A Novel Methodology for Auditing the Threats in Cloud Computing – A Perspective based on Cloud Storage

[1]Nasreen Sultana Quadri, [2]Kusum Yadav, [3]Yogesh Kumar Sharma
nsultanaquadri@gmail.com kusumyadav@gmail.com
[1]Research Sholar, Department of Computer Science, JJTU University, India,
[2]Department of Computer Science, Hail University, Hail, Saudi Arabia,
[3]Department of Computer Science, JJTU University, India.

Abstract
Cloud computing is a technology for delivering information in which resources are retrieved from the internet through a web-based tools and applications, rather than a direct connection with the server. It is a new emerging computing based technology in which any individual or organization can remotely store or access the information. The structure of cloud computing allows to store and access various information as long as an electronic device has access to the web. Even though various merits are provided by the cloud from the cloud provides to cloud users, it suffers from various flaws in security. Due to these flaws, data integrity and confidentiality has become a challenging task for both the storage and retrieval process. This paper proposes a novel approach for data protection by an improved auditing based methodology in cloud computing especially in the process of cloud storage. The proposed methodology is proved to be more efficient in auditing the threats while storing data in the cloud computing architecture.

Keywords:
Cloud Computing, Auditing threats, Cloud security, Information technology, Deployment, Multi-tenancy

1. Introduction

Various weeks had been done in the past in the area of providing Security in the Cloud Computing. Obtaining an acceptable level of security in Cloud environments is much harder compared to other traditional Information technology (IT) systems due to its specific Cloud characteristics such as: architecture, openness, multi-tenancy, etc. Conventional security mechanisms are no longer suitable for applications and data in the Cloud since new security requirements have emerged. Furthermore, there is a clear need for a trusted Security Audit method for Cloud Providers. This chapter identifies the security requirements that are specific to Cloud Computing and highlights how these requirements are linked to the Cloud Security Policy while illustrating the structure of a General Security Policy Model. It also proposes a methodology that can be adopted by Cloud Providers for auditing the security of their systems. Although Cloud Security Concerns have been mentioned as one of the top challenges pertaining to Cloud adoption, it is not clear which security issues are specific to Cloud Computing. ISACA and Cloud Security Alliance presented guidelines to mitigate the security issues in cloud [101][102]. P. Radha Krishna Reddy et al. [103] introduced a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. Ramgovid et al [104] presented the management of Security in Cloud focusing in Gartner's list [105]. However, there are several questions that remain open like: Which are the security requirements that exist only in Cloud? What is the structure of a security policy for cloud environments? And does the user have to solely depend on the service provider for proper security measures? By utilizing the general Security Policy cited in [106], we are proposing a methodology for auditing the Security level of a Cloud Provider. In this chapter, we present the Cloud specific security threats, while we propose a list of General Recommendations that should appear in every Security Policy of SaaS environments. Then, we present the proposed Model-Methodology for auditing the Security level of a Cloud Provider and at the end we provide conclusions derived from the undertaken survey.

2. Literature Review

Cloud Computing is a mixture of technologies that supports various stakeholders (Cloud Provider, Service Provider and Users). But how a Cloud differs from other models and what exactly the organizational impact is when moving to a Cloud is not clear yet. For the users, Cloud Computing is a synthesis of computing services without any understanding of the technologies being used. For an organization, it is a scale of different services provided to users for innovating and growing their business income. However, the threats that an organization faces as it shifts to Cloud Computing environments are different.

Various schemes with private verifiability can achieve higher scheme efficiency, public verifiability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information [2]. Then, clients are able to delegate the

Manuscript received February 5, 2024
Manuscript revised February 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.2.14

evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. In the cloud, the clients themselves are unreliable or cannot afford the overhead of performing frequent integrity checks [3]. Thus, for practical use, it seems more rational to equip the verification protocol with public verifiability, which is expected to play a more important role in achieving economies of scale for Cloud Computing. That is, the outsourced data themselves should not be required by the verifier for the verification purpose [4]. To consider the problem of efficiently proving the integrity of data stored at untrusted servers. In the provable data possession (PDP) model, the client preprocesses the data and then sends it to an untrusted server for storage, while keeping a small amount of meta-data [5]. The client later asks the server to prove that the stored data has not been tampered with or deleted (without downloading the actual data). However, the original PDP (provable data possession) scheme applies only to static (or append-only) files. Open Security Architecture (OSA) provides free frameworks that are easily integrated in applications, for the security architecture community. Its patterns are based on schematics that show the information traffic flow for a particular implementation as well as policies implemented at each step for security reasons [6].

End Users need to access certain resources in the cloud and should be aware of access agreements such as acceptable user conflict of interest. In this model, end user signatures may be used to confirm someone is committed to such policies [8].The client organization should run mechanisms to detect vulnerable code or protocols at entry points such as firewalls, servers, or mobile devices and upload patches on the local systems as soon as they are found. Thus, this approach ensures security on the end users and on the cloud alike [3]. However, the cloud needs to be secure from any user with malicious intent that may attempt to gain access to information or shut down a service. For this reason, the cloud should include a denial of service (DOS) protection[9].One way of enforcing DOS protection is done by improving the infrastructure with more bandwidth and better computational power which the cloud has abundantly. However, in the more traditional sense, it involves filtering certain packets that have similar IP source addresses or server requests. The next issue concerning the cloud provider to end users is transmission integrity[10]. One way of implementing integrity is by using secure socket layer (SSL) or transport layer security (TLS) to ensure that the sessions are not being altered by a man in the middle attack. At a lower level, the network can be made secure by the use of secure internet protocol (IPsec). Lastly, the final middle point between end users and the cloud is transmission confidentiality or the guarantee that no one is listening on the conversation between authenticated users and the cloud. The same mechanisms mentioned above can also guarantee confidentiality.

3. Proposed Methodology

In Cloud Computing environment shown in figure 1 has various threats and are diverse depending on the delivery models. In the previous literature, various works has been done and theyu discussed, in general, the risks focusing more on SaaS Cloud Providers. All these risks require substantial security attention. Cloud Providers need to mitigate these security threats by adopting the appropriate security measures in accordance with a well formed Cloud Security Policy.

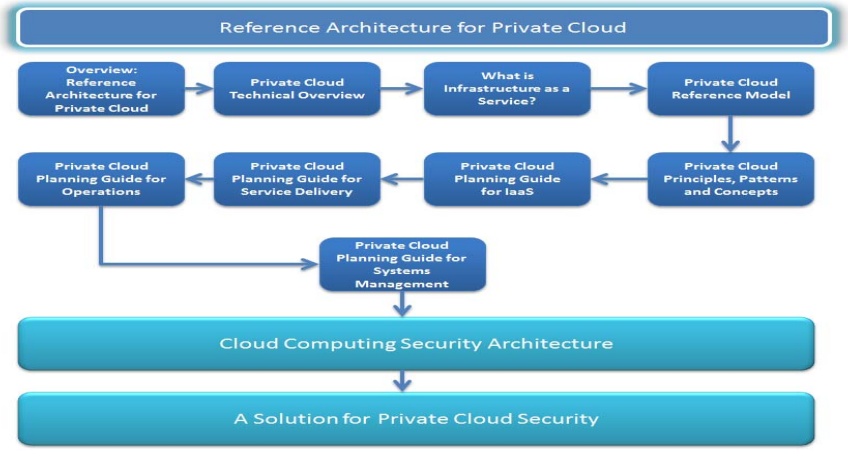

Figure 1: Architecture of a Cloud Model

By addressing the above mentioned requirements, cloud providers will gain the trust of their users. The proposed Methodology provides solutions for each threat and at the same time, it conforms them to the provisions of the Cloud Security Policy.

3.1. General Recommendations for the Security Policy

Despite that the security capabilities for a SaaS environment have been developed, we argue that if the Security Policy of the Cloud Provider features some general recommendations that reflect the security requirements of an organization or/and a user then, the Providers will mitigate the security risks and concerns. Thus, if an organization chooses a SaaS Provider that complies with the following recommendations, this would facilitate a Third Party Auditor to check the security level of the Cloud Computing environment. It would also ensure that the provision of all resources and the behavior of all users will be in accordance with the recommendations set and thus, compliance issues will be automatically avoided**.**

1. Invest in Education
2. Establish Cloud Strategy
3. Decide what goes to and under which control
4. Invest in Technologies that protect users' data
5. Audit the Provider's Services

3.3.1. Cloud based Learning

There is a need to identify the learning goals, the content structure and the learning experience of Cloud Computing in terms of a senior high technology education, in order to help learners coping with this emerging technology. At the same time, the research result could be effectively applied on integrating emerging technology into a formal technology education.

3.1.2. Establish Cloud Strategy

We would like to suggest a few basic steps that organizations can follow to define their Cloud Computing roadmap. This is not just about remedying the problem but more about creating a long-term strategic use of cloud computing that should bring a sustainable strategic value to the enterprise. This would result to a safer Cloud environment and an easier way to test which Provider is more suitable for the users.

3.1.3. Decide what goes to and under which control

One of the major problems that security professionals face is to identify which control goes where. The user should not manage or control the underlying Cloud himself as he is not obliged to have technical or managerial knowledge of Cloud. It's for the organizations to choose the controls that meet users' specific needs and provide security certifications and accreditations that would facilitate the procedure of audit control and would strengthen the trust towards Cloud Computing environment.

4. Invest in technologies that protect users' data

If the Provider is not certified for its software and hardware infra-structure by any industry security certification authority then the security control will be much more difficult. Users need a secure and consistent "place" for their data and expect through their SLA (Service Level Agreement) to have a report that will inform them about the encryption solutions, intrusion detection and prevention solutions, data centers and all other technologies and mechanisms that the provider uses .

4.1. Audit the Provider's services

Organizations or Third Party Control must offer to Cloud Service Providers the means to make their security data available to potential customers. Organizations provide outsourcing services that affect the control environment of their customers. The important element to remedy this problem would be to conduct an audit. The Cloud Auditor should create an audit plan that includes policies and procedures and could be used as a reference guide.

The key factor, to take away of this problem, is a conduct with a Cloud Auditor. The Cloud Auditor should have an audit plan, so that can be used as a guide. The Cloud Auditor provides a standard way to present, automated statistics about performance and security. So, SaaS Customers need only to select the safest Cloud Provider, according to the security functions of the auditor.

It is necessary to agree on the way recommendations for the Security Policies are presented to the Providers. They should be able to identify the recommendations that are relevant to the users' requirements and concerns. SaaS risks can be managed through this approach and Cloud Providers will be able to utilize systems with complex and dynamic

environments more easily. Furthermore, the proposed approach will save time, effort and money to the Providers.

4.2. Proposed Model-Methodology for Auditing

The proposed Model provides a solution to the security challenges of Cloud Computing. If Cloud Providers and Organizations follow this model, using the gates of the policy, they will succeed in having a secure Cloud Computing environment. More specifically, illustrates the structure of the General Security Framework and the interdependencies among its components. The Cloud Provider or a third party auditor must follow and audit the four general categories to avoid threats. In each category it is necessary to ensure and check what provisions are covered by the Cloud Provider according the following security measures- examples. A further analysis of how security controls should be linked to every security measure will be also provided. Until present, the aforementioned audit process was rather difficult because there is no commonly agreed procedure or a common Policy and thus, customers cannot easily rank their Providers in terms of the Security level they support. So, the proposed Cloud Security Model addresses the relationships of security measures and places them in a context together with their relevant security controls and concerns.

Category 1 – Processes/Functions Controls

It must be ensured that the security measures adopted by the provider meet the requirements set by the Cloud Security Policy. Users expect to have available a report about Cloud Provider's operations, logs and industry security certifications, as well as the assurance of the auditor that the provider is doing these right.

Category 2 – HR

A great number of executives, managers and personnel are not familiar with what cloud computing means. There is a lack of awareness about cloud environments together with a lot of concerns about the various risks and data security. Providers must aim to promote security through education and sharing of good practices with the personnel. The auditor should check if the cloud provider is considering the provisions of this category.

Category 3 – Legal Requirements & Compliances

The auditor should check whether the provisions of the legal framework under which the data is stored or transferred are satisfied. Moreover, the auditor should know in which country the data is located and thus what the regulations, the restrictions for storing, the processing and transferring that data are. In this way, the user can be assured that the storage and data processing carried out by the Cloud Provider Legally.

Category 4 – Technology

The auditor should check what software and hardware technologies are used as well as what the applications and the devices users entrust for storing and possibly sharing their data are. Cloud providers might also allow users' data to be transferred to another vendor or platform growing this way the risks on the users' data. Third party auditors can utilize this framework to understand the SaaS Provider's security context. All the previous threats are assigned to one of the four categories associated with the necessary security measures and then linked with a set of rules that make up the Security Policy of the Cloud Provider.

5. Conclusions and Future Enhancements

According to the problem of data security in cloud data storage, this is essentially to distributed storage system. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append is proposed. To reply on erasure-correcting code in the file distribution preparations to provide redundancy parity vectors and guarantees the data dependability. By utilizing the homo-morphic token with distributed verification of erasure-coded data, the scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, to almost guarantee the simultaneous identification of the misbehaving servers.Considering the time, computation resources, and even the related online burden of users, to provide the extension of the proposed main scheme to support third-party auditing, where users can safely delegate the integrity checking tasks to third-party auditors and be worry-free to use the cloud storage services. Through detailed security and extensive experiment results, which show that the scheme is highly efficient and resilient

to Byzantine failure, malicious data modification attack, and even server colluding attacks.

References

[1] Wang, J.-J.; Mu, S. Security issues and countermeasures in cloud computing. In Proceedings of the 2011 IEEE International Conference on Grey Systems and Intelligent Services (GSIS), Nanjing, China, 15–18 September 2011; pp. 843–846.

[2] L. Chang, L. Chin, A.Y. Chang, J. C .Chun, ― Information security issue of enterprises adopting the application of cloud computing,‖ IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM),pp 645-649, Aug. 2010.

[3] R. Maggiani, "Cloud computing is changing how we communicate," 2009 IEEE International Professional Communication Conference, pp 1-6, Jul. 2009.

[4] L. Geng F. David Z. Jinzy D. Glenn, ―Cloud computing: IT as Service, ―IEEE computer society IT Professional,‖ Vol. 11, pp.10-13, Apr.2009.

[5] Aman Bakshi, Yogesh B. Dujodwala, ―Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine,‖ ICCSN ’10 Proceeding of the 2010 Second International Conference on Communication. Softwareand networks, pp. 260-264, 2010.

[6] B. R. Kandukuri, R. V. Paturi and A. Rakshit, ―Cloud Security Issues,‖ 2009 IEEE International Conference on Services Computing, pp. 517-520,Sep. 2009.

[7] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I.Stoica, and M. Zaharia ,―A view of cloud computing,‖ Communication of the ACM, vol. 53, no. 4, pp.50–58, 2010.

[8] J. Yuan and S. Yu, ―Secure and constant cost public cloud storage auditing with deduplication,‖ in IEEE Conference on Communications and Network Security (CNS) , 2013, pp. 145–153.

[9] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, ―Proofs of ownership in remote storage systems,‖ inProceedings of the 18th ACM Conference on Computer and Communications Security . ACM, 2011, pp. 491–50