ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A Review on Reactive Security in Cloud Computing

Manisha Yadav, Suman Aggarwal

M.Tech Student, Dept. of CSE, AITM, Palwal, MD University, Haryana, India

Assistant Professor, AITM, Palwal, MD University, Haryana, India

ABSTRACT: The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be un-trusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has emerged recently. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user. As a matter of fact we can understand that in any resource we have less threat from invasion rather more threat from inside. Consequently the focus of this project is to demonstrate the reactive or passive measure of security in cloud computing ensuring that the trusted resource can share the data/communication even they are under the umbrella.

KEYWORDS : Cloud Computing, Security, Trusted Cloud Computing, Cryptography, Digital Signatures, Third Party Auditor.

I. INTRODUCTION

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) he third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homo-morphed authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

II. MOTIVATION

There are industries like aviation, mobile communication, hospitality, insurance, banking, supply chain, aerospace, telematics, to name a few; those who need such an application wherein cloud computing is highly used therefore, the traditional cryptographic technologies for data integrity and availability, based on Hash functions and signature

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

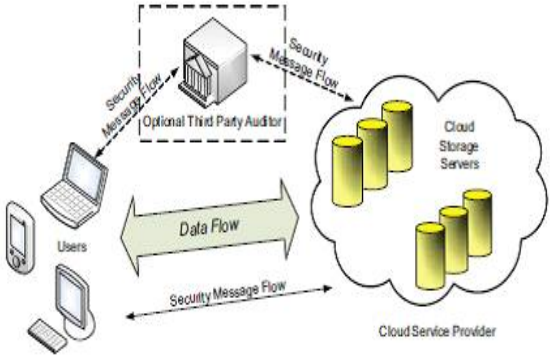
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

schemes cannot work on the outsourced data. it is not a practical solution for data validation by downloading them due to the expensive communications, especially for large size files. Moreover, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. Therefore, it is crucial to realize public audit ability for CSS (Cloud Security Solutions), so that data owners may resort to a third party auditor, who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and credibility in clouds. To implement public audit ability, the notions of proof of retrieve-ability and provable data possession have been proposed by some researchers. Their approach was based on a probabilistic proof technique for a storage provider to prove that clients' data remain intact.

- Lack of rigorous performance analysis for constructed audit system greatly affects the practical application of this scheme.
- It is crucial to develop a more efficient and secure mechanism for dynamic audit services, in which possible adversary advantage through dynamic data operations should be prohibits.
- Single TPA to audit for all files and to take more time to auditing the files.



III. OBJECTIVE

The Cloud Security protocols RSA, SHA and DES should encompass below security requirements for Secured Cloud Computing using TPA.

Data Integrity
Data integrity should be provided for every message that is transmitted over the network. This ensures that only authorized users are able to modify and access the messages. Also, the network must provide replay protection i.e. replay messages must be identified and discarded even if they comply with the integrity check criteria.

Confidentiality
Transmitted messages over the network must be protected from unauthorized access and thus, is a vital part of security. Protection should be provided against malicious software, spam, spyware and phishing attacks.

Data Availability
Data availability is a vital requirement for network security. The network should be able to avert the connection shutdown for an authorized individual or the complete system. Thus, eliminating or reducing the risk of denial of service (DoS) attacks.

Access Control
Access control refers to techniques and policies that ensure proper management of network resources and access is granted to various authorized users depending on permission level assigned to them.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Non Repudiation
Non repudiation ensures that validity of contract cannot be challenged by the sender or recipient. This can be achieved by implementing timestamps or digital signatures hence, ensuring that sender cannot deny having sent the message and recipient cannot deny the message receipt.

Authentication
Authentication assists in individual identification who tries to access the network and this can be achieved through the use of passwords, biometrics and digital certificates.

IV. LITERATURE REVIEW

Consider all of the risks, threats, and vulnerabilities from a technical perspective, he could probably add approximately 500 different items. The respondent also stated that some threats are common to all public and online services, such as distributed denial of service (DDoS) attacks and thus, they are not specific only to the cloud. Hence, some of the identified threats are not specific to cloud computing. In addition, he believes that a more generic term needs to be used for DDoS in a cloud environment, which is 'service discontinuity' because this term will have much more vulnerabilities than DoS. According to him, "For example, there are more than ten types of DDoS attacks and you do not want to go deep into that and your job is to make sure the continuity of the connection", which is defining threat from a business perspective. Illustrating the case of a SQL injection attack, he said that he "may not have a SQL server on the cloud or the database at all, on that particular service that I am having on the cloud." Moreover, DDoS attacks are common to all public and online services, and thus, they are not specific to the cloud only. Therefore, the types of threats in cloud computing need to be redefined because the above 41 threats are not the concern of the company, but to the cloud service provider.

V. PROPOSED SYSTEM

In this paper, we introduce a dynamic audit service for integrity verification of untrusted and outsourced storages and services on Cloud. Our audit system, based on novel audit system architecture, can support dynamic data operations and timely abnormal detection with the help of several effective techniques, such as fragment structure, random sampling, and index-hash table. Furthermore, we propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. A proof of- concept prototype is also implemented to evaluate the feasibility and viability of our proposed approaches. Our experimental results not only validate the effectiveness of our approaches, but also show our system has a lower computation cost, as well as a shorter extra storage for integrity verification.

VI. CONCLUSION

The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. As the approaches investigated in this paper clearly show, there is no single optimal approach to foster both security and legal compliance in an omni applicable manner. Moreover, the approaches that are favorable from a technical perspective appear less appealing from a regulatory point of view, and vice versa. The few approaches that score sufficiently in both these dimensions lack versatility and ease of use, hence can be used in very rare circumstances only.

As can be seen from the discussions of the four major multicloud approaches, each of them has its pitfalls and weak spots, either in terms of security guarantees, in terms of compliance to legal obligations, or in terms of feasibility. Given that every type of multicloud approach falls into one of these four categories, this implies a state of the art that is somewhat dissatisfying.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

REFERENCES

[1] Abbadi, I.M. and Martin, A. (2011), Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006
[2] Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.
[3] Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009
[4] Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.
[5] Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103
[6] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014
[7] Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysis and performance evaluation. Future Generation Computer Systems, 29, 387–401. doi:10.1016/j.future.2011.08.008
[8] Celesti, A., Fazio, M., Villari, M. and Puliafito, A. (2012). Virtual machine provisioning through satellite communications in federated Cloud environments. Future Generation Computer Systems, 28, 85–93. doi:10.1016/j.future.2011.05.021
[9] Che, J. Duan, Y, Zhang, T. and Fan, J. ().Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586 – 593. doi:10.1016/j.proeng.2011.11.2551
[10] Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ICCSEE.2012.193