function in accordance with the norms of law and at the same time preserve its interests. The majority of corporation and non-governmental organizations protect the information that can be damaged or used to threaten the national security or reveal some trade secrets of companies. There are also certain rules adopted by the state authorities for information clearance and the ways it should be gathered, stored, transmitted and damaged. These are security precautions that are needed for the organizations and individuals for ensuring their protection.

Experiment and analysis

The chart figures shows the attacks conducted on the simulation tools while using security models and when security models are not available. System with no security model is better than systems having the security model. Systems with security model require resources for the system. After conduction of the attack using the cloudism simulation tool and open stack process, the performance increases after each attacks making simulation of the cloud competing vital.

[Table 1.Cloud Computing Attacks]

Experiment results	Attacks	Using of SACS Extent	Not using SACS Extent
Cross VM attacks	10	25	70
Mandatory access attacks	15	43	90
Sql injection attacks	10	34	68
Directory traversal attacks	5	21	57
DDos attacks	25	35	68

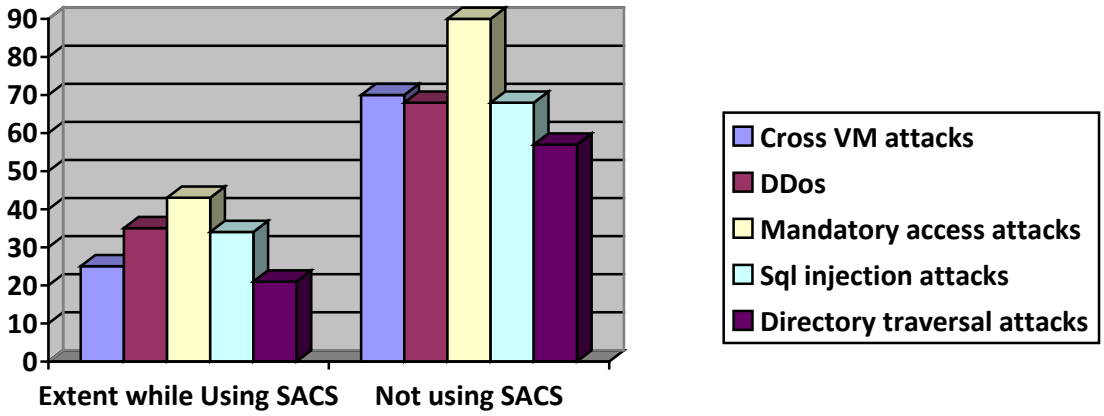

Figure 1. System Performance(1)

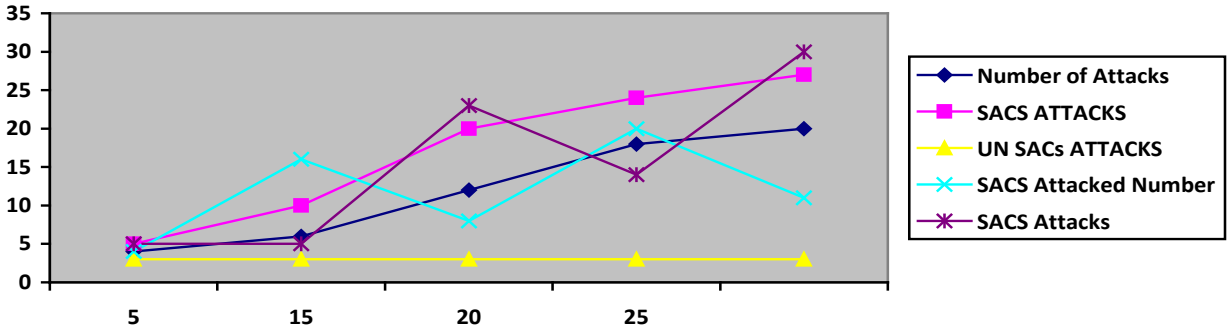

Figure 2 System Performance (2)

Summary

Cloud computing serves as the latest development that provides for easy access to higher performance computing services and storage through the web. It offers unique opportunities to many countries in the world through the web services. After identification of problems in cloud computing steps for mitigation are identified and solutions are proposed.

Acknowledgments

The work was supported by the National Natural Science Foundation (NSF) under Grants (Nos. 61472294, 61171075), Key Natural Science Foundation of Hubei Province (No. 2014CFA050), Applied Basic Research Project of Wuhan (No. 2015010101010021), National Key Basic Research Program of China (973 Program) under Grant No. 2011CB302601, Program for the High-end Talents of Hubei Province.

References

[1] AL-Museelem Waleed & Li Chunlin , Data Security and Data Privacy in Cloud Computing, Advanced Materials Research Vol. 905 (2014) pp 687-692.

[2] "Research and Markets Adds Report: State of Cloud Computing Security in the UAE." Manufacturing Close - Up (2013)ProQuest. Web. 22 Dec. 2013.

[3] "Research and Markets Offers Report: State of Cloud Computing Security in the UAE." Professional Services Close - Up (2013)ProQuest. Web. 22 Dec. 2013.

[4] "SafeCentral Integrates Browser Security Solution with NetSuite's Cloud Computing Platform." Business WireDec 01 2010. ProQuest. Web. 22 Dec. 2013 .

[5] "Security Experts from Core Security and Invincea Lead Special Issue on Cloud Computing Security for IEEE Security & Privacy Magazine." Business WireDec 08 2010. ProQuest. Web. 22 Dec. 2013 .

[6] Alzain, Mohammed A., Ben Soh, and Eric Pardede. "A New Model to Ensure Security in Cloud Computing Services." Journal of Service Science Research 4.1 (2012): 49-70. ProQuest. Web. 22 Dec. 2013.

[7] Antonopoulos, Nick, and Lee Gillam. Cloud Computing: Principles, Systems and Applications. London: Springer, 2010. Print.Auditing Cloud Computing: A Security and Privacy Guide. Wiley, 2011. Internet resource.

[8] Badamas, Muhammed A. "Cyber Security Considerations when Moving to Public Cloud Computing." Communications of the IIMA 12.3 (2012): 1-18. ProQuest. Web. 22 Dec. 2013.

[9] Bradner, Scott. "Cloud Computing Security: Who Knew?" Network World 26.17 (2009): 16. ProQuest. Web. 22 Dec. 2013.

[10] Gutwirth, Serge. Computers, Privacy and Data Protection: An Element of Choice. Dordrecht, The Netherlands: Springer, 2011. Print.

[11] Howell, Donna. "Security Still Top Cloud Issue, Pair of Recent Surveys Confirm Majority See Vulnerability Moving to Internet-Based Computing Slowed as Top Executives Preach Caution." Investor's Business DailyNov 07 2011. ProQuest. Web. 22 Dec. 2013 .

[12] Ismail, Noriswadi, and Edwin L. Y. Cieh. Beyond Data Protection: Strategic Case Studies and Practical Guidance. Berlin: Springer, 2013. Internet resource.

[13] Krutz, Ronald L, and Russell D. Vines. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, Ind: Wiley Pub, 2010. Internet resource. Proceedings. Berlin: Springer, 2011. Print.

[14] Mantri, Archana. High Performance Architecture and Grid Computing: International Conference, Hpagc 2011, Chandigarh, India, July 19-20, 2011. Proceedings. Berlin: Springer, 2011. Print.

[15] Prasad, Sushil K. Information Systems, Technology and Management: 4th International Conference, Icistm 2010, Bangkok, Thailand, March 11-13, 2010. : Proceedings. Berlin: Springer, 2010.