ISSN No: 2348-4845

International Journal & Magazine of Engineering, Technology, Management and Research

A Peer Reviewed Open Access International Journal

Security Enhancements from Single to Multiple Clouds

Firas Talal Ahmed
Master of Science (Information System),
Nizam College (Autonomous),O.U,
Basheer Bagh, Hyderabad.

ABSTRACT:

Security issues of data hosted in a Cloud Computing provider remain hidden seen excessive marketing that led to a totally unrealistic view of cloud computing security. Although Cloud Computing has not yet reached the level of maturity expected by its customers, and that the problems of confidentiality, integrity, reliability and consistency (CIRC) are still open, the researchers in this field have already considered a future cloud strategy which aims : a better QoS, reliability and high availability, it is the Multi-Clouds, Cloud of Clouds or Interclouds. This paper will present the security limitations in the single Cloud and the usefulness of adopting rather Multi-Clouds strategy to reduce security risks, through the use of DepSky which is a virtual storage system that ensures better availability and high confidentiality of data.

Key words:
DepSky, Qos, Interclouds, confidentiality, Multi-Clouds

INTRODUCTION:

Cloud computing is Internet based development and use of computer technology. In concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure “in the cloud” that supports them. It typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet.The term cloud is used as a metaphor for the Internet, based on how the Internet is depicted in computer network diagrams and is an abstraction of the underlying infrastructure it conceals.

Typical cloud computing services provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers. These services are broadly divided into three categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The name cloud computing was inspired by the cloud symbol that is often used to represent the Internet in flow charts and diagrams.“Cloud Computing” refers to the use of Internet based computer technology for a variety of services.

It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet on a pay-for-use basis, at a fraction of the cost of provisioning a traditional Data Center based solution. All the costs associated with setting up a data center such as procuring a building, hardware, redundant power supply, cooling systems, upgrading electrical supply, and maintaining a separate Disaster Recovery site can be passed on to a third party vendor. Since the customer is charged only for computer services used, cloud computing costs are a fraction of traditional technology expenditures.

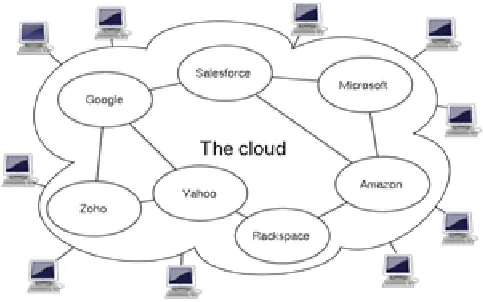

FIG: 1.1 Cloud Architecture

As a metaphor for the Internet, “the cloud” is a familiar cliché, but when combined with “computing,” the meaning gets bigger and fuzzier. Some analysts and vendors define cloud computing narrowly as an updated version of utility computing: basically virtual servers available over the Internet. Others go very broad, arguing anything we consume outside the firewall is “in the cloud,” including conventional outsourcing.Cloud computing comes into focus only when we think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT’s existing capabilities.

What does it mean to be a “cloud”?

A lot of times when we hear that something is “in the cloud,” it’s referring to something like Flickr, where you upload a photograph and the file exists somewhere, but you’re not sure where and you don’t really care. In other words, it is Software as a Service (SaaS) as opposed to software that you get on a disk or download and install on your home computer and use without an Internet connection. Other popular cloud-based services are gmail, Facebook, and salesforce.com.A cloud can also be a way of arranging its internal infrastructure, regardless of how the end user is consuming the computing power.

What IS a cloud?

Technically a computing cloud is a group of servers networked together with the following two characteristics:

- They are accessible over a network such as the Internet.

- They are virtualized, meaning multiple independent operating systems can be run on a server at once.

LITERATURE SURVEY

Byzantine disk paxos: optimal resilience with Byzantine shared memory

AUTHORS: I. Abraham, G. Chockler, I. Keidar and D. Malkhi,

We present Byzantine Disk Paxos, an asynchronous shared-memory consensus algorithm that uses a collection of n> 3t disks, t of which may fail by becoming non-responsive or arbitrarily corrupted. We give two constructions of this algorithm; that is, we construct two different t-tolerant (i.e., tolerating up to t disk failures) building blocks, each of which can be used, along with a leader oracle, to solve consensus. One building block is a t-tolerant wait-free shared safe register.

The second building block is a t-tolerant regular register that satisfies a weaker termination (liveness) condition than wait freedom: its write operations are wait-free, whereas its read operations are guaranteed to return only in executions with a finite number of writes. We call this termination condition finite writes (FW), and show that wait-free consensus is solvable with FW-terminating registers and a leader oracle.

We construct each of these ttolerant registers from n> 3t base registers, t of which can be non-responsive or Byzantine. All the previous t-tolerant wait-free constructions in this model used at least 4t + 1 fault-prone registers, and we are not familiar with any prior FW-terminating constructions in this model. We further show tight lower bounds on the number of invocation rounds required for optimal.

RACS: a case for cloud storage diversity

AUTHORS: H. Abu-Libdeh, L. Princehouse and H. Weatherspoon,

The increasing popularity of cloud storage is leading organizations to consider moving data out of their own data centers and into the cloud. However, success for cloud storage providers can present a significant risk to customers; namely, it becomes very expensive to switch storage providers. In this paper, the authors make a case for applying RAID-like techniques used by disks and file systems, but at the cloud storage level. They argue that striping user data across multiple providers can allow customers to avoid vendor lock-in, reduce the cost of switching providers, and better tolerate provider outages or failures. They introduce RACS, a proxy that transparently spreads the storage load over many providers.

Database Management as a Service: Challenges and Opportunities
AUTHORS: D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally

Data outsourcing or database as a service is a new paradigm for data management in which a third party service provider hosts a database as a service. The service provides data management for its customers and thus obviates the need for the service user to purchase expensive hardware and software, deal with software upgrades and hire professionals for administrative and maintenance tasks. Since using an external database service promises reliable data storage at a low cost it is very attractive for companies. Such a service would also provide universal access, through the Internet to private data stored at reliable and secure sites. A client would store their data, and not need to carry their data with them as they travel.

They would also not need to log remotely to their home machines, which may suffer from crashes and be unavailable. However, recent governmental legislations, competition among companies, and database thefts mandate companies to use secure and privacy preserving data management techniques. The data provider, therefore, needs to guarantee that the data is secure, be able to execute queries on the data, and the results of the queries must also be secure and not visible to the data provider. Current research has been focused only on how to index and query encrypted data.

However, querying encrypted data is computationally very expensive. Providing an efficient trust mechanism to push both database service providers and clients to behave honestly has emerged as one of the most important problem before data outsourcing to become a viable paradigm. In this paper, we describe scalable privacy preserving algorithms for data outsourcing. Instead of encryption, which is computationally expensive, we use distribution on multiple data provider sites and information theoretically proven secret sharing algorithms as the basis for privacy preserving outsourcing. The technical contributions of this paper is the establishment and development of a framework for efficient fault-tolerant scalable and theoretically secure privacy preserving data outsourcing that supports a diversity of database operations executed on different types of data, which can even leverage publicly available data sets.

Using Multi Shares for Ensuring Privacy in Database-as-a-Service
AUTHORS: M.A. AlZain and E. Pardede

Database-as-a-service (DAAS) is a new model for data management, where a service provider offers customers software management functionalities as well as the use of expensive hardware. This service enables data integration and access on a large scale in cloud computing infrastructures. Addressing data privacy in DAAS is considered a significant issue for any organizational database. Due to the fact that data will be shared with a third party, an un-trusted server is dangerous and unsafe for the user. This paper proposes the architecture of a new model appropriate for NetDB2 architecture, known as NetDB2 Multi-Shares (NetDB2-MS). It is based on multi-service providers and a secret sharing algorithm instead of encryption, which is used by the existing NetDB2 service. The evaluation is done through simulations. It shows a significant improvement in performance for data storage and retrieval for various query types.

DepSky: dependable and secure storage in a cloud-of-clouds
AUTHORS: A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa

The increasing popularity of cloud storage services has lead companies that handle critical data to think about using these services for their storage needs. Medical record databases, power system historical information and financial data are some examples of critical data that could be moved to the cloud. However, the reliability and security of data stored in the cloud still remain major concerns. In this paper we present DepSky, a system that improves the availability, integrity and confidentiality of information stored in the cloud through the encryption, encoding and replication of the data on diverse clouds that form a cloud-of-clouds. We deployed our system using four commercial clouds and used PlanetLab to run clients accessing the service from different countries. We observed that our protocols improved the perceived availability and, in most cases, the access latency when compared with cloud providers individually. Moreover, the monetary costs of using DepSky on this scenario is twice the cost of using a single cloud, which is optimal and seems to be a reasonable cost, given the benefits.

PROBLEM STATEMENT:

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds", "inter-cloud" or "cloud-of-clouds".

Drawbacks:

1. Cloud providers should address privacy and security issues as a matter of high and urgent priority.

2. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud.

PROBLEM DEFINITION:

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an un-trusted 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 is surveyed.

ADVANTAGES:

1. Data Integrity

2. Service Availability.

3. The user runs custom applications using the service provider's resources

4. Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure.

IMPLEMENTATION:
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. Cachinet al. give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers.One of the solutions that they propose is to use a Byzantine fault-tolerant replication protocol within the cloud. Hendricks et al. State that this solution can avoid data corruption caused by some components in the cloud. However, Cachinet al. Claim that using the Byzantine fault tolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place.

DATA INTRUSION:

According to Garfunkel, another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked (see for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

SERVICE AVAILIBILITY:

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. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers.

DEPSKY SYSTEM:

The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Bessani et al. explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas, writers only fail by crashing.

CONCLUSION:

It is clear that although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multi-clouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

REFERENCES:

[1] (NIST), http://www.nist.gov/itl/cloud/.

[2] I. Abraham, G. Chockler, I. Keidar and D. Malkhi,"Byzantine disk paxos: optimal resilience with-Byzantine shared memory", DistributedComputing, 18(5), 2006, pp. 387-408.

[3] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storagediversity", SoCC'10:Proc. 1st ACM symposium onCloud computing, 2010, pp. 229-240.

[4] D. Agrawal, A. El Abbadi, F. Emekci and A.Metwally, "Database Management as a Service:Challenges and Opportunities",ICDE'09:Proc.25thIntl. Conf. on Data Engineering,2009, pp. 1709-1716.

[5] M.A. AlZain and E. Pardede, "Using Multi Sharesfor Ensuring Privacy in Database-as-a-Service",44th Hawaii Intl. Conf. on System Sciences(HICSS), 2011, pp. 1-9.

[6] Amazon, Amazon Web Services. Web serviceslicensing agreement, October3,2006.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson and D. Song, "Provable datapossession at untrusted stores", Proc. 14th ACMConf. on Computer and communications security,2007, pp. 598-609.

[8] A. Bessani, M. Correia, B. Quaresma, F. André andP. Sousa, "DepSky: dependable and secure storagein a cloud-of-clouds", EuroSys'11:Proc. 6thConf. onComputer systems, 2011, pp. 31-46.

[9] K. Birman, G. Chockler and R. vanRenesse,"Toward a cloud computing researchagenda", SIGACT News, 40, 2009, pp. 68-80.

[10] K.D. Bowers, A. Juels and A. Oprea, "HAIL: Ahigh-availability and integrity layer for cloudstorage", CCS'09: Proc. 16th ACM Conf. onComputer and communications security, 2009, pp.187-198.

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

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

AUTHORS BIOGRAPHY:

FIRAS TALAL AHMED ,pursuing his Master of Science in Information System, from Nizam College (Autonomous),O.U,Basheer Bagh, Hyderabad,India.