International Journal For Technological Research In Engineering
Volume 4, Issue 10, June-2017 *ISSN (Online): 2347 - 4718*

A FEATHER-WEIGHT CLOUD INFRASTRUCTURE FOR DATA RESERVED AND SERVICE

M.P Mahadeva Prasad[1], Prasanna B.T[2]
[1]M.Tech 2nd Semester, Department of computer Science and Engineering, JSS Science and technological University, Mysore, India
[2]Assistant Professor, Department of Computer Science & Engineering, Sri Jayachamarajendra College of Engineering(SJCE), JSS S&T University Campus, Mysore, Karnataka, India

Abstract: ***A private cloud refers to a model of cloud computing where storage and services are provisioned over private IT infrastructure for the dedicated use of a single organization. Private cloud storage is a type of storage mechanism that stores an organization's data at in-house storage servers by implementing cloud computing and storage technology. Private cloud storage does help resolve the potential for security and performance concerns while still offering many of the benefits of cloud storage such as scalability, reliability, rapid deployment of the storage architecture. But unlike public cloud storage, it is not publicly accessible, Private cloud is accessed through Local Area Network. The systems must be implemented and maintained in a way that not only satisfies the performance and resource availability requirements, but also fully addresses the questions of security, privacy and data ownership. A cloud service is any resource that is provided over the Internet. The most common cloud service resources are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) In this paper, a private cloud is implemented suitable for small to medium businesses which demonstrate the usage of the cloud as a storage and cloud as a service. SHA-256 is implemented for the client authentication.***

Keywords: Cloud Computing, Private Cloud, Cloud As A Storage, Cloud as a Service, SHA-256 Message Digest.

I. INTRODUCTION

A wide variety of Cloud Services are available today, such as Dropbox[1] SkyDrive, Google App Engine[4], or Amazon EC2[8]. These CSs can be categorized into 3 types: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). In all of these three categories, there exist Cloud Services for storage purposes, to provide data storage through a well-defineApplication Programming Interface (API). On one hand, services supporting any data types are termed generic Cloud storage services. On the other hand, there exist Cloud services that support storage of a restricted set of data types. Those are termed data-specific Cloud storage services. Typically, Cloud services offering data-specific storage employ a data validation scheme of certain data types and/or properties. E.g., Google Picasa provides an API, where users are able to publish and organize pictures and albums, allowing the upload of images with a certain file format (such as JPG, PNG, or BMP), resolution, and size.Cloud computing is complete new technique put forward from industry circle, it is the development of parallel computing, distributed computing and grid computing, and is the combination and evolution of virtualization, utility computing, Infrastructure-as-a-Service (IaaS), Platform-as-a- Service (PaaS) and Software-as-a-Service (SaaS) . To users, cloud computing is a Pay-per-Use-On- Demand mode that can conveniently access shared IT resources through internet. Where the IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner, and least management of and interactions with service providersCloud technologies have infiltrated society in many aspects. With enterprises and cloud services, trust issues were bound to come up. Trust is depicted as a complex factor formed of control over assets, data ownership, failure prevention and security. In [2], the Eucalyptus was considered in details. Eucalyptus is an open source private and hybrid cloud software representative, suitable for the use in enterprises. It is compatible with Amazon Web Services (AWS) cloud interface, allowing interaction between a private and a public cloud. Private cloud systems are highly adjustable to user's needs and offer great flexibility in terms of the number of active users and feature implementations. There are several solutions, but also many different concepts for custom usage within organizations. In this paper, we explore how private cloud solutions may benefit small to medium businesses (SMB). A deployment of an open source private cloud system with software solutions such as ownCloud, provides business users with internal control of privacy and sole data ownership.

II. RELATED WORK

Atefi et al. presented in [3] the use of open source private cloud for digital forensics. Seafile was chosen due to its advanced features for preserving privacy, file syncing, and collaboration. In a prototype research from Mościcki et al. [5], a private cloud solution for internal use by the CERN employees has been analyzed in depth, as an alternative to the public cloud services. The authors chose ownCloud as a viable platform for an open source private cloud solution for file sharing and synchronization on a very large scale. OwnCloud competitors, such as Pydio, Seafile, SparkleShare and Syncany were discarded because of feature incompleteness, usability issues or failing to support necessary file formats. They found that only ownCloud satisfied most of their demands for building an open source

cloud solution which can compare well to commercial solutions. Cloud storage arouses everybody's enthusiasm and ushered in the rapid market growth as soon as that enter China, that has emerged a large number of cloud storage application in just a few short years, such as Huawei, 360, kinsman has launched its own cloud storage applications. Some enterprises based on the existing user base, establishing and developing their own cloud storage applications, some enterprises halfway decent, with his bare hands to build his own cloud storage system, the reason is only one: they all look good which cloud storage market[7]. At same time ,the user are also showing an unprecedented support and enthusiasm in cloud storage.115network location announced their registered users has exceeded 30 million, while Huawei's network location also announced its own registered users has exceeded 20 million, which not only reflect the cloud storage application of high-speed development, comparing with the amount of Internet users, 420 million Internet users, this is to remind us, the cloud storage market of our country still has a considerable development space. However, large user base of cloud storage system performance and load problem poses a challenge.[8,9] Open business capacity platform is a server platform based on PaaS (Platform as a service) business model. Currently, many cloud storage services are realized through outsourcing, cloud storage service operators do not need to build their own file storage system, they can use the interfaces provided by platform to outsource the data store tasks. Some of these platforms are focus on cloud storage, some have much business and cloud storage is a part of them. What the well-known cloud storage DropBox used is Amazon S3 platform. There are two operators in this kind of cloud service, the cloud service operator and the data storage operator. The cloud service operator communicates with the users and manages user's information while the latter try their best to manage the users' files on the platform. Users didn't feel the data storage operators but they stay with them all day long. With the development of mobile Internet, developing the open business capacity platform applies to mobile Internet is on the time. The platform can not only provides cloud service but also provides telecommunications business capacity and other business capacities.

III. SYSTEM ARCHITECTURE

System architecture is the conceptual design that defines the structure and demeanor of a system. An architecture description is a formal description of a system, organized in a way that fortifies reasoning about the structural properties of the system. It defines the system components or building blocks and provides an orchestration from which products can be procured, The System architecture for our proposed system is shown in Fig.1. The modules shown in diagram contains client/user, Database, Administrator. The client/user can register the machine, check the status, login and can perform the file operations on the file stored in cloud storage. Database is used to store the registration request of the clients to access the storage and maintains the users profile. Administrator can approve the requests stored in the database and generates SHA -256 message digest based on the machine username, MACID, mother board id and store the message digest in database which is used for the authentication of the clients.

IV. DESIGN OF PRIVATE CLOUD

A. Cloud as A Storage Module Design

1. User Registration Based on The Machine Credentials:

The registration process automatically fetches the system username, MACID, motherboard id used for generating the SHA-256 message digest. The system username, MACID, motherboard id are non-editable. The user has to input the cloud

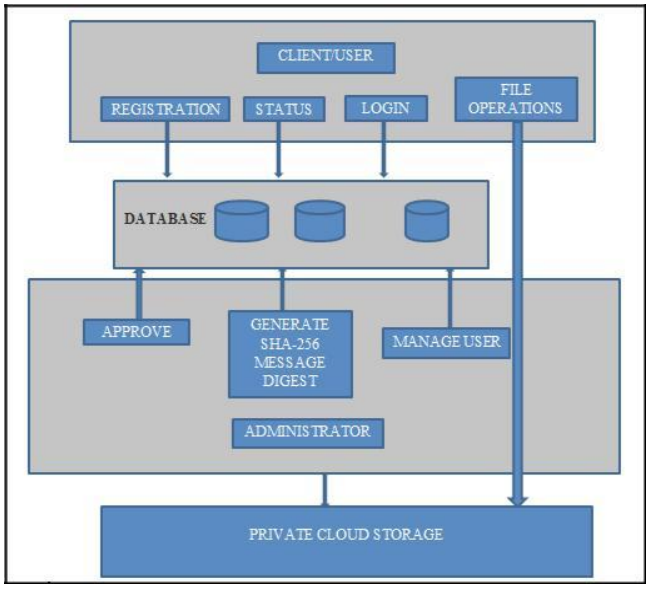

Fig. 1: The Proposed System Architecture

account name and valid email-id (where the password is sent) and send the request to the administrator. The registration request is added to the database with the above details (system username, MACID, motherboard id, cloud account name, E-mail id along with status(default status is 'N' not yet approved))which is to be approved by the administrator to access the cloud storage.The registeration request form is shown below.

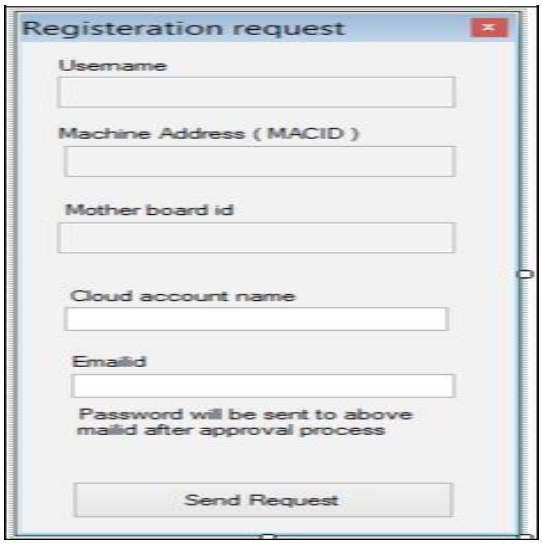

Fig. 2: User Registration form

2. Administrator Approval Process

Administrator can approve/delete the registration request stored in the database based on the availability of space in the network storage. When the administrator approves the request, the user status 'N' is changed to 'Y' which means that the respective user is approved to use cloud storage. The SHA is generated after the approval using SHA-256 algorithm and randomly generated Password is sent to the registered mail-id. The inputs to the SHA- 256 algorithm are system username, MAC-ID and mother board

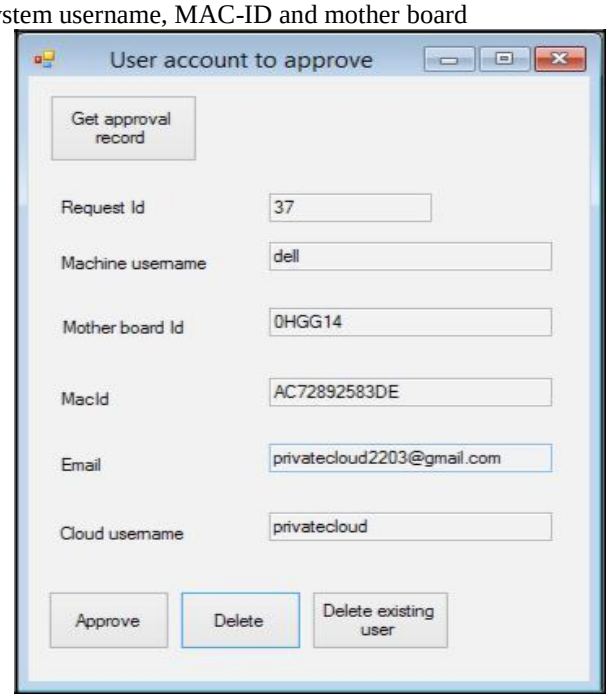

Fig. 3: Administrator approval form

3. SHA-256 MESSAGE DIGEST

SHA-256 transforms an input message into the 256 bits message digest. According to Secure Hash Signature Standard the input message whose length are shorter than 264 bits, should be operated by 512 bits in group and becomes a 256-bit message digest. The algorithm is summarized as follows:-

Step 1: Message Padding: Input binary message is appended with

1 & padded with Os until length = 448 mod 512.The original message length is then appended as 64-bit binary number. The padded message's length is a multiple of 512 bits, which decides how many '0' to be padded.

Step 2: Parsing: The padded message is then parsed into N 512-bit blocks: M (l), (2)…M (N).These M (i) message blocks are passed individually to the message expander.

Step 3: Message Expansion (Scheduler): Each 512 bit block can be divided into 16 32-bit words: $M_0^{(i)}$, $M_1^{(i)}$….. $M_{15}^{(i)}$, which are then expanded into 64 words labeled W0, W1… W63 under the certain rule prescribed by SHA-2 standard.

Step 4: Message Compression: The Wt words from Message expansion stage are then passed to the SHA compression function or the „SHA core". The core utilizes 8 working variables labeled a, b,……,h which are then initialized to predefined values $H0^{(0)}$ – $H7^{(0)}$ at the start of each call to the hash function.

Table 1 : Initial Hash Value of SHA-256.

a	$H_0^{(0)}$	6a09e667
b	$H_1^{(0)}$	bb67ae85
c	$H_2^{(0)}$	3c6ef372
d	$H_3^{(0)}$	a54ff53a
e	$H_4^{(0)}$	510e527f
f	$H_5^{(0)}$	9b05688c
g	$H_6^{(0)}$	1f83d9ab
h	$H_7^{(0)}$	5be0cd19

Step 5: The algorithm is implemented by 64-cycleb iterative computation each block. The eight working variables are labeled a, b, c...h, which are updating the value during the 64-cycle as follows.

$T_1 \rightarrow h + \sum_1(e) + Ch(e,f,g) + k_j + W_j$ $^{T}{}_{h}2_{\rightarrow}{}^{\rightarrow}{}_{g}{}^{\Sigma}0^{(a) + Maj(a,b,c)}$

g → f f → e

e → d+T_1 d → c

c → b b → a

a → T_1+ T_2

Step 6: After 64 iterations of the compression function, an intermediate hash value *H* (i) is calculated as follows:

H (i) → a + H (i-1)

$H^{1}{}_{2}$(i) → b + $H^{1}{}_{2}$(i-1)

$H_8^{(i)}$ → h + $H_8^{(i-1)}$

The SHA-256 compression algorithm then repeats and begins processing another 512-bit block from the message padder. After all the data blocks have been processed, final 256-bit output H_N is calculated as follows:-

$H^{(N)} = H_0^{(N)}$ & $H_1^{(N)}$……. $H_7^{(N)}$

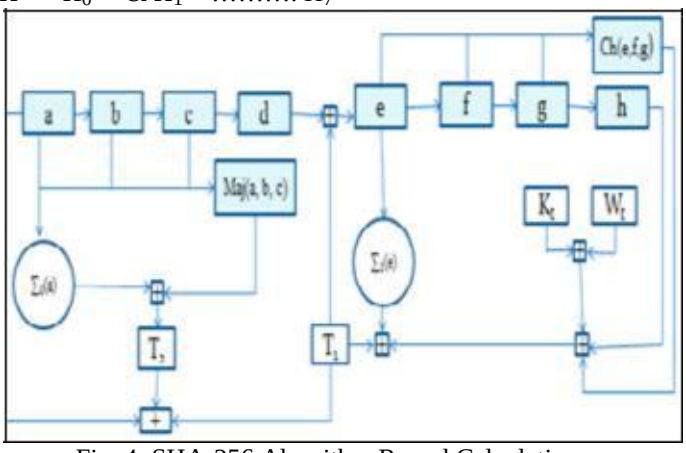

Fig. 4: SHA-256 Algorithm Round Calculation

4. User Authentication

There is a link present on the user login screen called check status which displays the status whether the admin has approved the registered user or not. When the user check status and if the admin has approved the user a file named authenticated is downloaded to the user machine which is used to validate the client. When the user login with valid username and password a message digest is dynamically generated by SHA algorithm using ,system username, MAC-ID and mother board id. If the dynamically generated

message digest matches the message digest present in the authenticated file generated during administrator approval process the user is given access to use the cloud storage.

5. File Operations

upload: It is the process of copying a file from user local storage to the cloud storage.The uploaded file is encrypted and saved in the cloud which is accessed only by the administrator or user who have uploaded the file.

Create/delete (folder): Users can create a new folder in network storage(private cloud storage) within the space provided to the user. New folder cannot be of the same name as the cloud account username. Delete removes the selected folder and the files associated with it from the cloud storage server. And the user can choose to delete the folder. All the contents of folder will be deleted.

Disk usage: Statistics the remaining space available for the respective user.And the total capacity which could be used will be distributed when users registered.

File structure: It displays the folder, subfolder and file present the storage allocated to the user in a tree view.

View: View previews the file in the default application. For ex:-word document is viewed in the Microsoft word,pdf file will be viewed in adobe reader.

Download: Display all files in the user profiles. Download the file specified by the user.

Rename: In computing, rename refers to the altering of a name of a file. It involves the process of copying file to temporary, deleting the original file and renaming temporary file to new filename, but file(folders) name in the same path should be different.

Delete file: File deletion is a way of removing a file from a cloud storage server. Once a file is deleted it is not recovered.

Properties: Properties contain the information about the filename, Date created, Date modified and the size of the file.

Refresh: Refresh displays the updated files in the context menu.

File download: Display all files in the user profiles. Download the file specified by the user.The user GUI is shown below.

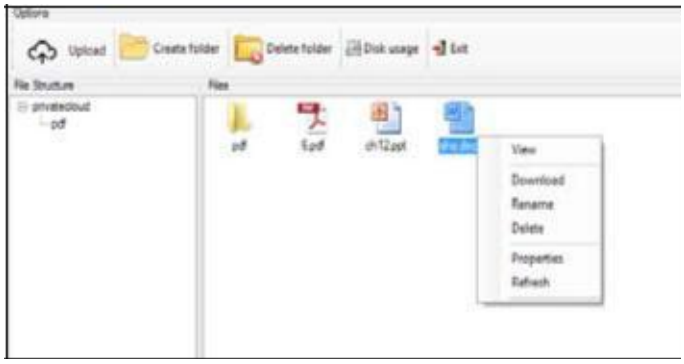

Fig. 4: USER GUI

B. Cloud as A Service

A cloud service is any resource that is provided over the Internet. The most common cloud service resources are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Push notification is very common in now a days for sending messages in departments like finance, banking, telecommunication, online shopping to inform the clients about their latest services. In this project a function has been created using .NET framework which sends an SMS using GSM modem and deployed in the server using Internet Information Service(IIS). The client can access this service from other computer connected over the LAN using the server IP address and service name(For ex: http://192.168.43.76 /Service/Sendsms.asmx). The client can create object for the service type and invoke the function to develop an application which sends SMS. The client who uses this function require just one line effort of invoking the function (For Ex:-Sendsms(string mobile number, string text) without concern about purchasing the GSM modem or logic, complexity in the code.

V. IMPLEMENTATION

Cloud storage system is built on one system (administrator/server) with windows operating system. The client/user application is installed on four different systems with windows operating system. The client and admin application is developed using .net framework using Microsoft visual studio IDE. Table shows the IP address, Role, Installed Software.

Sl.no	IP	Role	Installed software
1.	192.168.43.76	Admin/ server	Microsoft visual studio, IIS, SQL Management studio, SQL server
2.	192.168.43.36	User/ Client 1	Microsoft visual studio, SQL server
3.	192.168.43.18	User/ Client 2	Microsoft visual studio, SQL server
4.	192.168.43.2	User/ Client 3	Microsoft visual studio, SQL server

STEPS:

- User has to register their machine which automatically fetches system username, MACID, mother-board id, and the cloud account name, valid email-id are inputted by the user.
- Admin has to login to get the approval record if any user have sent the request.
- Admin have to approve the user to access the cloud storage.
- If the admin had approve the user a SHA is generated using username, MAC-ID, mother-board id and is stored in database used for validating the user. The password is randomly generated and sent to the user email-id. The folder with cloud account name is created in the network drive.
- User has to check the status. If the user have approved by the admin a auth.dat file is downloaded to the user machine which contains SHA.
- After the user has click login SHA is dynamically generated using username, MAC-ID, mother-board id.
- If the username and password is valid and if the

dynamically generated SHA matches the auth.dat the user is granted to use the service.

- After validating the user network mapping is done to access the network storage in the client side.
- Now the user is redirected to the user space GUI where he can perform file operations.

VI. CONCLUSION

With the rapid development of Internet technology, the data of the users' information have raised up largely. It makes cloud storage render a portable data storage. Public cloud services are very popular, however organizations are still cautious with moving their businesses into the cloud. But the problem in public cloud is our data will be stored in a third party server, they can always view our personal data. Private clouds offer shared infrastructure and services for a single enterprise. Enterprises gain cost advantages and realize greater security and control of resources because the infrastructure resides behind an enterprise's firewall. The user's can store their personal data to the cloud present within that organization. The solution we explored is scalable and is suitable not only for SMBs but also for larger deployments.

REFERENCES

[1] Dropbox: Dropbox Service. Available at: dropbox.com. March 2013

[2] R. Giordanelli, C. Mastroianni, "The cloud computing paradigm: Characteristics, opportunities and research issues," Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR), 2010.

[3] K. Atefi, Y. Saadiah, A. Atefi, "A survey on digital forensics investigation of Seafile as a cloud storage," in International Journal of Engineering Research And Management (IJERM), vol. 01, October 2014.

[4] Google Corporate: Google Products and Solutions. Available at: http://google.com/intl/en/about/products/. Last visited at: March 2013.

[5] J. Mościcki, M. Lamanna, "Prototyping a file sharing and synchronization service with Owncloud," in Journal of Physics: Conference Series, vol. 513, no.4, IOP Publishing, 2014.

[6] Amazon.com Web Services: Products and Services. Available at: http://aws.amazon.com/products. Last visited on: March 2013.

[7] Fang Hao , T. V. Lakshman , Sarit Mukherjee , Haoyu Song, Secure cloud computing with a virtualized network infrastructure, Proceedings of the 2nd USENIX conference on Hot topics in cloud computing, pp.16-16, June 22-25, 2010,

[8] Timothy Wood , Alexandre Gerber , K. K. Ramakrishnan , Prashant Shenoy , Jacobus Van der Merwe, The case for enterprise-ready virtual private clouds, Proceedings of the 2009 conference on Hot topics in cloud computing, June 15, 2009, San Diego, California.

[9] Michael Zink, Kyoungwon Suh, Yu Gu, Jim Kurose, Characteristics of YouTube network traffic at a campus network -Measurements, models, and implications, Computer Networks: The International Journal of Computer and Telecommunications Networking, v.53 n.4, p.501-514, March, 2009. id. The SHA-256 message digest is stored in the database for user authentication. The admin approval form is shown below.

