International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 5, Issue 6, Oct - Nov 2016; 1-6

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

CLOUD SECURITY WITH GATEWAY MODEL TO MEET ELASTIC NATURE

SHIRISHA KASIREDDY[1] & M. BALRAJU[2]

[1]Research Scholar, PHD Computer Science and Engineering, JNTUH, Hyderabad, India

[2]Principal and Professor, Krishna Murthy Institute of Technology and Engineering, JNTUH, Hyderabad, India

ABSTRACT

Cloud adoption is accelerating rapidly, driven by cost savings, agility, and efficiency. Whether users are extending internal resources or fully deploying in the cloud, organization needs to share the responsibility for security with service provider. This means that while cloud service providers (CSPs) cover the physical and network infrastructures and virtualization layer, responsible for securing the guest operating system, applications, data, and for meeting compliance regulations. If security doesn't go beyond the native cloud, then probably are not meeting shared responsibility. Users can increase overall protection and reduce administration by building elastic security into cloud architectures. To help shared responsibility, this paper provides the most complete set of recommended security capabilities and integrations available for cloud services such as AWS, Microsoft Azure, and VMware vCloud Air. When security is integrated with the leading cloud services platforms, cost and complexity go down, making it faster and easier for to meet security requirements while realizing the operational benefits of the cloud.

KEYWORDS: Cloud Security, CSP, Security Integration

INTRODUCTION

Cloud computing provides internet based services on a utility basis to the business process. The tenants share a pool of resources that are dispersedly owned and managed. Hence security is a major concern in the cloud environment. The consumers will loss the control of data in the cloud environment and hence a proper trust mechanism is necessary to ensure data security and privacy [1]. As the cloud computing is composed of different local systems and includes the members from multiple environments, therefore the security in cloud is complicate. In one side, the security mechanism should provide guarantees secure enough to the user, on the other side, the security mechanism should not be too complex to put the users into an inconvenient situation. The openness and flexibility of the computer and popular commercial operating systems have been important factors supporting their widespread adoption. However, that very same openness and flexibility have been proved to be a double edged sword, because it brings complexity, reduces trust degree and threat against security. So there should be a balance between the security and the convenience [2]. While downloading files from the internet, the users unknowingly downloads harmful software such as key logger. The user-sensitive data such as login and password gets hacked with the software such as Spyware, Trojans etc. while the user works with the user interface in order to access the web services. The data in the infected computer is no longer safe. Thus even after taking all the safety measures such as installing antivirus software also, there exist the risk of our sensitive data getting hacked when we use the web-service of cloud computing [3]. The five essential elements of cloud computing are the following:

a) On-Demand Self-Service: The cloud computing provides the cloud resources to the users whenever they are required without any human interaction.

b) Broad Network Access: The computing resources are available over the network (e.g. Internet) and for access heterogeneous platforms, such as tablets, PCs, Macs and smart phone.

c) Resource Pooling: The cloud providers serve multiple customers with computing resources. With the pool based model the clients will not know the location of their stored data.

d) Rapid Elasticity: For consumers, computing resources can be scaled as per the requirement.

e) Measured Service: The cloud infrastructure has the mechanism to measure the services provided for the customers in the shared pool of resources [4].

SECURITY THREATS IN CLOUD COMPUTING

Cloud computing faces various security threats for several reasons: a) Loss of control – the user's loss the control of data in the cloud environment and hence the usual cryptographic techniques cannot be directly applied for the purpose of data security. To ensure continuous and long term data security of the various kinds of data stored in the cloud, the problem of integrity and correctness of stored data in cloud becomes more challenging. b) Integrity of data – The stored data need to be frequently updated. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important area remains to be fully explored in the literature [5].

In cloud computing, many users and even the resources join or leave the cloud at random. There should be a trustworthy relationship among the users, resources and the cloud. Establishing the trustful relationship is a challenge because of the different security policies of the users and the resources in the cloud. In fact, there will be a Service Level Agreement between the cloud participants to maintain the confidentiality of their data [6]. The traditional way to ensure security of data during transmission and storage is to compress the data and encrypt it [7]. Unencrypted data of the client cannot be stored in the cloud because the cloud provider will have access to the data and hence the confidentiality of the data will be lost. Also, a malicious cloud provider can modify the client's data and hence, the integrity of the data will be lost. An encrypted file system is used to encrypt the user's data, manage and create keys which are used for data encryption and decryption.

The encryption and decryption of files is transparent to the user and the application [8]. The dependable and secure computing includes not only security and confidentiality, but also reliability, availability, safety and integrity [9]. Considering these facts, we propose a new way that is conducive to improve the secure and dependable computing in cloud. Cloud computing provides Internet-based services to customers and business and also provides significant cost effective IT resources as cost on demand IT based on the actual usage of the customer.

The cloud computing technology helps companies with much more efficient computing by centralizing resources, but at the risk of data privacy. The diversity of users multiplies the associated risk. Identity management (IDM) is one of the key components in cloud privacy and security. This can improve security and user satisfaction and help reduce some of the problems associated with cloud computing. The identity management can be deployed by a centralized component processing authentication and authorization requests [10].

CLOUD TPA

Employing Trusted Third Party services within the cloud, leads to the establishment of the necessary Trust level and provides ideal solutions to preserve the confidentiality, integrity and authenticity of data and communications [11]. In cryptography, when two parties want to interact with each other and if security is their major concern, they both can depend upon and trust this Third Party. The scope of a TTP within an Information System is to provide end-to-end security services, which are scalable, based on standards and useful across different domains, geographical areas and specialization sectors. The establishment and the assurance of a trust relationship between two transacting parties shall be concluded as a result of specific acceptances, techniques and mechanisms.

The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. Introducing a Trusted Third Party can specifically address the loss of the traditional security boundary by producing trusted security domains. As described by Castell, A Trusted Third Party is an impartial organization delivering business confidence, through commercial and technical security features, to an electronic transaction. It supplies technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic transaction.

Its services are provided and underwritten by technical, legal, financial and/or structural means" [12] This infrastructure leverages a system of digital certificate distribution and a mechanism for associating these certificates with known origin and target sites at each participating server [13]. TTPs are operationally connected through chains of trust (usually called certificate paths) in order to provide a web of trust forming the notion of a Public Key Infrastructure (PKI) [14]. For a good organization it is very essential to have a cloud that allows investigation from a single party, audit the outsource data to ensure the data security and save the users computation and data storage. It is very important to provide public auditing service for cloud data storage, so that the user trusts an independent third party.

PROPOSED SYSTEM

A. Cloud Security Broker

The Cloud Security Broker provides visibility, control, and data protection through frictionless API integration with the industry's widest range of clouds. New clouds can be added in minutes and multi-cloud policy controls provide consistent security across sanctioned business apps. Features include

Cloud Discovery: provides control over Shadow IT, analyzing network traffic to all cloud apps, identifying and categorizing more than 12,000 clouds, and analyzing risk with over 100 metrics.

Activity Monitoring and Anomaly Detection: creates visibility over users (both internal and external), content, and devices through an intuitive drill-down dashboard.

Compliance Scanning: discovers and classifies new and existing content, with outof-the-box policies and integration with enterprise DLP systems.

Granular policy controls: make it easy to create context-aware policies based on who, what, where, and why and automatically take appropriate actions to prevent data loss.

Policy-Based Encryption: selectively encrypt sensitive fi les preventing them from getting into the wrong hands, while authorized users can decrypt protected fi les from any device.

Direct Cloud Access: supports users from anywhere on any device, without routing traffic through a corporate gateway—ideal for distributed organizations and business partners.

B. Cloud Security Gateway

The Cloud Security Gateway provides inline protection, enabling you to encrypt or tokenize specific data fields while maintaining exclusive control over the encryption keys. Features include

Zero-Knowledge Protection: unauthorized outsiders or cloud providers have no way to access the data without the keys, which never leave your control.

Standards-Based, Validated Security: uses AES 256-bit encryption and is the only vendor in the space to have passed FIPS 140-2 validation.

Searchable Strong Encryption: provides a transparent user experience while supporting key functions like searching, sorting, reporting, indexing, charts, and more.

Enterprise Key Management: encryption keys never leave your organization and are never available to the cloud provider, preventing accidental or forced disclosure.

Tokenization: meets the most stringent requirements for data residency as sensitive data never leaves your network and is replaced by random token data in the cloud.

Malware Protection: detects and blocks malware from cloud applications or outside users, closing a gap in most organization's AV coverage.

CONCLUSIONS

The rapid move to the cloud by all types of organizations has passed a tipping point and the benefits are clear—flexibility, agility, cost savings, future-proofing and more. But this inescapable trend raises many issues for security-conscious organizations as cloud applications lack consistent visibility, data security, compliance, and control. While the cloud lets you outsource your infrastructure, your responsibility to protect critical business information never goes away. When sensitive data goes to the cloud you can't be certain that it's always protected and not exposed to threats, malicious insiders, or forced government disclosure. The cloud makes it easy for your users to share content and collaborate with anyone, but you need tools to make sure that sensitive data doesn't get into the wrong hands, putting your business at risk.

REFERENCES

1. Zhidong Shen, Qiang Tong, 2010 2nd International Conference on Signal Processing Systems (ICSPS): The Security of Cloud Computing System enabled by Trusted Computing Technology on pages V2-11 to V2-15.
2. Jason Reid Juan M. González Nieto Ed Dawson, "Privacy and Trusted Computing", Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE, 2003.
3. K. Mukherjee, G. Sahoo, "A Secure Cloud Computing" IEEE-2010 International Conference on Recent Trends in Information, Telecommunication and Computing, pages 369-371.
4. Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", 2010 24th IEEE

International Conference on Advanced Information Networking and Applications, pages 27-33.

5. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int ˝l Workshop Quality of Service (IW QoS ˝09), 2009.
6. Zhidong Shen, Qiang Tong, “The Security of Cloud Computing System enabled by Trusted Computing Technology”, 2010 2nd International Conference on Signal Processing Systems (ICSPS), pages v2-11 to v 2-15.
7. Xiaoyu Ruan, Rajendra S. Katti, “A New Source Coding Scheme with Small Expected Length and Its Application to Simple Data Encryption”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 10, OCTOBER 2006. http://technet.microsoft.com/en-us/library/ cc700811. As px
8. Algirds Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Land wehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing”, IEEE transactions on dependable and secure computing, vol.1, No.1, January-March, 2004.
9. Jun Chen; Xing Wu; Shilin Zhang; Wu Zhang more authors, “ A Decentralized Approach for Implementing Identity Management in Cloud Computing”, 2012 Second International Conference on Cloud and Green Computing (CGC 2012) on pages 770 – 776
10. Polemi, Trusted third party services for health care in Europe. Future Generation Computer Systems 14 1998, 51-59.
11. S, Castell. Code of Practice and Management Guidelines for Trusted Third Party Services. s. l.: INFOSEC Project Report S2101/02, 1993.
12. Commission of the European Community. Green Paper on the Security of Information Systems. 1994. Ver.4.2.1.
13. VeriSign. Directories and Public–Key Infrastructure (PKI). s. l.: Directories and Public –Key Infrastructure (PKI).
14. Farzad Sabahi, “Cloud Computing Security Threats and Responses”,IEEE confer. 2011, 978-1-61284-486-2/111
15. C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” IEEE INFOCOM 2010, San Diego, CA, March 2010.
16. William Stallings, “Cryptography and Network Security, Principles and Practice, 5th Edition”, on page 329-331
17. Sharma, N. ; Rathi, R. ; Jain, V. ; Saifi, M.W. , ”A novel technique for secure information transmission in videos using salt cryptography”, IEEE-2012 Nirma University International Conference on Engineering (NUiCONE), pg 1-6 http://docs.trendmicro.com/all/ent/sc/v2.0/en-us/ Webhelp_OP_WC/sc_ag/sc_ag_glossary/salt.htm

AUTHORS DETAILS

Mrs. K. Shirisha Reddy, a Research scholar in computer science and Engg from JNTUH, with B. Tech from JNTUH and M. Tech From JNTUH. Her Research work is on Integrity and Security in cloud computing.

She is working as Assoc prof in Vignana Bharathi Institute of Technology, Hyderabad. She is the author of more than 5 Research Journals. Her Research Interests include Cloud Computing, Data Mining, Big Data, and Internet of Things. She is the Member of IEEE-Women in Engineering.

Dr. M.B.RAJU, a Doctorate in Computer Science & Engineering from JNTUH, with B.E from Osmania University and M. Tech from JNTU, Hyderabad.

He started his career as an Electronics Engineer in 1991 and worked for about 5 years and proved his credentials. He later switched over to teaching in the year 1996 and served various organizations in and around Hyderabad at different portfolios. At Present he is working as Principal in Krishna Murthy Institute of Technology, Hyderabad. He is the author of more than 50 Journals and 20 conferences. His Research Interests include Image Processing, Web Mining, Text Mining, Cloud Computing, and Big Data.

Dr. M. BalRaju has Fellow Member ship in Computer Society of India (CSI), Life Member in Indian Society of Technical Education (ISTE), Life Member in Institution of Electronics and Telecommunication Engineers (IETE), Fellow Member in Institute of Electrical & Electronics Engineers (IEEE).He is Reviewer and Advisory Board Member for various National and International Journals.