International Journal of Scientific Research in Computer Science & Engineering
Research Paper Vol-1, Issue-5 ISSN: 2320-7639

A Systematic Approach for Ensuring Security and Efficiency in Cloud Computing

Vineet Chaturvedi1, Ashok Verma[2] and Neha Agarwal[3]*
[1*, 2,3]*Computer Science &Engineering, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India*
Available online at www.isroset.org

Received: 1 September 2013 Revised: 10 September 2013 Accepted: 08 October 2013 Published: 30 October 2013

Abstract— Cloud Computing is the latest trend of today's IT industries. It is the solution for the problem that occurs due to the resources availability and its utilization over the network. The popularity of cloud computing has increased due to its great policy of pay-as-you-use or resource-on-demand but still it lacks with certain issues of security, trust and efficiency when implemented or deployed on large enterprise such as in geological surveys, scientific applications, astrological applications, oceanography etc. There exist lots of solution in security issues and lots of research for its efficiency but none of them focus on the both issues together. In this paper we have proposed a model that will provide solution for both of these issues. The work mainly focus on the fast scheduling of events in cloud computing by using private key cryptosystem instead of public key cryptosystem and instead of using traditional IKE i.e. internet key exchange mechanism we used the concept of random key reusability which is an approach for providing authenticate and efficient key exchange as that of IKE. Also the various section are made for storing users data on basis of the confidentiality, authentication and integrity that will enhance the overall security of the data stored and retrieved in the cloud computing.

Keywords: CLC, IKE, Certification Authority, Sensitivity Rating, Random Key Reusability

I. INTRODUCTION

Cloud computing gets its name as a metaphor for the Internet. Typically, the Internet is represented in network diagrams as a cloud so as the computing over it is mainly termed as Cloud Computing. It is the computing that contains three important components in its architecture. The network, secondly server and third is the data centers over which the application or the services resides. Cloud computing is a construct that allows you to access applications that actually reside at a location other than your computer or Internet-connected device. It is the use of computing resources either software or hardware over the Internet. It is offered as pay-as-you go or pay-as-you use mode. Cloud computing is a very promising technology that helps companies reducing operating costs while increasing efficiency. In September 2011, the definition and specifications of cloud computing were standardized by the U.S. National Institute of Standards and Technology (NIST). The definition of Cloud Computing introduced by the NIST is Cloud computing is 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 diagram showing both the service and deployment model is given in Fig.1 (NIST definition).

1.1 Service Model In Cloud

Cloud computing providers offer their services according to three fundamental models [3]. The brief descriptions are as follows:

Infrastructure-as-a-Service(IaaS). It is the service that provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources, and allows the consumer to deploy and run arbitrary software, which can include operating systems and applications [2]. The consumer has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.(e.g.- Amazon EC2, S3, Sun's cloud service, Go Grid, 3 Tera etc)

Platform-as-a-Service (PaaS). It is the service that provides the consumer with the capability to deploy onto the cloud infrastructure; consumer created or acquired applications, produced using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations [2].(e.g. Microsoft azure service platform, force.com, Google App Engine etc)

Software-as-a-Service (SaaS). It is the service that provides the consumer with the capability to use the provider's applications running on a cloud infrastructure [2]. The applications are accessible from various client devices, through a thin client interface, such as a web browsers (e.g.-web-based e-mail Google Docs, Salesforce.com, Microsoft Azure, Zoho, etc).

1.2 Deployment Model

Four basic deployment models have been identified for cloud architecture solutions are described below:

Corresponding Author: *Vineet Chaturvedi*

A Private cloud is owned or rented by an organization. The whole cloud resource is dedicated to that organization for its private use.

A Public cloud is owned by a service provider and its resources are sold to the public. End users can rent parts of the resources and can typically scale their resource consumption up (or down) to their requirements.

A Community cloud is similar to a private cloud, but where the cloud resource is shared among members of a closed community with similar interests. An example of a community cloud is the Media Cloud set up by Siemens IT Solutions and Services for the media industry A community cloud may be operated by a third party (as in the Siemens case), or may be controlled and operated in a collaborative fashion as in the Grid Computing paradigm.
A Hybrid cloud is the combination of two or more cloud infrastructures; these can be either private or public, or community clouds. The main purpose of a hybrid cloud is usually to provide extra resources in cases of high demand, for instance enabling migrating some computation tasks from a private cloud to a public cloud.

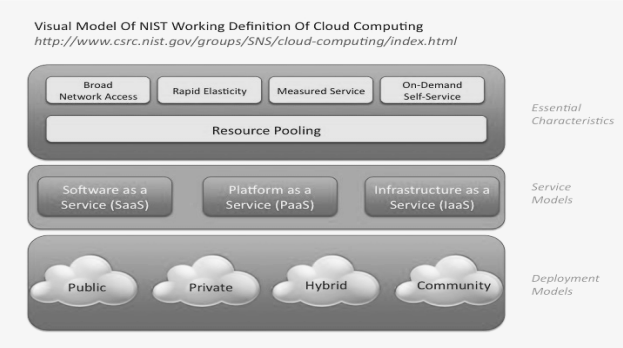

Fig.1 NIST visual model of cloud

II. SECURITY ISSUES

Security of data in cloud is one of the major issues which acts as an obstacle in the implementation of 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 [4].

2.1 Trust

The notion of trust in an organization could be defined as the customer's certainty that the organization is capable of providing the required services accurately and infallibly. It also expresses the customer's faith in all kinds of transactions done between the customer ant the organization [2].This is the most critical issue and depends upon various security measures and norms that are been provided by the cloud service providers.

2.2 Confidentiality and privacy

Confidentiality refers to only authorized parties or systems having the ability to access protected data. The threat of data compromise increases in the cloud, due to the increased number of parties, devices and applications involved, that leads to an increase in the number of points of access. Delegating data control to the cloud, inversely leads to an increase in the risk of data compromise, as the data becomes accessible to an augmented number of parties. Data confidentiality in the cloud is correlated to user authentication. Protecting a user's account from theft is an instance of a larger problem of controlling access to objects, including memory, devices, software etc [1]. Privacy is the desire of a person to control the disclosure of personal information. Organizations dealing with personal data are required to obey to a country's legal framework that ensures appropriate privacy and confidentiality protection.

2.3 Integrity

A key aspect of Information Security is integrity. Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware. Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication [2]. The Cloud service provider must provide the surety that there exist no modification in the customers' data, personal information as well as the services attained.

2.4 Availability

Availability refers to the property of a system being accessible and usable upon demand by an authorized entity. In cloud computing, Availability refers to data, software but also hardware being available to authorized users upon demand. Leveraging users from hardware infrastructure demands generates a heavy reliance on the ubiquitous network's availability [1]. Cloud computing services present a heavy reliance on the resource infrastructures and network availability at all times.

III. RELATED WORK

In the recent years, various researches are done for providing various solution for solving the security issues of cloud computing. In paper [5,6,7,8,9], the strategy followed to protect the data utilizes by providing various measures such as the SSL (Secure Socket Layer) 128-bit encryption and MAC (Message Authentication Code) is used for integrity check of data and performing encryption is cloud. In paper [2, 10, 11], they used a user-centered measure of cyber-security, and performed their measures to analyze cloud computing as a business model. They proposed a quantitative model of security measurement that enables cloud service providers and cloud subscribers to quantify the risks they take with the security of their assets, and to make security related decisions on the basis of quantitative analysis. The paper [1,12,13] introduced the concept of a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the

authentication, integrity and confidentiality of involved data and communications. Recently, much research work has also been done to address cloud security/privacy issues. Most of the approaches amongst them, however, were focused on cloud storage services. Yao et al [14] proposed a scheme to ensure cloud storage security by separating the encryption keys from the stored data which were encrypted by the keys. In [15], a privacy-preserving cloud data querying scheme is proposed from generally a data prospect of view, which aims to protect privacy-sensitive outsourced data. In paper [16,17], they provide solution for data security in cloud computing using 3 dimensional framework and digital signature with RSA Encryption algorithm. They use MD-5 for digital signature. The overall solution is provided by using either various encryption mechanisms or by performing various key management mechanisms in cloud computing using mainly the Public key Management procedures [18].

IV. PROBLEM DESCRIPTION

The problem that had been identified is that in cloud computing a central server is employed for not only receiving and processing user requests in the front, but it is also responsible for scheduling and splitting tasks. We call this server as cloud controller (CLC) or Cloud service provider (CSP). All these virtualized server instances running on clusters of servers are responsible of processing the divided tasks in a parallel fashion and returning the results afterwards, and then CLC is capable of assembling the results and return to the user. Mainly we have various Asymmetric-key encryptions mechanism for such purpose. Since it suffers from low efficiency and takes large time we must develop a mechanism that utilizes the symmetric encryption scheme. CLC must at first exchange a session key with each server instance through an authenticated key exchange scheme before distributing the divided data and tasks to server instances.
As a distinct session key is needed to be exchanged between the CLC and each server instance, conducting key exchanges between CLC and server instances becomes a tedious and time consuming task, especially in data-intensive applications such as scientific applications. IKE is one of the most efficient, secure, standardized and widely applied authenticated key exchange schemes for communications over an unsecure communication channel. However, the efficiency of IKE is very low when applied with large sets of data such as scientific, business or astronomical application, Unfortunately, the problem occurs in the authenticated key exchange schemes together with the security of the data in such computing.

V. PROPOSED SCHEME

The proposed work comprises of the random reuse strategy that will provide the efficient and authenticated key exchange mechanism over the existing IKE mechanism. It is achieved by using the concept of Diffie-Hellman key exchange operation together with the random key reuse mechanism in the session generated during computing. Before making such system in order to provide secure mechanism we will make our data priority on the basis of the three important issues of Confidentiality, Integrity and Authenticity which is given in the algorithm. These are the three section where our initial data get stores. After this the scheme works in the three basic steps. First, the system setup, second is the initial exchange and lastly the rekeying process.

Algorithm :

1.Input: Data, protection section, D[] array of n integer
Where D[]array consisting of C,I,A,SR,R of n integer size.
2. Output: Categorized data for corresponding section.
3. For i= 1 to n
3.1 C[i]=Value of Confidentiality.
3.2 I[i]=Value of Integrity.
3.3 A[i] =Value of Availability.
3.4 Calculate SR [i]= (C[i]+(1/A[i])*10+I[i])/2
4. For j=1 to10
For i=1 to n
IF SR[i]==1||2||3 then
S[i]=3
IF SR[i]==4||5||6 then
S[i] =2
IF SR[i]== 8||9||10 then
S[i] =1

System setup: The system chooses a large prime integer to form a Diffie-Hellman group, and generator # of group. We will make is a primitive root modulo. Normally is a Sophie Germain prime where is also prime, so that the group $%& maximizes its resilient against square root attack to discrete logarithm problem. A certificate authority (CA) is still needed same as in PKI that will ensure the authenticity between the CLC and the various server instances.Certificates are relatively long-termed data which are issued to all participants of communication before the commencing of communication, and CA won't be participating itself unless re-verification of identities and revocation and re-issuing certificates for participants are needed. As these will be performed in our scenario probably in lower frequency (e.g. once a day) than key exchanging (e.g. re-exchanging key in every new session), they won't affect the efficiency of a key exchange scheme for scheduling in general. Therefore, we will ignore all communications involving CA in our scheme and won't be discussing further details on issuing and revoking certificates.

Initial exchange: Initial exchange is used when a new task is to be executed, because that is when CLC need to decide how to distribute this new task to be executed on existing computation infrastructure, i.e., which of the server instances are involved. CLC picks a secret value x

< p, computes its public keying material gx in Zp, and broadcast the following message to the domain of server instances S which contain n instances S1,...S:

Round 1, C-> S: HDRc, SAc1, gx,Nc

Where HDR and SA for algorithm negotiation, gx for Diffie-Hellman key exchange, and for freshness verification. The initiator of a normal IKE scheme will generate n secret x1, x2, x3... xn, then compute and send out gx1, gx2 ....gxn ,either through multicast or one by one, to establish separated security channels with each receiver. In our scheme, although we still establish one for each server instance where i=1,2,.n, we are using only one single secret value 0' for CLC in all* messages in order to reduce cost. Upon receiving message the server instance will generate their secret key as shown in round 2.

Round 2, S→C:HDRSi, SAsi, gyi, NSi, CertReqc
for i=0,1,2,…..no N.

The session keys are now shared between CLC and each server instance for the use of encryption of later communications. Although the Diffie-Hellman key exchange is completed, initial exchange is not finished as the participants have to authenticate each other in order to prevent man-in-the-middle attacks. Similar as in IKE, CLC generates signatures " which are the signatures for these * messages, using its secret key from the key pair issued by CA and broadcast the following message

Round3,C>S:HDRc,{IDc,SAc2,Certc,CerReqs1Sig}gxy1
for i =1,2....no S:

The server instances can then verify the identity of the initiator of this conversation by using its session key to decrypt its own part of this message. Signatures can be verified through the public key contained in the certificate. Similarly, server instances will send out their own encrypted ID, signature and certificate to CLC for verification:

Round 4, S->C:HDRst{IDc,SAc2,Certc,Sig}gxy
for i=1,2,.....,n

where similar to round 2 but only signed separately, Sigst is signatures by Si to messages :

Mst = prf(prf(Nc|| Nst||gxy)||gyi||gx||IDsi) for i = 1, 2, ...n

Note that this round involves * messages as well. After the identities of both CLC and server instances are authenticated through round 3 and 4, CLC will send to S1, S2,Sn, the split task data which are encrypted with session keys gxy1,..gxyn using symmetric encryption such as AES. After task execution, returns to CLC the results which are encrypted using S1, S2, Sn as well. The prf function is often implemented as an HMAC function such as SHA-1 or MD5, which outputs a fixed-length short message (commonly 128 bits) and has high efficiency (around 200MB/s on today's desktop PCs) itself.

Rekeying: In a multi-step task data need to be transferred back and forth in a multi-step task. In this situation it is not necessary to re-authenticate because of the high data dependency in a same task. Therefore, only rounds 1 and 2 are needed to be performed, with new keying materials and minor changes to *SA* and *HDR* fields and. As rounds 3 and 4 only contains fast operations such as signature and nverification over short messages as well as symmetric key encryption/decryption and HMAC functions, the computational overhead of rekeying process is almost identical to the initial exchange from an efficiency prospect of view.

VI. EXPERIMENT & RESULTS

The experiments were performed for the both cases by firstly for the traditional IKE scheme and secondly for the random key reuse strategy proposed. The cloud computing infrastructure is made using OpenNebula cloud environment. On top of the hardware and Linux O.S. we installed KVM hypervisor on which further we used the simulator Hadoop for performing MapReduce Programming. We also used this on OpenStack Cloud environment. It is clear that the efficiency depends mainly on the size of the data sets used in the computing. The experiment were conducted on large numbers of data sets with different numbers of server instances. The 2 key exchange key is implemented using Java. We have taken the generator function g=2 and for parameters of Diffie-Hellman key exchange we used 1024 bits prime over 1024 bits MODP group. We used MD5 for pseudorandom function and RSA algorithm for signature. Experiments were conducted under multiple scenarios which will be demonstrated in the next section and compared with our scheme to the trivial scheme where CLC exchanges keys with each server instance using IKE in a separated fashion. Asymmetric-key cryptosystem are much slower (approximately 1000 times slower) than symmetric-key cryptosystems, thus large datasets are never encrypted with asymmetric-key cryptosystems in practice. We ran them under our cloud simulation environment, and tested total time consumption on CLC. The result is illustrated in the fig.2 in this section.

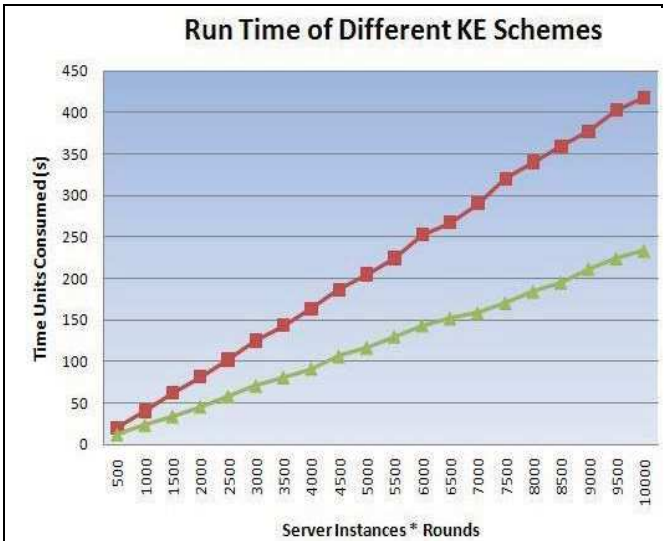

Fig.2 Performance compared with IKE

VII. CONCLUSION & FUTURE WORK

After performing the experiment it is found out that the efficiency mainly depend upon the size of the data sets used and the CLC process for splitting and distributing the instances. In this paper the proposed scheme gives the complete solution for providing security on the basis of the user's priority together with the increased efficiency for large application such as in scientific, geographical, astrological, etc. Our scheme mainly uses the working same as that of the traditional IKE scheme together with the randomness key reuse strategy. All the simulation and theoretical analyses were done and it is found that it reduces time consumption, computation load without compromising the security aspects. In future further new strategy can be found out to increase efficiency and providing security in cloud computing.

REFERENCES

[1]. Dimitrios Zissis, Dimitrios Lekkas "Addressing cloud computing security issues" Future Generation Computer Systems, Elsevier, 2012.

[2]. Rabai, L.B.A. et al., A cyber security model in cloud computing environments. Journal of King Saud University – Computer and Information Sciences (2012).

[3]. Rong C et al. Beyond lightning: A survey on security challenges in cloud computing. Comput Electr Eng (2012)

[4]. Shivlal Mewada, Umesh Kumar Singh and Pradeep Kumar Sharma, " Security Enhancement in Cloud Computing (CC)", ISROSET- IJSRCSE, Vol-1, Issue-1, pp(31-37), Jan-Feb 2013

[5]. Shivlal Mewada, Umesh Kumar Singh, Pradeep Sharma,"Security Based Model for Cloud Computing", Int. Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 1, No. 1, pp (13-19), December 2011.

[6]. R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging it platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems 25 (2009) 599–616.

[7]. Cong Wang, Qian Wang, and Kui Ren, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, IEEE INFOCOM 2010.

[8]. I.M. Abbadi, M. Alawneh / Computers and Electrical Engineering 38 (2012) 1073–1087

[9]. S. Marston et al. / Decision Support Systems 51 (2011) 176–189

[10]. Shuai Zhang and Shufen Zhang "Cloud Computing Research and Development Trend", IEEE, Second International Conference on Future Networks, 2010

[11]. K. Salah ,J. M. Alcaraz-Calero,S. Zeadally ,S. Almulla and M. Alzaabi "Using Cloud Computing to Implement a Security Overlay Network", IEEE, Security and Privacy, 2011

[12]. S. Marston et al.,Decision Support Systems 51 (2011)

[13]. National Institute of Standards and Technology. The NIST definition of cloud computing; 2011.http://www.nist.gov/itl/cloud/upload/cloud-defv15.pdf

[14]. J. Yao, S. Chen, S. Nepal, D. Levy, J. Zic, Truststore: making Amazon S3 trustworthy with services composition, in: Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, CCGRID'08, Melbourne, Australia, 2010, pp. 600–605

[15]. N. Cao, Z. Yang, C. Wang, K. Ren, W. Lou, Privacy-preserving query over encrypted graph-structured data in cloud computing, in: IEEE International Conference on Distributed ComputingSystems, ICDCS'11, 2011, pp. 393–402.

[16]. Pradeep Bhosale, Priyanka Deshmukh, Girish Dimbar, Ashwin iDeshpande: Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption-International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 8, October – 2012

[17]. F. Hu, M. Qiu, J. Li, T. Grant, D. Tylor, S. Mccaleb, L. Butler, R. Hamner, A Review on Cloud Computing : Design Challenges in Architecture and Security, Journal of Computing and Information Technology, 19 (1) (2011)

[18]. A. Groce, J. Katz, A new framework for efficient password-based authenticated key exchange, in: Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS'10, Chicago, USA, 2010, pp. 516–525

