IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111137

Communication between Two Cloud Using Depsky and Program Data Processors System

Dharini Pachare[1], A. Deharkar[2]

Final year, Shri Sai College of Engineering and Technology, Bhadrawati[1]

Professor, Shri Sai College of Engineering and Technology, Bhadrawati[2]

Abstract: In today□s life cloud, computing plays important role for the computing environment for reducing the cost of the computational cost and resources cost of the computing methods such as to storing the data and using the computing resources. It enables the use of the inter cloud communication for accessing the various information or data from different cloud. Inter cloud or multi cloud is term related to cloud of cloud, which provides the huge amount of data within the same cloud by adding the different cloud within single cloud. This method provides the service availability, storage of data and services within the same unit. Which provide the security to the whole data within the cloud by using the third-party auditing method, which requires applying the encryption key on data only one time, which can reduce the attacks on the cloud data? This paper also introduces the new method of multi cloud storage technique to store the data on the different small cloud within the system, which allows reducing the redundancy of data within the cloud.

Key Terms: Cloud Computing, Cloud Services, DepSky

I. INTRODUCTION

The use of cloud computing has increased rapidly in many organizations including because these services provide fast access to their applications and reduce their infrastructure costs [1, 2]. 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 entrusted cloud provider [3]. 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. Cloud computing describe as " a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" .

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment [4]. Users of online data sharing or network facilities are aware of the potential loss of privacy.

According to a recent IDC survey [5] 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, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. In different cloud service models, the security responsibility between users and providers is different. According to Amazon, their EC2[6] addresses security control in relation to physical, environmental, and virtualization security, whereas the users remain responsible for addressing security control of the IT system including the operating systems, applications and data. the way the responsibility for privacy and security in a cloud computing environment is shared between consumers and cloud service providers differs between delivery models. In SaaS, cloud providers are more responsible for the security and privacy of application services than the users.

This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud. In PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user' s applications from others. In IaaS, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the users' data.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111137

II. SECURITY RISKS IN CLOUD COMPUTING

The impact of security issues in the public cloud is greater than the impact in the private cloud. For instance, any damage which occurs to the security of the physical infrastructure or any failure in relation to the management of the security of the infrastructure will cause many problems. In the cloud environment, the physical infrastructure that is responsible for data processing and data storage can be affected by a security risk.

In addition, the path for the transmitted data can be also affected, especially when the data is transmitted to many third-party infrastructure devices [7]. As the cloud services have been built over the Internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the Internet; consequently, even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through networks which may be insecure. As a result, internet security problems will affect the cloud, with greater risks due to valuable resources stored within the cloud and cloud vulnerability. The technology used in the cloud is similar to the technology used on the Internet. Encryption techniques and secure protocols are not sufficient to protect data transmission in the cloud. Data intrusion of the cloud through the Internet by hackers and cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients [8].

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. The 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.
According to Garfinkel [19], 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 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 username) to be hacked (see [18] 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.

Another major concern in cloud services is service availability. Amazon [6] 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 [19]. Both Google Mail and Hotmail experienced service down- time recently [12].

If a delay affects payments from users for cloud storage, the users may not be able to access their data. Due to a system administrator error, 45% of stored client data was lost in LinkUp (Media Max) as a cloud storage provider [12].

III. MULTI-CLOUDS: PRELIMINARY

The term " multi-clouds" is similar to the terms " inter clouds" or " cloud-of-clouds" that were introduced by Vukolic [11,15]. 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 leads to different implementations and administrative domains.
Recent research has focused on the multi-cloud environment [3],[8],[10],[11] which control several clouds and avoids dependency on any one individual cloud.

Cachin et al. [11] identify two layers in the multi-cloud environment: the bottom layer is the inner cloud, while the second layer is the inter-cloud. In the inter- cloud, the Byzantine fault tolerance finds its place. We will first summarize the previous Byzantine protocols over the last three decades.

BFT protocols are not suitable for single clouds. Vukolic argues that one of the limitations of BFT for the inner-cloud is that BFT requires a high level of failure independence, as do all fault-tolerant protocols. If Byzantine failure occurs to a particular node in the cloud, it is reasonable to have a different operating system, different implementation, and different hardware to ensure such failure does not spread to other nodes in the same cloud. In addition, if an attack happens to a particular cloud, this may allow the attacker to hijack the particular inner-cloud infrastructure.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111137

IV. DEPSKY ARCHITECTURE

The DepSky architecture [8] consists of four clouds and each cloud uses its own particular interface. The DepSky algorithm exists in the clients' machines as a software library to communicate with each cloud (Figure 1). These four clouds are storage clouds, so there are no codes to be executed. The DepSky library permits reading and writing operations with the storage clouds. DepSky Data model. As the DepSky system deals with different cloud providers, the DepSky library deals with different cloud interface providers and consequently, the data format is accepted by each cloud. The DepSky data model consists of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation. DepSKy System model. 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. [8] 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. Cloud storage providers in the DepSky system model. The Byzantine protocols involve a set of storage clouds (n) where n = 3 f +1, and f is maximum number of clouds which could be faulty. In addition, any subset of (n – f) storage cloud creates byzantine quorum protocols [8].

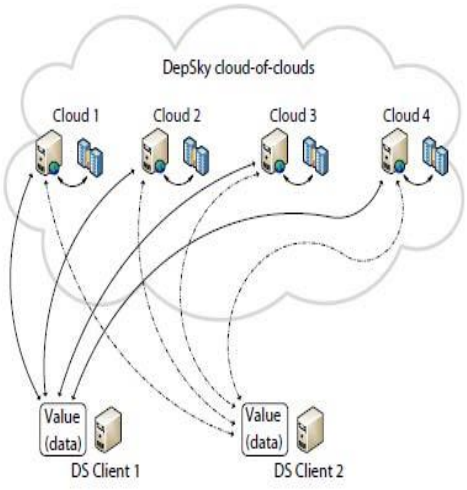

Figure 1. DepSky Data model

PDP in DepSky. The efficient PDP scheme is the fundamental construct underlying an archival introspection system that we are developing for the long-term preservation of data. Efficient PDP schemes will ensure that the computational requirements of remote data checking do not unduly burden the remote storage sites. Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an un-trusted server, can be used to realize audit services. Introduction of PDP in DepSky eliminate the extra n additional auditing requirement for each cloud data separately. By using the single PDP system and a single key for encryption the system can encrypt the data from the different cloud. The data can then decrypt or access by the user according to the inter cloud identification. While storing the data into the DepSky, which uses the different internal cloud using the hash method for dividing the same data into number of different blocks of same size, and store in the cloud. This method lets to increase the services availability by accessing the data from the different inter cloud. When storing the data, it adds some header information to identify the data block and access the data.

V. CURRENT SOLUTIONS OF SECURITY RISKS

To reduce the risk in cloud storage, customers can use cryptographic methods to protect the stored data in the cloud [12]. Using a hash function [35] is a good solution for data integrity by keeping a short hash in local memory. In this way, authentication of the server responses is done by recalculating the hash of the received data which is compared with the local stored data [12]. If the amount of data is large, then a hash tree is the solution . Many storage system prototypes have implemented hash tree functions, such as SiRiUS [20] and TDB this is an active area in research on cryptographic methods for stored data authentication. Cachinet al. [12] argue that although the previous methods allow consumers to ensure the integrity of their data which has been returned by servers, they do not guarantee that the server will answer a query without knowing what that query is and whether the data is stored correctly in the server or not. Proofs of Retrievability (PORs) and Proofs of Data Possession (PDP) are protocols introduced by Juels and Kaliski and Ateniese et al. [7] to ensure high probability for the retrieval of the user' s data. Cachinet al. [12] suggest using multiple cloud providers to ensure data integrity in cloud storage and running Byzantine-fault-tolerant protocols on them where each cloud

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022
DOI: 10.17148/IJARCCE.2022.111137

maintains a single replica [14]. Computing resources are required in this approach and not only storage in the cloud, but such a service also provided in Amazon EC2, whereas if only storage service is available, Cachin et al. [12] suggest working with Byzantine Quorum Systems by using Byzantine Disk Paxos[2] and using at least four different clouds to ensure users' atomicity operations and to avoid the risk of one cloud failure.

VI. CONCLUSION

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 many 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", Distributed Computing, 18(5), 2006, pp. 387-408.
[3] 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.
[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 Shares for 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 services licensing agreement, October3,2006.
[7] 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.
[8] 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.
[9] K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80.
[10] 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.
[11] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.
[12] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
[13] C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", DISC:Proc. 19thIntl.Conf. on Distributed Computing, 2005, pp. 497-498.
[14] M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998, pp. 173-186.
[15] G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer, 42, 2009, pp. 60-67.
[16] Clavister, "Security in the cloud", Clavister White Paper, 2008.
[17] 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.
[18] S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003, pp. 20-26.
[19] 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.
[20] E. Goh, H. Shacham, N. Modadugu and D. Boneh, "SiRiUS: Securing remote untrusted storage",NDSS: Proc. Network and Distributed System Security Symposium, 2003, pp. 131– 145.
[21] G.R. Goodson, J.J. Wylie, G.R. Ganger and M.K. Reiter, "Efficient Byzantine-tolerant erasure-coded storage",DSN'04: Proc.Intl. Conf. on Dependable Systems and Networks,2004, pp.1-22.
[22] E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), 2010, pp. 17-23.

