iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Securing Cloud Database Architecture While Migrating from one Cloud to another along with Data using AES

Adesh Patel[1],Sumit Kumar Yadav[2]
[1,2]*Lords Institute of Engg.& Technology Hyderabad(A.P.)*

Abstract:*Later engage in Cloud Computing has been determined by new offerings of Registering assets that are engaging because of for every use valuing and versatileadaptability, giving a critical playing point over the commonplace procurement andarrangement of gear that was a while ago needed. Cloud Computing is a new computing model that distributes the computing missions on a resource pool that includes a large amount of computing resources. More and more companies begin to provide different kinds of cloud computing services for Internet users at the same time these services also bring some security problems. Today most cloud computing system use cryptography techniques to provide data security and mutual authentication. This research paper helps in securing the data without affecting the original data and protecting the data. The vital data ineach level can be encrypted by using encryption/decryptionalgorithm and keys before store them in the Cloud. In thistechnique the aim is to store data in a secure and safe way inorder to avoid intrusions and attacks. Also, it will reduce the costand time to store the encrypted data in the Cloud Computing.The paper conducts a performance analysis by implementing theAdvanced Encryption Standard (AES) in all levels in order tocheck the performance of model.*
Keyword:*Cloud Computing, Migration, Architecture, Protocol, Cryptography.*

I. INTRODUCTION

Cloud computing is the developing standard with changing definitions yet for thisexploration venture, it is characterized in the term of a virtual framework which might begives imparted data and correspondence innovation administrations, by means of a web"cloud," for "various outer clients" through utilization of the Internet or "huge scale privatesystems." Cloud computing furnishes a machine client access to Information Technology (IT)benefits i.e., requisitions, servers, information space, without obliging a comprehension ofthe engineering or even responsibility for foundation. To fathom Cloud computing, arelationship to a power computing network is to be handy. A force organization keeps upand possesses the framework, a circulation organization disperses the power, and thepurchaser just uses the assets without the possession or operational obligations. Cloudcomputing is getting an incredible arrangement of consideration, both in productions andaround clients, from people at home to the U.S. government. Cloud computing is amembership based administration where you can acquire arranged space and machineassets. One approach to consider Cloud computing is to think about your experience withemail. Your email customer, in the event that it is live, Gmail msn, et cetera, deals withlodging the sum of the equipment and programming important to backing your particularemail account. When you have to get access to your email you open your web project, takeoff to the email client, and log in. The most discriminating some bit of the numericalproclamation is having web access. Your email is not housed on your physical machine; yougain access to it through a web association, and you can gain access to it anyplace. Assumingthat you are on a trek, at work, or down the road getting espresso, you can check your emailas long as you have admittance to the web. Your email is unique in relation to programmingintroduced on your workstation, for example, an expression handling system. When youmake an archive utilizing word handling programming, that record stays on the mechanismyou used to make it unless you physically move it. An email customer is like how cloudcomputing functions. But as opposed to entering simply your email, you can pick what datayou have admittance to inside the cloud. Essentially, a client's cloud computing accessempowers "imparted assets, programming, and data on-interest" on an expense foradministrationpremise.
According to the National Institute of Standards and Technology (NIST), cloud computingshows several characteristics:

A. Agility improves with users' ability to re-provision technological infrastructure resources.
B. Application programming interface (API) accessibility to software that enablesmachines to interact with cloud software in the

same way the user interface facilitates interaction between humans and computers. Cloud computing systems typically use REST-based APIs.

C. Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barrier to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

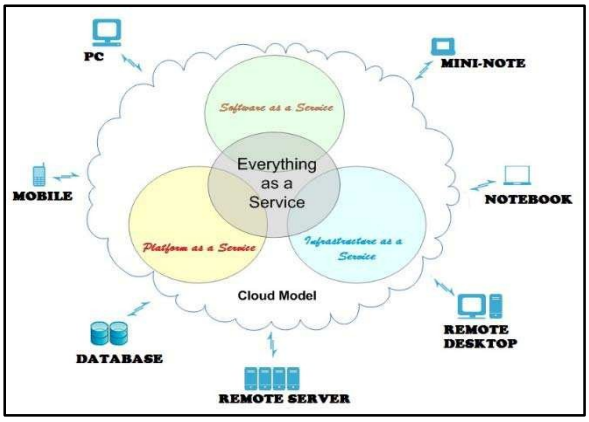


Figure1: Cloud Computing Model

D. Device and location independence enable users to access systems using a webbrowser regardless of their location or what device they are using (e.g., PC, mobilephone). As infrastructure is off-site typically provided by a third-party and accessedvia the Internet, users can connect from anywhere.

E. Virtualization technology allows servers and storage devices to be shared andutilization be increased. Applications can be easily migrated from one physical serverto another.

II. ARCHITECTURAL STRATEGIES FOR CLOUD COMPUTING:

Cloud computing represents a distributing computing mechanism that by the utilize of the high speed network, data processing is moved from private PC or servers to the remote computer clusters (big data centers owned by the cloud service providers), any user has a potential super computer at hand and can access the data and get the computing capability at any time, from anywhere, you only need to pay for the resources which you have used, don't care about who provide the resources and in what way.A cloud computing system consists of a collection of interconnected and virtualized computers dynamically provisioned as one or more unified computing resource(s) through negotiation of service-level agreements (SLAs) between providers and consumers. In cloud computing platforms, resources need to be dynamically re-configured and aggregated via virtualization and consumers' requirements can potentially vary over time and amendments need to be accommodated.

The cloud computing model revolves around three functional units or components as listed below:

A. Cloud Service Provider

It is an entity, which manages Cloud Storage Server (CSS), has significant storage space to preserve the clients' data and high computation power.

B. Client/Owner

It is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; it can either be individual consumer or organizations.

C. User

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

It is a unit, which is registered with the owner and uses the data of owner stored on the cloud. The user can be an owner itself as well.

Figure2: Cloud Architecture

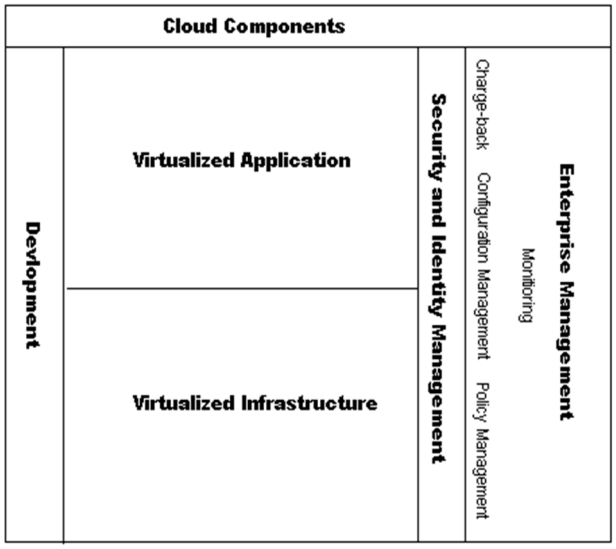


Figure3: Cloud Building Blocks

III. CLOUD SECURITY

Cloud computing have many advantages in cost reduction, resource sharing, time saving for new service deployment. While in a cloud computing system, most data and software that users use reside on the Internet, which bring some new challenges for the system, especially security and privacy. Since each application may use resource from multiple servers. The servers are potentially based at multiple locations and the services provided by the cloud may use different infrastructures across organizations. All these characteristics of cloud computing make it complicated to provide security in cloud computing. To ensure adequate security in cloud computing, various security issues, such as authentication, data confidentiality and integrity, and non-repudiation, all need to be

taken into account. Currently, WS-Security service is wildly used in the cloud to provide security for the system. In WS-Security, XML encryption and XML signature are used to provide data confidentiality and integrity. Mutual authentication can be supported by adding X.509 certificate and Kerberos tickets into SOAP message header. As mentioned earlier, there are three types of clouds in general: private cloud, public cloud and hybrid cloud. In a public cloud, resources are dynamically provisioned on a fine-grained, self-service basis over the Internet. Services in the cloud are provided by an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. While in most private clouds, with limited computing resources, it is difficult for a private cloud to provide all services for their users, as some services may more resources than internal cloud can provide. Hybrid cloud is a potential solution for this issue since they can get the computing resources from external cloud computing providers. Private clouds have their advantages in corporation governance and offer reliable services, as well as they allow more control than public clouds do. For the security concerns, when a cloud environment is created inside a firewall, it can provide its users with less exposure to Internet security risks. Also in the private cloud, all the services can be accessed through internal connections rather than public Internet connections, which make it easier to use existing security measures and standards. This can make private clouds more appropriate for services with sensitive data that must be protected.

IV. ALGORITHM

```
int counter =0;
int k=1;//for the fields specified by user ;
if(model. Is Selected ) // If the client has selected the specific model for his entry
{for (int i=0;i<counterfield;i++)
{if(counterfield.checked==true
{ Rbac rbc=new rbac();
rbc.roles.add(counterfield.text);
if(user.confirms.rbc.roles.added==true)
{put (xml.schema.action);
}
}
Else
{Move.next();
}
For(int i=0;i<fieldcount;i++)
{for(k!=null)
Draw(xmlschema.xml.rbc()) ;
Xmlschema.rbc.fieldcount=fieldcount ;
Xmlschema.xmltag=new xmltag("<"+fieldname+">");
Xmlschema.xmltag=new xmltag("<"+fieldname+"/>");
Xmlschema.show();
Put.Azure(spcefilled.rest.databaseschema);
Exit
Count++;
}
}
Else
{
This .close();
Goto whileback; // to return to main program
}
}
```

V. PROBLEM STATEMENT

The security of data of the user is prime responsibility of cloud provider. So, for efficient data security we need a mechanism that provides secure data encryption as well as secure shield against data theft. The related works mentioned above have focused on cloud security issues. They have provided different mechanisms for data security in cloud environment. Different researches have focused on the fact that user generally has to access large volumes of data from

the cloud in a secured manner. But the complexity of the cryptographic algorithm used, hasn't been given much importance. The complexity of the algorithm directly affects the speed of data access. We need some algorithm that will help in efficient and speedy secured data access.

VI. ADVANCE ENCRYPTION STANDARD

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. Keys play an important role. If weak key is used in algorithm then everyone may decrypt the data. Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. There are many examples of strong and weak keys of cryptography algorithms like DES, 3DES, and AES. If security were the only consideration, then 3DES would be an appropriate choice for a standardized encryption algorithm for decades to come. The principal drawback of 3DES is that the algorithm is relatively sluggish in software. 3DES has two attractions that assure its widespread use over the next few years. First, with its 168-bit key length, it overcomes the vulnerability to brute-force attack of DEA. Second, the underlying encryption algorithm in 3DES is the same as in DEA. This algorithm has been subjected to more scrutiny than any other encryption algorithm over a longer period of time, and no effective cryptanalytic attack based on the algorithm rather than brute force has been found. Accordingly, there is a high level of confidence that 3DES is very resistant to cryptanalysis. If security were the only consideration, then 3DES would be an appropriate choice for a standardized encryption algorithm for decades to come. The principal drawback of 3DES is that the algorithm is relatively sluggish in software. The original DEA was designed for mid- 1970s hardware implementation and does not produce efficient software code. 3DES, which has three times as many rounds as DEA, is correspondingly slower. A secondary drawback is that both DEA and 3DES use a 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable. Because of these drawbacks, 3DES is not a reasonable candidate for long-term use. As a replacement ,NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard (AES), which should have security strength equal to or better than 3DES and significantly, improved efficiency. In addition to these general requirements, NIST specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits.

VII. EXPRIMENTAL RESULTS

In this proposed scheme the data are segmented into three different levels according to their data importance ranking.

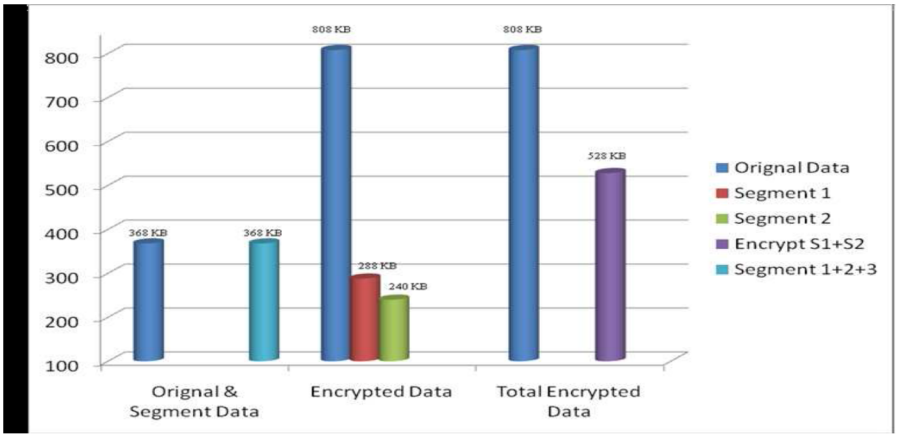


Figure4: Encrypted Data size

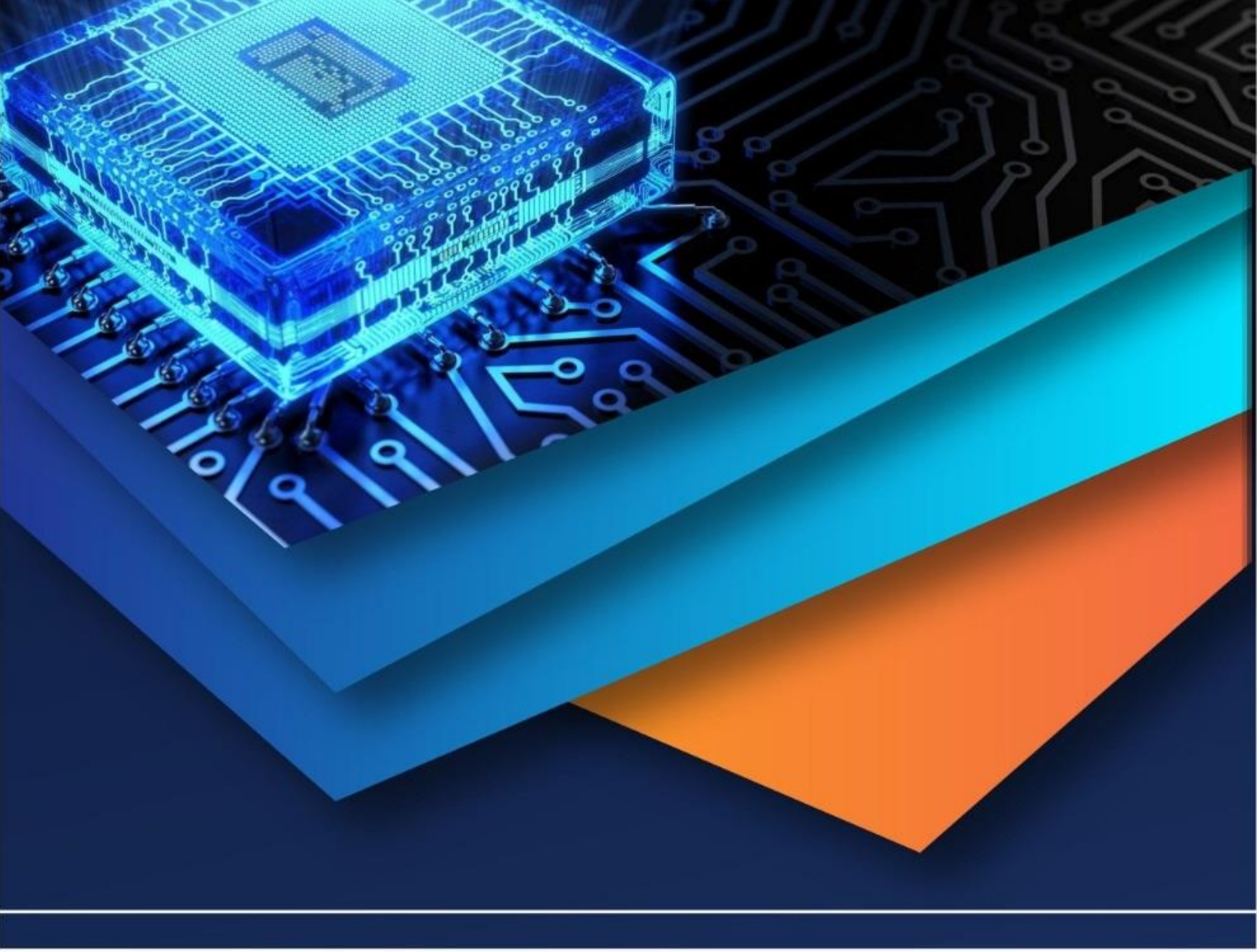
The data in each level can be encrypted by using encryption/decryption algorithms and keys before store them in the Cloud. In this technique the aim is to store data in a
secure and safe way in order to avoid intrusions and attacks. Also, it will reduce the cost and time to store the encrypted data in the Cloud Computing. The paper conducts a performance analysis by implementing the Advanced Encryption Standard (AES) in all levels in order to check the performance of model. The data size of original data model is 368 KB, this data model consist with all data fields of respective database. Data model is splits into three different segments by using SQL queries statements.

VIII. CONCLUSION

Cloud computing have many advantages in cost reduction, resource sharing and time saving for new service deployment. While in a cloud computing system, most data and software that users use reside on the Internet, which bring some new challenges for the system, especially security and privacy. Since each application may use resource from multiple servers. The servers are potentially based at multiple locations and the services provided by the cloud may use different infrastructures across organizations. All these characteristics This paper conducted some experiments on cloud security and it storage. This scheme proposed that, the data are segmented into three different levels according to their data importance ranking. The data in each level can be encrypted by using encryption/decryption algorithms and keys before store them in the Cloud. In this technique the aim is to store data in a secure and safe way in order to avoid intrusions and attacks. The experimental results show that, this proposed scheme efficient to reduce the cost and time to store the encrypted data in the Cloud Storage.

REFERENCES

[1]. Lombardi F, Di Pietro R. “Secure virtualization for cloud computing. Journal ofNetwork and Computer Application (2010)”, doi:10.1016/j.jnca.2010.06.008
[2]. Mohammad Hajjat, Xin Sun, Yu-Wei Eric Sung, David Maltz, Sanjay Rao KunwadeeSripanidkulchai, and Mohit Tawarmalani “Cloudward Bound: Planning for BeneficialMigration of Enterprise Applications to the Cloud”, IJSC VOL 2 ,2011
[3]. Sudipto Das‡ Shoji Nishimura Divyakant Agrawal Amr El Abbadi, “Live DatabaseMigration for Elasticity in a Multitenant Database for Cloud Platforms” UCSB ComputerScience Technical Report 2010-09.
[4]. Chaim Fershtman and Neil Gandal, “Migration to the Cloud Ecosystem: Ushering in aNew Generation of Platform Competition Forthcoming”, COMMUNICATIONS & STRATEGIES,no. 85, 1st Q. 2012
[5]. Aaron J. Elmore “Live Migration in Shared Nothing Databases for Elastic Cloud”,Volume 1 2011
[6]. Pat gelsinger, “Hybrid Cloud Data Migration”, Amazon journal 2012
[7]. Jayson Tom Hilter, “Elastic Migration of the cloud for security enhancement”,Volume 2 , EC2 Journals
[8]. Gribon Taylor “Planning the Migration of Enterprise Applications to the Cloud” WhitePaper, 2010 Cisco Systems, Inc. 2010
[9]. Dan Morphy, “Virtualization and Cloud Computing: Security Threats to Evolving DataCenters”, Mircrosoft Center of Excellence, Microsoft Journals, Volume 3 - 2011
[10]. Rob Livingstone, “Will legacy kill the migration", IJSCT , Volume 12 2011[11]. C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield,“Live migration of virtual machines,” in Proceedings of the 2nd Symposium on NetworkedSystems Design & Implementation (NSDIS). Berkeley, CA, USA: USENIX Association, 2005.
[12]. Christoph Kleineweber, Axel Keller, Oliver Nieh¨orster, and Andr´e Brinkmann, “Rule-Based Mapping of Virtual Machines in Clouds,” in Proceedings of the 19th InternationalEuromicro Conference on Parallel, Distributed and Network-Based Processing, PaderbornCenter for Parallel Computing, University at Paderborn, Germany, 2011.
[13]. Jinhua Hu, Jianhua Gu, Guofei Sun, Tianhai Zhao, “A Scheduling Strategy on ACO ofVirtual Machine Resources in Cloud Computing Environment,” in Proceedings of the 3rdInternational Symposium on Parallel Architectures, Algorithms and Programming
[14]. R. N. Calheiros, R. Buyya, and C. A. F. De Rose, “A heuristic for mapping virtualmachines and links in emulation test beds,” in Proceedings of the 9th InternationalConference on Parallel Processing (ICPP). Washington, DC, USA: IEEE Computer Society,2009, pp. 518–525.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY