iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Robust But Flexible Privacy Preserving Scheme Supporting Cloud Environments

Saima Majeed[1], Er. Bandana Sharma[2]
[1]*M. Tech 4th Semester. Department of Computer Science, Haryana Engineering College. Jagadhri, Kurukshetra University, Haryana, India.*
[2]*Assistant Professor, Department Of Computer Science, Haryana Engineering College, Jagadhri, Kurukshetra University, Haryana, India.*

Abstract: ***Fog is the Ruby cloud services library. The fog binary allows quick and easy access to configured cloud services. Whether you need compute, storage, or a multitude of other services, fog provides an accessible entry point and facilitates cross service compatibility. Fog allows you to setup a credential file to use rather than having to re-enter credentials (by default fog –C .fog). Fog has a Compute services that can connect to many different providers and operate similarly and provide on-demand service allowing to add and remove resources as needed.***
Keywords - Key-Policy Weighted Attribute based Encryption (KP-WABE), Virtual Machines (VMs), Mobile Cloud Computing (MCC), Attribute-based encryption (ABE), cipher text-policy attributed based encryption (CP-ABE)

I. INTRODUCTION

Cloud computing is growing in popularity and analysts predict its further diffusion, but security and privacy concerns might slow down its adoption and success. Clouds are inherently more vulnerable to attacks given their size and management complexity. As a consequence, increased protection of such systems is a challenging task. It becomes crucial to know the possible threats and to establish security processes to protect services and hosting platforms from attacks. Virtualization is already leveraged in clouds. It allows better use of resources via server consolidation and better load balancing via migration of virtual machines (VMs). Virtualization can also be used as a security component e.g. to provide monitoring of VMs, allowing easier security management of complex cluster, server farms and cloud computing infrastructure. However, it can also create new potential concerns with respect to security. Based on KvmSec a security extension to the Linux Kernel Virtual Machine, we present TCPS, a protection system for clouds aimed at transparently monitoring the integrity of cloud components [1].

A. Encryption Techniques in Cloud Computing

Cloud computing is becoming ubiquitous as it offers fast and efficient on-demand services for storage, network, hardware, and software through the internet. Cloud computing offers new facilities to enterprises, companies, and the general public, and provides low cost computing infrastructure for IT-based solutions. Cloud computing is not new; organizations such as universities, research laboratories, and the military in developed countries have long used networks for communication, but the term cloud is more recent. Cloud computing is being increasingly offered on the web as web technology has become faster and more complex. It is now used by a large number of users to store sensitive data on third party servers, either for cost saving or for simplicity of sharing. Cloud computing is now considered the fifth utility after gas, water, electricity, and telephony. There are a range of service-oriented cloud computing service models, including Infrastructure (e.g., Amazon's EC2, Amazon S3, IBM Blue cloud), Platform (e.g., Yahoo Pig, Google App Engine), and Software (e.g., saleforce.com, Gmail, Microsoft online) as a service [2]. Users have no need to hire IT professionals or to invest in their own software/hardware systems. Applications that run in the cloud can balance several factors including size of data, load balancing, bandwidth, and security. One of the major barriers to cloud adoption is data security and privacy, because the data owner and the service provider are not within the same trusted domain. Security issues are increasingly significant in lower layer Infrastructure as a Service (IaaS) to higher Platform as a Service (PaaS). These cloud layers are in deployed models (public, private, community, and hybrid) in high end Mobile Cloud Computing (MCC). Users hesitate to move into the cloud because certain loopholes in its architecture make cloud computing insecure. On-demand applications available in the cloud have increased; cybercrime has also increased to launch passive and active attacks. A range of different techniques or security algorithms are used to maintain the security and privacy of the cloud. These include encryption, limited service access, stringent access, and data backup and recovery to make data retrieval easy. To ensure the confidentiality and privacy of data from a cloud

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

service provider, a key source is an encryption technique that provides sufficiently robust security as illustrated in Figure 1.1 [1]. Attribute-based encryption (ABE) is a cryptographic technique which is very suitable for data access control in cloud computing, which simultaneously achieves data confidentiality and fine-grained data access control. In an ABE scheme, the access control policy is defined over various attributes [3].

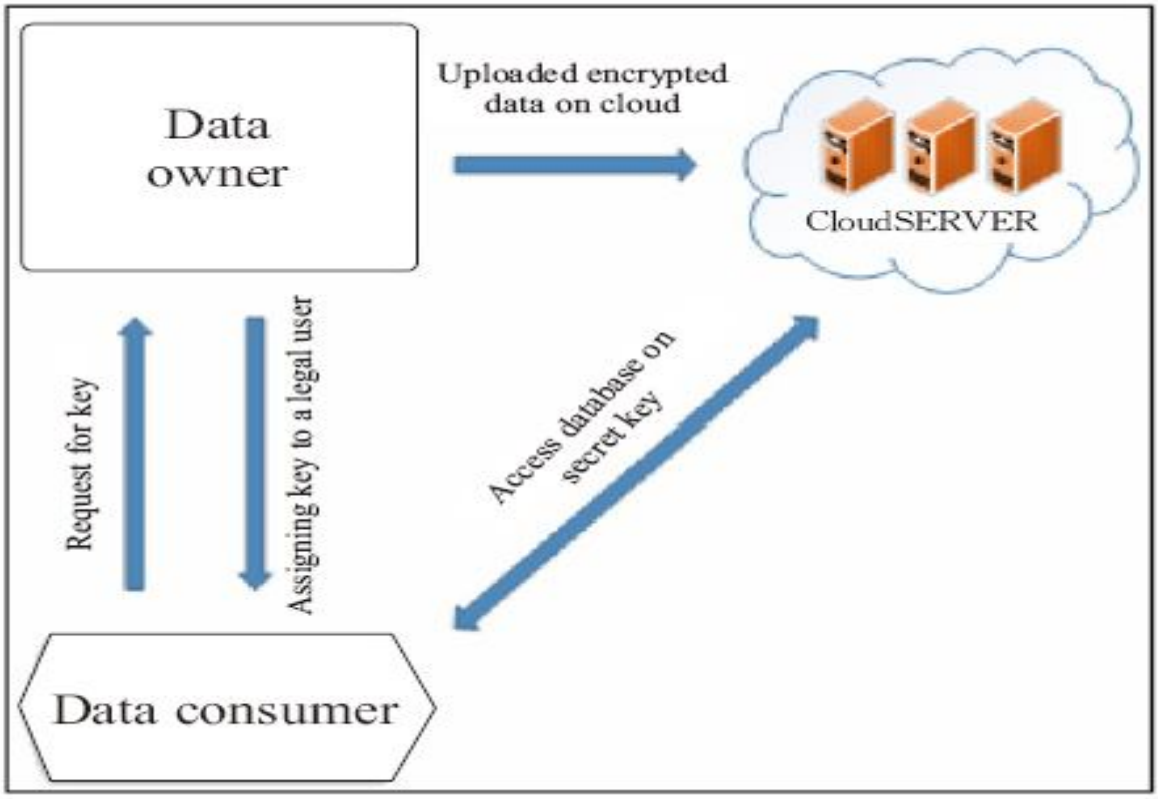


Figure 1.1 Secure data access in cloud. [1]

II. RELATED WORK

A. Muhammad Yasir Shabir et al., (2016) [1]

Cloud computing has become a significant computing model in the IT industry. In this emerging model, computing resources such as software, hardware, networking, and storage can be accessed anywhere in the world on a pay-per-use basis. However, storing sensitive data on un-trusted servers is a challenging issue for this model. To guarantee confidentiality and proper access control of outsourced sensitive data, classical encryption techniques are used. However, such access control schemes are not feasible in cloud computing because of their lack of flexibility, scalability, and fine-grained access control. Instead, Attribute-Based Encryption (ABE) techniques are used in the cloud. This paper extensively surveys all ABE schemes and creates a comparison table for the key criteria for these schemes in cloud applications.

B. Sadikin Rifki et al., (2015) [2]

A new fully secure cipher text-policy attributed based encryption (CP-ABE) scheme with high expressibility access policy is presented. Authors CP-ABE scheme uses tree-based access structure which includes AND, OR, threshold and NOT gates which granted high degree of expressibility for encrypt or to make an access policy. Moreover, author's scheme achieves full security CP-ABE definition where any access structure can be chosen as the challenge cipher text. The proposed CP-ABE uses composite bilinear groups and dual encryption paradigm to achieve full security CP-ABE definition. Authors argue that our CP-ABE scheme is secure and feasible.

C. Balamurugan B and Venkata Krishna P, (2014) [3]

Cloud computing has risen in the last decade to be the most aspired technology by the IT Industry. Cloud computing initially started

©IJRASET: All Rights are Reserved

as a technology for data outsourcing, later developed in to a newer computing platform for all IT related activities .The advent of cloud computing to deploy mission critical application has raised the value of cloud. On the contrary, cloud security is encountering infinite treats and vulnerabilities from several fronts. Security features like access control, digital signature, encryption and decryption are forced inside cloud environment to secure the cloud data. The paper surveys extensively all the varieties of the Attribute Based Encryption (ABE) access control techniques available to be used for cloud environments. Observations are made about the use of ABE and the ways access privileges are provided. The different ABE techniques are compared analyzed and recommendation for it to be used in deploying different cloud applications are mentioned.

D.A.Vijayalakshmi and R. Arunapriya, (2014) [4]

in this paper, authors proposed the secure data storage in clouds for a new decentralized access. The cloud verifies the authenticity of the series without knowing the user's identity in the proposed scheme. Authors feature is that only valid users can able to decrypt the stored information. It prevents from the replay attack. This scheme supports creation, modification, and reading the data stored in the cloud and also provide the decentralized authentication and robust. It can be comparable to centralized schemes for the communication of data, computation of data, and storage of data.

E. Ximeng Liu, Hui Zhu et al., (2014) [5]

When we step into the new internet era, large numbers of new techniques have emerged in order to make our life better. However, these new techniques require some new properties in order to keep personal information confidentially which the traditional encryption method cannot catch up with. Recently, a new encryption primitive called Attribute Based Encryption (ABE) have appeared because it can achieve both information security and fine-grained access control. Although the ABE scheme has these new characters which can keep the information security that can fit for the new widely used technique, nevertheless, the characteristic of attributes are treated in the identical level in most of traditional schemes. In the real scenario, the importance of each attributes is always different. In this paper, authors propose a scheme called Key-Policy Weighted Attribute based Encryption (KP-WABE) while the attributes have different weights according to their importance in the system. The KP-WABE scheme is proved to be secure under the *l*-th Bilinear Diffie-Hellman Inversion Assumption. Author's scheme can be considered as the generalization of traditional KP-ABE scheme when all attributes have equal weights.

F. Cong Wang et al., (2013) [6]

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services 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 integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, authors propose a secure cloud storage system supporting privacy-preserving public auditing. Authors further extend their result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

G.Cong Wang et al., (2012) [7]

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, authors propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the holomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

III. PROPOSED WORK

We propose a better type of encryption where the authentication mechanisms of different users can be associated with different access structures. We have developed granule access control systems that can facilitate granting disparity based access rights to a set of users and permits flexibility in specifying the access rights of individual users. The data will be stored on the servers in an encrypted form while different users with which the information is shared can be allowed to decrypt data sections based upon their identity. This process will effectively get rid of the need to depend on the storage server for preventing unauthorized data access.

IV. RESULTS & ANALYSIS

```
  Welcome to fog interactive!
  :default provides Aliyun, BareMetalCloud, Bluebox, Brightbox, Clodo, Cloudstac
k, DNSMadeEasy, Dnsimple, Dreamhost, GoGrid, IBM, Linode, Local, Openvz, Ovirt,
RiakCS, VcloudDirector, Vmfusion, Voxel, Vsphere and Zerigo
>>
```

Figure 4.1 Starting Fog Interactive

$ fog –C .fog

```
# Fog Credentials File
#
# Key-value pairs should look like:
# :aws_access_key_id:                 022QF06E7MXBSAMPLE
:default:
  :aws_access_key_id:           AKIAJ3CTYYNH6GIEARLA
  :aws_secret_access_key:       oevSCT59/p1Hnht1fW/
```

Figure 4.2 Fog Credentials File

```
>> server = Compute[:aws]
#<Fog::Compute::AWS::Real:-582155598 @connection_options={:debug_response=>true,
 :headers=>{"User-Agent"=>"fog/1.40.0 fog-core/1.44.3"}, :persistent=>false} @re
gion="us-east-1" @instrumentor=nil @instrumentor_name="fog.aws.compute" @version
="2016-11-15" @use_iam_profile=nil @aws_access_key_id="AKIAJ3CTYYNH6GIEARLA" @aw
s_credentials_expire_at=nil @signer=#<Fog::AWS::SignatureV4:0xba97aa1c @region="
us-east-1", @service="ec2", @aws_access_key_id="AKIAJ3CTYYNH6GIEARLA", @hmac=#<F
og::HMAC:0xba97a9cc @key="AWS4oevSCT59/p1Hnht1fW/Ks3zLN8MmYrTVLI4j86Uj", @digest
=#<OpenSSL::Digest: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852
b855>, @signer=#<Proc:0xba97a968@/usr/local/lib/ruby/gems/2.1.0/gems/fog-core-1.
44.3/lib/fog/core/hmac.rb:28 (lambda)>>> @endpoint=nil @host="ec2.us-east-1.amaz
onaws.com" @path="/" @persistent=false @port=443 @scheme="https" @connection=#<F
og::XML::Connection:0xba97a760 @excon=#<Excon::Connection:-45685bc0 @data={:chun
k_size=>1048576, :ciphers=>"ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POL
Y1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES2
56-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES2
56-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES1
28-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:EC
DHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-S
HA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-D
ES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA2
56:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS", :connect_timeout=>60,
```

Figure 4.3 Computing Encryption Details of Cloud Service

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

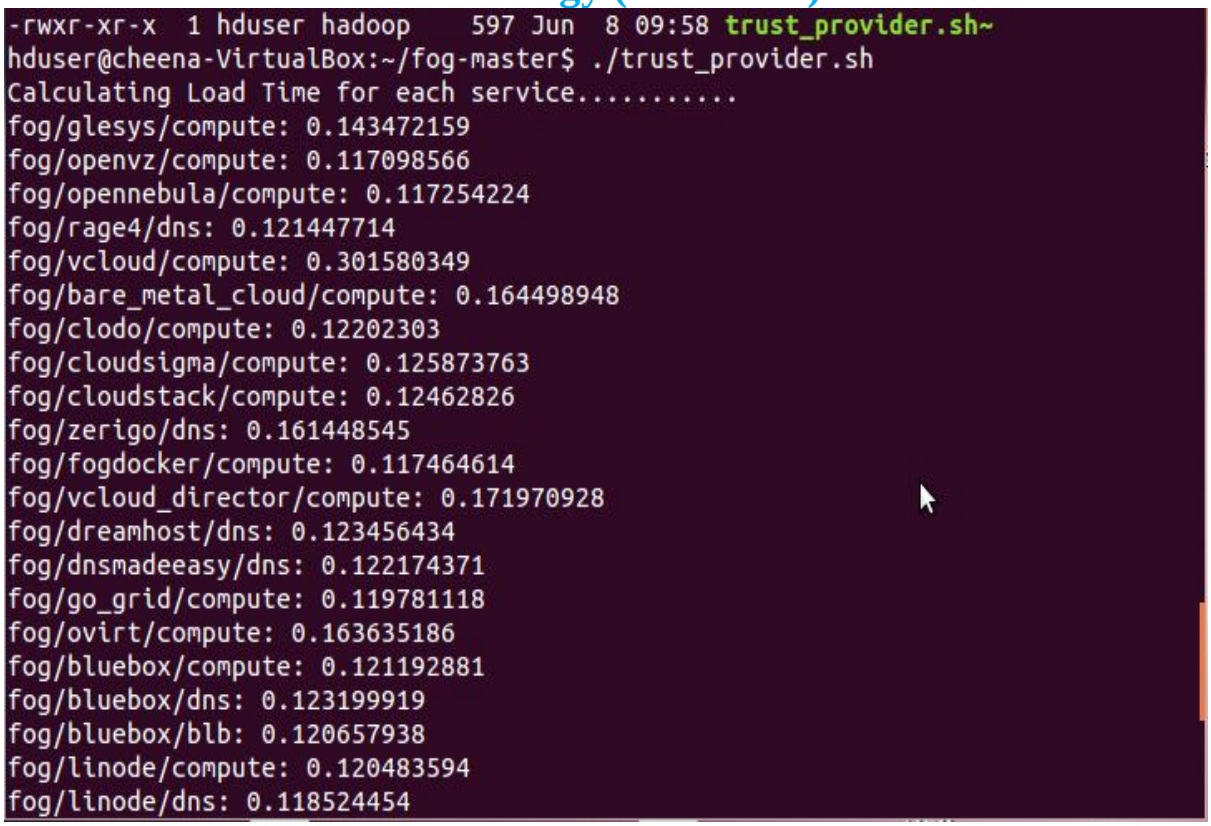


Figure 4.4 Computing Load Time for each Cloud Service

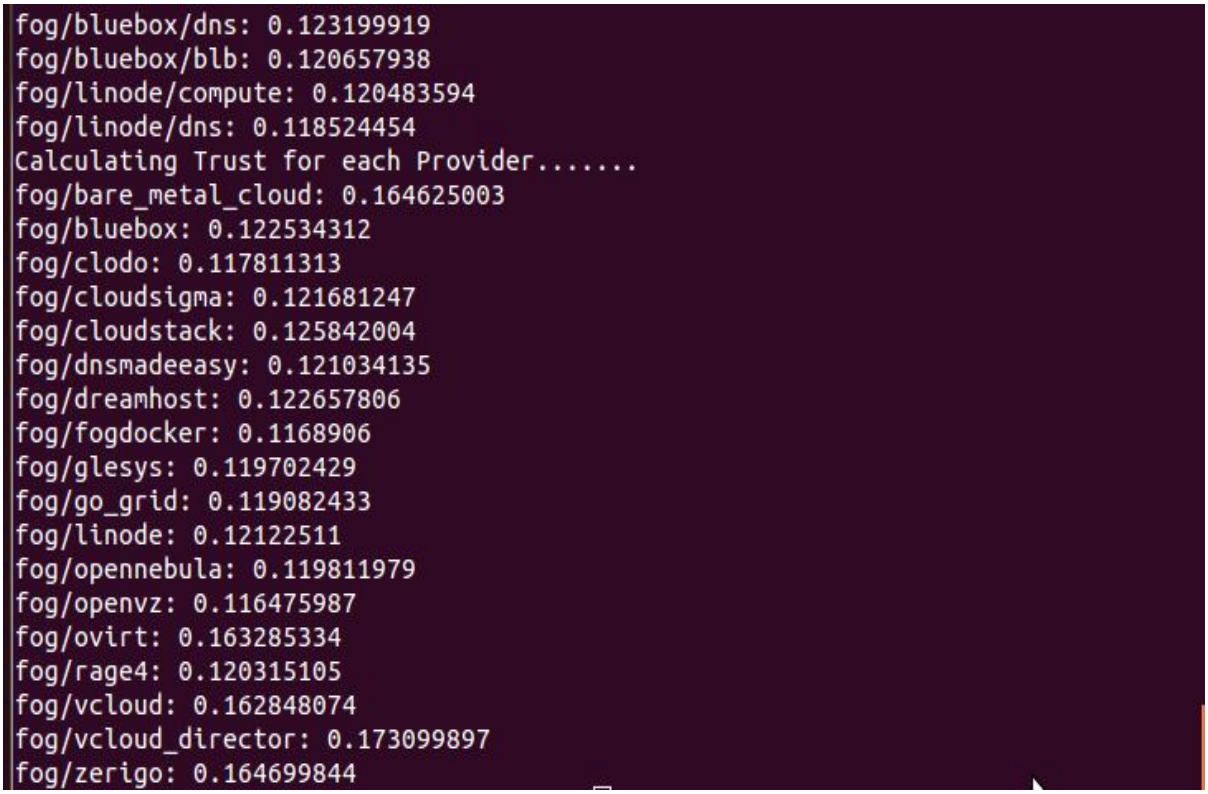


Figure 4.5 Computing Trust for each Cloud Provider

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Table 4.1 Trust for each Cloud Provider

Cloud Service	Trust Value
Bare-Metal-Cloud	0.164625
Blue-Box	0.122534
Cloud Sigma	0.121681
Ovirt	0.163285
Vcloud-Director	0.173099

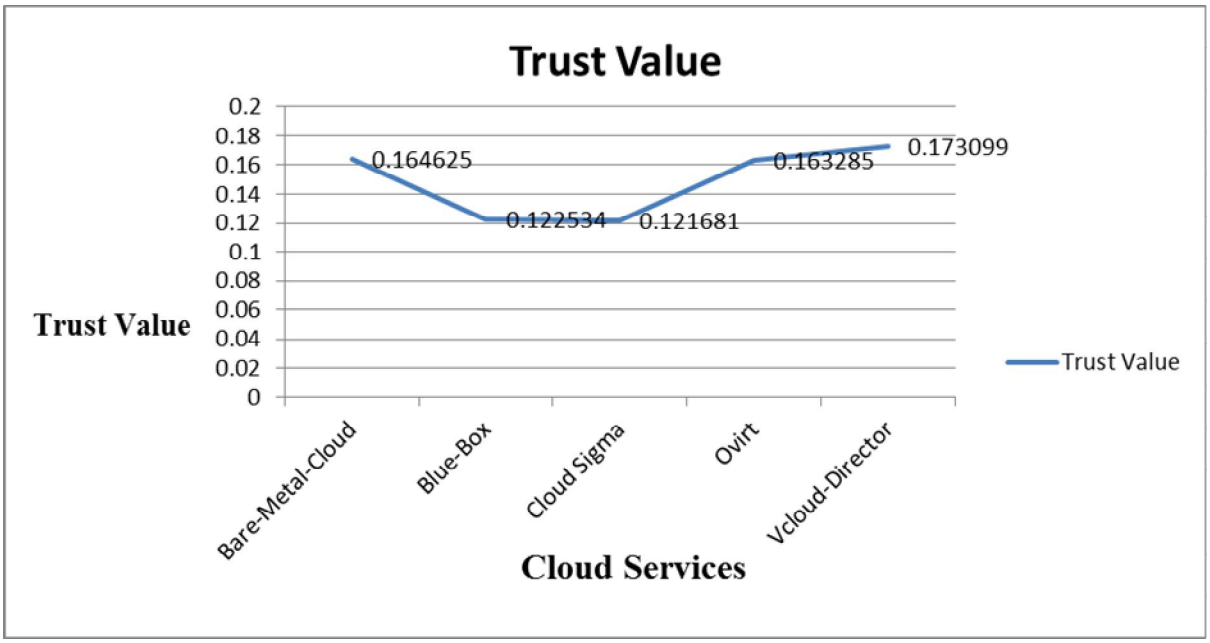


Figure 4.6 Trust values of Cloud Services

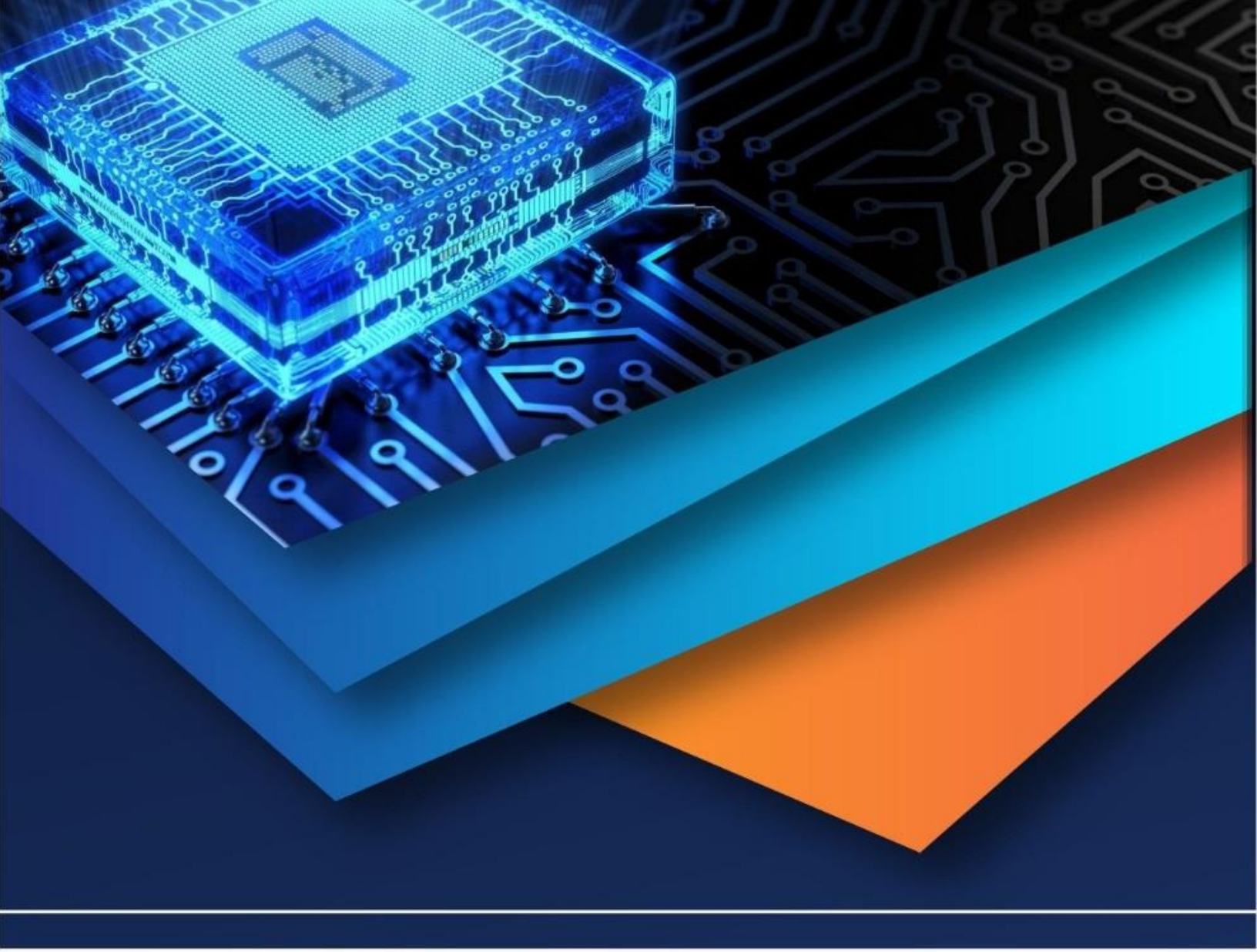
V. CONCLUSION & FUTURE SCOPE

Rather than signing up for accounts, worrying about internet connections, etc; time can be saved by using the mocks. Mocks provide us with an in-memory simulation of the service great for experimentation and testing. So the first thing is instruct fog to run all subsequent requests in Mock mode. fog uses Excon (a pure-Ruby HTTP library built for speed) for requests, so mocks create fake Excon responses to emulate the Real behavior. Experimented with several providers and services and it is a good foundation for working with cloud services.

REFERENCES

[1] Muhammad yasir shabir, asif iqbal, zahid mahmood and ataullah ghafoor, “analysis of classical encryption techniques in cloud computing”, tsinghua science and technology issnll1007-0214ll09/10llpp102-113 volume 21, number 1, february 2016.
[2] Sadikin rifki, youngho park and sangjae moon, “afully secure ciphertext-policy attribute-based encryption with a tree-based access structure”, journal of information science and engineering, 201
[3] Balamurugan b and venkata krishna p, “extensive survey on usage of attribute based encryption in cloud”, journal of emerging technologies in web intelligence, vol. 6, no. 3, august 201
[4] A.vijayalakshmi and r.arunapriya, “authentication of data storage using decentralized access control in clouds”, volume 5, no. 9, september 201
[5] Ximeng liu, hui zhu, jianfeng ma, jun ma and siqi ma, “key-policy weighted attribute based encryption for fine-grained access control”, icc'14 - w5: workshop on secure networking and forensic computing
[6] Cong wang, sherman s. -m. Chow, qian wang, kui ren, wenjing lou, “privacy-preserving public auditing for secure cloud storage” , ieee transactions on computers vol:62 no:2 year 2013
[7] Cong wang, qian wang, kui ren, ning cao, wenjing lou, “towards secure and dependable storage services in cloud computing”, ieee transactions on cloud computing volume: 5 , issue: 2, 2012

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)