Institute of Advanced Engineering and Science

International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.2, No.6, December 2013, pp. 423~428
ISSN: 2089-3337

Cloud Storage Vendors Wide Support and Security Key Features for Shifting Towards Business Perspective

Prasath. T*, Karthikeyan. S**
* Assistant Professor, Departement of Computer Science and Engineering, Arunai Engineering College, Thiruvannamalai.
** Assistant Professor, Departement of Computer Science and Engineering, Arunai Engineering College, Thiruvannamalai.

Article Info

Article history:

Received Sep12th, 2013
Revised Oct 20th, 2013
Accepted Nov 26th, 2013

Keyword:

Cloud computing
Security
Storage
vendors
Services

ABSTRACT

The emerging trends that suits well with the shifting terminologies of computational environment. The cloud computing plays the vital role in today's business activities. The essential fact of computing rapid technological shift towards cloud. The storage medium of cloud provides common public spacing, privatized infrastructure, and other platform supports are facilitated. Here in this paper a brief scrutiny under gone on various cloud storage vendors. The various cloud storage vendors provides data storage, space availability, scaling, sharing, secure transmission between cloud storage medium. Here different vendors wide data storage mediums are discussed with their security features and data access managing capabilities are rendered.

First Author,
Departement of Computer Science and Engineering,
Arunai Engineering College, Thiruvannamalai, India
Email: prasath.27101987@gmail.com

1. INTRODUCTION

To store the data we depend on our own hard drives, and it gives feel that we have enough capacity with us. But the need for the capacity might occur and the present using storage may not satisfy the need based on memory. At that situation the user will be interested or needed to extend the memory to do this the user has to promote the memory device into a large capacity one by spending some capital. This condition will occur both in home or organization to overcome this now a day's most of the organization moves their data to cloud storage in which the expansion of memory for storage can to done based on the users need at any time. Because of the usage of cloud storage the hard drive usage, maintenance of the drive, expansion in hard drives gets decreased and the capital investment was done with profit. This cloud storage facility was provided by various providers with logical solutions.

Facility of portable connection was provided by them. Cloud providers introduces certain high quality plan will less cost so that the user will spend less money instead of spending in buying a new storage device to expand the capacity. With the help of internet connection the data stored in the cloud storage was retrieved and shared among others, the data maintaining effect was carried by the cloud providers itself, this data processing task was done anywhere in the world by the cloud service user. The security concerns issues related to the cloud storage that focuses on reliability and security. The users of cloud are guaranteed to entrust the data that are stored via internet connectivity. The information that are provided can be accessed from anywhere at any time. Cloud storage providers consider the security issues and follow various security providence methods and technologies to save the data from the hackers and from data loss.

2. AMAZON WEB SERVICES

An Amazon web service brings a large cloud computing platform that enable customer to build an extensive range of applications with high obtain ability, dependability and flexibility. To provide end to end security and privacy AWS builds services with security practices, security features and provides how to use those features. Additionally the customers have to use those features and practices for secure application environment. Here the customer has to ensure the confidentiality, integrity, and availability of their data is of maintaining trust and confidence.

It provides information about IT control environment to customers through white papers, reports, certifications and third- party attestations. The information assists customers in understanding relevant to AWS services and how it has been validated by the independent auditors and also it assist customers to validate whether the controls are working efficiently in IT environment.

Security Features: Amazon Web Services gives more number of ways to identify yourself and to access AWS account securely. The user can find whole list of IDs that support on the security IDs page under user account. The AWS provides additional security options for further protection of user account and control access such as Identity and Access Management (IAM), Multi-Factor Authentication (MFA), and Key Rotation.

2.1. Identity and Access Management (IAM)

Identity and Access Management (IAM) create multiple users and manage each user within your AWS account. To access AWS resources a user identity with unique security IDs can be used. Identity and Access Management removes the necessity to share passwords or access keys and creates easy to enable or disable a user's access. It implements security practices such as least privileges, assigning unique IDs to each user within AWS account. To perform their jobs the user need to access the AWS resources. By default IAM is secure one, no new user have access to AWS till the permissions granted. IAM minimize the use of user AWS account IDs. Instead of all relations with AWS resources must occur in IAM user security IDs.

2.2. Multi-Factor Authentication (MFA)

Multi-Factor Authentication offers better control over user AWS account settings and management of AWS resources. Multi-Factor Authentication is need to provide six digit single use code in addition to your user name and password IDs and the user get single use code from an authentication device or a special application on mobile phone in their physical ownership. In this two factors are checked before access is granted in their user account: First they need to provide AWS email as well as password and exact code from authentication device. It is easy to obtain an authentication device from participating third party provider or download and install appropriate software on your mobile phone.

2.3. Key Rotation

It is important to change the password frequently. Amazon Web services support multiple concurrent access keys and certificates. In this feature they can rotate keys and certificates in and out of operation without any downtime. Under AWS account the IAM APIs rotate the access keys of your AWS account as well as for users.

2.4. AWS Public PGP Key

The security team encourages customer communication. This process is established for reporting security vulnerabilities and requesting penetration testing. For sensitive communication the AWS created signed PGP key that will be need for user to send.

3. HP CLOUD SECURITY

HP apply global security skill to keep the user information and process lonely and it is secluded equally to logical and physical intimidation. The HP security experts cover the user needs, the security in HP are:

3.1. Physical Security

- In this the admittance control is via key card or biometric palm scanner.
- Monitoring includes both indoor and outdoor video observation and security workers on 24x7x365 basis in on site.
- To identify individual customers labeling is need on the equipment that could be used.
- HP security has multiple feeds and backup safety measures for both data links and power.

Here on the machine hall the customers and visitors are not allowed.

3.2. Client Data Isolation

The cloud compute services operate on shared infrastructure model, so it take steps to isolate, secure and protect each client information and processes. Here the components of data isolation include:

- Fiber channel zoning logically isolates servers.
- Logical unit security is used to isolate on storage devices and masking files are not legally available to other users.

Isolating/segregating each occupant on client dedicated broadcast domains for every clients application transfer and backup.

3.3. Data Security

The HP knows that the enterprise information is stored only in outside of user own systems. The safeguards of data security include:

- For security and traceability there will be individual administrative logins.
- For HP managed systems the two-factor-authenticated access is restricted to user accounts.
- The login IDs will be encrypted.
- Tools can be used to protect default password and incorrect configurations on HP managed servers.
- Firewall and VPN monitoring management are used. While replacing the online storage and backup media are scrubbed.

3.4. Audit Compliance

Here the HP requires audits, so it builds the elements to simplify the process.

- Facilitate any audits, typically conducted with third-party organizations, in conjunction with your security officers and ours.
- Correlate security intelligence from multiple sources and map it to your environment.
- All data centers are ITIL-process-compliant and ITIL-certified.

3.5. Application and Data Availability

HP gives business stability and helps better manage risk in the way that best fits your needs:

- Remote backup and restore
- Redundancy/failover
- Intrusion detection systems (IDS) and intrusion protection systems (IPS)
- Security consulting for custom needs
- Hardened OS configurations
- Log collection for infrastructure servers
- Option for clients to extend their existing identity management into the HP cloud.

4. AZURE

4.1. Security

Azure in data centers managed and operated by Microsoft Global Foundation Services(GFS). Microsoft operations staff are managed, monitored and administered that they have years of experience in delivering largest online services. Azure includes security practices at the application and platform layers to enhance security for application developers and service administrators. To support customers in evaluation of cloud services the Cloud security publishes Cloud Control Matrix (CCN).

4.2. Penetration Testing

To improve Windows Azure security controls and processes the Microsoft conduct penetration testing. The security is an important part of our customers application development and deployment. So, they established policy for customers to carry out authorized penetration testing hosted in Windows Azure. This testing should be conducted by certain terms and conditions. The notice should be submitted within 7 day for penetration testing.

4.3. Privacy

Privacy is one of the foundations of Microsoft's trustworthy computing. It is an integral part of our product and service lifecycle and offers customers privacy choices and manage the data that they store. The privacy principles state specific privacy statements, internal privacy standards that guide how to collect and protect customer data.

4.4. Location of Customer Data

Microsoft operates Windows Azure in data centers around the world. Customer Data include all text, sound, software or image files that are provided to Microsoft by, or on behalf of, a customer through its use of Windows Azure. For example, data a customer uploads for storage or processing in Windows Azure and applications that a customer uploads for hosting in Windows Azure.

5. CLOUDME

CloudMe can be only accessed if there is an internet explorer version 7 .Simple WebUI(alpha)52 is used for other browser to access the CloudMe but it was a very limited functionality. WebDAV protocol can also be accessed for CloudMe storage. Easy upload is a tool used to monitor local folders and upload folders. Windows, Linux, and Mac OS these are available for tool. In mobile devices also CloudMe Web desktop is designed. Different tools are available Simple WebUI (alpha), Easy Upload (Version 1.09), CloudMe Lite (Version 1.0.5 beta) and Web Desktop (Version 3.38 Beta) these are provided by the Client Software Version. It used many cloud storage providers because it is the premium business model. 3 GB online storage space is provided and service is free.25 GB or 100 GB storage can be extended. No limit size if we use 100 GB CloudMe storage.

5.1. Security

Country, username, password, email and last name the user should enter for registration. The password should be at least six characters long. The registration is not successfully completed if the password is too short. If the registration is failed the user does not give any additional feedback. If the user wants to reset the password the user can reset using CloudMe site. The reset page is sent to the user email address. The text is transmitted using HTTP or Plain text. The data is not encrypted between the server and client. The encryption is not done in the server. Other users of CloudMe service can share the folders. Arbitrary machines are used mainly for Cloud web desktop. To upload files on multiple computers Easy Upload tool is used in CloudMe. To check the application updates automatically Easy Upload tool is used on the client application.

6. Crashplan

Crash Plan is situated in Minneapolis, USA is operated by Code 42 Software56.Linux, Mac OS X and Windows are available for both the client application and server application. Online storage space is not provided for free version.10 GB online storage is used in the CrashPlan. To manage users CrashPlanPRO is designed for business. Features of free version is upgraded security, continuous backup and web restore function. Separate login and 200 computers is used. 7.49 Per month per user an unlimited plan. Server application CrashPlanPRO is mainly designed to store inside the company network. If the user want to upload empty hard drive is sent to the user then the hard drive is sent to the CrashPlan. To restore the hard drive the user should send along with its backup to the server and it is restored locally. The user cannot access any encrypted data using the CrashPlan software.

6.1. Security

User can create the account by giving their details such as first name, last name, email address and password. Account is created at the time of installation of software. Password should be six characters long if the password is too short it indicate the message as very weak that is it is shorter than six characters. At least six characters should be there otherwise password is weak. Password is strong means it contains six characters long. Letters, numbers and special characters it includes any of these which contains very strong. If the user registers the account, account is activated immediately the users don't want to activate the account. Once the email is activated the user receives a message welcome to CrashPlan. The email address given by the user is already available the user receives a message the email address already exist give alternate email.

7. Dropbox

Windows, Mac OS X and Linux are the client application. ipad, Blackberry, iPhone, and android are some of the applications are available.2 GB storage space is provided for dropbox. Amazon web services (AWS) storage used for Certifications Dropbox. Folder is uploaded. Through web interface files can be restored and uploaded. Files can be restoring to any version and records are stored for previous session. The user records are maintained for last 30 days. Synchronization user data is processed in the client application where data is automatically processed on multiple computers. Subscribers can share the files using Dropbox. Nonsubscribers of Dropbox access the information in URL where the folder is copied in a public folder.

7.1. Security

TLS is used for protected communication channels for registration and login process. email address can be created during the registration on the website or during the client installation. The user has to enter the last name, first name, email address and password. If the password is less than six characters the user gets a message the password is too short. The email address given by the user is already exists the user gets a message the email address already available, it prompt the user to give an alternate email address. The user given password is quality it showed in the form of colored bar. User can choose any lowercases, special characters, uppercase and digits for password. Once the user account is registered the user does not get any activation email from dropbox. Incrimination attack arises here. If the new account is created the user can use the email address once the registration form is complete. User want to enter use the user should enter the username and password if the user enters the wrong in any one of the username and password the user does not get any message which is incorrect, it simply says wrong.

8. MOZY

Windows and Mac OS X these are the operating system which runs on the client application. iPhone and Android are some of the applications are available. To maintain the account information and to download the software web interface is used.2 GB storage space is allotted for the user.125 GB storage space is available for multiple computers and 50 GB storage space is available for one computer. If we need we can purchase additional storage. The user can purchase the storage space up to 1 GB no limitation for purchasing the storage space. The account can be renewed by pay a fees or invoices and we can terminate the account immediately without any notice. Client application is maintained with the backup data. Backup files are not stored in the specific files or folders where to place it. Music, photos, emails are some of the different categories of Mozy. The information are searched on the hard disk automatically. Last 30 days records are stored in the previous session. Synchronization does not support in the Mozy.

8.1. Security

The user should enter a username, password, first name and last name to register the account. TLS is used for secure communication channels. The password should be at least six characters long otherwise the message will be displayed to the user has weak password. To strengthen the password they should give six characters long. If the email address already exists it is shown to the user.to download or to upload we use web interface. The information is entered only once because it is stored locally. The information is encrypted in the client side before transmitting to the server. The drawback in Mozy is that the user can choose the personal key but the user should be careful without lose the key. Backup data will be maintained in the multiple devices. List of multiple devices will be displayed in the web interface. Deletion or restorations are performed in the multiple devices. Mozy data center location are placed in Europe. Mozy EMC infrastructure is used in the Mozy website.

9. CONCLUSION

Here the paper concludes that the broad discussion of different vendors of cloud storage shows that how features are extensively utilized and service are provided with elasticity. The different vendors provide the storage area and as per the usage of service billing and pricing strategies are done. Each and every vendors enhanced their own security features and provides basic authentication facilities. Security is the major concern in all the computational trends so as to apply an efficient cloud storage medium for business perspective, the comparative solutions are defined.

REFERENCES

[1] Amazon Web Services: Overview of Security Processes March 2013.

[2] Moritz Borgmann, Tobias Hahn, Michael Herfert, Thomas Kunz, Marcel Richter, Ursula Viebeg, Sven Vow´e “On the Security of Cloud Storage Services”, March 2012.

[3] http://www.rackspace.com.

[4] http://www.nirvanix.com.
[5] Charlie Kaufman and Ramanathan Venkatapathy "Windows Azure Security Overview", August, 2010.

BIOGRAPHY OF AUTHORS

Mr. T. Prasath, assistant professor in Arunai Engineering College, Thiruvannamalai. Completed M.Tech (CSE) in Christ college of Engineering and Technology, Pondicherry University, Pondicherry. Completed Under Graduation (B.E.) at I.F.E.T College of Engineering, Gangrampalayam, Villupuram. Anna University Affiliated.

Mr. S. Karthikeyan, assistant professor in Arunai Engineering College, Thiruvannamalai. Completed M.E. (CSE) in Arunai Engineering College, Thiruvannamalai.. Completed Under Graduation (B.E.) at Arunai Engineering College, Thiruvannamalai.. Anna University Affiliated.