VOL. 3, NO. 6, June 2012 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems

[1] Dr Nashaat el-Khameesy, [2] Hossam Abdel Rahman
[1] Prof. and Head of Computers & Information systems Chair, Sadat Academy
[2] Computers & Information systems Chair, Sadat Academy
[1, 2] Sadat Academy for management Science –Computer & Information Dept -Maady-Cairo-Egypt
[1] Wessasalsol@gmail.com, [2] HAbdel@Enr.gov.eg

ABSTRACT

The reported recent success of cloud computing has attracted attention for cost effective IT services with many signs for continuing spread out if not dominating in the coming years. However, challenges are being faced by both research and professional communities including quality reliable services, optimized architectures and security. Meanwhile, IT services in Cloud Computing face the overwhelming challenges to ensure the proper physical, logical and personnel security controls, especially when considering the fact that cloud computing moves the application software and databases to the large data canters. Moreover, while moving such large volumes of data and Software, the management of the data and services may not be fully trustworthy.

In this paper, the main focus is given to highlight the security aspects of data storage from perspectives of threats and attacks from one side and approaches for solutions from the other side. The paper also proposes an effective and flexible distributed scheme with two salient features, opposing to its predecessors. Our scheme achieves the integration of storage correctness insurance and data error localization.

Keywords: *Cloud computing, Threats and attacks, personnel security controls, storage correctness, distributes storage system*

1. INTRODUCTION

In cloud computing, moving data into the cloud offers great convenience to users since they don't have to worry about the complexities of direct hardware management [1]. Meanwhile, the emerging trend of outsourcing data storages at third parties (cloud storage) has recently attracted tremendous amount of attention from both research and industry communities [2]. Outsourced storage makes shared data and resources much more accessible as users can retrieve them anywhere from personal computers to smart phones, however the users will be at the mercy of their cloud service providers for the availability and integrity of their data. [3].

On the other hand, security remains the critical issue that concerns potential clients, especially for the banks and government sectors. A major challenge for any comprehensive access control solution for outsourced data is the ability to handle requests for re-sources according to the specie security policies to achieve congeniality, and at the same time protect the users' privacy [4]. Several solutions have been proposed in the past, but most of them didn't consider protecting privacy of the policies and users' access patterns as essential aspect for users [5].

In this paper we address the main aspects related to security of cloud storage. It presents an attempt to propose an effective and flexible security policy and procedures explicit to enhance the Data storage security in the cloud. The paper covers briefly a number of aspects including: major challenges and problems, Cloud Deployment Models and their design Goals, methods for enhancing cloud data storage and Finally the Conclusions.

2. THREATS AND ATTACKS FROM STORAGE PERSPECTIVES

While the benefits of storage networks have been widely acknowledged, consolidation of enterprise data on networked storage poses significant security risks. Hackers adept at exploiting network-layer vulnerabilities can now explore deeper strata of corporate information [6].

Following is brief listings of some major drivers to implementing security for networked storage from perspectives of challenging threats and attacks:

- Perimeter defence strategies focus on protection from external threats. With the number of security attacks on the rise, relying on perimeter defence alone is not sufficient to protect enterprise data, and a single security breach can cripple a business [7].
- The number of internal attacks is on the rise thereby threatening NAS/SAN deployments that are part of the "trusted" corporate networks [8]. Reports such as the CSI/FBI's annual Computer Crime & Security Survey help quantify the significant threat caused by data theft
- The problem of incorrectness of data storage in the cloud

- The data stored in the cloud may be updated by the users, including insertion, deletion, modification, appending, reordering, etc [9].
- Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats [10].

Moreover, risks due to compromised storage range from tangible loss such as business discontinuity in the form of information downtime, to intangibles such as the loss of stature as a secure business partner. With the number of reported security attacks on the rise, a firm understanding of networked storage solutions is a precursor to determining and mitigating security risks.

3. CLOUD DEPLOYMENT MODELS

By large, based on the reported literatures and implementations, the cloud can be deployed in three models which have different features and approaches to be below.

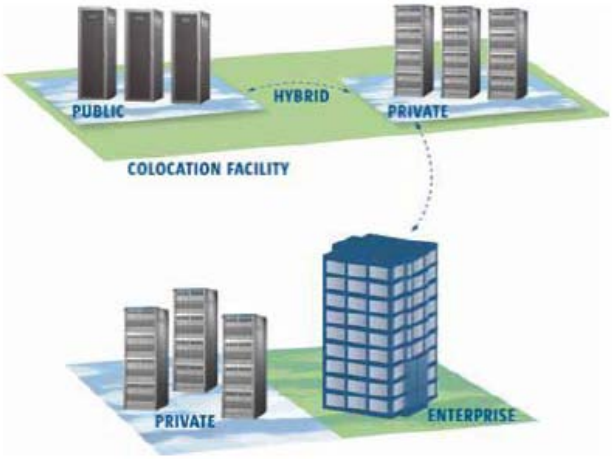

Fig 1

The cloud can be deployed in three models. The Fig: 1 explains its structure. They are described in different ways. In generalized it is described as below:

a. Public Cloud

A public cloud is one in which the services and infrastructure are provided off-site over the internet. These clouds offer the greatest level of efficiency in shared resources; however, they are also more vulnerable than private clouds. Public clouds are run by third parties, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks.

b. Private Cloud

A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings. [11].

c. Hybrid Cloud

A hybrid cloud environment consisting of multiple internal and/or external providers "will be typical for most enterprises". By integrating multiple cloud services users may be able to ease the transition to public cloud services while avoiding issues such as PCI compliance. [12].

d. System Model

Cloud networking can be illustrated by three different network entities:

User: who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations?

Cloud Service Provider (CSP): who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

Third Party Auditor (TPA): who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

e. Adversary Model [13].

There are two different sources for Security threats faced by cloud data storage.

1. CSP can be self-interested, un-trusted and possibly malicious.

It may move data that is rarely accessed to a lower tier of storage for monetary reasons, but

It may hide a data loss incident due to management errors, Byzantine failures and so on.

2. Economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users 'data

while remaining undetected by CSPs for a certain period [14].

There are two types of adversary

- Weak Adversary: The adversary is interested in corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user.

- Strong Adversary: This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent.

4. DESIGN GOALS

To ensure the security and dependability for cloud data storage, we aim to design efficient mechanisms for dynamic data verification and operation and achieve the following goals:

- Storage correctness: to ensure the data are kept intact all the time in the cloud.
- Fast localization of data error: to effectively locate the malfunctioning server when data corruption has been detected
- Dynamic data support: to maintain the same level of storage correctness assurance even if users modify, delete or append their data files in the cloud.
- Dependability: to enhance data availability against Byzantine failures, malicious data modification and server colluding attacks.
- Lightweight: to enable users to perform storage correctness checks with minimum overhead
- The Network Access Storage Data security system should explicitly separate the policy enforcement mechanism from the policy decision process and the file manager must be able to communicate policy decisions to the drive [15].
- The protocol should prevent unauthorized modification of client requests and capabilities along with protecting privacy of requests if dictated by the policies of clients or file managers.
- To minimize interaction with the file manager, the drive should be able to validate client operations without direct communication with the file manager.
- To allow for low memory drive implementations, there should be no long term state shared between drive and client. Overall state requirements of the drive should be kept at a minimum, but additional memory should enhance performance [16].
- The security protocol should add as little overhead as possible in terms of computation and the number and size of messages.

5. PROPOSED SOLUTIONS TO ENHANCE CLOUD DATA STORAGE

Control Access Data Storage that includes the necessary policies, processes and control activities for the delivery of each of the Data service offerings. The collective control Data Storage encompasses the users, processes, and technology necessary to maintain an environment that supports the effectiveness of specific controls and the control frameworks [17].The Security, correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed by the following:

❖ **Providing Security Policy & Procedure for Data Storage**

The Defence in Depth (referred to as did in this paper) is an excellent framework advocating a layered approach to defending against attacks, thereby mitigating risks.

❖ **Defence in Depth for Data Storage in cloud computing**

❖ **Layer 1 – Devices on the Storage Network [18]**

The following risk-mitigation measures are recommended:

- Authentication schemes provided by the OS should be evaluated. Schemes utilizing public- private key based authentication such as SSH or Kerberos, which also encrypt authentication communications on the network, should be used
- Authorization using Access Control Lists (ACL) to setup role-based access and appropriate permissions will enhance security
- Strong password schemes like minimum length passwords and periodic change of passwords should be enforced. The default username and passwords that are configured on the device should be changed
  Constant monitoring of published OS-vulnerabilities using database, SANS Security Alert Consensus newsletter and the NAS vendor's support site, is a
- necessity to prepare for possible attacks
- Logging and auditing controls should be implemented to prevent unauthorized use, track usage and for incident response

Layer 2 – Network connectivity [19]

NAS appliances face similar vulnerabilities as IP based network devices. Common techniques used to protect IP networks are also applicable to Storage Network:

- Extending network perimeter defence strategies like using a Firewall and IDS device to filter traffic reaching the NAS appliance will increase protection
- Use VLANs for segregating traffic to the NAS appliances
- Separate and isolate management interface from data interfaces on the Storage Network, thus enforcing out-of-band management which is more secure
- Monitor traffic patterns on the data interfaces of the NAS devices for unusual activity
- Implement port binding on switches to prevent WWN spoofing. Port binding binds a WWN to a specific switch port allowing connections of that device only through the predefined port thereby preventing other devices to assume the WWN's identity
- Implement vendor specific security techniques. For example, Brocade's Secure Fabric OS provides for additional security by enforcing switch authentication
- Create a separate management network which is isolated from the data network, thus preventing insecure in-band management activities

Layer 3 – Management access [20]

Management access is a significant source of attack. To address the vulnerabilities, the following guidelines provide help

- Disable the use of telnet and HTTP and enforce management access through SSH and HTTPS for encrypted communication
- Create separate user accounts based on the management tasks assigned to the users
- Implement strong authentication mechanisms like two-factor authentication using tokens, biometrics, etc
- Strong password schemes like minimum length passwords and periodic change of passwords should be enforced
- Implement authorization using Access Control Lists to setup role based access and appropriate permissions
- Enforce logging and auditing to prevent unauthorized use, track usage and for incident response [21].
- Restrict the management of the storage network
- devices from specific hosts

a. Correctness Verification and Error Localization

- Error localization is a key prerequisite for eliminating errors in storage systems.
- .
- We can do that by integrating the correctness verification and error localization in our challenge-response protocol
- The response values from servers for each challenge not only determine the correctness of the distributed storage, but also contain information to locate
-

b. Reliability of the analysis strategy of the experiment

The reliability of secure data storage strategy depends on security procedure and the backup data coefficients [22]. When one or more nodes cannot be accessed, the secure strategy can ensure that the data will be restored as long as one of the k nodes can be accessed. However, traditional data storage methods require all the data in the k nodes to be retrieved. Thus, the more blocks the data are split into, the poorer the reliability of traditional data storage

6. CONCLUSIONS

This paper suggests a methodical application of "defence in depth" security techniques that can help allay security risks in networked storage. More importantly, a defence in depth based networked storage security policy provides a comprehensive framework to thwart future attacks as the current technologies are more clearly understood. The emerging standards in storage security in conjunction with defence in depth will help in making storage much more resilient to future threats.

- In this abstract, we summarize the problem of data security in cloud data storage, which is essentially a distributed storage system. To enhance the security storage in cloud data storage.
- We investigated the problem of data security in cloud data storage, which is essentially a distributed storage system.
- We proposed an effective and flexible security policy and procedure with explicit data support, including block update, delete, and append.
- Our scheme achieves the integration of storage correctness insurance and data error localization
- Accountability for security and privacy in public clouds remains with the organization.
- Federal agencies must ensure that any selected public cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organization.
- Organizational data must be protected in a manner consistent with policies, whether in the organization's computing centre or the cloud.

- The organization must ensure that security and privacy controls are implemented correctly and operate as intended.

REFERENCES

[1] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11,Issue 11, July 2011.

[2] What is Cloud Computing? Retrieved April 6, 2011, available at: http://www.microsoft.com/business/engb/solutions/Pages/Cloud.aspx

[3] What is Cloud Computing? Retrieved April 6, 2011, available at: http://www.ibm.com/developerworks/cloud/newto.html#WHATIS

[4] What is Cloud? Retrieved April 6, 2011, available at: http://www.rackspace.co.uk/cloud-hosting/learn-more/whatis-cloud/

[5] Recession is good for cloud computing – Microsoft agrees http://www.cloudave.com/2425/recession-is-goodfor- cloud-computing-microsoft-agrees/

[6] S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi, and P. Samarati. Ecient and private access to outsourced data. In Proc. of the 31st International Conference on Distributed Computing Systems (ICDCS 2011), Minneapolis, Min- nesota, USA, June 2011.

[7] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control. In ACM Workshop on Cloud Computing Security, 2009

[8] Subashini S, Kavitha V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011) vol. 34 Issue 1, January 2011 pp. 1-11.

[9] IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. http://blogs.idc.com/ie/?p=210.

[10] New IDC IT Cloud Services Survey: Top Benefits and Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=730

[11] Rohit Maheshwari, Department of Computer Science, Kautilya Inst. Of Technology, International Journal of Recent Technology and Engineering (IJRTE) ,March. 27, 2012

[12] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology, International Journal of Recent Technology and Engineering (IJRTE) , April ,12- 2011

[13] National Institute of Standards and Technology - Computer Security Division http://csrc.nist.gov/groups/SNS/cloud-computing/

[14] Security Guidance for Critical Areas of Focus in Cloud Computing. http://www.cloudsecurityalliance.org/guidance/csaguide.pdf.

[15] An Information-Centric Approach to Information Security. http://virtualization.sys-con.com/node/171199.

[16] EMC, Information-Centric Security. http://www.idc.pt/resources/PPTs/2007/IT&Internet_Security/12.EMC.pdf.

[17] End-User Privacy in Human–Computer Interaction. http://www.cs.cmu.edu/~jasonh/publications/fnt-end-user-privacy-in-human-computer-interaction-final.pdf.

[18] ESG White Paper, the Information-Centric Security Architecture. http://japan.emc.com/collateral/analyst-reports/emc-white-paper-v4-4-21-2006.pdf.

[19] Latest cloud storage hiccups prompts data security questions. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130682&source=NLT_PM.

[20] Catteddu, D. and Hogben, G. Cloud Computing: benefits, risks and recommendations for information security. Technical Report. European Network and Information Security Agency, 2009.

[21] Danwei Chen, Yanjun He, Computer Technology, Nanjing University of Posts and Telecommunications, Journal of Convergence Information Technology Volume 5, Number 7- September 2010

[22] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology, International Journal of Recent Technology and Engineering (IJRTE) , April ,12- 2011