An Advanced Survey on Cloud Computing and Alleviation Techniques

Vivekanandhan M.
Software Programmer
India

ABSTRACT

Cloud computing is a set of resources and services that are offered by the network or internet. Cloud computing extends various computing techniques like grid computing, distributed computing. Today cloud computing is used in both industrial field and academic field. Cloud facilitates its users by providing virtual resources via internet. As the field of cloud computing is spreading the new techniques are developing. This increase in cloud computing environment also increases security challenges for cloud developers. Users of cloud save their data in the cloud hence the lack of security in cloud can lose the user’s trust.

Keywords

Cloud Computing, Cloud Security Standard, Authentication, Security Threats Security, Authentication, Saas, Paas, Iaas

1. INTRODUCTION

Cloud computing is another name for Internet computing. The definition of cloud computing provided by National Institute of Standards and Technology (NIST) says that: "Cloud computing is a model for enabling on-demand and convenient network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. For some it is a paradigm that provides computing resources and storage while for others it is just a way to access software and data from the cloud. Cloud computing is popular in organization and academic today because it provides its users scalability, flexibility and availability of data. Also cloud computing reduces the cost by enabling the sharing of data to the organization. Organization can port their data on the cloud so that their shareholders can use their data. Google apps is an example of cloud computing

2. CLOUD SECURITY ISSUES

Organization uses various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and services has various cloud security issues. Each s

2.1 Multi-tenancy

A cloud model is built for reasons like sharing of resources, memory, storage and shared computing [2]. Multi-tenancy provides efficient utilization of resources, keeping cost lower. It implies sharing of computational resources, services storage and application with other tenants residing on same physical/logical platform at provider’s premises. Thus, it violates the confidentiality of data and results in leakage of information and encryption and increase the possibility of attacks.

2.2 Elasticity

Elasticity is defined as the degree to which a system is able to adapt to workload changes by provisioning and deranged resources in an autonomic manner, such that the available resources match the current demand at any time as closely as possible. Elasticity implies scalability. It says that consumers are able to scale up and down as needed. This scaling enables tenants to use a resource that is assigned previously to other tenant. However, this may lead to confidentiality issues.

2.3 Insider attacks

Cloud model is a multitenant based model that is under the provider’s single management domain. This is a threat that arises within the organization. There are no hiring standards and providers for cloud employees [3]. So, a third-party vendor can easily hack the data of one organization and may corrupt or sell that data to other organization.

2.4 Outsider attacks

This is the one of the major concerning issue in an organization because it releases the confidential information of an organization in open. Clouds are not like a private network, they have more interfaces than private network. So, hackers and attackers have advantage of exploiting the API, weakness and may do a connection breaking [4]. These attacks are less harmful than the insider attacks because in the later we sometimes unable to identify the attack.

2.5 Data Loss

As in cloud, there are multiple tenants, data integrity and safety could not be provided. Data loss can results in financial, customer count loss for an organization. An important example of this can be updating and deletion of data without having any backup of that data.

3. DATA STORAGE AND SECURITY IN THE CLOUD

Many cloud service providers provide storage as a form of service. They take the data from the users and store them on large data centers, hence providing users a means of storage. In spite of claims by the cloud service providers about the safety of the data stored in the cloud there have been cases when the data stored in these clouds have been modified or lost due to some security breach or some human error. Attack vectors in a cloud storage platform have been discussed and how the same platform is exploited to hide files with unlimited storage in [5]. In [5], authors have studied the storage mechanism of Dropbox (a file storage solution in the cloud) and carried three types of attack viz. Hash Value manipulation attack, stolen host id attack and direct download attack. Once the host id is known, the attacker can upload and link arbitrary files to the victim’s Dropbox account.

Various cloud service providers adopt different technologies to safeguard the data stored in their cloud. But the question is: Is the data stored in these clouds really secure? The virtualized nature of cloud storage makes the traditional mechanisms unsuitable for handling the security issues [23]. These service providers use different encryption techniques such as: public key encryption and private key encryption to secure the data stored in the cloud. A similar technique providing data storage security, utilizing the homomorphic token with distributed verification of erasure-coded data has been discussed in [7]. Trust based methods are useful in establishing relationships in a distributed environment. A domain-based trust-model has been proposed in [8] to handle security and interoperability in cross clouds. Every domain has a special agent for trust management. It proposes different trust mechanisms for users and service providers

The following aspects of data security should be taken care while moving into a cloud:

1. Data-in-transit
2. Data-at-rest
3. Data Lineage
4. Data Remanence
5. Data Provenance

In case of data-in-transit, the biggest risk associated with the encryption technology that is being used, whether it is up-to-date with the present-day security threats and makes use of a protocol that provides confidentiality as well as integrity to the data-in-transit. Simply going for an encryption technology does not serve the purpose. In addition to using an encryption

– decryption algorithm for secure data transfer, data can be broken into packets and then transferred through disjoint paths to the receiver. It reduces the chances of all the packets being captured by an adversary. And the data cannot be known until all the packets are coupled together in a particular manner. A similar approach has been discussed in [50, 51].

Managing data at rest in an IaaS scenario is more feasible in comparison to managing the same over a SaaS and PaaS platform because of restricted rights over the data. In a SaaS and PaaS platform, data is generally commingled with other users' data. There have been cases wherein even after implementing data tagging to prevent unauthorized access, it was possible to access data through exploitation of application vulnerability [25]. The main issue with data-at-rest in the cloud is loss of control, even a non-authorized user/party may have access to the data (it is not supposed to access) in a shared environment. However, now-a-days,storage devices with in-built encryption techniques are available which are resilient to unauthorized access to certain extent. Even in such a case, nothing can be done in case the encryption and decryption keys are accessible to the malicious user. A lockbox approach wherein the actual keys are stored in a lockbox and there is a separate key to access that lockbox is useful in the above-mentioned case. In such a scenario, a user will be provided a key based on identity management technique corresponding to the COI (community of interest) he belongs to, to access the lockbox. Whenever the user wants to access the data, he needs to acquire the COI key to the lockbox and then th e user gets appropriate access to the relevant data [9]. Homomorphic encryption techniques, which are capable of processing the encrypted data and then bringing back the data into its original form, are also providing better means to secure the data-at-rest. A simple technique for securing data at rest in a cloud computing environment has been mentioned in [52]. This technique makes use of public encryption technique.

Tracing the data path is known as data lineage and it is important for auditing purpose in the cloud. Providing data lineage is a challenging task in a cloud computing environment and more so in a public cloud. Since the data flow is no longer linear in a virtualized environment within the cloud, it complicates the process of mapping the data flow to ensure integrity of the data. Proving data provenance is yet another challenging task in a cloud computing environment. Data provenance refers to maintaining the integrity of the data, ensuring that it is computationally correct. Taxonomy of provenance techniques and various data provenance techniques have been discussed in [53]. Another major issue that is mostly neglected is of Data-Remanence. It refers to the data left out in case of data transfer or data removal. It causes minimal security threats in private cloud computing offerings, however severe security issues may emerge out in case of public cloud offerings as a result of data-remanence [54, 56]. Various cases of cloud security breach came into light in recent past. Cloud based email marketing services company, Epsilon, suffered a data breach, due to which a large section of its customers including JP Morgan Chase, Citibank, Barclays Bank, hotel chains such as Marriott and Hilton, and big retailers such as Best Buy and Walgreens were affected heavily and huge chunk of customer data was exposed to the hackers which includes customer email ids and bank account details [55].

A similar incident happened with Amazon causing the disruption of its EC2 services. Popular sites like: Quora, Four-Square and Reditt were the main sufferers [57]. The above-mentioned events depict the vulnerability of the cloud services. Another important aspect is that the known and popular domains have been used to launch malicious software or hack into companies' secure database. A similar issue happened with Amazon's S3 platform and the hackers were able to launch corrupted codes using a trusted domain [58]. Hence the question that arises now is who to be provided the "trusted" tag. It established that Amazon was prone to side-channel attacks, and a malicious virtual machine, occupying the same server as the target, could easily gain access to the confidential data [59]. The question is: should any such security policy be in place for these trusted users as well? An incident related to the data loss occurred, sometime back, with the online storage service provider "Media max" (also known as "The Linkup") when due to system administration error; active customer data was deleted, leading to huge data loss [60]. SLA (Service Level Agreement) with the Cloud Service providers should contain all the points that may cause data loss either due to some human or system generated error. Hence, it must be ensured that redundant copies of the user data should be stored in order to handle any sort of adverse situation leading to data loss. Virtualization in general increases the security of a cloud environment. With virtualization, a single machine can be divided into many virtual machines, thus providing better data isolation and safety against denial of service attacks [68]. The VMs (Virtual Machine) provide a security test-bed for execution of untested code from un-trusted users. A hierarchical reputation system has been proposed in the paper [61] for managing trust in a cloud environment.

Virtualization in general increases the security of a cloud environment. With virtualization, a single machine can be divided into many virtual machines, thus providing better data isolation and safety against denial of service attacks [68]. The VMs (Virtual Machine) provide a security test-bed for execution of untested code from un-trusted users. A

hierarchical reputation system has been proposed in the paper [61] for managing trust in a cloud environment.

4. SECURITY POLICY ENHANCCEMENT

Standards for security define procedure and processes for implementing a security program. To maintain a secure environment, that provides privacy and security some specific steps are performed by applying cloud related activities by these standards. A concept called "Defence in Depth" is used in cloud to provide security [9]. This concept has layers of defence. In this way, if one of the systems fails, overlapping technique can be used to provide security as it has no single point of failure. Traditionally, endpoints have the technique to maintain security, where access is controlled by user.

4.1 Security Assertion Markup Language (SAML)

SAML is basically used in business deals for secure communication between online partners. It is an XML based standard used for authentication, authorization among the partners. SAML defines three roles: the principal (a user), a service provider (SP) and an identity provider (IDP) [10]. SAML provides queries and responses to specify user attributes authorization and authentication information in XML format. The requesting party is an online site that receives security information.

4.2 Open Authentication (OAuth)

It is a method used for interacting with protected data. It is basically used to provide data access to developers. Users can grant access to information to developers and consumers without sharing of their identity [3]. OAuth does not provide any security by itself in fact it depends on other protocols like SSL to provide security.

4.3 Open ID

OpenID is a single-sign-on (SSO) method. It is a common login process that allows user to login once and then use all the participating systems [11]. It does not based on central authorization for authentication of users.

4.4 SSL/TLS

TLS is used to provide secure communication over TCP/IP. TLS works in basically three phases: In first phase, negotiation is done between clients to identify which ciphers are used. In second phase, key exchange algorithm is used for authentication [12]. These key exchange algorithms are public key algorithm. The final and third phase involves message encryption and cipher encryption.

5. CONCLUSION

This paper describes some of the cloud concepts and demonstrates the cloud properties such as scalability, platform independent, low-cost, elasticity and reliability. Although there are various security challenges in cloud computing but in this paper, we have discussed some of them and also the techniques to prevent them, they can be used to maintain the secure communication and remove the security problems. This survey is basically done to study all the problems like attacks, data loss and unauthenticated access to data and also the methods to remove those problems. As the cloud computing is dynamic and complex, the traditional security solutions provided by cloud environment do not map well to its virtualized environments. Organization such as Cloud Security Alliance (CSA) and NIST are working on cloud computing security. In this paper we have discussed a few security approaches but several other approaches are also there that are in the process. Some standards are also specified which can be used to maintain secure communication and security in a cloud as many systems communicate in it and perform operations.

As part of our ongoing work, we are further analyzing other IT Security Issues in cloud paradigm and determine if they should be incorporated into our cloud security application.

6. ACKNOWLEDGMENT

This Technical paper could not have been written without my parents and friends who encouraged and challenged me through my academic program. And giving me the strength to reach for the stars and chase my dreams, and authors mentioned in the reference.

7. REFERENCES

[1] Amit Hendre and Karuna Pande Joshi CSEE Department, University of Maryland Baltimore County Baltimore, MD, USA "A Semantic Approach to Cloud Security and Compliance" 2015 IEEE

[2] Vahid Ashktorab , Seyed Reza Taghizadeh "Security Threats and Countermeasures in Cloud Computing Volume 1, Issue 2, October 2012

[3] Victor Chang, Muthu Ramachandran, Member, IEEE "Towards achieving Data Security with the Cloud Computing Adoption Framework", 2015,IEEE

[4] Prince Jain Malwa Polytechnic College Faridkot, Punjab-151203, India "Security Issues and their Solution in Cloud Computing" International Journal of Computing & Business Research ISSN (Online): 2229-6166

[5] Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, Edgar Weippl, "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space", Proceedings of the 20th USENIX conference on Security, Berkley, USA, 2011.

[6] Seny Kamara, Kristin Lauter, "Cryptographic cloud storage", Lecture Notes in Computer Science, Financial Cryptography and Data Security, pp. 136- 149, vol. 6054, 2010.

[7] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", 17th International workshop on Quality of Service,2009, IWQoS, Charleston, SC, USA, pp.1- 9, July 13-15, 2009, ISBN: 978-1-4244-3875-4.

[8] W. Li, L. Ping, X. Pan, "Use trust management module to achieve effective security mechanisms in cloud environment", 2010 International Conference on Electronics and Information Engineering (ICEIE), Volume: 1, pp. V1-14 - V1-19, 2010. DOI: 10.1109/ICEIE.2010.5559829.

[9] R. A. Vasudevan, A. Abraham, S.Sanyal, D.P. Agarwal, "Jigsaw-based secure data transfer over computer networks", Int. Conference on Information Technology: Coding and Computing, pp. 2-6, vol.1, April, 2004.

[10] R. A. Vasudevan, S. Sanyal, "A Novel Multipath Approach to Security in Mobile Ad Hoc Networks (MANETs)", Int. Conference on Computers and Devices for Communication, CODEC'04, Kolkata, India.

[11] Tim Mather, Subra Kumaraswamy, Shahed Latif, “Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)”, O’Reilly Media, Sep. 2009; ISBN: 978-0596802769. http://oreilly.com/catalog/9780596802776.

[12] Jeff Sedayao, Steven Su, Xiaohao Ma, Minghao Jiang and Kai Miao, “A Simple Technique for Securing Data at Rest”, Lecture Notes in Computer Science, pp. 553- 558, 2009.

[13] Yogesh L. Simmhan, Beth Plale, Dennis Gannon, “A Survey of Data Provenance Techniques”, ACM SIGMOD, vol. 34, issue. 3, Sep, 2005, NY, USA.

[14] Krishna Prakash and Balachandra “security issues and challenges in mobile computing and m-commerce” International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015

[15] Justin LeJeune, Cara Tunstall, Kuo-pao Yang and Ihssan Alkadi, CSIT Department at SLU “An Algorithmic Approach to Improving Cloud Security: The MIST and Malachi Algorithms”, 978-1-4673-7676 ,2016 IEEE

[16] Abdullah , Imran, Fida Hussain “The Secure Data Storage in Mobile Cloud Computing”

[17] Computer Engineering and Intelligent Systems

[18] P. R. Gallagher, “Guide to Understanding Data Remanence in Automated Information Systems”, The Rainbow Books, ch3 and ch.4, 1991.

[19] Farzad Sabahi, “Secure Virtualization for Cloud Environment Using Hypervisor-based Technology”, Int. Journal of Machine Learning and Computing, pp. 39-45, vol. 2, no. 1, February, 2012.

[20] David Goldman, “Why Amazon’s Cloud Titanic Went Down”, CNNMoney, April, 2011. http://money.cnn.com/2011/04/22/technology/amazon

[21] Rory Smith (SOC Analyst), “The Use of Legitimate Channels to distribute malicious software to Users”, Security Samurai, Aug. 2, 2011. http://www.thesecuritysamurai.com/2011/08/02/the- use-of-legitimate-channels-to-distribute-malicious- software-to-users-by-rory-smith-soc-analyst/

[22] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage, “Hey, you get off my cloud: Exploring information leakage in third party compute clouds”, CCS’09, Proceedings of the 16th ACM conference. On Computer and Communications Security, pp. 199-212, ACM New York, NY, USA, 2009. ISBN: 978-1- 60558-894-0.

[23] Michael Krigsman, “MediaMax/The Linkup: When the Cloud fails”, IT Project Failures, News and Blogs, ZDNet, August, 2008. http://www.zdnet.com/blog/projectfailures/mediamax-the-linkup-when-the-cloud-fails/999

[24] K. Hwang, S Kulkarni and Y. Hu, “Cloud security with virtualized defence and Reputation-based Trust management”, Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695-3929-4.

[25] Larry Dignan (Editor in Chief- ZDNet), “Epsilon Data Breach: What’s the value of an email address”, IT Security Blogs, Tech Republic, April 5, 2011. http://www.techrepublic.com/blog/security/epsilon- data-breach-whats-the-value-of-an-email-address/5307

[26] www.iiste.org ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.5,2015.