INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY (IJIT)

Volume 1, Issue 1,
January- June (2014), pp. 21-28
© IAEME: www.iaeme.com/IJIT.asp

IJIT
©IAEME

RELIABLE SECURITY IN CLOUD COMPUTING ENVIRONMENT

A.Madhuri[1], T.V.Nagaraju[2]

[1]Pursuing M. Tech (CS), [2]Asst.Professor(CSE)
[1]QIS college of Engineering and technology, ongole, Andhra Pradesh, India.
[2]QIS college of Engineering and technology, ongole, Andhra Pradesh, India.

ABSTRACT

Cloud computing is the newest term for the ongoing-dreamed vision of computing as a utility. The cloud provides convenient, on-demand network access to a centralized pool of configurable computing resources that can be rapidly deployed with great efficiency and minimal management overhead. The industry leaders and customers have wide-ranging expectations for cloud computing in which security concerns remain a major aspect 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 “multiclouds”, “intercloud” or “cloud-of-clouds”. The proposed design allows users to audit the cloud storage with very light weight communication and computation cost. Our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

Keywords: Cloud computing, Security Risks, single cloud, multi-clouds, data integrity, Service Availability.

1. INTRODUCTION

Cloud computing security (sometimes referred to simply as "cloud security") is a growing sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are "cloud-based" (security-as-a-service). In a cloud computing environment, the original computing infrastructure is used only when it is needed. For example, in order to process a user request, a service provider can draw the required resources on-demand, perform a specific job and then resign the not required resources and often arrange them after the job is complete. Contrary to traditional computing paradigms, in a cloud computing environment, data and the application is controlled by the service provider. This leads to a natural concern about data safety and also its protection from internal as well as external threats. Usually, in a cloud computing paradigm, data storage and computation are performed in a single datacenter. There can be various security related advantages in using a cloud computing environment. However, a single point of failure cannot be assumed for any data loss. the data may be located at several geographically distributed nodes in the cloud. There may be multiple points where a security breach can occur. Compared to a traditional in house computing, it might be difficult to track the security breach in a cloud computing environment.The use of cloud computing has increased rapidly in many organizations. Small and medium companies use cloud computing services for various reasons, including because these services provide fast access to their applications and reduce their infrastructure costs. 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”, “intercloud” or “cloud-of-clouds”.

Cloud Computing provides Internet-based services, computing, and storage for users in all markets including financial, healthcare, and government and those underlying computing infrastructure is used only when it is needed. In traditional computing paradigms, in a cloud computing environment, data and the application is controlled by the service provider. This leads to a natural concern about data safety and also its protection from internal as well as external threats. Despite of this, advantages such as-On demand infrastructure, pay as you go, reduced cost of maintenance, elastic scaling etc. are compelling reasons for enterprises to decide on cloud computing environments. Usually, in a cloud computing paradigm, data storage and computation are performed in a single datacenter. There can be various security related advantages in using a cloud computing environment. However, a single point of failure cannot be assumed for any data loss.

2. PROPOSED SYSTEM ARCHITECTURE

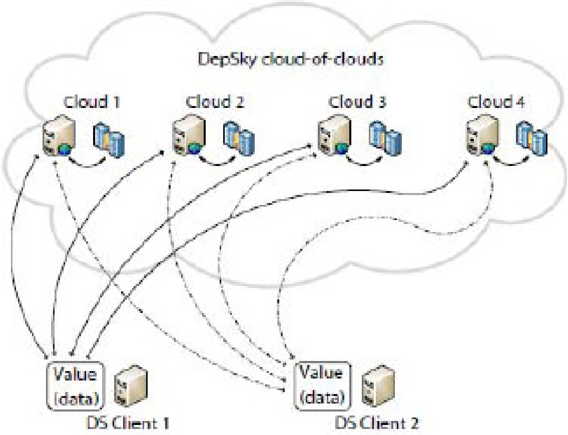

Figure 1: System Architecture

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.

ADV. OF PROPOSED ARCHITECTURE

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.

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. 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.

3. SECURITY RISKS IN CLOUD COMPUTING

The state of preventing a system from vulnerable attacks is considered as the system's security. Security risks involved with the governmental use of cloud computing have various risk factors. Seven important identity factors for risk in a cloud computing model are: Access, Network load, Data Security, Data Location and Data Segregation.

3.1 Access

The data in a private organization allows only the Authenticated users to access the data. The access privilege must be provided only to the concerned customers and auditors in order to minimize such risks. When there is an access from an internal to external source, the possibility of risk is more in case of sensitive data. Segregation of the data is very important in cloud computing as the data is distributed over a network of physical devices. Data Corruption arises if appropriate segregation is not maintained. Currently, there are no federal policies addressing how government information is accessed.

3.2 Network Load

Cloud network load can also prove to be detrimental to performance of the cloud computing system. If the capacity of the cloud is greater than 80%, then the computers can become unresponsive due to high volumes .The computers and the servers crash due to high volume motion of data between the disk and the computer memory. The percentage of capacity threshold also poses a risk to the cloud users. When the threshold exceeds 80%, the vendors protect their Services and pass the degradation on to customers. It has been indicated that in certain cases the outage of the system to the users are still not accessed. Flexibility and scalability should be considered pivotal when designing and implementing a cloud infrastructure. Money and time also plays an important role in the design of the infrastructure. Customers will always have expectations on the durability and the efficiency of the system. Going Forward the customers will also demand the need of Interoperability, ability to switch providers and migration options. Another risk factor of cloud computing is the implementation of the application programming interfaces (API).

3.3 Data Security

Another key criterion in a cloud is the data security. Data has to be appropriately secured from the outside world. This is necessary to ensure that data is protected and is less prone to corruption. With cloud computing becoming an upcoming trend, a number of vulnerabilities could arise when the data is being indiscriminately shared among the varied systems in cloud computing. Trust is an important factor which is missing in the present models as the service providers use diversified mechanisms which do not have proper security measures. The following sub section describes the risks factors in cloud environments.

3.4 Data Location

Data Location is another aspect in cloud computing where service providers are not concentrated in a single location but are distributed throughout the globe. It creates unawareness among the customers about the exact location of the cloud. This could hinder investigations within the cloud and is difficult to access the activity of the cloud, where the data is not stored in a particular data centre but in a distributed format. The users may not be familiar with the underlying environments of the varied components in the cloud.

3.5 Data Segregation

Data Segregation is not easily facilitated in all cloud Environments as all the data cannot be segregated according to the user needs. Some customers do not encrypt the data as there are chances for the encryption itself to destroy the data. In short, cloud computing is not an environment which works in a toolkit. The compromised servers are shut down Whenever a data is needed to be recovered. The available data is not correctly sent to the customer at all times of need. When recovering the data there could be instances of replication of data in multiple sites. The restoration of data must be quick and complete to avoid further risks.In different cloud service models, the security responsibility between users and providers is different. According to Amazon, their EC2 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.

4. ALGORITHM USED

Secret Sharing Algorithm

Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead.In cryptography, secret sharing refers to a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead. that will share a secret between several parties, such that none of them can know the secret without the help of others. Either all or a subset of them will need to get together and put their parts together to obtain the original secret. A simplistic solution can be achieved by XOR ing the secret with a random number, then giving the result to one party and the random number to the other. Neither one can find out what the secret was without the other. To retrieve the secret they only need to XOR the two parts together again. This can be extended to any number of parties. A more sophisticated way would be to allow the secret to be retrieved from a subset of the parts distributed. In the previous example, if any of the parties loses their part, or refuses to disclose it, then nobody can reveal the secret. This isn't much good if one of our cloud service providers fails. On the other hand, if we can share the secret between three people, but only require any two to regenerate the original, then we have some redundancy. This is an example of a (k,n) threshold scheme with k=2 and n=3.How do we achieve this though? Well, Adi Shamir proposed a simple secure secret sharing algorithm. It is based on drawing graphs. To uniquely define a straight line, you need two points on that line. Similarly, to define a parabola you need three points. A cubic requires four, etc. So, we can distribute points on a line to each party we want to share the secret with. The order of the line will determine how many of them need to get together to regenerate it. So, we could define a random straight line and distribute three points on it to three different parties. However, only two of them need to get together to regenerate the original secret.We set up a (k,n) threshold scheme by setting the free coefficient to be the secret and then choosing random numbers for each of the other coefficients. The polynomial then becomes the following:

$$y = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_{k-1}x^{k-1}$$

where a0 is our secret. Now we can distribute points on the line to each of the n parties simply by calculating y for a series of different values for x. We can use the Lagrange

Basis Polynomials to reconstruct the equation of the line from k points. However, we do not need to reconstruct the whole line, we are only interested in the free term. This simplifies the equations that we need to use. For example, if we have a straight line, then we only need two points (x0,y0) and (x1,y1). We can then calculate a0 as follows:

$$a_0 = -y_0 \frac{x_1}{x_0 - x_1} - y_1 \frac{x_0}{x_1 - x_0}$$

Similarly, for a parabola and three points (x0,y0), (x1,y1) and (x2,y2) wehave:

$$a_0 = y_0 \frac{x_1 x_2}{(x_0 - x_1)(x_0 - x_2)} + y_1 \frac{x_0 x_2}{(x_1 - x_0)(x_1 - x_2)} + y_2 \frac{x_0 x_1}{(x_2 - x_0)(x_2 - x_1)}$$

This should be fairly simple to implement and use. You would need to sign up to a few cloud services, but you wouldn't have all your eggs in one basket and you wouldn't be reliant on weak passwords.

5. DEPSKY MULTI-CLOUD MODELS

This section will explain the recent work that has been done in the area of multi-clouds. Bessani et al. present a virtual storage cloud system called DepSky which consists of a combination of different clouds to build a cloud-of-clouds. The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud models.

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. explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily whereas, writers only fail by crashing.

6. CONCLUSION AND FUTURE WORK

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.For data security and privacy protection issues, the Fundamental challenges are separation of sensitive data and access control. Our objective is to design a set of unified identity management and privacy protection frameworks across applications or cloud computing services. As mobility of employees in organizations is relatively large, identity management system should achieve more automatic and fast user account provisioning and de-provisioning in order to ensure no un-authorized access to organizations' cloud resources by some employees who has left the organizations. Authorization and access control mechanisms should achieve a unified, reusable and scalable access control model and meet the need of fine-grained access authorization. Accountability based privacy protection mechanisms will achieve dynamical and real-time inform, authorization and auditing for the data owners when their private data being accessed.

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. 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.
3. 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.
4. 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.
5. C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.
6. 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.
7. A. Juels and B.S. Kaliski Jr, "PORs: Proofs of retrievability for large files", CCS '07: Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 584-597.
8. S. Kamara and K. Lauter, "Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptograpy and data security,2010, pp. 136-149.
9. A. Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp. 612-613.
10. 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.
11. Prof. Manas Kumar Sanyal, Sudhangsu Das and Sajal Bhadra, “Cloud Computing-A New Way to Roll Out E-Governance Projects in India”, International journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 2, 2013, pp. 61 - 72, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.
12. Abhishek Pandey, R.M.Tugnayat and A.K.Tiwari, “Data Security Framework for Cloud Computing Networks”, International journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 1, 2013, pp. 178 - 181, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.
13. Rohinig.Khalkar and Prof. Dr. S.H.Patil, “Data Integrity Proof Techniques in Cloud Storage”, International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 2, 2013, pp. 454 - 458, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.
14. Gurudatt Kulkarni, Jayant Gambhir and Amruta Dongare, “Security in Cloud Computing”, International journal of Computer Engineering & Technology (IJCET), Volume 3, Issue 1, 2012, pp. 258 - 265, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

AUTHORS PROFILE

A. MADHURI Pursuing M.Tech (CS), QIS college of Engineering and Technology, Vengamukkalapalem, Ongole, Prakasham Dist, Andhra Pradesh, India. His research interests include cloud computing and Computer Networks.

T.V.Nagaraju Currently Working as Asst.professor in Dept of CSE, QIS college of Engineering and Technology, Vengamukkalapalem, Ongole, Prakasham Dist, Andhra Pradesh, India. His research interests include Software Engineering and Operating System.