Malware Check At Provider's Site Before Replicating and Synchronizing in Storage Clouds

Hemanth Kumar.K
Department of CSE
KMM Institute of Technology and Sciences
Tirupati, India

Haribabu Valleti
Department of CSE
KMM Institute of Technology and Sciences
Tirupati, India

Abstract:- **Cloud storage provides features like copying, backup and restore, synchronization and file sharing. As the service providers and the number of users increases the security issues also increases. As an example, a user may upload a file containing bad sector or some malware. There may be a chance that the uploaded malware could affect the entire cloud or if it is shared file that could cause damage to other cloud users. When coming to replication and synchronization among multiple clouds while mining these affected clouds, that will be hazardous. In this paper, we are proposing a two-side malware check to prevent attacks from user uploaded data. This will give an enhanced security to the storage clouds, so the providers can maintain a constant trust among all their clients.**

Keywords: irrevocable, synchronization, exacerbate, incriminating.

I.INTRODUCTION

Cloud computing has revolutionized the way computing and software services are delivered to the clients on demand. It offers users the ability to connect to computing resources and access IT managed services with a previously unknown level of ease. Due to this greater level of flexibility, the cloud has become the breeding ground of a new generation of products and services.However, the flexibility of cloud-basedservices comes with the risk of the security and privacy of users'data. Thus, security concerns among users of the cloud havebecome a major barrier to the widespread growth of cloudcomputing. Cloud computing is now trending technology all over the world and further implementations in this field makes it popular and it is now widely adopted by my organizations and individuals. The following is a small brief of cloud computing:

A. Cloud Computing

Cloud computing is a model which enables convenient, efficient, 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. In this section we have divided cloud computing into further part i.e. Service models, Cloud Component for more understanding about cloud.

B. Types of Service Models in Cloud

Cloud computing providers offer their services according to three fundamental models Infrastructure as a service (IaaS), and software as a service(SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models.

1) Software as a Service (SaaS): The capability provided to the consumer is to use the provider„s applications runningon a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2) Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructureconsumer created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

3)Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

The Cloud storage comes under Infrastructure of the cloud computing. Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications andservices from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its security.

The ever-increasing amount of valuable digital data both at home and in businessneeds to be protected, since its irrevocable loss is unacceptable.Cloud storageservices promise to be a solution for this problem. In recent years, their popularityhas increased dramatically. They offer user-friendly, easily accessible and cost-saving ways to store and automatically back up arbitrary data, as well as datasharing between users and synchronization of multiple devices.

However, individuals and especially businesses hesitate to entrust their data tocloud storage services since they fear that they will lose control over it. Recentsuccessful attacks on cloud storage providers have exacerbated these concerns. Theproviders are trying to alleviate the situation and have taken measures to keep theircustomers' data secure.

II. CLOUD STORAGE AND ITS CHALLENGES

While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced data. Since cloud service providers (CSP) are separateadministrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data protection. Examples of outages and security breaches of noteworthy cloud services appear from time to time. Secondly, there do exist various motivations for CSP to behave unfaithfully towards the cloud users regarding the status of their outsourced data.

As the usage of Cloud Storage increases it is very important to concentrate on the security of the information that was stored in them. The service providers, due to competition in the market they may not completely involved on the security of the cloud.

The challenges that are describing here were some concerns that the service providers need to take care of.

*A) Interoperability and Standards:*The issue of standards and interoperability exist since the early days of the computer business. The service providers should maintain interoperability and set of standards to satisfy the majority part of the customers. By providing interoperability the customers of cloud can access them from anywhere, anytime and by any computing device.

B) Data management and Scalability: Data stored on the clouds mast be neatly managed or organized for quick access. And Scalability refers to even though the size of the cloud, number of customers increases but the performance should be same.

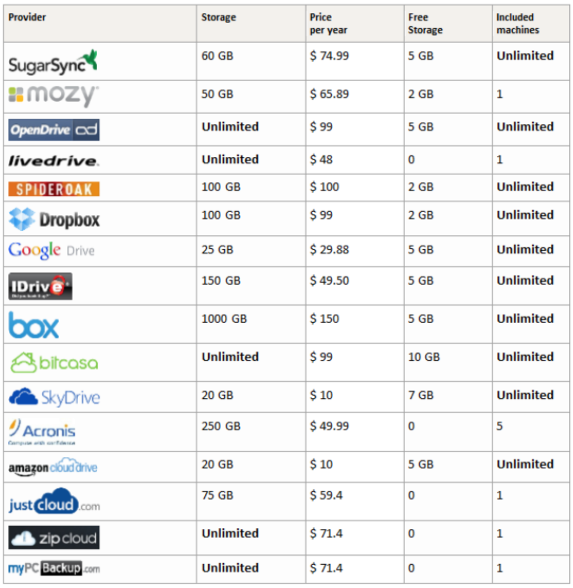
C) Confidentiality: Some uses these clouds to store confidential data and that must not be accessed by anyone other than the particular owner. It completely depends upon the service providers.

D) Availability: When a cloud server fails due to some reason, the service provided by it must not halt. It must keep on continuing its service in an alternative way. Here comes the need of replication. So that, the cloud is available all the time without any interruptions.

E)*Protect Data Privacy:* Data privacy protection has alwaysbeen an important aspect of a service level agreement for cloud storage services. The existing authentication procedures are also not enough in these days to give complete protection against attacks on the data stored in the cloud.

III. SERVICE PROVIDERS AND THEIR APPROACH

SugarSync, openDrive, spideroak, IDrive, box, zipcloud, justcloud, liveDrive, acronis, Dropbox, Mozy, TeamDrive, bitcasa, myPCbackup, Ubuntu One, Wuala, Amazon clouddrive, Google Drive and SkyDrive are the examples of Cloud storage service providers. The following figure shows the space provided by each cloud and cost details for further more usage.



Provider	Storage	Price per year	Free Storage	Included machines
SugarSync	60 GB	$ 74.99	5 GB	**Unlimited**
mozy	50 GB	$ 65.89	2 GB	1
OpenDrive	**Unlimited**	$ 99	5 GB	**Unlimited**
livedrive	**Unlimited**	$ 48	0	1
SPIDEROAK	100 GB	$ 100	2 GB	**Unlimited**
Dropbox	100 GB	$ 99	2 GB	**Unlimited**
Google Drive	25 GB	$ 29.88	5 GB	**Unlimited**
IDrive	150 GB	$ 49.50	5 GB	**Unlimited**
box	1000 GB	$ 150	5 GB	**Unlimited**
bitcasa	**Unlimited**	$ 99	10 GB	**Unlimited**
SkyDrive	20 GB	$ 10	7 GB	**Unlimited**
Acronis	250 GB	$ 49.99	0	5
amazon cloud drive	20 GB	$ 10	5 GB	**Unlimited**
justcloud.com	75 GB	$ 59.4	0	1
zipcloud	**Unlimited**	$ 71.4	0	1
myPCBackup.com	**Unlimited**	$ 71.4	0	1

Fig 1: Cloud storage providers and their strategy

All of them take differential measures to keep the data secure.The main tasks of Cloud Providers are: storing chunks of data, responding to a query by providing the desired data, and removing chunks when asked. All these are done using virtual id which is known as key for Amazons simple storage service (S3). Providers receive chunks from the distributor and store them. Each provider is considered as a separate disk storing clients' data. The cloud provider responds to the query of the distributor by providing data. Providers also receive remove requests from the distributor and acts accordingly by removing the corresponding chunk.

But main challenge is the individual who uploads the bad data that may contain a trojanware or a malware which can affect the cloud's performance and steals the private data.To eliminate the disadvantage of storing all data of aclient to the same provider, data can be split into chunksand distributed among multiple cloud providers. Theadvantage of this distributed system can be visualized whenan attacker chooses a specific client but the distributionof data obliges him to target multiple cloud providers,making his job increasingly difficult.The distributed approach can take the form of Redundant Array of Independent Disks (RAID) technique used for traditional databases.

IV. REPLICATION AND SYNCHRONIZATION

As we have said about to distribute data among various clouds rather than to store at one place, it is important to consider replication and synchronizationas a part of it.

Replication is the process of copying data, and the problems associated with replication are those of managing and maintaining multiple copies of the same information. Choosing an appropriate replication topology can have a major impact on how you address these problems. In its simplest form, the implementation of this use case copies all data in a data source to all other instances of the same data source, whether these data sources are located in the cloud or on-premises. In this scenario, applications running on-premises and services running in the cloud may be able to query and modify any data. They connect to the most local instance of the data source, perform queries, and make any necessary updates. At some point, these updates must be transmitted to all other instances of the data source, and these updates must be applied in a consistent manner. The following figure shows how the replication takes place:

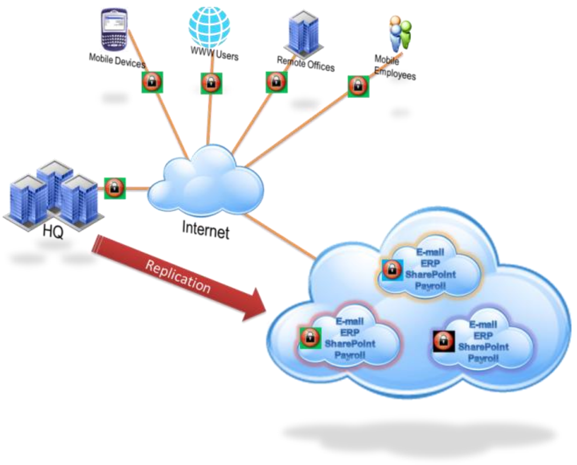


Fig 2: Replication in Clouds

Data changes, it is rarely entirely static. Applications inevitably insert, update, and delete records. In a replicated environment you must ensure that all such changes are propagated to all appropriate instances of a data source. Synchronizing data can be expensive in terms of network bandwidth requirements, and it may be necessary to implement the synchronization process as a periodic task that performs a batch of updates. Therefore you must be prepared to balance the requirements for data consistency against the costs of performing synchronization and ensure that your business logic is designed with eventual rather than absolute consistency in mind. Every time you update the data , you need to perform synchronization between all related clouds. Even if you are using a device to transact with the cloud then the device must also participate in synchronization process to get the updated data instantly.

V. WAYS OF ATTACKING

Initially we have discussed about the features and services provided by storage clouds. The copy feature means a servicejust mirrors a part of the localdisk in the cloud. If local hard-ware drops out (e.g. a stolen lap-top) data can be recovered fromthe cloud. If the data on the cloud is affected by a malware then that could cause a huge loss.

The synchronization feature which enables a user to synchronize all of his devices (desktop, laptop, tablet, mobile phone). In the process of synchronizing if one device already affected by a malware will spread to all other devices that are synchronizing. And this will cause other security issues like damaging important data and stealing private files and so on. The other king of attack we can observe is 'phishing'. Phishing is an unauthorized access to our account and credit card information.

The file sharingfeature which is used for collaboration with project partners and sharing files between a group of people. The mainadvantage of cloud storage is sharing any kind of data. Sometimes the same be a disadvantage if the people shared a virus affected file or something irrelevant.

Among all the above features file sharing can cause damage to a huge extent within no time. Even a mobile user who connects to that affected cloud will also be a victim. The following figure shows how the sharing can drastically be affected:

Fig 3: File Sharing in Storage Clouds

Another way of attacking that we are describing here is the attack on personal information like email details and social information if the email or the social network is depending upon the cloud storage. Absolutely this can be called as hacking in technical perspective. In these days the attacks are like they can dig up almost everything they want. The following figure describes how the social networks are now depending upon clouds and how they are accessed by the people with their devices.

Fig 4: Social Network's Cloud

The following is a scenario which describes the clouds are not fully protected. On registration a cloud storage service should verify that the email address of theuser really belongs to that user. A simple notification email which does not requireany further step is not suitable to provide sufficient security.Below we describe an attack on CloudMe, Dropbox and Wuala that is based on missing email verification. In the scenario, an attacker is using a cloud storageservice to store illegal or incriminating files in the name of his victim. It is necessary,that the victim is no registered customer of the corresponding service yet. Weassume that the attacker knows a valid email address of his victim. The attackconsists of the following steps:

(1) The attacker registers an account using the name and email address of hisvictim.

(2) The attacker uploads incriminating material using the account of his victim tothe cloud storage service. This can be illegal content, e.g., pictures with childabuse.

(3) The attacker notifies authorities, e.g., the police, about the illegal and incriminatingmaterial.

Instead of notifying authorities, it is also possible to incriminate the victim atfriends and colleagues. This might have unpleasant consequences for the victim.We assume that a notification email (\Welcome . . . ") sent by the cloud storageservice to the victim after step (1) will be ignored as spam by most users.All providers have been informed about the problem.

VI. PRESENT LOGIN AND REGISTRATION

Before customers are able to use a cloud storage provider to synchronize or back uppersonal data, they have to complete a registration process. Cloud storage providersusually require the creation of a user account before any services can be used. On the one hand, it is in the interest of the service provider to establish a single pointof contact through which all subsequent configuration, logging and above all accounting will take place. On the other hand, a customer who wishes to entrustpersonal data to the service provider wants to be certain that he communicates with the intended service and above all establishes a relationship of trust andcontracts the service provider to perform its duties as pledged. During the registrationprocess, the service provider and the new customer agree upon credentials these must later be used to log in and use the service. If at any time an attacker isable to eavesdrop on the communication, he might obtain the credentials, compromisethe account and gain access to uploaded data. Beyond that, if an attacker isable to manipulate the messages exchanged between customer and service provider,he might act as a proxy and defraud both of them.

In order to prevent these attacks,all communication between service provider and customer must be secured in terms of authenticity, confidentiality and integrity. The de-facto standard toachieve these goals on the web is to use the Transport Layer Security (TLS) protocol. Since service providers need to authenticate themselves against the

client machine by presenting a certificate, customers can examine it and use it toverify that they are really communicating with the intended service provider. Thatway, they have a means to detect impending phishing attacks, where attackers hosta website which looks very similar to the intended service and try to get users toenter their credentials.

When customers register to services which are free of charge, apart from theemail address only a unique key like a user name is needed to tie the customerto an account. However, storage services that need to be paid for necessitate thecollection of the customer's accounting data. To protect these, additional securitymeasures should be enforced by the service provider or optionally a third-partypayment service could be brought in to handle the accounting entirely.

VII.PROPOSED SECURITY MEASURES

The concerns will cause dissatisfaction in clients if their data in the storage clouds was not secure anyway. So, the proposed two-side malware check helps to continue the trust among all their clients. The two-side malware check introduces two time scanning of uploaded data to aware that the data uploaded was good and have no bad sectors.

Firstly, as to use the cloud storage service the users must install system software that acts as a tool to upload the user's data from their device. And the file being uploaded must be scanned for bad sectors and if any must be noticed to the clients and stop them from uploading.

Secondly, the file uploaded must be scanned at the server or provider's site to guarantee that the cloud contains unaffected data. It is very important to perform this scanning as there may be a case that the client doesn't take care of what data he was uploading. But the service providers must do check and scan for bad sectors and if necessary block that data and notify the client to delete it from the client's device as well as from the cloud.

VIII. EFFECT OF THE PROPOSED SYSTEM

The proposed system From the user's perspective he/she feel safe that, even though their device or computer is affected with malware, the data or files uploaded by them will be secured in the cloud. The malware check from user's side will only check the files that being uploaded and it is monitored by the tool which was suggested by the cloud storage service provider.

And from the service provider's perspective, by any chance if their tool at user's site fails to scan the affected files, the data stored and being stored will be malware free. So, there is no chance of distrust for the cloud users.

The complete control on the cloud gives us complete security. The proposed security system will surely helpful in extending present the securitysystem.

IX. FUTURE WORK

Many cloud storage providers now allowing their users to use the cloud limitedly i.e. the users can store the data from 2 GB to 15GB max. So, we have this idea of what if we combine all the clouds to form a hybrid cloud. We mean that the tool used to scan files before uploading is used to scan files and to upload them to any cloud based the free space available. And if there is no problem with the security of cloud then cloud to cloud communication is possible with low costs.

If you have no issue on security of the cloud we can share files between non homogeneous clouds. At present we are allowed to share the files within the same cloud. If we break the boundaries between clouds, any cloud user can share his data to any other cloud user. Hopefully we will soon represent the said mechanism with a clear view of terms and conditions and proceedings.

X. CONCLUSION

Individuals or companies considering using cloud storage services areadvised to check whether a cloud provider meets these security requirements.In addition, it is worthwhile to consider using more than one service to reduce theimpacts of service downtime. Further, calculation of the time to recover all datafrom the cloud is recommended. Depending on the individual amount of data, thismay take several days. Having a plan for a provider change in the future reducesthe dependency on a particular provider (provider lock-in). This will be relevant,for example, if the chosen provider is getting to expensive or is not longer compliantwith governmental rules.As a major result, the study shows that most of the analyzed cloud storageproviders are aware of the extreme importance of data security and privacy, hencethey have taken protection measures. However, a solution which meets all of themandatory security requirements has not been found with any of the analyzedproviders.

XI.REFERENCES

[1].Moritz Borgmann, Tobias Hahn, Michael Herfert, Thomas Kunz,Marcel Richter, Ursula Viebeg, Sven Vowe "On the securities of Cloud Storage Services", SIT technical reports March 2012.

[2]. Kai Hwang, Deyi Li "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE 2010.

[3]. Amazon Web Services: Overview of Security Processes, may 2011.

[4]. J. Wang, J. Wan, Z. Liu, and P. Wang. Data mining of mass storagebased on cloud computing. In IEEE Computer Society, pages 426–431,2010.

[5]. Peter Mell, and Timothy Grance, “The NIST Definition of Cloud Computing”, The National Institute of Standards and Technology, USA, 2011.

[6]. IT Strategists, “Top Cloud Computing Companies and Key Features”, Link: http://www.itstrategists.com/Top-Cloud-Computing-Companies.aspx.

[7]. Schmidt, M. ; Baumgartner, L. ; Graubner, P. ; Bock, D. ;Freisleben.B,Malware Detection and Kernel Root kit Prevention in Cloud Computing Environments, 2011.

[8]. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, Privacy-Preserving Public Auditing for Secure Cloud Storage.

[9]. G.Ateniese *et al*., “Provable Data Possession at Untrusted Stores,” *Proc. ACMCCS ‘07*, Oct. 2007, pp. 598–609.

[10]. M. A. Shah *et al*., “Auditing to keep Online Storage Services Honest,” *Proc.USENIX HotOS ‘07*, May 2007.

[11]. K. D. Bowers, A. Juels, and A. Oprea, “Hail: A High-Availability and Integrity Layer for Cloud Storage,” *Proc. ACM CCS ‘09*, Nov. 2009, pp. 187–98.

[12]. C.Wang *et al*.,”Ensuring Data Storage Security in Cloud Computing,” *Proc.IWQoS ‘09*, July 2009, pp. 1–9.

[13]. Q. Wang *et al*., “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” *Proc. ESORICS ‘09*, Sept. 2009, pp. 355–70.

[14]. C. Wang *et al*., “Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,” *Proc. IEEE INFOCOM ‘10*, Mar. 2010.