IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 1 (Sep. - Oct. 2013), PP 71-76
www.iosrjournals.org

Security Threat Solution over Single Cloud To Multi-Cloud Using DepSky Model

Monali Shrawankar, Associate Prof. Ashish Kr. Shrivastava
(*M. Tech Scholar, Dept. of Computer Science Engineering, NIIST, Bhopal, India)*
(Head PG Dept. of Computer Science Engineering, NIIST, Bhopal, India)

Abstract: *Cloud computing delivers IT resources as a Service over Internet The advantage of cloud computing is everlasting but it brings more issues including security. Ensuring the security of cloud computing is a foremost factor in the cloud computing environment, as users often store sensitive data with cloud storage providers but these providers may be untrusted. Cloud storage providers may be single cloud or multi-cloud. But it is found that the research into the use of multi-clouds providers to maintain security has received less attention from the research community than the use of single clouds. In this paper, we have created a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework applied multi-clouds and the date constraint validation to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity. We present a virtual storage cloud system called DepSky which consists of combination of different clouds to build a cloud of cloud.*

Keywords : *Cloud computing, cloud storage, data integrity, data intrusion, multi-clouds, service availability single cloud.*

I. INTRODUCTION

Cloud Computing[1] can be characterized as the moving of computing assets like processing power, network and storage assets from desktops and localized servers to large data hubs hosted by companies like Amazon, Google, Microsoft etc. These assets are provided to a user or business on highly scalable, elastic and pay-as-you-use basis. Figure1. shows a typical cloud computing architecture. The two most important components of cloud computing architecture are:

1. Front end
2. Back end

The Front end is the part glimpsed by the client i.e. the computer client. This encompasses the client's mesh and the submissions utilized to access the cloud via a user interface such as a World Wide Web browser. The Back end of the cloud computing architecture is the 'cloud' itself, comprising diverse computers servers and data storage devices. As shown in Fig.1, The cloud comprises of levels mostly the back-end levels and the front –end or client –end levels. The front-end levels are the ones you glimpse and interact with when you access your internet message on Gmail for example. You are utilizing programs running on the front-end of a cloud. The same is factual when you access your face book account. The Back-end comprises of the hardware and software architecture that fuels the interface you glimpse front end. Because the computers are set up to work simultaneously, the applications can take benefit of all that computing power as if they were running on one particular appliance.

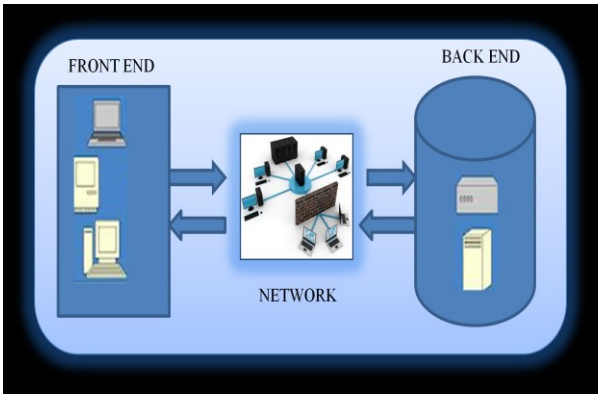


Figure 1. Cloud computing architecture

Cloud computing also permits for a lot of flexibility, counting on the demand, you can boost how much of the cloud assets you use without the need for assigning specific hardware for the job or just decrease the allowance of assets allotted to you when are not essential. Cloud service providers should ensure the customers' service infrastructure. The use of cloud computing Subashini and Kavitha [2] argue services for numerous reasons encompassing because this service supply fast access the applications and decrease service charges. Though cloud computing is targeted to provide better utiliza- tion of resources using virtualization techniques and to take up much of the work load from the client, it is fraught with security risks (Seccombe et al., 2009). The complexity of security risks in a complete cloud environment is illustrated in Fig. 2. The lower layer represents the different deployment models of the cloud namely private, community, public and hybrid cloud deployment models. The layer just above the deployment layer represents the different delivery models that are utilized within a particular deployment model. These delivery models are the SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) delivery models. These delivery models form the core of the cloud and they exhibit certain characteristics like on-demand self-service, multi-tenancy, ubiquitous network, measured service and rapid elasticity which are shown in the top layer. These fundamental elements of the cloud require security which depends and varies with respect to the deployment model that is used, the way by which it is delivered and the character it exhibits. Some of the fundamental security challenges are data storage security, data transmission security, application security and security related to third-party resources.

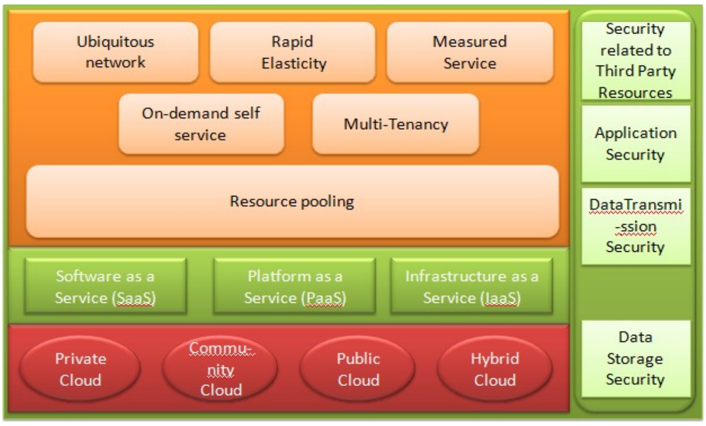


Figure 2. Complexity of security in cloud environment.

Cloud computing providers should address privacy and security as issue for higher and urgent main concerns. The considering with "single cloud‟ providers[13] is evolving less popular service with customers due to promise difficulties such as service accessibility failure for some time and malicious insider's attacks in the single cloud. So now single cloud move towards multi clouds, ‟interclouds‟ or" cloud of clouds‟.

II. The Problem Identified

As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider in single cloud. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. Moving database to a large data center involves many security challenges such as virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, data loss or theft. Problems identified insecurity factors as

- Data integrity: One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider.
- Data intrusion: Another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. Someone gains access to an Amazon account password; they will be able to access all of the account's instances and resources.
- Service Availability: Another major concern in cloud services is service availability. Amazon mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy.

III. Related Work

A wide variety of security techniques are proposed for single as well as multi-cloud providers. During this section, we have a tendency to describe and discuss such techniques, commenting on their usability and also the disadvantages with our proposed model.

K.D.Bowers suggested HAIL i.e; a distributed cryptographic system (High-Availability and Integrity Layer) [7] that allows a set of servers to prove to a client that a stored file is intact and retrievable. HAIL manages file integrity and availability across a collection of servers or independent storage services. HAIL relies on a single trusted verifier e.g., a client or a service acting on behalf of a client—that interacts with servers to verify the integrity of stored files. It aggregates cryptographic protocols for proof of recoveries with erasure codes to provide a software layer to protect the integrity and availability of the stored data, even if the individual clouds are compromised by a malicious and mobile adversary. HAIL has at least three limitations when compared with DEPSKY: it only deals with static data (i.e., it is not possible to manage multiple versions of data), it requires that the servers run some code (opposite to DEPSKY that uses the storage clouds as they are), and does not provide guarantee of confidentiality of the stored data.

Abu-Libdeh suggested RACS[8] i.e; Redundant Array of Cloud Storage system employs RAID5-like techniques (mainly erasure codes) to implement high-available and storage-efficient data replication on diverse clouds. Differently from DEPSKY, the RACS system does not try to solve security problems of cloud storage, but instead deals with “economic failures” and vendor lock-in. In consequence, the system does not provide any mechanism to detect and recover from data corruption or confidentiality violations. Moreover, it does not provide updates of the stored data [8].

There are a number of studies on gaining constancy from untrusted clouds. For instance, similar to DepSky, Depot improves the flexibility of cloud storage, as Mahajan et al. believe that cloud storages face many risks [13]. However, Depot provides a solution that is cheaper due to using single clouds, but it does not tolerate losses of data and its service availability depends on cloud availability [8]. Other work which implements services on top of untrusted clouds are studies such as SPORC [11] and Venus [12]. These studies are different from the DepSky system because they consider a single cloud (not a cloud-of-clouds). In addition, they need code execution in their servers. Furthermore, they offer limited support for the unavailability of cloud services in contrast to DepSky [6].

IV. PROPOSED SOLUTION

A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. This model focuses on the issues related to the data security aspect of cloud computing as shown in Figure 3. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient’s medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are surveyed.

3.1 MODULES ARE DESIGNED

- Client Registration: Client registered all those details for entering a multi-cloud. Register has been done in cloud server for storing the file in multi-cloud storage for the purpose of security by the client and file will be uploaded by client in multi-cloud storage.
- Administrator validating model: To facilitate employees accessing file collaboration from end point device are discovery that this online services can also display in file server. Registration and uploaded file by the client will be verified by the administrator as well as ability to remove & add the file for authentication purpose.
- Security Provider Cloud (MCSS2): This cloud will totally dedicate in providing security to the user. All the user that will be using services from cloud need to first login through this security provider cloud. This cloud will first do registration of the user and provide username and password to the user. After it will verify the user and after security provider cloud approval user will be able to enter into service provider cloud. Security provider cloud will always monitor the activity the user who is using services of the cloud. It can approve reject or block the user according to the need.
- Service Provider Cloud (MCFS1): Service provider work will only be providing services to the user; it will not look into security point since it will be handled by another cloud i.e security provider cloud. After user is registered and approved by security provider cloud, it will be connected to service provider cloud through web service and user and use services available to that cloud.
- One of the prominent service offer 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.

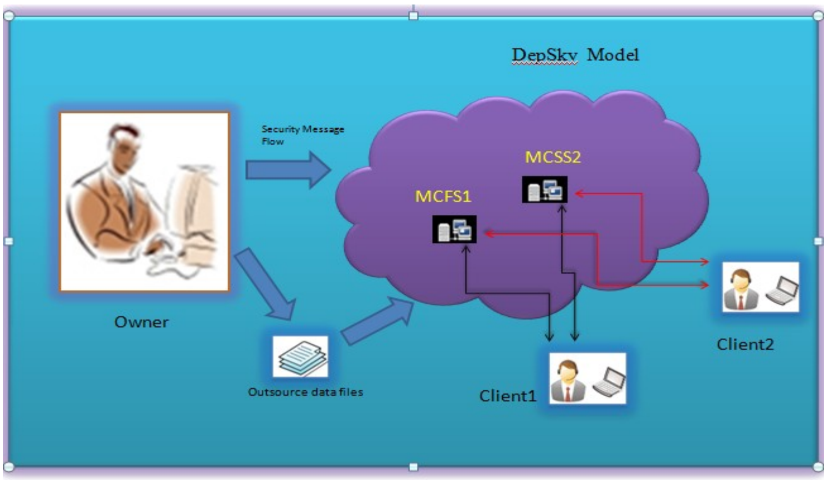


Figure 3. Proposed Model

3.2 DEPSKY SYSTEM: MULTI-CLOUD MODEL

The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" that were introduced by Vukolic [5]. These terms suggest that cloud computing should not end with a single cloud. Using their illustration, a cloudy sky incorporates different colors and shapes of clouds which lead to different implementations and administrative domains. Bessani et al. [6] present a virtual storage cloud system called DepSky which consists of a blend of different clouds to construct a cloud-of-clouds. The DepSky scheme locations the accessibility and the confidentiality of data in their storage system by using multi-cloud providers, blending Byzantine quorum scheme protocols, cryptographic secret sharing and erasure ciphers. As shown in Figure 4. The DepSky architecture [6] consists of four clouds and each cloud uses its own specific interface. The DepSky algorithm lives in the purchasers' machines as a programs library to broadcast with each cloud (Figure 4). These four clouds are storage clouds, so there are no ciphers to be executed. The DepSky library allows reading and writing procedures with the storage clouds and their multiple side clients. The DepSky scheme form comprises three components: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Bessani et al. [6] explain the distinction between readers and writers for cloud storage. Readers can go wrong randomly (for example, they can go wrong by smashing into, they can go wrong from time to time and then display any behaviour) while, writers only fail by crashing

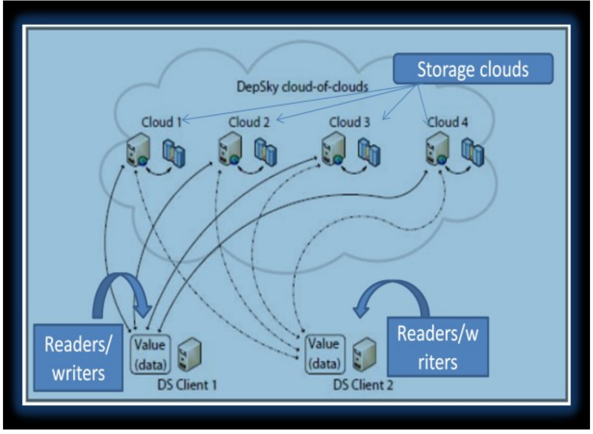


Figure 4: DepSky Architecture

3.3 DATA INTEGRITY IN MULTI CLOUD

We provide a very quick and effective means for supplying data integrity for client data in multi cloud. Our means is a hash based approach. The users file is dividing to numerous blocks. At any instant of time the file are stored in two distinct clouds. For each impede hash is calculated and the hash is furthermore maintained in the cloud. When any client requests for the cloud, the file blocks are retrieved from two cloud positions. The blocks are ideally kept in distinct storage servers in the cloud. The blocks are assembled to pattern while it is through the hash value of impede matching with retained hash worth the integrity is verified. We also hold track of number of times the files for corrupted for the user and the number of times the files are corrupted in the cloud server. If the enumerate of the number of times file corrupted for client are higher, then it concludes that the authentication of the user has a leakage and his documents are purposely corrupted by compromise of authentication parameters. In our suggested scheme we will hold diverse grades of security and distinct security profiles will be enabled founded on the file corruption threshold parameter. Furthermore from the enumerate of number of times files getting corrupted in cloud server, reputation of storage server is found. This will help the administrators to use mechanism like firewalls to advance the security of smaller status storage servers. Based on the status of all servers in the cloud storage the status of the cloud calculated. If the reputation of cloud is lower the cloud facts and figures is backed up to other cloud and cloud is taken all the contents and that storage cloud is drooped from use for storage. While penalizing the cloud for its smaller status , we should also address that compromise in client security may be due to client fault and penalizing should not be done due to this fault. The file corruption condition must be accounted in bas status only when largest security profile is assigned to client and still data corruption occurs.

3.4 DATA INTRUSION IN MULTI CLOUD

To bypass data intrusion, i.e. client authentication is hacked and fake users login and corrupt the data we provided a multi grade security profile for the user. The grades of security for the client are very adaptive. If the client data is corrupted, he is move to largest security profile level beginning from the lower security profile level. In our suggested answer we supply but numerous levels can be supplied.

1.UserTitle, password founded authentication
2.Secure meeting id dispatched to user on his wireless phone for authentication
3. Biometric authentication.

The default security profile is Level 1 client name/Password founded authentication. If the client files are often corrupted with grade 1, than for the specific user level 2 authentication is utilised. In level 2 clients has to go in his client id and get the password to get access to on his listed mobile number and he has to login using that password. This means is more secure than level 1. If the client document is still getting corrupted in level 2, the authentication is migrated to level 2. In level 2 biometric authentication is supplied which is much more protected than Level 1.

3.5 SERVICE AVAILABILITY IN MULTI CLOUD

Service availability is multi cloud is guaranteed with replicated file storage in two clouds. The file is replicated in the minimum of two clouds so that any point of time one cloud is always available. At each cloud , the file blocks are kept in the cloud storage , to guarantee high availability for the block. 1+1 replication for blocks are kept in servers, so that even if one of server is down the blocks can be retrieved from other server.

Figure 5. shows dataflow diagram of our proposed model. First client can login into server by giving his registration details. Under date constraint validation, client run his application and upload the file whatever he want. Client can first go through administration approval process. If client is approved can login and upload and download the file. This file is replicated internally and stored on both MCSS1 and MCFS2 and also to the cloud owner.

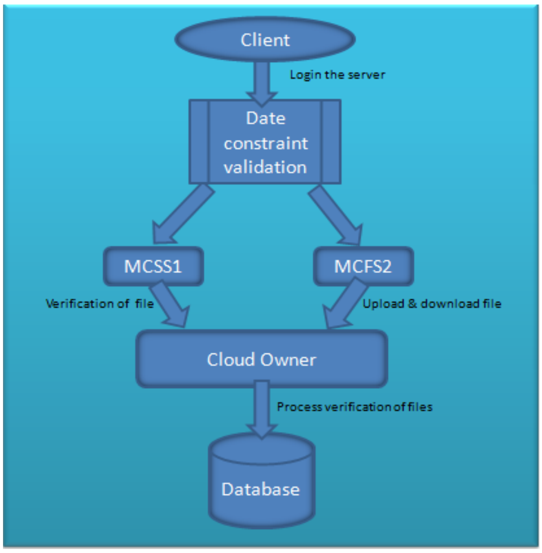


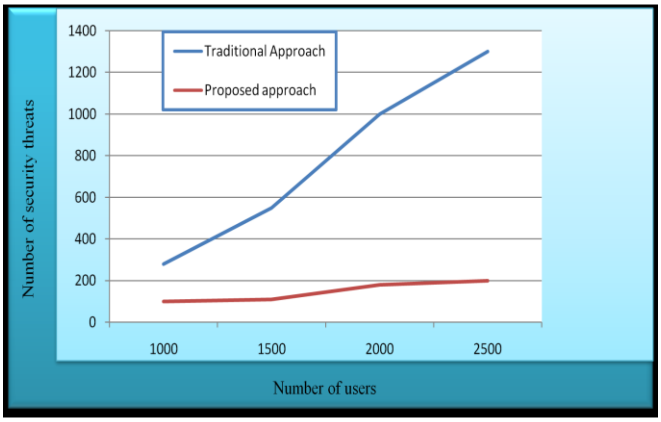
Figure 5: Dataflow diagram for a proposed model

V. RESULTS AND DISCSSIONS

In any cloud computing environment, the scope of activities can be divided into three major steps as: preliminary activities, initiating activities and concluding activities. The preliminary activities include a wide range of steps from identifying the security, privacy and organizational requirements[3] to analyzing the security and privacy provided by the security provider and the levels of risks involved with respect to control objectives of the organization .We have surveyed in our base paper[6] and compared all the security mechanisms in multi-cloud environment like RACS[8], HAIL[7] with DepSky model[6] and concluded that it is a virtual storage cloud system consisting of a combination of different clouds to build a cloud of clouds. Finally, the Depsky system presents an experimental evaluation with several clouds that is different from other previous work on multi clouds.

VI. PERFORMANCE ANALYSIS

We simulated the proposed answer for supplying service accessibility, attack against data intrusion and data integrity. We assessed the performance in periods of number of security risks with and without our means. We diverse the number of users in the cloud for 4 cloud anecdotes and 10 storage server in each cloud. From the performance journal that our suggested mechanism is able to decrease the number of security attacks gradually thanks to the adaptive user security profile setting and the status founded server filtering.



VII. CONCLUSION:

It is clear that whereas the use of cloud computing has quickly advanced; cloud computing security is still considered the major topic in the cloud computing natural environment. Customers do not want to misplace their private data as a outcome of malicious insiders in the cloud. In supplement, the decrease of service availability has initiated many difficulties for a large number of customers recently. Furthermore, data intrusion directs to numerous problems for the users of cloud computing. In this paper, we have proposed answers for three most widespread security threats in cloud storage. We have verified that our means performs better in decreasing the security risk on cloud.

REFERENCES

[1] http://www.techaaka.com/cloud-computing-architecture.html
[2] 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.
[3] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi, “A surveys on gaps, threat remediation challenge, and some thoughts for proactive attack detection in the cloud computing”, School of Information and Communication Technology, CQ University QLD 4702, Australia. Received 15 August 2011. Revised 11 January 2012. Accepted 18 January 2012. Available online 27 January 2012.
[4] Cloud Computing Security: From Single to Multi-Clouds,2012 ,45th Hawaii International Conference on System Sciences.
[5] M. Vukolic,"The Byzantine empire in theintercloud", ACM SIGACT News, 41,2010, pp.105-111.
[6] 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.
[7] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp.187-198.
[8] 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.
[9] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.
[10] 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.
[11] A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October2010, pp. 1-14.
[12] 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.
[13] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin and M. Walfish, "Depot: Cloud storage with minimal trust", OSDI'10: Proc. of the 9th USENIX Conf. on Operating systems design and implementation, 2010, pp. 1-16.