Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 67 (2014) 21398-21401

ISSN: 2229-712X

Review of security issues in cloud computing related to Single and Multi-clouds

Ashish Kr. Shrivastava and Monali Shrawankar
Department of Computer Science & Engineering, NIIST Bhopal.

ARTICLE INFO

Article history:
Received: 19 July 2013;
Received in revised form:
22 January 2014;
Accepted: 3 February 2014;

Keywords
Cloud computing,
Single cloud,
Multi-clouds,
Cloud storage,
Data integrity,
Data intrusion,
Service availability.

ABSTRACT

The use of cloud computing has accrued quickly in several organizations. Cloud computing provides several edges in terms of low price and accessibility of information. making certain the safety of cloud computing could be a major think about the cloud computing atmosphere, as users typically store sensitive data with cloud storage suppliers however these suppliers is also untrusted. Addressing "single cloud" suppliers is foretold to abate fashionable customers owing to risks of service handiness failure and also the risk of malicious insiders within the single cloud. A movement towards "multi-clouds", or in different words, "interclouds" or "cloud-of-clouds" has emerged recently. This paper surveys recent analysis associated with single and multi-cloud security and addresses doable solutions. it\'s found that the analysis into the utilization of multi-cloud suppliers to take care of security has received less attention from the analysis community than has the utilization of single clouds. This work aims to market the utilization of multi-clouds owing to its ability to cut back security risks that have an effect on the cloud computing user.

Introduction

The use of cloud computing has increased quickly in many organizations. Cloud computing provides many edges in terms of low value and accessibility of knowledge. These days tiny and Medium Business (SMB) corporations are more and more realizing that just by sound into the cloud they will gain quick access to best business applications or drastically boost their infrastructure resources, all at negligible price. Cloud suppliers ought to address privacy and security problems as a matter of high and pressing priority. The cloud offers many edges like quick readying, pay-for-use, lower prices, measurability, speedy provisioning, speedy physical property, present network access, and larger resiliency, hypervisor protection against network attacks, cheap disaster recovery and information storage solutions, on-demand security controls, real time detection of system change of state and speedy reconstitution of services. Handling "single cloud" suppliers is changing into less popular customers thanks to potential issues like service accessibility failure and therefore the risk that there are malicious insiders within the single cloud. In recent years, there has been a move towards "multiclouds" or "intercloud" or "cloud-of-clouds. This paper focuses on problems associated with information security side of cloud computing. Additionally, the potential for migration from one cloud to multi-cloud atmosphere is examined and analysis associated with security problems in single and multi-clouds in cloud computing is surveyed.

Security risks in cloud computing:

According to a recent IDC survey, the top challenge for 74% of CIOs in relation to cloud computing is security. Protecting private and important information such as credit card details or patients' medical records from attackers or malicious insiders is of critical importance. Moving databases to a large data centre involves many security challenges such as virtualization vulnerability, accessibility vulnerability, and privacy and control issues. Subashini and Kavitha [9] gift some basic security challenges that area unit information storage security, application security, information transmission security, and security associated with third-party resources. In several cloud service models, the protection responsibility between users and suppliers is totally different. In keeping with Amazon, their EC2 addresses security management in reference to physical, environmental, and virtualization security, whereas, the users stay answerable for addressing security management of the IT system together with the operational systems, applications and information. According to Tabakiet al. [15] the manner the responsibility for privacy and security in an exceedingly cloud computing atmosphere is shared between shoppers and cloud service suppliers differs between delivery models.

1. In SaaS, cloud suppliers area unit tried and true for the protection and privacy of application services than the users. This responsibility is a lot of relevant to the general public than the non-public cloud atmosphere as a result of the purchasers want a lot of strict security needs within the public cloud.
2.In PaaS, users area unit answerable for taking care of the applications that they build and run on the platform, whereas cloud suppliers area unit answerable for protective one user's applications from others.
3. In IaaS, users area unit answerable for protective operational systems and applications, whereas cloud suppliers should give protection for the users' information. Resources within the cloud area unit accessed through the Internet; consequently though the cloud supplier focuses on security within the cloud infrastructure, the info continues to be transmitted to the users through networks which can be insecure. As a result, web security issues can have an effect on the cloud; with bigger risks attributable to valuable resources hold on among the cloud and cloud vulnerability. The technology utilized in the cloud is comparable to the technology utilized in the net. Secret writing

Tele:
E-mail addresses: akshere.ashish@gmail.com

techniques and secure protocols aren't comfortable to shield information transmission within the cloud. Information intrusion of the cloud through the net by hackers and cybercriminals must be self-addressed and also the cloud atmosphere must secure an and personal for purchasers [9]. We will address 3 security factors that significantly have an effect on single clouds, namely data integrity, data intrusion, and service availability.

Data Integrity

Data integrity is one amongst the foremost vital components in any system. Data integrity is definitely achieved during a standalone system with one information. Data integrity in such a system is maintained via info constraints and transactions. Transactions ought to follow ACID (atomicity, consistency, isolation and durability) properties to make sure data integrity. Most information bases support ACID transactions and might preserve data integrity. The information hold on within the cloud might suffer from harm throughout transition operations from or to the cloud storage supplier. Cachinet al. [3] provides samples of the danger of attacks from each within and outdoors the cloud supplier, like the recently attacked Red Hat Linux's distribution servers. Another example of broken information occurred in 2009 in Google Docs, which triggered the Electronic Privacy data Centre for the Federal Trade Commission to open associate investigation into Google's Cloud Computing Services [3]. Another example of a risk to data integrity recently occurred in Amazon S3 wherever users suffered from information corruption [14].

Data Intrusion

According to Garfinkel [10], another security risk that will occur with a cloud supplier, like the Amazon cloud service, could be a hacked countersign or data intrusion. If somebody gains access to AN Amazon account countersign, they are going to be able to access all of the account's instances and resources. So the taken countersign permits the hacker to erase all the data within any virtual machine instance for the taken user account, modify it, or perhaps disable its services. What is more, there is an occasion for the user's email (Amazon user name) to be hacked (see for a discussion of the potential risks of email), and since Amazon permits a lost countersign to be reset by email, the hacker should still be able to log in to the account when receiving the new reset countersign.

Service Availability

Another major concern in cloud services is service availability. Amazon mentions in its contract that it is attainable that the service may be untouchable from time to time. The user's internet service could terminate for any reason at any time if any user's files break the cloud storage policy. Additionally, if any injury happens to any Amazon internet service and therefore the service fails, during this case there will be no charge to the Amazon Company for this failure. Corporations seeking to shield services from such failure want measures like backups or use of multiple suppliers.

Current Solutions of Security Risks

In order to scale back the danger in cloud storage, customers will use cryptographic strategies to safeguard the hold on data within the cloud. Using a hash function [13] could be a smart solution for data integrity by keeping a short hash in local memory. During this manner, authentication of the server responses is completed by recalculating the hash of the received data that is compared with the local stored data. If the amount of data is large, then a hash tree is that the solution [13]. In such a case, Mykletun et al. [5] and Papamanthou et al. [6] claim that this can be a full of life space in analysis on cryptographic strategies for stored data authentication. Cachinet al. [3] argue that though the previous strategies enable shoppers to make sure the integrity of their knowledge that has been came by servers, they are doing not guarantee that the server can answer a question while not knowing what that question is and whether or not the info is hold on properly within the server or not. Cachinet al. [3] suggest victimisation multiple cloud suppliers to confirm data integrity in cloud storage and running Byzantine-fault-tolerant protocols on them wherever every cloud maintains a single replica [4],[12]. Computing resources square measure needed during this approach and not solely storage within the cloud, such a service provided in Amazon EC2, whereas if solely storage service is offered.

Also Bessani et al. [13] use Byzantine fault-tolerant replication to store information on many cloud servers, therefore if one in all the cloud suppliers is broken, they are still ready to retrieve information properly. Data Encryption is taken into account the answer by Bessani et al. [13] to deal with the matter of the loss of privacy. They argue that to safeguard the keep information from malicious corporate executive, users ought to cipher information before it is keep within the cloud. because the information are accessed by distributed applications, the DepSky system stores the cryptographic keys within the cloud by victimisation the key secret sharing algorithmic rule to cover the worth of the keys from a malicious corporate executive. Within the DepSky system, information is replicated in four industrial storage clouds (Amazon S3, Windows Azure, Nirvanix and Rackspace); it's not relayed on one cloud, therefore, this avoids the matter of the dominant cloud inflicting the supposed vendor lock-in issue [1]. Additionally, storing the quantity of knowledge in every cloud within the DepSky system is achieved by the utilization of erasure codes. Consequently, therefore exchanging information between one supplier to a different can lead to a smaller price. The DepSky system aims to cut back the value of victimisation four clouds (which is fourfold the overhead) to doubly the value of employing a single cloud that could be a vital advantage [2].

Limitations of current solutions

With respect to above security solutions, Van Dijk and Juels [16] gift some negative aspects of information cryptography in cloud computing. Additionally, they assume that if the info is processed from totally different purchasers, encryption cannot guarantee privacy within the cloud. Though cloud suppliers square measure alert to the malicious business executive danger, they assume that they need vital solutions to alleviate the matter [11]. Rocha and Correia [8] classified four styles of attacks that may have an effect on the confidentiality of the user's knowledge within the cloud. These four styles of attacks might occur once the malignant business executive will verify text passwords within the memory of a VM, cryptographic keys mechanisms don't seem to be ok to contemplate the problem confidentiality and to guard data from these attacks. This doesn't mean that these mechanisms don't seem to be useful; rather that they are doing not concentrate on finding issues that Rocha and Correia address in their analysis & counsel trustworthy computing and distributing trust among several cloud suppliers as a unique answer to finding security problems and challenges in cloud computing The thought of replicating knowledge among totally different clouds has been applied within the single system DepSky [2]. Also Rocha and Correia [8] gift the constraints of this work that happens as a result of

the very fact that DepSky is merely a storage service like Amazon S3, and doesn't provide the IaaS cloud model On the opposite hand, this method provides a secure storage cloud, however doesn't give security of information within the IaaS cloud model. This is often as a result of it uses Encryption and stores the encrypted key within the clouds by employing a secret sharing technique, that is inappropriate for the IaaS cloud model.

Another drawback in this model is block size and its length are fixed and hence the modification of blocks cannot be done anywhere. Based on this work two Dynamic PDP [20] has been proposed. First is basic scheme, called DPDP-I and Second is the "blockless" scheme, called DPDPII. But these schemes are also not effective for a multi-cloud environment. Second approach is POR scheme [21], it describes the preprocessing steps that the clients should do before sending their file to a CSP. But this also not allow for updating the data efficiently. An improved version of this protocol called Compact POR has been proposed. This technique which uses homomorphism property to aggregate a proof into authenticator value but their solution is also static and could not prevent the leakage of data blocks in the verification process. The dynamic scheme with cost by integrating the Compact POR scheme and Merkle Hash Tree (MHT) into the DPDP has been proposed. Several POR schemes and models have been recently proposed by using RAID techniques. It introduced a distributed cryptographic system that allows a set of servers to solve the PDP problem. It is based on an integrity protected error correcting code (IP-ECC), which improves the security and efficiency of existing tools. Here , a file must be transformed into distinct segments with the same length, which are distributed across servers. It is more suitable for RAID rather than a cloud storage. Cloud computing is a trend in the present day scenario with almost all the organizations are entering into it.

Cloud computing is the collection of virtualized and scalable resources and provide service based on "pay only for use" strategy. It is a faster profit growth point by providing a comparably low-cost, scalable, position-independent platform for clients" data. It is constructed based on open architectures and has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. Such a distributed cloud environment is called Multi-Cloud.

Cloud computing is different from information technology by, Outsourced resources – This includes both hardware and software. On-site file server can provide a source for file handling, data storage, and information backup. In cloud computing also provide this service but the vendor foots the costs of these computer resources.

Pay-as-you-go – Cloud computing will require a basic start up fee followed by a monthly usage charge but it cost lower than installing On-site file management. User can pay charge based on cloud time consumption, operating space and additional software features. On-demand – In cloud computing, user pay for what you use. It satisfies every known business computer need, not all features are used by every purchaser. Thus the purchaser is freed to pursue more profit-oriented activities.

Research Scope

Past more researches has been conducted with respect to security concerns into single clouds and multi-clouds, clears that multi-cloud received less attention in research than single cloud as shown in Figure 1 and Figure 2. With this research findings, we aim to integrate secrete sharing algorithm with DepSky Model to address Security risks like Data Intrusion, Data Integrity, Service availability. The research scope of this paper is in mainly three security risks like data Integrity, Service Availability and Data Intrusion as shown in Figure 1 and Figure 2. Along with these, this paper also surveys additional security risks as mentioned below:

Data Storage and Security

Many cloud service provider provide storage as a service. They take the data from the user and stored on the large data centers, hence providing a user means of storage. Although these service provider says that data stored in a cloud is safe but there have been some cases where data is been modified or lost due to security holes. Various cloud providers adopt various technologies to resolve the problem of cloud data storage. The virtualized nature of cloud make the traditional mechanism unstable for handling the security risks so these service provider use different encrypting technique to overcome these problems.

Application Level Security

Application level security refers to the usage of software and hardware resources to provide the security to application such as attackers are not make any changes in the application format. Now a day's attacker launched them as a trusted user and system consider them as trusted user and allow full access to attacking party. The reason behind this is using outdated network policies. With the technological advancement these security policies become obsolete as there have been instances when system security have been breached, but with the recent technology advancements it is quit possible to imitate a trusted user. The threat to application level security include sql injection attack ,dos attack ,captcha breaking , xss attack. Hence, it is necessary to install high level security check to minimize these risks. These traditional methods to deal with increased security issue have been to develop a task oriented basic device which can handle the specific task and provide high level of security. But with application level threat being dynamic and adaptable to the security check in place, these closed system have to observed to be slow in compare to the open ended system.

Single to Multi-cloud

The use of cloud computing have increase in many organization. The cloud computing provide a many benefit in terms of cost and availability. The pay per use model know as cloud computing. One of the prominent service offers by cloud computing is cloud data storage, in which subscriber don't want to store their data on their own server, instead of that there data stored in cloud service provider. This service don't provide only flexibility and scalability for data storage but it also provide the customer with the benefit of only for the amount of data they need to store for the particular period of time. In addition to these benefits customer can access their data from anywhere as long as they are connected to internet. Since the cloud service provider is the different market entities, data integrity and privacy are the most common issues that need to be address in cloud computing. Even thought the cloud service providers have standard regulation and power infrastructure to ensure the customer data privacy and provide a better availability. The political influence might become an issue with the availability of the service.

Conclusion

It is clear that whereas the use of cloud computing has quickly expanded; cloud computing security is still advised the major issue in the cloud computing natural environment. Customers do not want to misplace their personal data as a outcome of malicious insiders in the cloud. In addition, the

decrease of service availability has initiated numerous troubles for a large number of customers lately. Furthermore, data intrusion leads to numerous problems for the users of cloud computing. The purpose of this work is to review the recent research on single clouds and multi-clouds to address the security dangers and answers. We have found that much study has been done to ensure the security of the single cloud and cloud storage whereas multi-clouds have obtained less attention in the locality of security. We support the migration to multi-clouds due to its ability to decline security risks that sway the cloud computing user. The different cluster configurations considered in this work have been selected manually, without considering any scheduling policy or optimization criteria, with the main goal of analyzing the viability of the multi-cloud solution from the points of view of performance and cost. Although a detailed analysis and comparison of different scheduling strategies is out of the scope of this paper and it is planned for further research, for the sake of completeness, in order to highlight the main benefits of multi-cloud environment capabilities.

Figure 1. Research and its scope related to Single Cloud

Ref	Year	Data Integrity	Data Intrusion	Service availability	Privacy/Security Mechanisms
[3]	2011	√			Multi shares+ secret sharing algorithm
[9]	2010			√	SPORC, (fork)
[10]	2010				cryptography
[11]	2010				Depot, (FJC)
[13]	2010	√			Venus
[8]	2009	√			encrypted cloud VPN
[12]	2009	√		√	TCCP
[14]	2009	√			homomorphic token + erasure-coded
[4]	2007	√			PDP schemes

Figure 2. Research and its scope related to Multi-Cloud

Ref	Year	Data Integrity	Data Intrusion	Service availability	Privacy/Security Mechanisms
[5]	2011	√	√	√	DepSky,(Byzantine + secret sharing + cryptography)
[2]	2010				RAID-like techniques+ introduced RACS
[7]	2010	√			ICStore ,(clientcentric distributed protocols)
[6]	2009	√		√	HAIL (Proofs + cryptography)

References

1. H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.
2. A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.
3. C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
4. M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998, pp. 173-186.
5. E. Mykletun, M. Narasimha and G. Tsudik, "Authentication and integrity in outsourced databases", ACM Transactions on Storage (TOS), 2,2006, pp. 107-138.
6. C. Papamanthou, R. Tamassia and N. Triandopoulos, "Authenticated hash tables", CCS '08: Proc. 15th ACM Conf. on Computer and communications security, 2008, pp. 437-448.
7. RedHat, Error! Hyperlink reference not valid..
8. F. Rocha and M. Correia, "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", Proc. 1stIntl. Workshop Dependability of Clouds, Data Centers and Virtual Computing Environments, 2011, pp. 1-6.
9. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.
10. S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp. 1-15.
11. E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), 2010, pp. 17-23.
12. J. Hendricks, G.R. Ganger and M.K. Reiter, "Lowoverhead byzantine fault-tolerant storage", SOSP'07: Proc. 21st ACM SIGOPS symposium on Operating systems principles, 2007, pp. 73-86.
13. R.C. Merkle, "Protocols for public key cryptosystems", IEEE Symposium on Security and Privacy, 1980, pp. 122-134.
14. Sun, http:// blogs.sun.com /gbrunett/entry/ amazon_s3_silent_data_corruption.
15. H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.
16.M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing", HotSec'10: Proc. 5thUSENIX Conf. On Hot topics in security, 2010, pp.1-8.
17. C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp. 1-9.
18. M. Vukolic, "The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp.105-111.
19. A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky and D. Shaket, "Venus: Verification for untrusted cloud storage", CCSW'10: Proc. ACM workshop on Cloud computing security workshop, 2010, pp. 19-30.
20. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted Stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.
21. M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.
22.J. Viega, "Cloud computing and the common man", Computer, 42, 2009, pp. 106-108.
23. R. Perez, R. Sailer and L. van Doorn, "vTPM: virtualizing the trusted platform module", Proc. 15th Conf. on USENIX Security Symposium,2006, pp. 305-320.
24. A. Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp. 612-613.
25. G. Brunette and R. Mogull (eds), "Security guidance for critical areas of focus in cloud computing", Cloud Security Alliance, 2009.
26. N. Santos, K.P. Gummadi and R. Rodrigues, "Towards trusted cloud computing", USENIX Association, 2009, pp. 3-3.