Proc. of the Intl. Conf. on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

Cloud Computing, Security Issues and Potential Solution by Using ICMetrics or Biometrics Based Encryption

Masudur Rahman, Wah Man Cheung

***Abstract*- Cloud computing is an emerging field of computer networking which is providing opportunities to use hardware, infrastructure or application as a service. Many organisations are considering cloud computing as cost effective, secure and suitable solution for their needs. However security concerns are involved with using cloud services provided by a third party. In this paper, we investigate cloud computing by considering security awareness of the cloud services, critical security threats involved with cloud computing, good practice to ensure security within the cloud and the possibility of using ICMetrics or Biometrics based encryption to provide efficient security within a cloud computing environment.**

***Keyword*- Cloud computing, cloud computing threats and risks, good security practice for cloud computing, ICMetrics.**

I. Introduction

Mike Gunderloy[1], a technology writer, compared the handling of information with the of handling the money. He explained the storage of the information in a way of keeping this in local computer's hard drive by considering the risk of failure of the drive or any potential disaster.

Masudur Rahman,
Faculty of Business and Services,
Colchester Institute
United Kingdom

Wah Man Cheung
Faculty of Business and Services,
Colchester Institute
United Kingdom
School of Computer Science and Electronic Engineering,
University of Essex
United Kingdom

On the other hand like money, users can keep information in a bank of "server" that exists in the "cloud", where the user can withdraw their money anytime from any networked ATM. Robin Hasting[2] has defined the cloud as "a massive network of cloud storage devices (servers and others) that exists somewhere over the internet. Cloud is a network of servers which is capable of running a service, providing storage opportunities or a platform to deliver certain tasks. Organisation can adopt the cloud computing solution by outsourcing or setting up their own. One of the main advantages of using cloud computing has been described by Chris Brogan[3], a renowned blogger. When his personal computer died, he faced less trouble than expected because of his increased use of cloud computing, documents were on Google Docs, Calendar was in his Gmail account, important information was stored in online storage space, extensive use of Flicker and Delicious (previously known as Del.icio.us). Using cloud computing provides a great deal of support and assurance in terms of data backup, disaster recovery and business continuity, while accessibility of the information from anywhere with the proper access right make the whole process very convenient in today's internet dependant world. In many cases, cloud computing provides a cost effective, efficient and secured networked service. For example, it might not be suitable for the small organisation to buy expensive servers, IDS or to employ a security expert to ensure their data security and backup, where organisations like Amazon, Google or Microsoft offer successful cloud solutions like SaaS, PaaS, or HaaS with adequate resources and security; which would be suitable for any organisation regardless of the size or revenue. However there are many security concerns involved with adopting the cloud computing within the organisation.

Proc. of the Intl. Conf. on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

The following sections of this paper present a survey on security awareness of the cloud service providers, threats and risk involved in cloud computing, recommendations of good practice for cloud service providers and recommendations to implement ICMetrics or Biometrics within cloud based virtual machines (VM) for efficient and effective data encryption.

II. A survey on cloud service providers

Despite the advantages of using cloud computing, recent research shows serious security concerns exists. The Ponemon Institute's study "security of cloud computing providers" revealed some alarming issues related to the data security. The study sponsored by CA Technologies and conducted on 103 cloud computing providers from the US and 24 providers from different European countries, shows that a significant number of cloud service providers do not consider the "security of the user's data" as their responsibility but the responsibility of the customers to keep their information secure while stored in the cloud. According to this study, most of the service providers' key focus was to provide features and functions according to the needs of the customers but these service providers do not provide the assurance of adequate security of these products or services.

Some key findings of this survey are[5]:

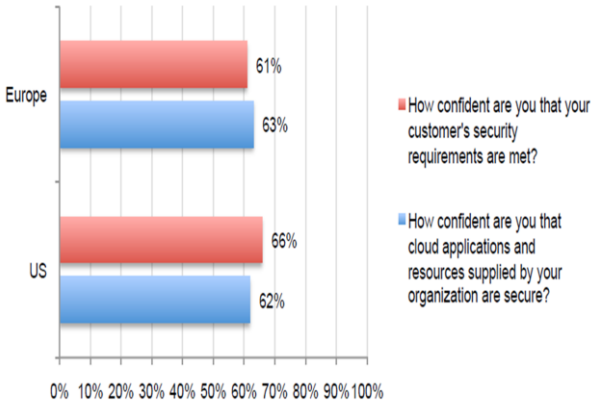

Figure 1[4]

- Most of the participant organisations do not consider the security as a key success factor neither do they believe that their products or services provide the assurance of protecting customers confidential information. A more alarming finding was 66% of US and 61% of European participants were "not sure" about adequate security of their cloud services (Figure 1).

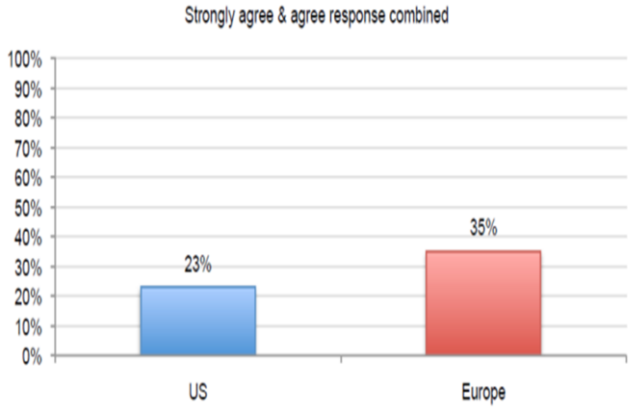

Figure 2[4]

- Furthermore, only 35% of European participants said management "strongly agree" or "agree" about the concern related to in cloud information security, while this number in US is only 23%. (Figure 2)

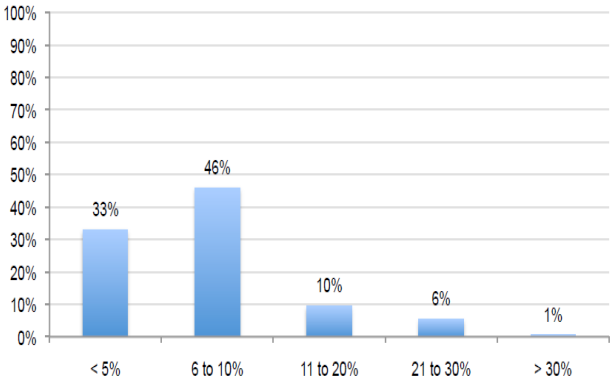

Figure 3[4]

- Fewer than half of the cloud service providers from the US and Europe allocate 10% or less of their resources to ensure the security of the system or the information, which may not be enough to provide sufficient and reasonable security of the customer's information. (Figure 3)

Proc. of the Intl. Conf. on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

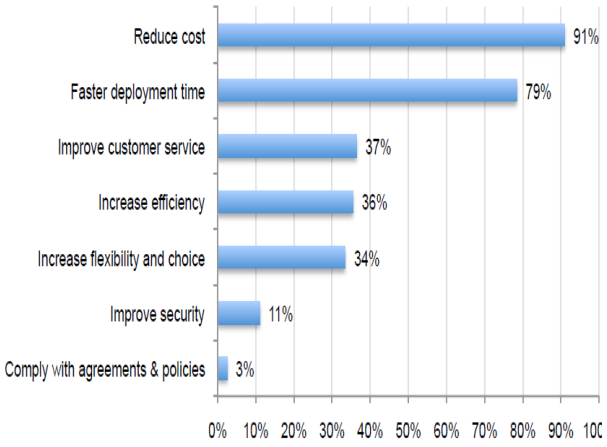

Figure 4[4]

- Most cloud providers said that customers are interested in using a cloud service as it is cost effective. To make it cost effective, many of the participants do not have dedicated security expert within the organisation. (Figure 4)

- Most cloud providers said that the customers need to ensure their own data security. A significant number of the providers do not always conduct the penetration testing on their system to identify the vulnerabilities before deploying the system for the customers.

The Ponemon study has raised a serious question about cloud service providers' efforts to ensure the security of information; therefore organisations needs to be careful before adopting the cloud solution. However, the lack of assurance about security by the cloud service providers is not the only issue related to the use of cloud services, there are more serious concerns involved; which we will explore in the next section of this paper.

III. Security threats for cloud computing

To reduce the cost of an organisation's IT Operation and maintenance, many organisations are moving towards the adoption of cloud solutions, which heavily depend on "virtualisation". According to International Data Corporation (IDC) survey, 87.5% participants believe that "security" is the most important challenge of cloud computing[5]. The security risks related to cloud computing can be categorised. Ramgovind[6] and Nitin Sing Chauhan[7] have suggested an approach of identifying security risks based on six major elements. These are: Confidentiality, Integrity, Authentication, Authorisation, Non-repudiation and Availability. Each of these elements of information security is crucial for customers who expect to ensure the data security, integrity, availability while the down time of the service needs to be minimised. Even though there is a significant development in security tools; it is important to identify the security threats and adopt a security framework or model to comply with the legislation as well as to keep the customers' confidence. In the next section, we will categorise the threats involved in cloud computing.

IV. Potential threats to the cloud computing

API is a way of communicating with the cloud services from the client end. Cloud computing providers need to ensure the vulnerabilities of the API's have been identified and ensure the security of the API's. API vulnerabilities can be used by the attacker to attack the PaaS or IaaS based cloud service.

According to Nagaraju Kilari[8], virtualisation is a key aspect of many cloud services where it has four important security threats namly isolation failure, dependency on Hypervisor, service disruption and shared technology. VM-Hopping and VM-Escape are two newest threats derived from these four virtualisation risks. Within cloud environment, one physical machine may have many virtual machines implemented with the help of Hypervisor technology. Attacker may use one virtual machine (VM) to spy on other VM's within the same physical host; this is called VM- Hoping. When the attacker takes the control of one VM, and by using that they may take control of the host machine as well as all the other VMs hosted on that machine; this is termed VM-Escape. Any of these incidents

Proc. of the Intl. Conf. on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

may cause disruption or data loss for the organisation.

Isolation is one of the key benefits of virtualisation as well as cloud computing, while this advantage can become one of the critical threats for the cloud if not deployed properly[9]. VM-Hopping can be used as a result of the violation of isolation. But the worst case scenario is when the attacker takes control of a VM first and then manages to control the other VMs or host machine because of the weak isolation. If the host machine gets compromised, the attacker will be able to get root access permission.

Disruption of the cloud service is becoming a critical issue because of the increasing threats of Denial of Service (DoS) attack or DDoS attack. But the situation gets worst when the host computer of the cloud service provider become the victim of the DoS or DDoS attack. If the host computer lost the service, all the VMs hosted in that host will face service disruption in terms of availability. The virtualisation process fully depends on the security of the underlying software kernel. A virtualisation host is capable of hosting many VMs where each of these VM's configuration information will be stored on this underlying kernel software. If this kernel gets compromised the attacker will be able to hijack the VMs hosted on this kernel.

Loss of data is the burning issue in relation to data storage in cloud computing. If the data stored in a server is in different country, the legislation may allow ensuring data safety in different ways. Some cloud service providers may retain the client's information even after client has deleted the data. However, the biggest security threats may come from by the improper access control, lack of adequate security of information, hacking activities, insufficient authentication and authorisation process; any of these issues can be used by the attacker to gain access to the information.

Cloud service providers are profit oriented businesses and may not disclose some known vulnerabilities to the clients. As a result, clients may become the victims of unknown threats. Furthermore, as the information will be hosted somewhere over the cloud a range of different people will be needed to ensure security or continuous service; employee, contractor or even the supplier of the cloud computing provider may become the threat to the information. Service providers need to have adequate system in place to ensure the physical and logical security of the information along with sufficient hardware and software resources.

Apart from the threats, explained above, cloud computing can be the victim of some common networked threats such as: virus, malware, Brute Force Attack against the secured password, Rainbow Table Attack, SQL Injection, Cross Site Scripting (XSS), DNS Poisoning, Phishing Attack, Session hijacking, Man-in-the-middle attack, application software vulnerabilities, inadequate service level agreement (SLA) etc.; where the client needs to be proactive and efficient to secure their own information[18].

IV. Recommendations to secure cloud computing

Cloud computing offers range of different and diversified services according to the market demand where the customers can use effective services in a cost effective way if security can be ensured. In this section, we recommend a set of good practice and possible future technical implementation guidelines to reduce the security threats of using cloud computing.

Cloud computing service providers need to do penetration testing on their API's before implementing the system[8]. API needs to be the subject of regular vulnerability checks because of new threats. All applications within cloud environment need to be checked and updated in a timely manner. Service providers need to ensure security in line with the law and legislations. Implementing effective IT governance within the organisation will help the service provider to offer better and secure service to the clients as well as to comply with the law[13].

Advanced hardware and software security components such as IDS, IPS or networked antivirus have given the opportunity to protect an organisation from potential threats like DoS or DDoS attack. Effective system configuration with an efficient access control list and a hardware/software security infrastructure will play a significant role in securing cloud computing[14]. Cloud computing providers keep data in different servers to reduce the risk of single point of failure and to ensure data backup, where the security of all physical storage needs to be ensured. Implementing ISO 27001 along with a disaster recovery/business continuity plan will help service providers to gain

Proc. of the Intl. Conf. on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

the confidence of clients as well as to continue the business in adverse situation[15].

Enterprise Single Sign on (ESSO) has been used by many service providers in recent years to allow clients to use different services with single sign on[16]. This is an effective approach to providing better password security, where encryption may play a significant role. Encrypting data can provide a great deal of security while storing the data over the cloud. To do so, data needs to be encrypted before storing and needs to be decrypted while accessing the information. Encryption and decryption of large amount of data can be expensive and time consuming because of technology constraints. Public key encryption technology has been proven to be effective in ensuring security within large organisation. This type of encryption can be used to encrypt the password, specific information or even the whole data storage space; for example the hard drive. However, the biggest challenge with public key cryptography is to arrange the expensive and complicated technologies as well as the key management where the individual user needs to keep their own "private key" safe and secure[17].

However, some of the security practice' described above may not be adequate and efficient enough to provide the sufficient level of security to the client's information over the cloud.

Furthermore, Ponemon Institute's research on cloud computing service providers has revealed the lack of commitment to considering security as an element of competitive advantage for cloud computing business. Therefore service providers need to have an effective and emerging security solution which will provide the best possible security for their clients information in a cost efficient way.

In the next section, we will explain a potential security infrastructure for cloud computing by using ICMetrics or Biometrics to provide better security within cloud computing environment.

VI. ICMetrics / Biometrics for the data encryption in cloud computing

In many cryptographic systems, success of the cryptosystem will depend on the client end where Encryption/decryption key would be stored. If the end device gets compromised by the attacker, the crypto system will become vulnerable. Yevgeniya Kovalchuk[10] has described the ICMetrics technology, which is capable of generating unique identifiers based on electronic systems' behaviour that can be used as cryptographic key. Biometrics technology can be used in a similar way to generating and storing an encryption key. However, Rhuma Tahir[11] argues that the low entropy and short length of the generated ICMatrics key can make it vulnerable against the cryptographic attack. Therefore, ICMetrics key needs to be strengthened by increasing the entropy and key length to ensure secure communication. Rhuma Tahir[12] has proposed the generation of strong ICMetrics session key based on SHA-2 key derivation function. This function is capable of generating the key with increased key length and high entropy.

Implementation of ICMetrics within cloud based storage and client end would provide resilience against information security threats. Cloud providers may provide the opportunity for individual client's virtual machines, to be encrypted by the ICMetrics or Biometrics based encryption technology. Each and every single VM within the host will be encrypted by the ICMetrics therefore "isolation" of virtual machines (VMs) will be ensured. On client end, low resource embedded systems can be used for the ICMetrics functions. All the information stored within the cloud host computer will be encrypted by the client therefore if the host kernel gets compromised, client's information may not be disclosed. ICMetrics or Biometrics will provide a great deal of support to the client in terms managing the security keys.

VII. Conclusion

Cloud computing is one of the most important emerging technologies this century and is changing the landscape of networking. The technology offers many benefits along with some security threats. Following industry standards, good practice and complying with the law may allow the service providers to offer secure cloud computing but still many cloud service providers are not aware of the security concerns related to this technology. Using ICMatrics or Biometrics in cloud technology may help clients to ensure their information security while the service providers may consider this to be a cost effective security solution.

Proc. of the Intl. Conf. on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

VIII. Future work

We will investigate the opportunities for implementing ICMetrics or Biometrics encryption technology within a cloud computing service infrastructure and will try to build a model for this. We believe implementing this technology will provide better resilience within cloud storage against the security threats.

References

[1] Mike Gunderloy, "Is Your Information under the Mattress or in the ATM?" Web Worker Daily, July 30,2008, http://webworkerdaily.com/2008/07/30/information-under-mattress-or-in-atm (accessed March 17,2013).

[2] Robin Hastings, "Cloud Computing", Library Technology Reports, www.techsource.ala.org, May/June 2009 (accessed July 10, 2013).

[3] Chris Brogan, "Life In The Clouds," Chris Brogan:Community and Social Media, July 31, 2008, http://www.chrisbrogan.com/life-in-the- clouds/, (accessed July 10, 2013).

[4] Ponemon Study on Cloud Security: http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final- april-2011.pdf (Accessed 11th July 2013)

[5] Haoyong Lv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, 2011, pp. 214-216

[6] Ramgovind S, Eloff MM and Smith E, "The Management of Security in Cloud Computing", IEEE, 2010.

[7] Nitin Singh Chauhan and Ashutosh Saxena, "Energy Analysis of Security for Cloud Application".

[8] Nagaraju Kilari and Dr. R. Sridaran, "A Survey on Security Threats for Cloud Computing

[9] Jyotiprakash Sahoo, Mohapatra and Lath R, "Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues", IEEE, 2010, pp.222-226

[10] Yevgeniya Kovalchuk, Housheng Hu, Dongbing Gu, Klaus McDonald-Maier, "ICMetrics Low Resource Embedded Systems"

[11] Rhuma Tahir, Housheng Hu, Dongbing Gu, Klaus McDonald-Maier, "Resilience against Brute Force and Rainbow Table Attacks using Strong ICMetrics Session Key Pairs"

[12] Rhuma Tahir, Housheng Hu, Dongbing Gu, Klaus McDonald-Maier, "A Scheme for the Generation of Strong ICMetrics Session Key Pairs for Secure Embedded System Applications"

[13] Ron Speed, "IT Governance and the Cloud: Principles and Practice for Governing Adoption of Cloud Computing"

[14] Harold F. Tipton, "Official (ISC)2 Guide to the SSCP CBK, Second Edition

[15] Charu Pelnekar, "Planning for and Implementing ISO 27001"

[16] Michael Mendelson, " Securing Cloud –based Applications How Enterprise Single Sign-on Was Implemented to Drive Value"

[17] Shon Harris, CISSP Exam Guide, Third Edition.

[18] Kimberly Graves, "Certified Ethical Hacker Study Guide, Version 6"

About Author :

Keen to do research on security of cloud computing and implement an effective and efficient security solution for cloud service providers as well as the users.

Masudur Rahman