Comparative Study of Security Mechanisms in Multi-cloud Environment

Monali Shrawankar
Master of Computer Science & Engineering
NIIST BHOPAL

Ashish Kr. Shrivastava
Associate Professor
NIIST BHOPAL

ABSTRACT

The advantage of cloud computing is everlasting but it brings more issues including security. Double-checking the security of cloud computing is a foremost factor in the cloud computing natural 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.

This paper surveys many running research related to single clouds and multi-clouds security and address possible solutions and methodology. The main focus of this paper is use of multi-clouds and data security and reduce security risks. This paper gives a comparative analysis of various security mechanisms like HAIL[8], ICStore[10], RACS[9], DepSky model[7] using secret sharing algorithms[14]. Thus it could assist in analyzing best fit scenario for elegant secured cloud computing environment.

Keywords

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

1. INTRODUCTION

Cloud Computing can be characterised as the moving of computing assets like processing power, network and storage assets from desktops and localized servers to large facts and figures 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. It decreases the administrative and maintenance cost of IT associations. From an individual's perspective Cloud Computing is a revolutionary concept as it eliminates the obstacles conceived due to need of finance and resources therefore endowing very simple large scale deployment an submission. The cloud computing is a cost-effective, service availability, flexible and on demand service delivery platform for providing business through the internet. Cloud computing services used in small and medium companies for various reasons because these services provide fast access to their applications and reduce their infrastructure costs. There is use of multi-clouds in recent years.

This paper focuses on the issues related to the data security aspect of cloud computing. As facts and figures and data will be distributed with a third party, cloud computing users that can advantage its customers, such as very quick access to their data from any position, scalability, pay-for-use, facts and figures storage, facts and figures recovery, defence against hackers, on-demand security controls, and use of the mesh and infrastructure facilities want to bypass an un trusted cloud provider. Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure.

1.1 Cloud Computing Architecture

The two most important components of cloud computing architecture:
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 utilised 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 facts and figures storage devices.

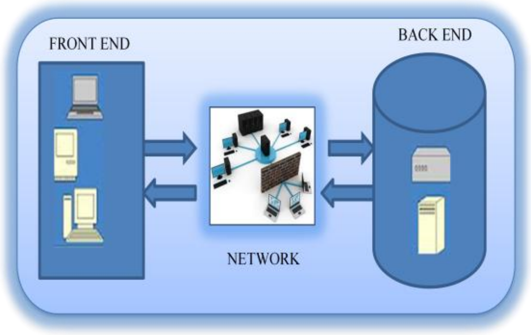

Figure 1. Cloud computing architecture

1.2 How Cloud Computing Works?

As shown in Figure.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 utilising 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. 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 users or customers' service infrastructure. The use of cloud computing Subashini and Kavitha [1] argue services for numerous reasons encompassing because this service supply fast access the applications and decrease service charges. Cloud computing providers should address privacy and security as issue for higher and urgent main concerns. The considering with "single cloud‟ providers[12] 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‟.

2. SECURITY IN CLOUD COMPUTING:

Cloud customers may pattern their anticipations founded on their past knowledge and associations desires. They are likely to perform some sort of review before selecting a cloud service provider. Customers are anticipated furthermore to do security checks that are cantered on three security notions: confidentiality, integrity and accessibility. On the other hand, cloud service providers may pledge a allotment to entice a clientele to signal a deal, but some gaps may manifest subsequent as swamping barriers to hold their promises. Many promise cloud customers are well cognizant of this and certainly, still sitting on the margins. They will not undertake cloud computing except they get a clear suggestion that all breaches are inside agreeable limits. All applicable data are visualized into cloud computing security in a snapshot which is presented in Figure 2 [2]. We coordinated cloud computing security into three sections: security classes, security in service consignment models and security dimensions [13].

Security in cloud services is founded on the following:
1. Powerful mesh security is likely round the service consignment platform
2. Data encryption: for data in transit (particularly over broad area networks), and sometimes retained facts and figures, but it cannot be applied to data in use.
3. Get access to controls to ensure that only authorized users gain get access to submissions, data and the processing environment and is the prime means of protecting cloud-based services
4. Service providers are able to examine undertaking in their environment and supply accounts to clients.

Logs need to be carefully constructed to appraisal the actions of their scheme administrators and other constrained users or risk making accounts that blend events relating to different customers of the service. Both the associations seeking cloud answers and the service providers have to double-check cloud security is addressed [4]. Some of the assesses to double-check security in cloud are good governance, compliance, privacy, persona and get access to administration (IAM), Data defence, Availability, Business Continuity and catastrophe Recovery designs etc. (see Figure.3)

Security performances a centred role in stopping service flops and cultivating trust in cloud computing. In specific, cloud service providers need to protect the virtual natural environment, which enables them to run services for multiple purchasers and offer distinct services for distinct clients. We will address 3 security components that significantly have an effect on single and multi-clouds, namely data integrity, data intrusion, and service availability.

2.1 Data Integrity

Data integrity is one amidst the foremost vital constituents in any system. Data integrity is decisively accomplished throughout a standalone scheme with one data. Data integrity in such a scheme is sustained by info constraints and transactions. Transactions should to pursue ACID (atomicity, consistency, isolation and durability) properties to make certain data integrity. Most data bases support unpleasant transactions and might maintain data integrity.

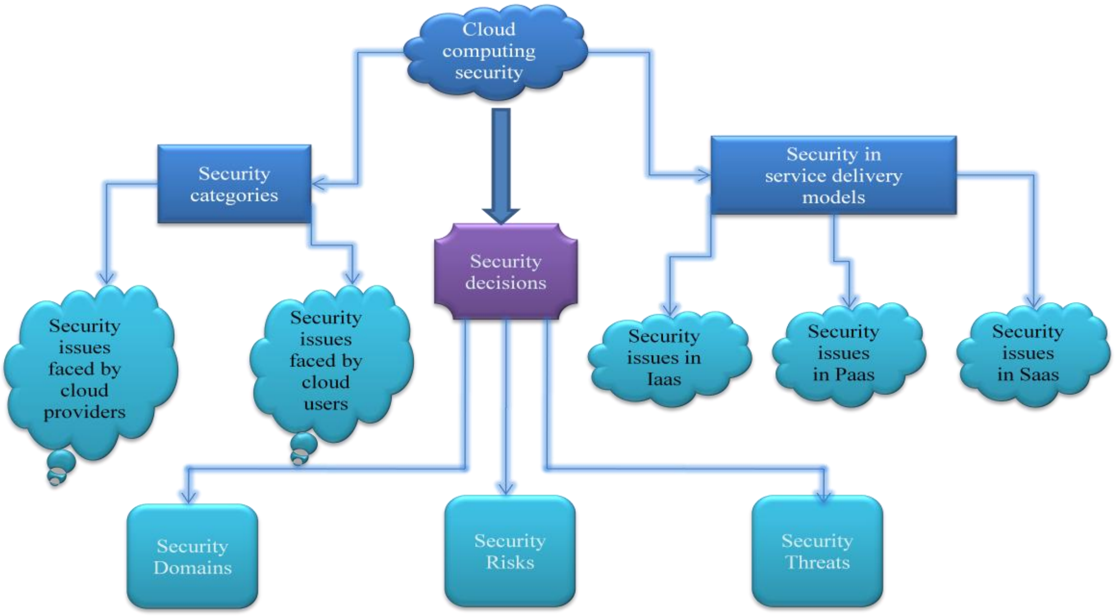

Figure 2 : Graphical View of Cloud Computing Security

2.2 Data Intrusion

The importance of data intrusion detection schemes in a cloud computing natural environment. We find out how intrusion detection is performed on programs as a Service, Platform as a Service and Infrastructure as Service offerings, along with the accessible owner, network and hypervisor-based intrusion detection options. Attacks on systems and data are a truth in the world we live in. Detecting and answering to those attacks has become the norm and is advised due diligence when it comes to security [5].

2.3 Service Availability

Another foremost anxiety in cloud services is service accessibility. Service accessibility is most important in the cloud computing security. Amazon currently mentions in its authorising agreement that it is possible that the service might be unavailable from time to time. The user's world wide world wide World Wide Web service may terminate for any cause at any time if any user's documents shatter the cloud storage principle. In supplement, if any damage happens to any Amazon world wide world wide web service and the service fails, in this case there will be no ascribe to the Amazon Company for this malfunction. Businesses searching to defend services from such malfunction need assesses such as backups or use of multiple providers [5][3].

3. DEPSKY SYSTEM: MULTI-CLOUDS MODEL

The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" that were introduced by Vukolic [6]. These terms suggest that cloud computing should not end with a single cloud. Using their illustration, a cloudy sky incorporates different colours and shapes of clouds which leads to different implementations and administrative domains. This section presents the DEPSKY system. It begins by presenting the scheme architecture, and then defines the data and scheme models, the two main algorithms (DEPSKY-A and DEPSKY-CA. This part will explain the latest work that has been finished in the locality of multi-clouds. Bessani et al. [7] 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 [7].

3.1 DepSky Architecture

The DepSky architecture [7] 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 (see Figure 5). 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.

3.2 DepSKy scheme form

The DepSky scheme form comprises three components: readers, writers, and four cloudstorage providers, where readers and writers are the client's tasks. Bessani et al. [7] 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.

3.3 DepSky Algorithms

3.3.1 DEPSKY-A– Available DepSky

The first DEPSKY protocol is called DEPSKY-A, and improves the accessibility and integrity of cloud-stored facts and figures by replicating it on some providers utilising quorum methods.

3.3.2 DEPSKY-CA– confidential & available DepSky

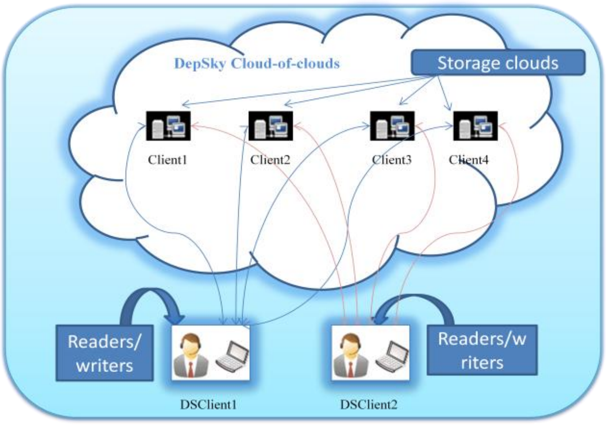

Figure 4: DepSky Architecture

The DEPSKY-A protocol has two major limitations. First, a data unit of dimensions S consumes n_S storage capacity of the scheme and costs on mean n times more than if it was stored in a lone cloud. Second, it stores the facts and figures in cleartext, so it does not give confidentiality assurances. To cope with these limitations we employ an information-efficient mystery distributing scheme that combines symmetric encryption with a academic secret distributing design and an optimal erasure code to partition the data in a set of blocks in such a way that f +1 blocks are essential to recover the original data and for less blocks do not give any data about the stored data.

4. COMPARATIVE ANALYSIS OF EXISTING APPROACHES IN MULTI-CLODS SECURITY MECHANISMS

Following are the mechanisms can be used in multi-cloud environment:

4.1 HAIL

It is a distributed cryptographic system (High-Availability and Integrity Layer) [K.D.Bowers 2009] [8], 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 [7].

4.2 RACS: Redundant Array of Cloud Storage

The cloud services marketplace is in its infancy. And while it may be at the forefront of technology, as a market—an *economic entity*—it is not so unique. The commoditization of cloud services has brought with it the characteristics of an economy, good and bad. In cloud computing, it is fitting that technological devices should be used to address economic problems, and that is what RACS [Abu-Libdeh 2010][9]is: A simple application of technology to change the structure of a market. In RACS, consumers have a tool that can be used to adjust the trade-off between overhead expense and vendor mobility. The main underlying technique that RACS employs to provide its flexibility is RAID at the cloud storage level, which is increasingly common. HAIL [8] uses RAID-like techniques across storage vendors to ensure high-availability and integrity of data stored in the clouds. The difference between systems like HAIL, peer-to-peer storage systems, and RACS is that RACS focuses on economic failures and how to prevent them without excessive overheads, while still benefiting from greater availability and durability of other RAID like systems. This 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 [7].

4.3 ICStore: Intercloud Storage

Cachin et al. [10] present a design for intercloud storage (ICStore), which is a step closer than RACS and HAIL as a dependable service in multiple clouds. Cachin et al. [10] develop theories and protocols to address the CIRC attributes (confidentiality, integrity, reliability and consistency) of the data stored in clouds. Intercloud Storage precisely addresses and improves the CIRC attributes (confidentiality, integrity, reliability and consistency) of today's cloud storage services. HAIL [8] uses erasure coding to disperse data over multiple providers, of which a fraction may collude against the user. It combines cryptographically sound proofs for the retrievability of the data (so that the provider cannot only pretend to have stored it) with the erasure-coded distributed storage. For data integrity, HAIL relies on a symmetric-key MAC, which the users must keep secret. The retrievability methods of HAIL may be combined with our ICStore architecture, but our integrity guarantees are stronger. Our approach is closest to that of RACS [9], which casts RAID techniques to the Intercloud, as we have already discussed. However, ICStore goes beyond RACS in dependability guarantees by addressing confidentiality, integrity and consistency and also allows for client failures and asynchrony by employing asynchronous fault-tolerant client-driven storage protocols [11].

Differently from DEPSKY, ICStore does not use the secret sharing algorithm on the provision of confidentiality. However it is not clear if information-efficient secret sharing [14] or some variant of this technique could substitute the erasure codes employed on these protocols [7].The overall comparative analysis of these multi-cloud strategies with respect to security threats mechanism is shown in Figure 6.

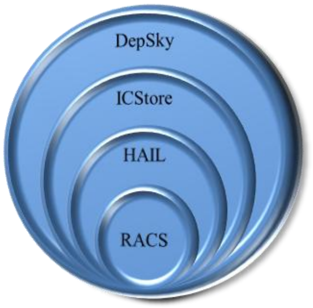

Figure 5: Stacked view of Multi-cloud Strategies

5. RESEARCH SCOPE:

Past more researches has been conducted with respect to security concerns into multi-clouds which we have summarized below in table 1.

Table1. Summary of security mechanisms in Multi-cloud

Sr.	Research Finding	Research Scope
1.	RAID-li\ke techniques + introduced RACS[9]	Deals with "economic failures" & Vendor loc\k-in, does not address security issues
2.	ICStore(Client-centric distributed protocols)[10]	Address only CIRC attributes
3.	HAIL (Proofs + Cryptography)[8]	Only manages file integrity & availability across a collection of servers, does not guarantee data confidentiality

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. Along with these, this paper also surveys additional security risks as mentioned below:

5.1 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.

5.2 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. 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 observe to be slow in compare to the open ended system.

6. 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.

7. REFERENCES

[1] 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.

[2] 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.

[3] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[4] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, "Security and Privacy in Cloud Computing: A Survey", Sixth International Conference on Semantics, Knowledge and Grids, August 2010.

[5] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds",2012 ,45th Hawaii International Conference on System Sciences.

[6] M. Vukolic,"The Byzantine empire in theintercloud", ACM SIGACT News, 41,2010, pp.105-111.

[7] 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.

[8] 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.

[9] 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.

[10] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.

[11] G. Chockler, R. Guerraoui, I. Keidar, and M. Vukoli´c, "Reliable distributed storage," IEEE Computer, vol. 42, no. 4, pp. 60–67, 2009.

[12] F. Rocha and M. Correia, "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", Proc. 1stIntl. WorkshopDependabilityof Clouds, Data Centers and Virtual Computing Environments, 2011, pp. 1-6.

[13] 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.

[14] Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp. 612-613.