A FRAMEWORK TO ENSURE SECURED DATA ACCESS IN CLOUD COMPUTING

K.V.Jagannadham[1], J.Ratna Kumar[2]

[1] M.Tech Student, Computer Science Department, BITS College, Andhra Pradesh, India
[2] Head of the departmentt, Computer Science Department, BITS College, Andhra Pradesh, India

ABSTRACT

Cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics and more—over the Internet ("the cloud"). Cloud computing is a next generation technology for IT companies. It has different characteristics like On-demand self-service, Rapid elasticity, Resource pooling, and many more. It also provides on demand computational infrastructure which has the power to reduce the cost to build the IT based services. It provides various types of services over the internet. Some of the services provided by the cloud are Infrastructure-as-a-service (IaaS), Software as a service (SaaS) etc. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems from a cloud provider on a pay-as-you-go basis, where users can keep their data as per the requirement. So, it is a challenging issue for the user, as all the data are stored in some inter-connected resource pool but this resource pool are situated over different places of the world. An unauthorized users may be accessed this data through virtual machines. So, it is a very dark side of cloud data storage, this insecurity creates a big problem for users. Therefore cloud computing data security & accessing is a major problem. In order to solve the data security in cloud computing, we have proposed a new framework and an Encryption Schemes which will generate each user a unique access code basing on some parameters and allow them retrieve the data efficiently. The performance evaluation and validation of the proposed model is carried out and the result of performance analysis shown that our architecture are feasible, scalable and efficient.

Keyword: - *Cloud Computing, Infrastructure as a Service (IaaS), Secured Data Access*

1. INTRODUCTION TO CLOUD COMPUTING

The official definition of cloud computing is provided by the National Institute of Standards and Technology's (NIST) in their Special Publication 800-145 "The NIST Definition of Cloud Computing".[2]

NIST Definition of Cloud Computing

NIST has defined cloud computing as, "…. a model for enabling ubiquitous, 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."

The NIST definition of cloud computing has been shown in Figure-1.

Though there are several types of services are providing the cloud but Data store is one of the latest features which is providing by the cloud to the client companies or any other users. But due to the lack of proper security control policy and weakness in protection, many client are not ready to implement cloud computing technology. The superior of cloud computing providers are Microsoft Azure, Amazon Web Services (AWS), Amazon Simple Storage services (S3) and Amazon Elastic Compute Cloud (EC2) etc.[7].

So, securing client data is a very important criteria for good quality of services and cloud computing faces the challenge of security threats for number of reasons. Firstly adopting the traditional cryptographic approach for the aim of data security in cloud computing is a threat as the data are stored in remote location and users do not have any control on it. So, it requires a data verification approach and it has no explicit knowledge about the whole data.

So, it is very tough to verify the actual data. It is very difficult to verify the correctness of data storage in the cloud as it is located in third party's location. Secondly, the data are stored in third-party data warehouse and the data may be frequently updated by the user, including modification, deletion, insertion, recovering and other operation.

So, we need a more dynamic advanced technology operation to prevent data loss from the cloud storage. Lastly, but it is not the last as data centers which are running in simultaneously in distributed manner[1] and all data are stored in different physical locations, so it is very important to give correctness assurance in the distributed protocols. The following aspects are summarized as our contributions on: Firstly, an encryption schemes based framework is proposed and these schemes can hide the plaintext in cipher text which can store to the cloud. It is generating a secret key of small size which is suitable for data centric application. These should protect an unauthorized user to access data from cloud storage. These schemes incorporate storing data and retrieve data efficiently.

Rest of the paper is organized as follows: The architecture of cloud computing and its services are discussed in Section 2. We propose our system architecture, notations, and design and security model in section 3. We conclude our remarks on our proposed model and its future scope in Section 4.

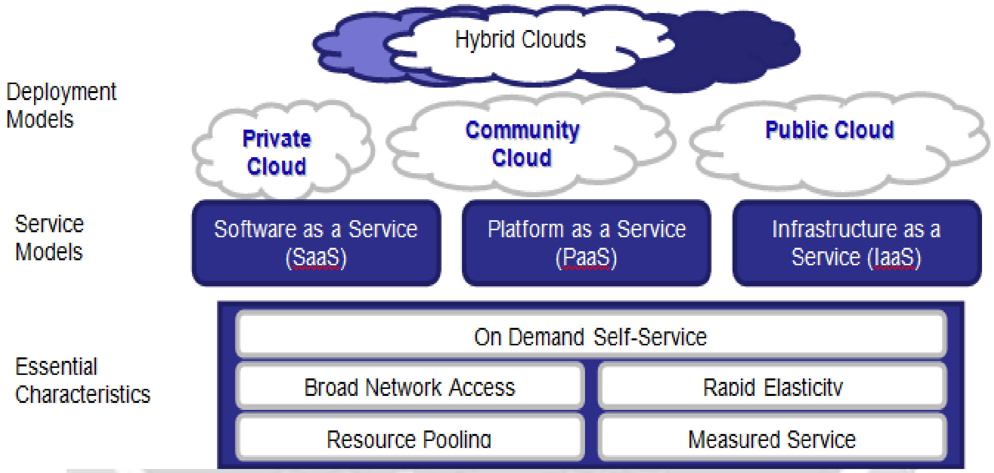

Figure 1: The NIST Cloud Definition Framework

2. CLOUD ARCHITECTURE, CHARACTERISTICS AND BENEFITS

2.1 Five essential characteristics of cloud computing

The essential characteristics of cloud computing are elaborated as follows:

a. On-demand self-service: Users are able to provision cloud computing resources without requiring human interaction, mostly done though a web-based self-service portal.
b. Broad network access: Cloud computing resources are accessible over the network, supporting heterogeneous client platforms (e.g., mobile phones, tablets, laptops, and workstations).
c. Resource pooling: Service multiple customers from the same physical resources, by securely separating the resources on logical level. Examples of resources include storage, processing, memory, and network bandwidth.
d. Rapid elasticity: Resources are provisioned and released on-demand and/or automated based on parameters. This will make sure your application will have exactly the capacity it needs at any point of time.
e. Measured service: Resource usage are monitored, measured, and reported (billed) transparently based on utilization. In short, pay for use.

2.2 Deployment Models

There are four separate types of clouds, according to the NIST. They are:

1. Public clouds – accessible by any user
2. Private clouds – clouds accessible only to a single organization or company
3. Community clouds, which are a subset group of users with needs and concerns in common
4. Hybrid clouds, which are combinations of the previous three types.

2.3 Benefits of cloud computing

Here are six common reasons organizations are turning to cloud computing services:

1. Cost
2. Speed
3. Global scale
4. Productivity
5. Performance
6. Reliability

3. SCHEMATIC SYSTEM ARCHITECTURE FOR PROPOSED MODEL

In general, most of the Cloud Service Providers (CSPs) are giving access to their cloud services basing on either email id or phone number, which can be prone to security attacks. So here in this paper we are proposing a new method for accessing the cloud services provided by the CSPs.

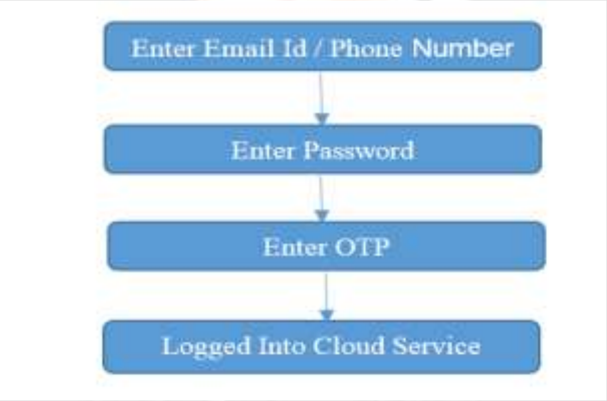

Figure 2: Existing 2-factor Authentication System for Cloud Login

We are generating a new access code for each user basing on some parameters like user's first name, last name, date of birth, personal message, email address etc. For this we use cipher text based algorithm for generating unique access code. Existing and new proposed systems are shown in Figure-2 & Figure-3.

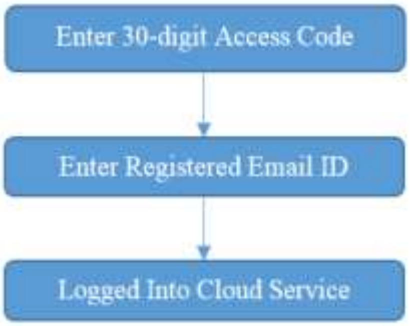
Enter 30-digit Access Code
Enter Registered Email ID
Logged Into Cloud Service

Figure 3: Proposed System for Cloud Login

3.1: Steps for generating unique access code

1. Take user input.
2. ***GenerateAccessCode:*** This method generates unique access code taking the user given input. Check for the uniqueness of the generated code with already generated codes and store this unique Access code in the database.

3.2: Algorithm for GenerateAccessCode:

1. Take each input separately and make them blocks.
2. Form the inputs into single string with a delimiter.
3. Separate into blocks of characters.
4. Read characters byte by byte.
5. Shift bits and add them to a variable.
6. Repeat the same for other blocks.
7. Append the blocks to get the required 30 characters.
8. Check the value we got by XOR hashing and modify the same if required.

Our new proposed system uses the access code generated by taking the user given input and sent the same to the user by email. In the new login process, user first give the user given access code, and then user has to give registered email address given at the time of generating unique access code. We will authenticate the user basing on user given access code & registered email address, then only we will proceed further into the cloud services provided by the Cloud Service Provider (CSP).

4. CONCLUSIONS

In this paper we have proposed a new framework for authenticating the user, based on unique access code that is generated with our encryption algorithm and registered email address. To ensure the security of the client data at cloud space, we proposed an effective and efficient encryption strategy for enhancing user access methodology.

This area needs lots of research and testing before adopting to this system from existing system. Our scope in this paper is limited to the new proposal only, and this needs to be validated further.

In the future, we will like to extend our model by considering some more attributes like expiration date for access code and extend our logic for generating a more robust access code and avoid the communication delay for getting One Time Password (OTP).

5. ACKNOWLEDGEMENT

I would like to acknowledge my family members, who are always supporting me in my endeavors. I would also like to thank Mr. K.S.R. Murthy, P.G. Coordinator, BITS College and my friend and colleague Mr. Ajay Kumar Lebaka for providing their valuable inputs.

6. REFERENCES

[1]. *NIST Cloud Computing Reference Architecture Special Publication 500-292* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
[2]. Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, Jan, 2011, http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf.
[3]. Microsoft Azure Documentation, online at https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/
[4]. IBM Cloud Documentation, link at https://www.ibm.com/blogs/cloud-computing/2014/01/cloud-computing-defined-characteristics-service-levels/
[5]. NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[6]. A paper by Mrinal Kanti Sarkar & Sanjay Kumar on "A Framework to Ensure Data Storage Security in Cloud Computing"

[7]. Amazon.com, “Amazon Web Services (AWS)”, Online at https://aws.amazon.com, 2008.
[8]. Likhwa MLOTSHWA, Awie LEONARD, FelixNTAWANGA “A Conceptual Framework for Cloud-Computing Management: An End-user Environment Perspective” ISBN: 978-1-905824-51-9
[9]. Naziya Khan, Mrs. Asha Khilrani paper on "A Study of Security Requirements in Cloud Computing Environment", IJARCCE Vol. 5, Issue 6, June 2016 pages 254-257

BIOGRAPHIES

	Mr. K.V. Jagannadham, B.E., M.B.A, is a M.Tech student of BITS College, VIZAG. He has graduated from Andhra Univeristy College of Engineering in Mechanical, also did his MBA from Andhra University and currently pursuing in P.G. in Computer Science and Technology.
	Mr. Jala Ratnakumar, B.Tech,M.Tech,(M.Th),(MBA),(Ph.D), is currently working in BITS College, VIZAG as Associate Professor and Head Of Dept. of Computer Science & Engineering. He has a vast experience of 13 years in this field. Currently he is pursuing his Ph.D.