RESEARCH ARTICLE OPEN ACCESS

Cloud Security Solutions: A Review

Sugandh Bala Gupta [1], Dr. Pankaj Kumar [2]
Department of Computer Science & Engineering
SRMGPC, Lucknow
India

ABSTRACT
Cloud computing is an evolving paradigm with changing definitions, but an industry wide accepted definition standardized by National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient, ubiquitous, on-demand network access to a shared puddle of configurable computing resource (e.g., servers, networks, storage, services and applications) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In this paper we review the different security facts associated with cloud computing environment.

Keywords:- Cloud Computing, Security, Saas, Paas.

I. INTRODUCTION

The objective of cloud computing is to apply customary supercomputing, or the power of high performance computing, typically used by military and research facilities to perform tens of trillions of calculations per second, application -oriented consumer, such as financial portfolios, to offer personalized information to provide data storage or feeding large immersive computer games.

To do this, we use cloud computing networks large groups of servers running normally low-cost technology for consumer PCs with specialized connections to spread data-processing chores across them. This shared infrastructure has large reserves of the systems are joined together. Often virtualization techniques are utilized to exploit the power of cloud computing.

Cloud computing has started to gain extensive appreciation in corporate data centres, as it permits the data centre to operate as Internet through the training process of computing resources to access and share resources in a virtual way protected and scalable.

For a trivial and average size business, the benefits of cloud computing is presently driving adoption. In the trivial and average size business sector there is often an absence of time and fiscal resources to buy, deploy and maintain an infrastructure (e.g. the server, software and storage).

Cloud computing has been standardized by the NIST to have three distinct layers in the cloud software stack: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Each layer has different levels of abstraction from the physical hardware from which the software runs on top of. We first consider each of the different levels shown in Figure 1.

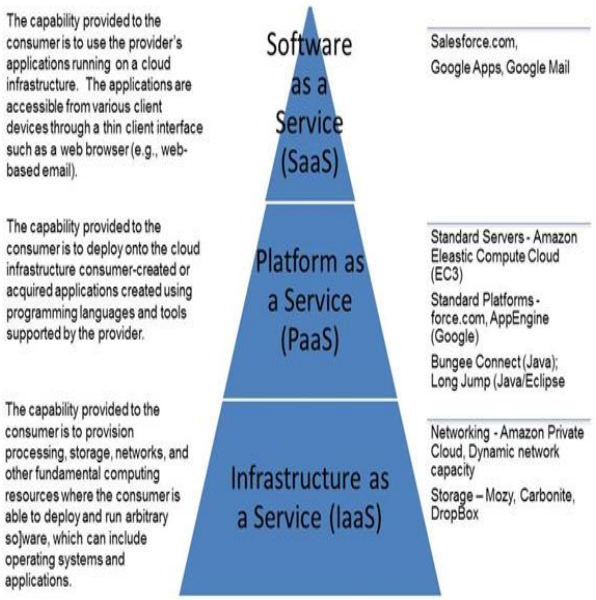

Figure 1: Cloud computing software layers

II. CLOUD SECURITY

Cloud computing security is an sprouting sub-domain of network security, computer security and more largely, information security. It refers to a broad set of technologies, policies and controls deployed to

shield data, applications and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are "cloud- based". The scope of the cloud security spans across all the three service delivery models deployed in any of the four cloud deployment models (private, public, hybrid and community cloud) and exhibiting the five essential characteristics of the cloud. It is this span of the scope of security in the cloud that makes it very important and at the same time much complicated. The wide scope of the security thus has multiple facets including but not limited to security related to application, data transmission, data storage, authentication and authorization, network, virtualization and physical hardware. This raises multiple questions with respect to each of these facets. This thesis provides solutions to the questions related to application and data security which falls under the SaaS layer.

III. CURRENT SECURITY SOLUTIONS

A detailed literature survey was done in the area of application and data security and the knowledge of which was used in developing the framework for cloud security

A. Application and data transmission security

Security in cloud is a promising topic of research, already addressed in many research and academic publications. A good overview of the issues in cloud is provided by Molnar and Schechter[1] who investigated the pros and cons of storing and processing data by the public cloud provider with regards to security. They detail about the new forms of technological, organizational, and jurisdictional threats resulting from the usage of cloud, as they also provide a selection of countermeasures.

The different threat and attack models given by Akhawe et al[2] can be used to formally analyze the attacks in cloud computing scenarios. However, their approach is limited to HTTP communication only. The model does not take into account application layer messages.

Youngmin Jung and Mokdong Chung[3] proposed an Adaptive security management model for cloud computing algorithm. They suggest an adaptive access algorithm to decide the access control to the resources using an improved Role Based Access Control (RBAC) technique. The proposed model determines dynamically security level and access control for the resources. But this model is based on provision of security based on cloud providers' decision and mainly considers different types of resources to arrive at the security level and access control. This model is targeted towards decisions of the client and services along with the resources to arrive at security levels. Also, this model is framed considering the cloud provider also as an third party un-trusted provider, thus making the system non-vulnerable even at the hands of the provider.

Gruschka and Lo Iacono[4]showed how XML Signature wrapping attacks can be performed to attack Amazon's EC2 service. They detailed a vulnerability that enabled an attacker to execute operation on the cloud control, while having possession of a signed control message from a legitimate user.

Manal and Yunis[5] outlined six security considerations for cloud computing namely resource sharing, data ownership, reduced encryption in favour of speed, refusal of services, data loss due to technical failure and attackers going after provider or the implementation. He also proposes a theoretical model for overcoming these issues through management of policies. For example, he proposes to classify the policies based on different types of data, like Client financial data, Intellectual property and so on. But creation and management of these policies are practically cumbersome and inefficient. Though many of the security issues in the past were due to inefficient policies, enabling an efficient policy is next to impossible. Policies can only be an additional measure but as long as the security framework is not efficient, even the most strategically created security policy will fail.

Though existing cloud providers use APIs that have the structure of web services standards such as SOAP and also standard cryptographic primitives for authentication is done through SSL protocol. Also they have IT infrastructure comprising of proxies and gateways containing malware and intrusion detection techniques. There are two problems arising out of this solution. The first one is that the API structures are still proprietary because they use the provider's own semantics within the standard structures. This will have a great impact on user's ability to move their

data from one provider to the other. The other one is that, the public key cryptography, a central concept in cryptography is used to protect web transactions and its security relies on the hardness of certain number theoretic problems. These are also the main place where quantum computers have shown to have exponential speedups.

These problems include factoring and discrete log, computing the unit group and class group of a number field as pointed out by Gentry and Szydlo[6] and Pell's equation described by Gentry et al)[7]. The existence of these algorithms implies that a quantum computer could break Diffie-Hellman and elliptic curve cryptography as discussed by Marisa et al [8] and RSA which are currently used, as well as potentially more secure systems such as the Buchmann-Williams key-exchange protocol. It's just a matter of processing power that is required to crack these cryptic techniques. In that case, employment of standard cryptographic techniques will be efficient only over a matter of time. As processing power gets exponential and quantum algorithms like Simon's quantum algorithm [9] gain better strength, these cryptographic techniques are bound to be disrupted, may not be immediate but in near future.

In 2004, Bertino[10] proposed a model for secure publication of XML documents. In the presence of third party publishers, the owner of a document specifies access control policies for the subjects. The subjects obtain the policies from the owner when they subscribe to a document. When the subject requests a document, the publisher will apply the policies and give fragments of the documents to the subject. Now, since the publisher is untrusted, it may give false information to the subject. Therefore the owner encrypts various combinations of documents and policies [10]. Using Merkle signature and the encryption technique the subject verifies the authenticity and completeness of the document. This model provided holds good for conventional scenarios but in case of cloud systems the range of vulnerabilities are even higher and hence should be targeted in a different way. The model proposed by Bertino[10] can still be used in conjunction with the framework that is developed. The framework developed as a result of the research enables to provide confidentiality behind this level. This refers to the requirement of a subject in the cloud receiving a response to an access request must be able to verify the completeness of security of the response. This can pertain to data or any document. The framework developed in this research provides a solution for this in the path of using checksum validations for every request and response, the details of which will be discussed in the later sections.

There are numerous research works happening in the region of cloud safety. Numerous groups and organization are concerned in developing security solutions and standards for the cloud. The Cloud Security Alliance (CSA) is gathering solution providers, non-profits and individuals to penetrate into discussion about the present and future finest practices for information assurance in the cloud ("Cloud Security Alliance (CSA) - security best practices for cloud computing"[11]). The Cloud Standards web site is gathering and coordinating information about cloud-related standards under development by the groups. The Open Web Application Security Project (OWASP) maintains listing of top vulnerabilities to cloud-based or SaaS models which is updated as the menace landscape changes [12]. The Open Grid Forum publishes papers to containing safekeeping and infrastructural specifications and information for grid computing researchers and developers [13].

The finest security solution for web applications is to develop a development scaffold that has strong security architecture. Tsai et al [14] put forth a four-tier structure for web-based development that though seems attractive, only implies a security feature in the process. "Towards best practices in designing for the cloud" by Berre et. al. [15] is a road map toward cloud-centric development and the X10 language is one way to attain better utilization of cloud capabilities of immense parallel processing and concurrency as agreed by Saraswat and Vijay [16].

Krugel et al [17] point out the value of filtering a packet-sniffer output to particular services as an effectual way to address security issues shown by anomalous packets directed to precise ports or services. An often- ignored solution to accessibility vulnerabilities is to shut down unused services, keep patches updated, and diminish permissions and access rights of applications and users.

Raj et al [18] suggest resource seclusion to guarantee security of data during processing, by separating the processor caches in virtual machines, and isolating those virtual caches from the hypervisor cache. Hayes

points out that there is no way to know if the cloud providers correctly deleted a client's purged data, or whether they saved it for some unidentified reason [19].

Halton and Basta [20] suggest one technique to avoid IP spoofing by using encrypted protocols wherever achievable. They also suggest evade ARP poisoning by requiring root access to alter ARP tables; using static, rather than dynamic ARP tables; or at least make certain changes to the ARP tables are logged.

B. Data storage security

Hayes [19] points out an attractive crinkle here, "Permitting a third-party service to take custody of personal documents raises awkward questions about control and ownership: If you move to a competing service provider, can you take a data with you? Could you lose access to documents if you fail to pay a bill?" [19]. The issues of privacy and control cannot be resolved, but only assured with tight service-level agreements (SLAs) or by keeping the cloud itself private.

One easy solution, to be a extensively used solution for UK businesses is to merely utilize in-house "private clouds" [20]. Nurmi et al [21] illustrated a preview of one of the available home-grown clouds in their presentation "The Eucalyptus Open-Source Cloud-Computing System".

Ignoring fragmentation with respect to providing security, data fragmentation is not a new concept. Concepts like these are already in use for providing optimization of data access in distributed systems. But most of them do not take security as the concern for fragmentation. One such work is regarding fragmentation and allocation of data in distributed database systems done by Katja et al [22]. Here they propose a model to fragment data horizontally or vertically with relation to the tuples so that data can be accessed or updated in an optimized manner. Another work is related to enhancement of Adaptive Data Replication Algorithm (ADRW) algorithm to achieve dynamic fragmentation and object allocation in distributed databases is done by Azzam et al [23]. Here they deal more about the cost involved in accessing data fragments from remote sites.

Gibbs et al [24] describes about different problems created by the fragmentation of information across a number of different databases that are maintained and controlled by different function units within an organization.

IV. CONCLUSION

Cloud computing is a distributed computational model over a large pool of shared-virtualized computing resources (e.g., storage, processing power, memory, applications, services, and network bandwidth), where customers are provisioned and de-provisioned recourses as they need. Cloud computing represents a vision of providing computing services as public utilities like water and electricity. In this paper we reviewed security concems of cloud environment and analysed different existing solutions.

REFERENCES

[1] Molnar, D., Schechter, S. "Self hosting vs. cloud hosting: Accounting for the security impact of hosting in the cloud", Economics of Information Security (WEIS), 2010

[2] Akhawe, D., Barth, A., Lam, P. E., Mitchell, J.C. and Song, D. "Towards a formal foundation of web security", CSF, pp. 290-304, 2010.

[3] Youngmin, J. and Mokdong, C. "Adaptive security management model in cloud computing environment", International Conference on Advanced Communication Technology (ICACT), pp 1664-1669,2010.

[4] Gruschka, N. and Iacono, L. "Vulnerable Cloud: SOAP Security Revisited", IEEE International Conference on Web Services , IEEE Computer Society, pp. 625-631, 2009.

[5] Manal, M.Y. "A 'cloud-free' security model for cloud computing", International Journal of Services and Standards, Vol.5, No.4, pp. 354-375, 2009.

[6] Gentry, C. and Szydlo, M. "Cryptanalysis of the revised NTRU signature scheme", In Proceedings of Eurocrypt '02, Vol. 2332 of LNCS. Springer-Verlag, 2002.

[7] Gentry, C., Peikert, C. and Vaikuntanathan, V.s "Trapdoors for hard lattices and new cryptographic constructions", 40th ACM Symp. on Theory of Computing (STOC), pp.197-206, 2008.

[8] Marisa, W., Paryasto, K., Sarwono, S. and Arif S., "Issues in Elliptic Curve Cryptography Implementation", In Internetworking Indonesia Journal, Vol.1, No.1, pp. 29-33, 2009.

[9] Simon, D.R. "On the power of quantum computation", SIAM J. Comput., Vol.26, pp.1474-1483, 1997

[10] .Bertino, E. "Selective and Authentic Third Party Distribution of XML Documents", IEEE Transactions on Knowledge and Data Engineering, Vol.16, No.10, 2004.

[11] .Cloud Security Alliance, "Security best practices for cloud computing", http://www.cloudsecurityalliance.org,

[12] OWASP,http://owasptop10.googlecode.com/files/ OWASP% 20Top% 20 10%20-%202010.pdf.

[13] Open Grid Forum, http://www.ogf.org/

[14] Tsai, W., Jin, Z. and Bai, X. "Internet ware computing: issues and perspective", Asia-Pacific Symposium on Internetware, ACM, Beijing, China, pp. 1-10, 2009.

[15] Berre, A.J., Roman, D., Landre, E., Heuvel, W.V.D., Skar, L.A., Udnaes, M. and Lennon, R. "Towards best practices in designing for the cloud", ACM SIGPLAN conference companion on Object oriented programming systems languages and applications, Orlando, Florida, USA, pp. 697-698, 2009.

[16] Saraswat, Vijay. "Report on the Programming Language X10", x10- lang.org, http://dist.codehaus.org/x10/documentation/languag espec/x10-latest.pdf.

[17] Krugel, C., Toth, T. and Kirda, E. "Service specific anomaly detection for network intrusion detection", In proceedings of the 2002 ACM symposium on Applied Computing, pp. 201-208, 2002.

[18] Raj, H., Nathuji, R., Singh, A. and England, P. "Resource management for isolation enhanced cloud services", ACM workshop on Cloud computing security, Chicago, Illinois, USA, pp. 77-84,2009. Hayes, B. "Cloud computing", Commun, ACM, pp. 9-11, 2008.

[19] Hayes, B. "Cloud computing", Commun, ACM, pp. 9-11, 2008.

[20] Basta, A., Halton, W. "Computer Security and Penetration Testing", Delmar Cengage Learning, 2007.

[21] Milne, J. "Private cloud projects dwarf public initiatives", http://www.cbronline.com/news/private_cloud_pr ojects_dwarf_public_initiatives_281009

[22] Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L. and Zagorodnov, D. "The Eucalyptus Open-Source Cloud- Computing System" IEEE/ACM International Symposium on Cluster Computing and the Grid, pp. 124-131, 2009.

[23] Katja, H. and Ralf, S. "Distributed Database Systems-Fragmentation and Allocation," Cluster of Excellence MMCI, October 2010.

[24] Azzam, S., Wesam, A., Samih, A. and Abdulaziz, Y. "A Dynamic Object Fragmentation and Replication Algorithm in distributed database systems", American Journal of Applied Sciences, pp. 613-618, 2007.

[25] Gibbs, M.R., Graeme, S. and Reeva, L. "Data Quality, Database Fragmentation and Information Privacy", Surveillance and Society, http://www.surveillancesociety.org/articles3(1)/data. pdf,pp.45-58.