International Journal of General
Engineering and Technology (IJGET)
ISSN(P): 2278-9928; ISSN(E): 2278-9936
Vol. 6, Issue4, Jun – Jul 2017; 47-54

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

STEP BY STEP SECURING CLOUD ENVIRONMENT

RINI MAHAJAN1[1] & DHEERENDRA SINGH[2]

[1]Assistant Professor, CSE Quest Group of institutions, Mohali, Punjab, India

[2]Associate Professor, CSE CCET Sector-26, Chandigarh, Punjab, India

ABSTRACT

Cloud computing is pervasive nowadays. It has brought tremendous advancement in the world of internet. Although Cloud is very advantageous, it has introduced many security concerns. Many researchers have worked on cloud security; research is still going on, because we don't have any fool proof solution for it. Security is not required only on one level rather on all the levels, e.g. IAAS, PAAS & SAAS. Privacy of data & security of data in cloud environments is ensured through various methods such as authentication, encryption, data protection & access control, identity management, etc. This paper covers all the steps of maintaining security in cloud in detail to make the cloud environment robust.

KEYWORDS: Authentication, CSP, Cloud Forensic, Encryption, IAAS, PAAS, SAAS

INTRODUCTION

In the current era, most of the world is connected through the internet. Cloud is the result of Advancement in computer. It is a latest development in the field of internet computing, which allows user to access internet based application and resources from anywhere in the world through internet. It is based on real time & provides services to the customers according to their demands. These services are accessed by common Internet protocols and networking standards. Cloud computing also provides organizations and companies to have a flexible and cost-effective IT infrastructure [1]. The cloud provides various types of services such as

- IAAS –infrastructure as a service which deals with hardware & virtual machines.
- PAAS (Platform as a service) -It provides various platforms to run the application on the cloud. One who wishes to create a cloud application must need cloud platform. A cloud platform provides cloud based services for creating applications
- SAAS software as a service- various applications can be accessed through the cloud through various interfaces.

SAAS is considered as most vulnerable among three types of services [2]. Now days, a number of researchers are working in the direction of maintaining security, but still cloud is vulnerable to many attacks. The further section discusses about various security risks, attacks & threats.

Cloud Computing Security Risks

The cloud provides internet based services everywhere in the world. So, it is open to traditional as well as all internet based attacks. In a cloud environment, customers' data are in the hands of third party provider such as Google,

Amazon, Microsoft, and so on. Data are uploaded & store on the data center, which is managed by CSP (Cloud Service Provider). The most prominent risk in this case is associated with the storage of that data.

While managing data, various risks are associated with it: securing data while uploading, to ensure that the data in data center encrypted at all times and most importantly the access to those data need to be controlled; this control should also be applied to the hosting company, including the administrators of the data center. Data security risks are compounded by the open nature of cloud computing. A further area of risk is the use of content after access. Cloud computing, more than any other form of digital communication technology, has created a need to ensure that protection is applied at the inception of the information, in a content centric manner, ensuring that a security policy becomes an integral part of that data throughout its life cycle [3,4,5] Cloud computing has a lot of security issues that are gaining great attention nowadays, including the data protection, network security, virtualization security, application integrity, and identity management.[1]

Principal Security Dangers of Cloud Computing (Threats & Attacks)

Cloud is already well-established now. For many organizations the question has moved on from 'should we move to cloud?' to 'how do we move to the cloud? They are concerned about potential risks, including malware, hacker-based theft, data leakage or breach, denial-of-service (DoS) attacks etc. Although cloud computing can offer small businesses significant cost-saving benefits such as pay-as-you-go access to sophisticated software and powerful hardware; the service does come with certain security risks such **as Secure data transfer, Secure software interfaces, Secure stored data, Data separation**, **data breaches, data loss, account or service traffic hijacking. Denial of service, malicious insiders, cloud abuse, etc. [5].** If an integral component gets compromised, say, a hypervisor, a shared platform component, or an application it exposes the entire environment to a potential of compromise and breach.

Cloud is open for different types of attacks. DDoS (Distributed Denial of Service) is one of the most known attacks that are used. Due to that customers are not able to access their services. Another type of attack on the cloud computing technology is a man in the middle attack. In which the intruders come in-between two communicators & hack information. A lot of different types of attacks could happen in the cloud technology. Besides the above mentioned, most known attacks involve phishing, IP spoofing, message modification, traffic analysis, IP ports, Side Channel attacks, Authentication attacks, Inside-job attacks, etc. [6] Due to these attacks, we need a better security policy in cloud computing We Users should have a defensive, in-depth strategy, including compute, storage, network, application, and user security enforcement, as well as monitoring. Service providers each have their own way of managing security. There are three specific groups of IT security products — activity logs, host-based intrusion protection systems and network-based intrusion protection systems, and data audit. [7, 8].

Following Section Describes the Various Steps to Maintain Security in Cloud Environment to Make it Useful for Various Organizations Without Worrying about their Data.

First & foremost step is Authentication

Authentication in Cloud Computing

Important & sensitive info is stored on cloud, so authentication is necessary. It ensures that the right person is accessing cloud services. For access to high value assets hosted in the cloud, customers may require that they provide supports strong, multi-factor, mutual and/or even biometric authentication [9]. Public and private types of cloud are using

various designs for authentication with RSA. RSA cryptosystem accepted: knowledge based authentication, two factor authentication, adaptive authentication, multifactor authentication and single password authentication. The benefits of this authentication mechanism are that it enables identity management and access management [3]

Access Control in Cloud Environment

There are many authentication methods based on user name & passwords. They are very easy to implement, but weak. This is the reason that with authentication, some strong access control mechanism must also be incorporated to provide a full zone of security. Customers must ensure that the cloud provider has processed and functionality that govern who has access to the customer's data and applications. Conversely, cloud providers must allow the customer to assign and manage the roles and associated levels of authorization for each of their users in accordance with their security policies. These roles and authorization rights are applied on a per resource, service or application basis. For example, a cloud customer, in accordance with its security policies, may have an employee whose role allows generation of purchase requests, but a different role and authorization rights is granted to another employee responsible for approving the request. The cloud provider must have a secure system for provisioning and managing unique identities for their users and services [9].

User authentication, authorization, and access control (AAA) are very important concerns to access the cloud. Cloud supports the feature of Multitenancy where a single instance of software running on a server is utilized to serve multiple clients. This feature is known to cause interoperability, authentication, and identification problems because of the usage of distinct negotiation protocols by different clients. A management interface is essential so that the cloud services can be accessed by users. [10,11]. Customer organizations may also wish to federate identity across applications to provide single-sign-on (SSO) along with single sign-off to assure user sessions get terminated properly. For example, an organization using separate SaaS applications for CRM and ERP may require single-sign-on, sign-off, and authorization across these applications (using standards such as SAML 2.0 [14], WS-Federation [12] and OAuth [13]).

The traditional model for access control is an application-centric access control, where each application keeps track of its collection of users and manages them, is not feasible in cloud based architectures because of these methods we need a lot of memory for storing the user details such as username and password. So cloud requires a user centric access control where every user request to any service provider is bundled with the user identity and entitlement information. For example window azure uses a conditional access control mechanism.

Encryption

Strong encryption technology is a core technology for protecting data in transit to and from the cloud as well as data stored. It is the most effective way to achieve data security. Cryptography can help emergent acceptance of Cloud Computing by more security concerned companies. The first level of security where cryptography can help Cloud computing is secure storage. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. It is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet. An encrypted file will appear scrambled to anyone who tries to view it. It must be decrypted in order to be recognized. Some encrypted files require a password to open, while others require a private key, which can be used to unlock files associated with the key. A complex algorithm is used to encode information.

To decode the encrypted files, a user need the encryption key. While it's possible to crack encrypted information, it's very difficult and most hackers don't have access to the amount of computer processing power they would need to crack the code. Encryption is also used to secure data sent over wireless networks and the Internet.

The goal of encrypted cloud storage is to create a virtual private storage system that maintains confidentiality and data integrity while maintaining the benefits of cloud storage: ubiquitous, reliable, shared data storage. Encryption should separate stored data (data at rest) from data in transit. Depending upon the particular cloud provider, we can create multiple accounts with different keys. Microsoft allows up to five security accounts per client. For secure communication between the host domain and the guest domain, or from hosts to management systems, encryption technologies, such as Secure HTTP (HTTPS), encrypted Virtual Private Networks (VPNs), Transport Layer Security (TLS), Secure Shell (SSH), and so on should be used. Encryption will help prevent such exploits as man-in-the-middle (MITM), spoofed attacks, and session hijacking. [15,16,17]

Cloud Computing and Identity

Digital identity holds the key to flexible data security within a cloud environment Digital identity can be used to form the basis of data security in the cloud. Access, identity, and risk are inherently connected when applied to the security of data, because access and risk are directly proportional [19]: As access increases, so then risk to the security of the data increases. Access controlled by identifying the actor attempting the access is the most logical manner of performing this operation. Ultimately, digital identity holds the key to securing data, if that digital identity can be programmatically linked to security policies controlling the post-access usage of data. [18]

SSL (Secure Socket Layer)

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. In cloud computing, all data flow over the internet need to be secure in order to prevent in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as the Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security.

SSL (Secure Socket Layer) is a protocol developed by Netscape that enables a web browser and a web server to communicate securely; it allows the web browser to authenticate the web server & establishes a secure and encrypted communication channel between two Internet connected devices [20].

The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is http using a Secure Socket Layer (SSL). A secure socket layer is an encryption protocol invoked on a Web server that uses HTTPS. SSL is a type of sockets communication and resides between TCP/IP and upper layer applications, requiring no changes to the application layer.

The SSL protocol uses the RSA algorithm which is a public key algorithm for encryption and decryption. SSL protocol also uses the concept of Certificates. Certificates are digital documents attesting to the binding of a public key to an individual or other entity. An SSL certificate contains the following information:

- The domain for which the certificate was issued.
- The owner of the certificate

- The physical location of the owner
- The validity dates of the certificate

SSL provides confidence in the integrity and security in cloud network infrastructure [21].

Applying Cloud Forensics

The number of crimes related to computers and the Internet have grown over the last decade. This resulted in digital forensics evolving enough to assure proper representation of cyber crime evidence data in court. Digital forensic practitioners must try to adopt and extend their digital forensic skills and tools into cloud computing environments as well as help cloud organizations and cloud consumers in establishing and developing forensic capability, as well as reduce cloud security risks. Cloud forensics is the application of digital forensics in cloud computing as a subset of network forensics. Basically, it is a cross-discipline between cloud computing and digital forensics. As per the official definition of NIST: Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data. Cloud Forensics have numerous uses, such as i**nvestigation, Troubleshooting**, **Log Monitoring, Data and System Recovery**, **Due Diligence/Regulatory Compliance etc.**

Forensics as a Service

The concept of FaaS is slowly emerging in cloud computing and showing the advantages of a cloud platform for large scale digital forensics. Forensics as a Cloud Service can be developed in order to ensure massive computing power that will facilitate investigations of cyber crime on all levels. [22,23]

CONCLUSIONS

Although many organizations are moving to the cloud, but before moving, they should take care of all the concerns of cloud security. They should apply security on different levels according to the sensitivity of the data & information. Cloud has many advantages, but if security breaches occur, then those will become disadvantages. Traditional models of security are not enough for the cloud environment, because those were developed for home organizations. Since the cloud is internet based and crosses the organization's boundary, new advanced methods of maintaining security are to be used with it.

REFERENCES

1. Jakimoski, K. (2016). Security Techniques for Data Protection in Cloud Computing, International Journal of Grid and Distributed Computing Vol. 9, No. 1 (2016), pp. 49-56
2. Shabana Rehman, Rahul Gautam, Research on Access Control Techniques in SaaS of Cloud Computing, Security in computing and communication, second International Symposium Proceedings SSCC-2014, page 92-100
3. R. Buyya, J. Broberg, and A. Goscinski, "Cloud Computing Principles and Paradigms" Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
4. W. Publishing, and J. Wiley, Barrie Sosinsky, "Cloud Computing Bible" Published by Wiley Publishing, Inc.,

5. A.T. Velte, T. J. Velte, and D. Ph, "Cloud Computing : A Practical Approach." Published by The McGraw-Hill Companies. Onankunju, B. K. (2013). Access Control in Cloud Computing, 3 (9), 1–3.
6. B. K. Onankunju, "Access Control in Cloud Computing," International Journal of Scientific and Research Publications vol. 3, no. 9, pp. 1–3, 2013.
7. http://www.slideshare.net/lordgvd/cloud-computing-security-and-forensics-14551763
8. http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/
9. Security for Cloud Computing, Cloud Standard customer council, March 2015
10. Dongyan Jia, Fuzhi Zhang, Sai Liu, "A robust collaborative filtering recommendation algorithm based on multidimensional trust model," Journal of Software, vol. 8, no. 1, pp. 11-18, Jan. 2013.
11. Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, Guangtao Xue, Minglu Li, Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing, Department of Computer
12. Science and Engineering, Shanghai Jiao Tong University, Shanghai, Ramgovind S, Eloff MM, Smith E (2010),
13. Z. Shen and Q. Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", In Proceedings of 2nd International Conference on Signal Processing Systems, (2010), pp. 11-15.
14. Ullah, S., Xuefeng, Z., & Feng, Z. (2013). TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing, 7 (2), 15–26.
15. L. Yousef, M. Butrico and D. Da Silva, "Toward a Unified Ontology of Cloud Computing", Grid Computing Environments Workshop, GCE '08, (2008), pp. 1-10.
16. M. Tebaa, S. El Hajji, a El Ghazi, S. El Hajji, and A. El Ghazi, "Homomorphic Encryption Applied to the Cloud Computing Security," Proc. World Congr. Eng., vol. 1, pp. 4–6, 2012 ISBN: 978-988-19251-3-8 ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)
17. Implementing secure cloud services An executive guide to assessing your cloud maturity Cloud Security Company85 Executive Guide International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 2, February 2014.
18. R. Arora and A. Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms," International Journal of Engineering Research and Applications (IJERA), vol. 3, no. 4, pp. 1922–1926, 2013, ISSN: 2248-9622
19. H. Li, Y. Dai, L. Tian and H. Yang, "Identity-based authentication for cloud computing", Cloud Computing, (2009), pp. 157-166.
20. Benantar, M.: Access Control Systems: Security, Identity, Management and Trust Models. Springer US (2009)
21. Irvin Singh Dua, "Data Security in Cloud Oriented Application Using SSL/TLS Protocol" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 12, December 2013 ISSN 2319 – 4847

22. P. Patidar and A. Bhardwaj, "Network Security through SSL in Cloud Computing Environment," IJCSIT) International Journal of Computer Science and Information Technologies vol. 2, no. 6, pp. 2800–2803, 2011.

23. http://www.slideshare.net/lordgvd/cloud-computing-security-and-forensics-14551763

24. http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/

25. http://www.dummies.com/how-to/content/detection-and-forensics-in-cloud-computing.html