International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.5 Issue: Special 5, pp:992-1128 20 May 2016

Securing Cloud Computing Environment using a Novel Method of Cryptography

Yatheendra K V
Computer Science and Engineering
VTU PG Center,Mysuru.
Yatheendra72@gmail.com

Shashirekha H, Asst Professor
Computer Science and Engineering
VTU PG Center,Mysuru.

Abstract—*Cloud computing is an internet-based computing, where shared resources, software, and information are provided with consumers on-demand. They guarantee a way to share distributed resources and services that belong to different organizations. In order to build secure cloud environment, data security and cryptography must be assured to share data through distributed environment. So, this paper provides more flexibility and secured communication environment by deploying a cryptography service. This service entails both Quantum Key Distribution (QKD) and enhanced version of Advance Encryption Standard (AES). Moreover, this service solves the key distribution and key management problems in cloud environment which emerged through the two implemented modes, on-line and off-line modes.*

INTRODUCTION

Nowadays, computing is categorized according to their usage pattern. Parallel computing, cluster computing, and distributed computing are well-known paradigms of these categories [1]. A parallel computing is a form of computation where a large task is divided into unrelated smaller tasks in such a way that these smaller tasks can be concurrently computed [2]. Whereas, a cluster computing acts a group of linked computers that are tightly coupled with high speed networking and work closely together [3]. Moreover, a distributed computing is a collection of hardware and software systems that contain more than one processing or storage element but appearing as a single coherent system running under a loosely or tightly controlled regime [4]. The computers in the distributed system do not share a memory instead they pass messages asynchronously or synchronously between them[5]

The new generation of distributed computing environment requires integration between distributed computing systems and networking systems [6], which allows computer networks to be involved in distributed computing as full participants like other computing resources such as CPU capacity and-memory/disk space. Emerging trends in distributed computing paradigm include Grid computing [7], Utility computing [8]and Cloud computing [9], which have enabled the utilization of wide variety of distributed computational resources as a unified resource. These emerging distributed computing technologies, with the rapid development of new networking technologies, are changing the entire computing paradigm toward a new generation of distributed computing. This paper discusses in detail the well-known emerging technology in distributed computing is cloud computing and focuses on key management and cryptographic issues in cloud environment.

Cloud computing is a specialized form of Distributed, grid,and utility computing and it takes a style of grid computing where dynamically stable and virtualized resources are available as a service over the internet. Furthermore, cloud computing technology provides many maturity features such as on-demand, resources scalability, portal applications, etc.However, these features influenced by many security issues(defeating attackers, key distribution and cryptographic aspects) due an open environment associated with cloud computing [9].

In spite of different groups try to solve the security issue cloud communications, many gaps and threads are still uncovered or handled. Consequently, in order to overcome these vulnerabilities and secure those services, cryptographic security mechanisms are installed and followed in many cloud environments. The other major issue of Cloud is represented by data security. Since a proper, cloud service provider independent security model is not developed yet, there is a loss of control over data in cloud computing. This is mainly because of unknown physical location of hardware and software, absence of cloud security standards, lack of compliance standards, such as HIPAA [10], SOX[11], and a risk of data loss due to improper backups or system failures in the virtualized environment.

So, this paper deploys a secure quantum cryptographic service in order to secure data transmission channels by provisioning secret key among cloud's instances. This service combined between QKD system and an innovative version of AES [12], and it is implement on cloud platform which builds depending on bare-metal Hyber-V hypervisor and system center manager.The reset of the paper is organized as follows: Section 2shows the existing studies related to cryptographic algorithms and key management in cloud computing, Section 3 describes the modern cloud cryptographic algorithms, the applied algorithm and the performance evaluation of this algorithm are discuss in Section 4, the developed cryptographic service is explain in Section 5, Section 6 and 7 explain the experimental environment of cloud computing architecture and discusses indetail its main building modules including an illustrative example that represents the main functions used through the interaction between the main modules, Section8 provides the empirical analysis for the proposed environment and finally,Section 9 presents the conclusion and future works.

II EXISTING STUDY

Different studies' attempts to solve the security problem in cloud communications and data security, nevertheless, many gaps and threads are still uncovered or handled. In the meantime, all proposed attempts consider the main cryptography criteria such as data privacy and confidentiality.

For example, Bethencourt et al [11] presented an Attribute Based Encryption (ABE) model in the cloud environment and social networks. This model allows the clients to be involved into two or more groups. To compute the key for the client involved in two groups the logical expression are

used.However, the drawbacks are the computational cost in ABE and re keying the entire in revoked members in the same group.In case he data are for all then re keying should be to everyone connected with the data owner. Consequently, Sun et al.[12]proposed the model in which the clients are grouped according to their roles. The clients can access the certain type of data only. Sometimes it may possible to have two groups may seethe certain data. It is the freedom to the data owner to create the groups and number roof users in the groups.

Mather et al [13] discuss the inadequate encryption and key management capabilities currently offered, as well as the need for multi-entity key management. Moreover, they are discussed the status of cloud security, the result is a compilation of security related subjects to be developed on topics like security management, data security and storage, and identity and access management. They also explore the unquestionable urge for more transparency regarding which party provides each security capability, as well as the need for standardization and for the creation of legal agreements reflecting operational Service Level Agreement (SLA's).Cutillo et al [14] presented the Simple Shared Key 1-Clientside storage model. With this model, the encryption key (Ka)will be generated for the attribute and shard with all clients in the group given by data owner using the public key of the clients.

In case the data owner want to change the data encryption key (Ka) to revoke a particular client then data owner needs to change the Ka by Ka' and again the new key Ka' needs to be distributed to everyone. Here the data decryption key will be stored with the clients. In this, the key should be transferred only to that group not to all the clients connected to the network. This is a useful advantage of this model.

Rawal et al [15] looks for the perfect alliance between cloud computing and quantum computing, which guarantees data protection for hosted files on remote computers or servers.He encrypted heavy duty of data by using the data processing servers as a quantum computer, which hides input, processing and output data from malicious and attacks.

Miao Zhou [16] present the tree-based key management in cloud computing. The fundamental idea of this work is to design a secure and flexible key management mechanism for the outsourced data in cloud computing. In this thesis, an innovative tree-based key management scheme is proposed.The outsourced database remains private and secure, while some selected data and key nodes are shared with other parties in the cloud. Flexibility of key management is achieved and the security is proved in the standard model. Finally, summarizes the key management and cryptographic studies incloud environment and shows the innovative model which contributed and main pros and cons.

III. MODERN CLOUD CRYPTOGRAPHIC ALGORITHMS

Data in the cloud environment are described as transmitter, stored or processed by CSP. Any client enterprise applies the same data classification used when the data are resident on own machine or locally platform.Therefore, they are applying necessary cryptographic security requirements to data stored, transmitted or processed by CSP.The SLA cannot achieve all these requirements; it must be done by an efficient cryptographic algorithm and authentication function such as AES, Kerberos, and SHA-256[17]. Once data is safely transmitted to a CSP, it should be stored, transmitted and processed in a secure way.

In [17], authors implemented the mentioned symmetric and asymmetric algorithms in order to ensure the data security in acloud environment, and examine the performance of sucha lgorithms, considering the time of the encryption/ decryption process and the size of the output encrypted files. This study reveals that the symmetric encryption techniques are faster thanthe asymmetric encryption techniques and AES algorithm guarantees more efficiency from others.Despite the encryption process uses complex techniques for random key generation based on mathematical models and computations, its encryption strategy considered vulnerable. So,if the intruder is good enough in the mathematical computation field such quantum attack, he/she can easily decrypt the cipher and retrieve the original transmitted or stored documents.Furthermore, a key distribution is another critical issue which noticed in most modern encryption algorithms. It arises from the fact that communicating parties must somehow share a secret key before any secure communication can be initiated,and both parties must then ensure that the key remains secret. Of course, direct key distribution is not always feasible due to risk,inconvenience, and cost factors [18].

In some situations, direct key exchange is possible through secure communication channel. However, this security can never guarantee. A fundamental problem remains because, in principle, any classical private channel can be monitored passively, without the sender or receiver knowing that eavesdropped has taken place [19]. This is because classical physics-the theory of ordinary-scale bodies and phenomena such as magnetic tapes and radio signals- allows all physical properties of an object to be measured without disturbing those proprieties. So, a Quantum Key Distribution technology (QKD)overcomes these barriers depending on unconditional security aspects and quantum physics phenomena [20].

IV. APPLIED ALGORITHM

Data transformation through communication channels needs highly secured levels; therefore, many cryptographic encryption algorithms rely on unpredictable complex encryption key. To assure the strength of such keys, QKD has been integrated and QAES, a new version of the AES, has been developed [21].The QAES algorithm developed system incorporates both the QKD and the AES algorithm in order to provide an unconditional security level [22] for any cipher system built asymmetric encryption algorithms or other algorithms. The AES enhanced version exploits the generated key based QKD in the encryption /decryption process. Since the unconditional security depends on the Heisenberg uncertainty principle [19][20], instead of the complex mathematical model in key generation and truly randomness characteristic associated with quantum key generation [23], more attack resistance is assured and the cipher system is hard to be attacked. Furthermore, the randomness characteristic elps to adopt the QT as a source to generate random numbers that are used with various encryption algorithms.

The round key session enjoy the dynamic mechanism, in which the contents of each key session changes consequently in each round with the change of the key generation. Such dynamic mechanism aids in solving the mechanism problems like avoiding the off-line analysis attack, and resistance to the quantum attack.Figure 1 examines the performance of our applied algorithm on private cloud environment (illustrated below), considering the time of the encryption/ decryption process and the size of the output encrypted files, this examination implemented using several input file sizes: 500kb,

1000kb, 1500kb, 2000kb,3000kb, and 4000kb and the running time is calculated in milliseconds.

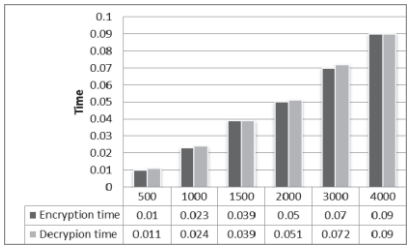

Figure 1. An efficient of QAES on our cloud environment

Comparing the QAES with other encryption algorithms reflects a higher security level. However, as shown in Eq.2, this algorithm takes time more than others due to the time required for quantum key generation (time for quantum negotiation and time required for the encryption / decryption process) for more elaborates see [22, 23].

Tqenc =Tqkg+ T (Enc (P)) (1)

Where Tqenc = Total encryption, Tqkg= time for key generation and

T(Enc (P))= time requires by encryption algorithm

V. CRYPTOGRAPHY SERVICE

This section presents a new cryptographic service layer in the cloud environment, Quantum Cryptography as a Service(QCaaS), this service provides the secret key provisioning to VMs' clients, separating both clients' cryptographic primitive and credential accounts based on secure cloud domain. It is applied to the multiple clients, who renting the VMs,concurrently. Integrating such service achieves both confidentiality and integrity protection.

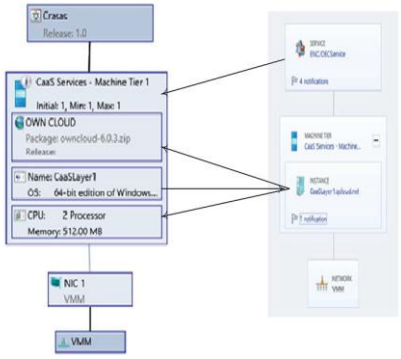

Figure 2. QCaaS architecture

More precisely, figure 2 show that the QCaaS has mini-OS directly connected with the cloud platform and isolated from he cloud instances. Consequently, it assures both the appropriate load for cloud performance optimization and the client controlling activities (client prevent the cloud administrator from gained or preserve his own data).Accordingly, a secured environment for each client's VMs,with no possibility for insiders or external attackers, is guaranteed. To sum up, After the signing in verification and the VM renting, QCaaS deploys the client wizard and the CSP wizard to achieve the encryption/decryption processes and connect to the Quantum Cloud environment see figure in section.

VI. EXPERIMENTAL CLOUD COMPUTING ENVIRONMENT

In the cloud computing environment many operations such as the number of VMs, quality of services (QoS), storage capacity and other features are realized depending on the IaaS layer. This essential layer helps clients to rent virtual resources like network, cloud instances, VM and configure them according their needs. Generally, these VMs provide public services (web services and self-portal applications) offered to clients over either the public cloud or the private cloud.

Accordingly, the bare-metal Hyper-V hyper-visor and the System Center 2012 SP1 components are explained and implemented, these components are: system center virtual machine manager (SCVMM), system center operation manager(SCOM), Application controller (APPC), Operation services manager (OSM), data protection manager (DPM), and demonstrator (OC). The host server (Cloud Providers) utilizes the Core i5 (4.8GHz) with 16GB of RAM with 2TB-HDD asthe main hardware. Our cloud environment generates the encryption keys based on quantum mechanics instead ofmathematics and computations, which in turn, providesunbroken key and eavesdropper detection.

Our proposed environment aims to (i) improve the availability and the reliability of the cloud computing cryptographic mechanisms by deploying both key generation and key management techniques based on QCaaS layer, (ii)manipulate heavy computing processes that cannot be executed using personal computer only.Generally, our cryptographic service in this environment is deployed in two implemented modes, online and off line modes. With online mode, consumer and cloud provider are directly negotiation in order to encrypted file transmission and key generation.

However, in off-line, the cloud provider deploys a stream of quantum keys as a Pseudo Random Number (PRN) [23] which exploit to build the initial key session (seed) for selected encryption algorithm.

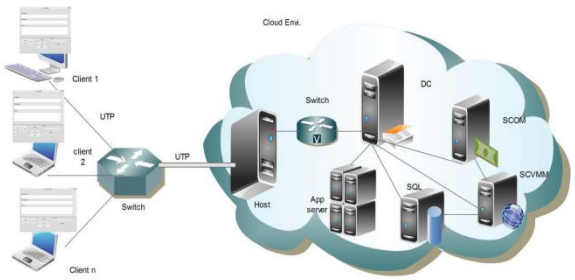

Figure 3. Experimental environment

Figure 3 shows that the our cloud environment consists of the cloud network that entails the windows server 2012 data center server and the Hyper-V installations and configurations with N- full-VMs. These VMs classified as, cloud infrastructure such SCVMM, SCOM, APPC, SQL, domain controller (DC), cloud instances (VMs rented from the client),and VMs for cryptographic processes. Finally, in order to build sheer knowledge about proposed cryptographic service,following pseudo code and illustrative example in section describe the main phases in the proposed cloud environment.

ISSN:2319-6890)(online),2347-5013(print)
20 May 2016

/*renting VM's*/ Input=Key :K1,k2,..,Kf and File Blocks=b1,b2,..,bn
1- Client send request r to CSP
2- CSP compute the resource availability r_a
While r<= r_a
{
CSP invoke the client to wait
}
Else
3- CSP deploy the registration wizard
4- Client enter the user (U) and password (****)
5- CSP register the CA, MAC for the client machine
6- CSP assigns VM-IP to trusted client through domain controller connection (dc)
7- IF client required cryptographic service (QCaaS)
{
Go to step 8
}
Else
Go to step 29
8- IF online negotiation methodology provide
{
/* QCaaS Side*/
9- QCaaS generates randomly the K-qubits in the b_k base generating string S.
10- FOR each bit sk in S classify sk in the base b_i resulting in the k-qubit.
11- QCaaS sends the generated k-qubits to Client (C).
/* Client Side*/
12- Client builds a binary string m Key-message K-qubits.

13- For each mk in m
{
IF ($mk = S_k$)
14- Client applies the gate to the XZ or ZX k-qubit.
15- Client sends K-qubits to QCaaS
}

/* Negotiation Part*/
16- QCaaS measure K-qubit in one of four bases (Bk) using BB84.
17- QCaaS checks the K-qubits Message used by Client and compute err_{rate}.
18- IF err rate> 0.25
19- QCaaS destroyed the connection
Else
20- QCaaS sends new string Sf to Client and XOR
21- Client build a new binary Kf string N-bits length
22- Client sends Kf to QCaaS
}
Else
/*offline negotiation */
23- QCaaS generate series of qubits randomly.
24- QCaaS select the appropriate QAES- length
25- QCaaS deploys the selected key securely to the client
/*encryption process*/
26- Client choose file F, to send to the cloud
27- Client encrypt file using selected key (step)
E (F XOR K_i)=f'
28- Client send encrypted file (f') to cloud
29- Client send the original file (f) to the cloud
Output: cipher file: f' on local machine
Plain file: f on CSP.

VII. ILLUSTRATIVE EXAMPLE

This is a simple example that illustrates the sending operation done by the QCaaS using online connection and explains the corresponding results and actions taken by the system. The system interactions are written in normal font, the user behaviors are in bold, and our illustrations to some actions will be in capital letter.THE SYSTEM ASKS THE USER TO LOG IN OR

REGISTER IF IT IS HIS FIRST TIME.

User>> beginning send the query to the system based on client screen.

System>> sign in or register as a new user see Figure 4.

Figure 4. New user registration and login screen

User >> omer

User>> pass@123

THE CLIENT_ID AND THE PASSWORD WILL BE SAVED IN THE SQL DATABASE

System CSP>> check the identity for omer machine, assign it to q cloud.net domain, and authenticated.

System client>> welcome "omer"; this is a new page for you.

User>> send the requet to rent VM from the system.

System CSP>> verify the VMs availability , choose appropriate of them

System CSP>> assign IP-VM to end user via q cloud .net domain.

System client>> provide GUI-console for authenticated user, see figure 5.

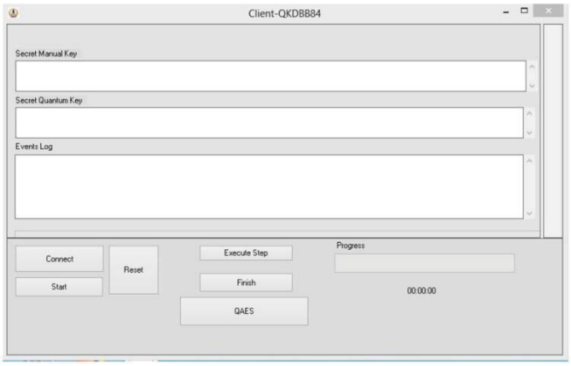

Figure 5. Client-cryptographic wizard

User>> Press the connection bottom to assigned cloud instance.

System CSP>> return the successful connection, deploy QCaaS service

User>> Invoke to build a secure communication, start negotiation with CSP to generate secret key.

IN THIS CASE, THE SYSTEM DETERMINES THE FINAL

SECRET KEY BASED ON BB84 PROTOCOL.

System CSP>> Running the CSP-QCaaS wizard, starting negotiation to generating keys, see Figure 6.

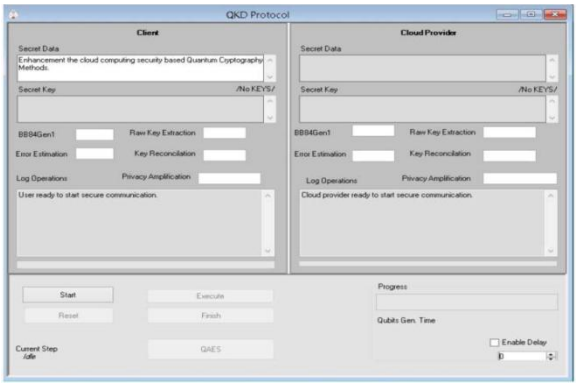

Figure 6. CSP-cryptographic wizard

doi : 10.17950/ijer/v5i5/002

User>> Invoke QCaaS, which appropriate QAES- length selected

System client>> prepare the QAES- 128;192; 256 bits, see Figure 7.

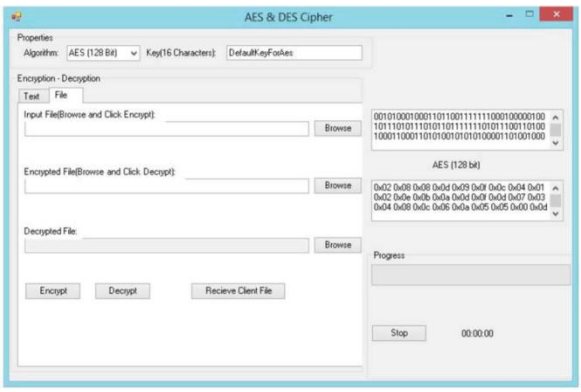

Figure 7. QAES main screen

User>> determined the file on machine (using Browse_bottom) to send it to the quantum cloud

System client>> encrypted file using appropriate QAES using secret key generation.

En (f, qk) =f'

User>> send the documents (d') to the system through VPN connection, see Figure 8.

Figure 8. Sending encrypted files using customizes port

User>> wait some seconds based on the internet connections speed.

System QCaaSr>> receive the encrypted document, decrypted it based on the own secret key

De (f', qk) =f

System client >> files have been sent successfully.

User>> sign out from the system.

VIII. RESULTS AND ANALYSIS

In this section, our cloud environment is analyzed based on the QCaaS functions, and defeating of DoS.A. Defeating the DoS attack This type of attack is considered a critical threat in VMs environment and can be outcomes of hypervisor mis configuration. DoS allows a single VM to consume all available resources, therefore, it causes in starving other cloud-VM running on the same physical device and avoiding network host to detect it, which leads to a shortage in hardware resources. However, Quantum Cloud hypervisors guard against VM from gaining 100%use of any shared hardware resources,including CPU, network, RAM, and bandwidth. This feature provides by creating a standard Quota (see figure 9) and centralized control by qcloud.net domain, such quota deployed standard resources for each new VM created like domain controller name, no.of processors, hardware resources and other. If any VM exceeds this

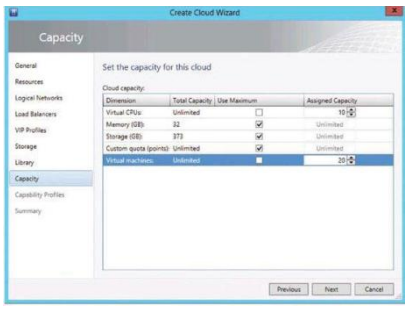

Figure 9. VMs quota

B. QCaaS funcations

QCaaS protects the client's cryptographic key and file through the communication. Moreover, due to the isolation criteria for the resources, QCaaS prevents an attacker from information extraction through the cloud.

• Securing the client : QCaaS provides the encryption/decryption process by cooperating both client's machine and cloud servers, this corporation defeats two types of attacks (man-in –the-middle attack and authentication attack) [for more details see[17]].

• Client Encryption Permissions: QCaaS helps client for encrypting the flying data, which in turn, provides a higher level of security.

• Key Protection: key generation and key distribution processes are critical in any cloud storage environment, therefore, keys must be carefully generated and protected. QCaaS achieves these processes by dynamic key generation based QKD

IX. CONCLUSION

Cloud computing allows consumers to use applications without installation and access their personal files at any other computer via the internet. The rapid growth of cloud computing usage leads to more complications in the security management task that is mainly responsible for providing a secured environment for both the consumer and the CSP.This paper provides a trusted solution for enhanced security issues in cloud environment by deploying a QCaaS .QCaaS reveals many roles such as (i) serving the client security communication and protect their sensitive data, (ii) verification and monitoring the identity of original user, (iii) deploying an encryption service embeds with each VM rents by the consumers, and (v) achieves the encryption/decryption processes using QAES. In general, our attempt enjoy certain advantages when compared with the others, especially with respect to the secret key generation used

in the encryption/decryption process. It can be considered as the first cloud environment that integrates both the CSP principles and the QKD mechanisms.

In the future work, third trusted party (TTP) should by adding between cloud environment and client enterprise. This TTP works as a quantum cipher cloud and responsible for key generation and deploying of the two parties in a trusted environment.

REFERENCES

[1] A.D. Kshemkalyani, M. Singhal, Distributed Computing: Principles,Algorithms, and Systems, ISBN: 9780521189842, paperback edition Cambridge University Press, March 2011. 756 pages., 2008.

[2] Rajkumar B., James B., Andrzej M., Cloud Computing: Principles andParadigms, ISBN: 978-0-470-88799-8, 664 pages, 2011.

[3] CSA, Security a-a-services guidance for critical areas in cloudcomputing, Category 8, 2012.

[4] Doelitzscher F., Reich C., Knahl M., Clarke N., An autonomous agentbased incident detection system for cloud computing, 3rd IEEEinternational on cloud computing technology and sciences, CloudCom2011, CPS. Pp 197-204.

[5] Dabrowsiki C., Mills K., VM leakage and orphan control in open sourcecloud, 3rd IEEE international on cloud computing technology andsciences, CloudCom 2011, CPS. Pp 554-559.

[6] Nelson G., Charles M., Fernando R., Marco S., Tereza C.,Mats N.,MakanP., A quantitative analysis of current security concerns andsolutions for cloud computing, Journal of cloud computing: advanced,systems and applications, springer Vol.1 , No.11, 2014.

[7] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Cryptographic Cloud Computing Environment as aMore Trusted Communication Environment", International Journal ofGrid and Higher Performance Computing (IJGHPC), Vol.6 , issue 2014.

[8] Chadwick D., Casanova M., Security API fro my private cloud, 3rdIEEE international on cloud computing technology and sciences,CloudCom 2011, CPS. Pp 792-798.