The faults of Data Security and Privacy in the Cloud Computing

AL-Museelem Waleed1,a, Li Chunlin2,b, Naji, Hasan.A.H3,c
1, 2, 3 School of Computer Science, Wuhan University of Technology, Wuhan, CHINA
awaleed_aboanas@hotmail.com, b waleedalmuseelem@gmail.com, c hasanye1985@gmail.com

Abstract—According to Winkler [1], public cloud is based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

The main benefits of using public cloud services include:

- Easy and inexpensive set-up.
- Scalability to meet needs.
- No resource wastage.

The term "public cloud" was invented to differentiate between the standard model and the private cloud, which is a proprietary network or data center that uses cloud-computing technologies, such as virtualization.

Examples of public clouds include Amazon Elastic Compute Cloud [2], IBM's Blue Cloud, and Sun Cloud. Despite of the advantages it also has some faults in its infrastructure. With the customer being unaware of their data storage over the internet, 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. The paper identifies the faults and proposes solutions to combat the identified problems.

I. 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.

Nowadays 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. This type of system allows employees to work remotely.” (Hurwitz, Judith., Boor & Kaufman).

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 posed in implementation of public cloud service, including mitigation steps [4].

The report gives out in details what are to be considered and guidelines on implementing cloud computing with computer organizations.

The paper is categorized into sections: Section one presenting the Abstract [5]. Section two provides the introduction, section three includes the literature review, section four represents the problem statement, section five contains the proposed solution, section six containing the experiment results and analysis using ubuntu simulation, section seven presents the conclusion and future work and finally the references in section eight.

II. 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.

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) offerings such as cloud storage and online office applications are perhaps the most familiar, but widely available Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) 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 collaboration and webmail [14].

III. PROBLEM STATEMENT

The capacitance of cloud computing that is to be used by 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


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.
Thanks to cloud computing, more work is usually done in less time. Once hardware and software are purchased, there is no need in constant replacement due to cloud computing, which significantly reduces capital costs. Cloud computing also allows tracking and planning projects within the certain budget, making reasonable business forecasts for the future.

Regarding the fact that cloud computing is based upon the utilization of hardware and software, it is easy to use and there is no need in personnel training. Minimizing licensing of software met due to cloud computing and this improves company flexibility. However, there are several disadvantages of cloud computing. The first is probable downtime. If Internet connection is not reliable, providers are expected to suffer server outages. Additionally, cloud computing may not always be favorable for large companies, which utilize huge resources and keep much information. Cloud computing provides availability of all details and in some cases it cannot be appreciated. Apart from that, there is a great chance of choosing ineffective cloud computing vendor who will offer ineffective and inflexible package.

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.

Respectively, the costs related to central server are also slightly reduced. Additionally, numerous virtualization tools allow users rapidly maintain various testing environments with the opportunity to restore them to their original state. Finally, virtualization is easy to be applied, without fearing numerous hardware compatibility concerns, base computing environments and so on.

Thus, in some cases virtualization can be unfavorable. For example, virtualization has a single point of failure, which means when the central server breaks down, the rest crashes as well. In addition, visualization always demands expensive computers with powerful parts, which may be a costly solution for many small and medium-sized businesses. Finally, when dealing with databases, it would be extremely difficult to implement virtualization as databases and warehousing both require disk operations as well as numerous network updates.

Concerning cloud computing, one should also be aware that organizations must evaluate their existing governance against the cloud security model and understand the residual risks and what compensating controls need to be implemented. Governance areas for concern include risk management, legal and compliance, life-cycle management and portability [14].

Organizations must evaluate their existing governance against the cloud security model and understand the residual risks and what compensating controls need to be implemented. Governance areas for concern include risk management, legal and compliance, life-cycle management and portability [15].

Operational security concerns include business continuity, disaster recovery, incident response, encryption, vulnerability assessment, identity access management and virtualization [16].

The cloud multi-tenant environment security controls are developed for a general service offering which may or may not provide adequate security for every organization. Organizations need to assess their vulnerabilities and implement threat prevention policies and technologies; otherwise, reacting to breaches will become more the rule than the exception [17].

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.

Because of the organizational and cultural complexities of executing cloud strategies, companies are opting, to "out task" certain aspects of their operations because skilled resources are in short supply. Companies who understand the organizational impacts of cloud and who can acquire these skills, set the right security policies, and build closer relationships with the lines of business will be the best able to mitigate the two big risks associated with cloud security [18].

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.

7. Protection of transferred data.
8. Service provider giving clients security policies.
10. Lack of availability of data backups.
11. Multi-Tenancy.
A future of SAAS that allows a single program running in multiple machines It increases vulnerability.

IV. PROPOSED SOLUTION

The authenticity and confidentiality of data are based on data encryption method. Encryption of data, which includes digital signatures, clients are provided with superset signatures and metadata along having querying results. Encryption variety incorporates querying encrypted data that utilizes several cryptographic
methods in data encryption Simulation tool. 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. Although the techniques can be observed only on the planning level, they are suggested to be used due to the balanced system of business organization. No matter what tools or techniques are used, it is necessary to be precisely sure that by means of software and planning management activities each company is more likely to be successful of business. Moreover, one should also consider that the success comes after prolific and productive efforts that can be the result of only highly qualified and experienced staff. 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. Generally, network security threats can combine various risks, problems and attacks, which are very frequently called the security vulnerabilities. The human behavior in the body of employees is the first danger in terms of security network. Apart from that, organizations can be also vulnerable for threats, because not all of them are engaged in using properly configured networks and not all of them have enforced the reasonable and sensible security policy without consulting the expert. That is why if we are targeted to design the secure network, we need to incorporate fault-tolerant solutions and systems.

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.

V. 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>
<thead>
<tr>
<th>ATTACKS</th>
<th>Experiment results</th>
<th>Using of SACS</th>
<th>Not using SACS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross VM attacks</td>
<td>10</td>
<td>25</td>
<td>70</td>
</tr>
<tr>
<td>Mandatory access attacks</td>
<td>15</td>
<td>43</td>
<td>90</td>
</tr>
<tr>
<td>SQL injection attacks</td>
<td>10</td>
<td>34</td>
<td>68</td>
</tr>
<tr>
<td>Directory traversal</td>
<td>5</td>
<td>21</td>
<td>57</td>
</tr>
<tr>
<td>DDos attacks</td>
<td>25</td>
<td>35</td>
<td>68</td>
</tr>
</tbody>
</table>

© 2014 ACADEMY PUBLISHER
VI. CONCLUSION

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.

VII. FUTURE WORK

Regarding cloud computing, it is necessary to take into account numerous security issues as an important part to consider. The security issues include data handling, management, governance, and data protection of personal information. Cloud computing regularly encounters security challenges. As for this paper, it has communicated the initial steps in the security challenge.

ACKNOWLEDGMENT

The work was supported by the National Natural Science Foundation (NSF) under grants (No.61171075), National Key Basic Research Program of China (973 Program) under Grant No.2011CB302601, Special Fund for Fast Sharing of Science Paper in Net Era by CSTD (FSSP) No.20130640001, Program for the High-end Talents of Hubei Province, Specialized Research Fund for the Doctoral Program of Higher Education under Grant...
No.2012043110014 and the Open Fund of the State Key Laboratory of Software Development Environment (SKLSDE-2013KF). Any opinions, findings, and conclusions are those of the authors and do not necessarily reflect the views of the above agencies.

REFERENCES


AL-Museelem Waleed, I'm from Kingdom of Saudi Arabia birth in 5th January 1981 at Capital City Riyadh. Currently I'm a PhD student in College of Computer Science and Technology at Wuhan University of Technology. I received M.S in Computer Science and Technology from Wuhan University of Technology, China, in 2012. My research interests are cloud computing security and data privacy.

Li Chunlin, she is a Professor of Computer Science in Wuhan University of Technology. She received the M.S in Computer Science from Wuhan Transportation University in 2000, and PhD in Computer Software and Theory from Huazhong University of Science and Technology in 2003. Her research interests include cloud computing and distributed computing.
Naji, Hasan.A.H, He is currently a PhD student in college of Computer Science and Technology at Wuhan University of Technology. He received his B.S and M.S from Wuhan University of Technology, China, in 2008 and 2010 respectively. His research interests are cloud computing, Service Oriented Computing (SOC) and ontology.