International Journal of Applied Engineering and Technology ISSN: 2277-212X (Online)
An Open Access, Online International Journal Available at http://www.cibtech.org/jet.htm
2014 Vol. 4 (1) January-March, pp.82-87/Sharma and Bhardwaj
Review Article

A REVIEW: PAPER ON SECURE CLOUD STORAGE: POSSIBLE ATTACKS AND SOLUTIONS

***Manish Sharma and Yogesh Bhardwaj**
Department CSE, JECRC University, Jaipur, India
**Author for Correspondence*

ABSTRACT
Cloud computing is emerging software technology based on the network and it is a technique that provide to access data from server. It describes extremely scalable computing assets provided as an external service via the internet on a pay- as- you-go basis. As we all know about cloud computing so there are many factors which we have to focus on. "Security" is one of the major topic in cloud computing or we can say security of customer's sensitive information. With the increase in popularity of cloud data storage, efficiently proving the integrity of the data stored at an untrusted server has become significant. A cloud storage system, consisting of a group of storage servers, provides long storage services over net. Storing information in third party's cloud system causes serious concern over information confidentiality. General coding schemes protect information confidentiality, however also limit the functionality of the storage system as a result of a couple of operations are supported over encrypted information. Present review provides secure cloud storage and some possible threats as well as their solutions.

Keywords: *Cloud Computing, Security, Storage, Threats*

INTRODUCTION
Cloud computing is emerging software technology based on the network or virtualization technique it is a technique that provide to access data from server. Cloud Computing is ever where it represents all that other stuff that makes the network works it kind of like "etc." for the rest of the solution map. It describes highly scalable computing resources provided as an external service via the internet on a pay- as- you-go basis. The main theme of the cloud computing is that customers or we can say client to use the services from the basis of their need and pay according to their actually use resources aces by customers from these cloud at any time from any location via the internet. Cloud computing (so-called, cloud) represents one of the magnificent shifts in information technology which can enhance collaboration, agility, scaling and availability, and provide the potential for cost reduction through optimized and efficient computing. Different from the existing technologies and computing approaches, cloud is defined (Mell and Grance, 2009) with five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), SPI service models (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)), and deployment models (Public, Private, Hybrid, Community). Due to its characteristics and models, Gartner Inc. expected worldwide cloud services revenue to reach $148.8 billion in 2014, and estimated that over the next five years entrepreneurs would spend $112 billion on SaaS, PaaS and IaaS (Gartner Inc., 2010). Data outsourcing has become quite popular in recent years both in industry (e.g., Amazon S3, Dropbox, and Google Drive) and academia (Ateniese *et al.*, 2007; Ateniese *et al.*, 2008; Dodis *et al.*, 2009; Erway *et al.*, 2009). A client outsources her data to the third party data storage provider (server), which is supposed to keep the data intact and make it available to her. Cloud computing is foreseen to be the upcoming architecture to be employed in industries, owing to its vast merits in information technology history. Need for self-services, universal network processing of a network location autonomous resources availability, spontaneous resources flexibility, pricing is determined on the level of usage also on the risk of the transfer (Ateniese *et al.*, 2008). As a disarray invention with foreseen implication, cloud computing is mending way it uses business with IT. The basic point of view pattern is changing the way it is being focused over the cloud. In the view of users i.e. combining individuals and IT industries, storing the data remotely on cloud bring more benefits. Manual storage is completely lessened, we can access it universally with ubiquitous

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)

geographical location, The expenditure on hardware, software and personal maintenance is brought down (Blibech and Gabillon, 2005). In recent years, the popularity of cloud storage services has increased dramatically. For instance, the popular service Dropbox surpassed 25 million registered users at the beginning of 2011 (Blibech and Gabillon, 2005). Ubuntu One has reached more than one million registered users in July 20112 as well as Mozy3. These services are used to store the huge amount of digital data which is accumulated in both private and business sectors. Individuals own ever-increasing collections of digital photographs, videos, music (MP3 files), and e-books. Most business processes have been digitalized, i.e., information such as communication data, accounts, contracts, advertising material, construction or business plans only exists in digital form (GitHub, 2011). The data is often of great value and its irrecoverable loss or damage could be a total disaster for its owner. For parents, videos of their children growing up may be very important, PhD students may rely on digital material, e.g., a collection of Internet references, to be used for a dissertation. For a company, the loss of data could ruin the basis for business. This requires secure methods of preserving important data in order to prevent unrecoverable data loss, whilst constantly keeping up with increasing demands for storage space. It is necessary to regularly make extra copies of the information, so as to be able to restore it to an earlier version if need be. These copies further escalate the demand for storage space. Additional requirements arise from the variety of devices used to access the data simultaneously. Private and business users demand an easy way to synchronize and access their data independent of both device and location. The software providing these features must also be tailored to the needs of the individual with no technical background. In order to meet these demands, companies make large investments into their IT infrastructure. Additional hardware and software is required, as well as for its operation and maintenance. Larger companies might have to consider building a dedicated data center. These expenses connect with the continuing need to reduce costs in order to stay competitive (Crosby and Wallach, 2011).

This paper is structured as follow. Section 2 presents the scope and definition of cloud storage services, Section 3 for threats and section 4 for solution. Conclusion and future work are summarized in section 5.

Cloud Storage Services and Scope

Basically, a cloud storage system can be considered to be a network of distributed data centers which typically uses cloud computing technologies like virtualization, and others some kind of interface for storing data. To increase the availability of the data, it may be redundantly stored at different locations. In general, all of this is not visible to the user. Many cloud storage providers are active on the market, offering various kinds of services to their customers. This study distinguishes between two types of cloud Storage services: Basic cloud storage services are generally not designed to be accessed directly by users but rather incorporated into custom software using application program- ming interfaces" (API). Examples of such basic cloud storage services are Amazon S34, Rackspace5 and Nirvanix6. Advanced cloud storage services mostly employ basic cloud storage services for the actual storage of data, and provide interfaces such as client or web applications which greatly simplify the use of the service for the customer. Many services may also provide an easy to use API to allow integration of the service's capabilities into third-party software. Examples of advanced cloud storage services are Dropbox7, and Mozy8.

Scope: The main challenge of cloud storage is guaranteeing control, and the necessary integrity and confidentiality of all stored data. This study's intended readership is those companies and individuals interested in or planning to use cloud storage services. It aims to sensitize users to existing
privacy, security and legal issues.

Overview of Possible Threats

There are many possible threats in Cloud Computing.

Abuse and Nefarious Use of Cloud Computing: IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity often coupled with a ‘frictionless’ registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)

activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

Impact: - Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

Insecure Interfaces and APIs: Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency.

Impact: - While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

Malicious Insiders: The threat of malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance. To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

***Impact*: -** The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat.

Shared Technology Issues: IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (*e.g.*, CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.

Impact: - Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)

strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.

Data Loss or Leakage: There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.

Impact: **-** Data loss or leakage can have a devastating impact on a business. Beyond the damage to one's brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust. Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon data that is lost or leaked, there might be compliance violations and legal ramifications.

Account or Service hijacking: Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

Impact:- Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach.

Unknown Risk Profile: One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concern complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications. Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs. Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas.

Impact**: -** When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging? How are your data and related logs stored and who has access to them? What information if any will the vendor disclose in the event of a security incident? Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.

Solutions

Solution against Abuse and Nefarious Use of Cloud Computing: -

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

Solution against Insecure Interfaces and APIs: -

- Analyze the security model of cloud provider interfaces.

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)

- Ensure strong authentication and access controls are
- Implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

Solution against Malicious Insiders: -

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

Solution against Shared Technology Issues: -

- Implement security best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for
- Administrative access and operations.
- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

Solution against Data Loss or Leakage: -

- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyzes data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

Solution against Account or Service hijacking:-

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

Solution against Unknown Risk Profile:-

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (*e.g.*, patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information.

Conclusion

Main objective of present review is to know about the cloud computing and cloud storage and its secure services. In this paper possible threats which affect the cloud storage services are discussed and also their solutions are given. So this paper is useful to find out the additional threats and give a future scenario to resolving those threats. In future we supposed to find out additional threats and build a model which is used to configure and resolve those possible threats and vulnerabilities.

REFERENCES

Ateniese G, Burns R, Curtmola R, Herring J, L. Kissner L, Peterson Z and Song D (2007). Provable data possession at untrusted stores. *ACM CCS.*

Ateniese G, Kamara S and Katz J (2009). Proofs of storage from homomorphic identification protocols. *AsiaCrypt.*

Ateniese G, Pietro RD, Mancini LV and Tsudik G (2008). Scalable and efficient provable data possession. *SecureComm.*

Battista GD and Palazzi B (2007). Authenticated relational tables and authenticated skip lists. *DBSec* 31– 46.

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)

Blibech K and Gabillon A (2005). Chronos: an authenticated dictionary based on skips lists for timestamping systems. *SWS* 84–90.
Blibech K and Gabillon A (2006). Anew time stamping scheme based on skip lists. *ICCSA* (3) 395–405.
Crosby SA and Wallach DS (2011). Authenticated dictionaries: Real-world costs and trade-offs. ACM Trans. Inf. Syst. Secur., 14(2):17.
CSA (2010). Top Threats to Cloud Computing V1.0. Available: http://www.cloudsecurityalliance.org/top threats.html
CSA– Cloud Security Alliance (2009). Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Available: http://www.cloudsecurityalliance.org/guidance/
Dodis Y, Vadhan S and Wichs D (2009). Proofs of retrievability via hardness amplification. *TCC*.
Erway C, K¨upc C, Papamanthou C and Tamassia R (2009). Dynamic provable data possession. *ACM CCS*.
Gartner Inc., (2010). Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010, June 2010. Available: http://www.gartner.com/it/page.jsp?id=1389313
GitHub (2011). Brownie cashlib cryptographic library. Available: http://github.com/brownie/cashlib
Mell P and Grance T (2009). The NIST Definition of Cloud Computing Version 15. *Information Technology Laboratory, NIST* (National Institute of Standards and Technology). Available: http://csrc.nist.gov/groups/SNS/cloud-computing/

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)