Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Asymmetric Key Cryptography Based Technique to Detect and Isolate a Zombie Attack in Cloud Architecture

[1]Amandeeep Kaur, [2]Er. Anupama Kaur
[1] M.Tech (CSE) Student, [2] Assistent Professor, Dept. CSE,
[1, 2] S.U.S. College of Engineering & Technology Tangori, Mohali, Punjab, India

Abstract-- Cloud Computing is growing very fast because of there features like resource capability, Network infrastructure, storage capability, cost effective ,quick access of information .On other side Cloud computing inevitable posses a new challenges because of virtualization and traditional security mechanisms being followed are in sufficient to safeguard the cloud assets . Cloud Computing is easily can be targeted by the attackers. A group of malicious users or illegitimate users are attack on system and denial the services of legitimate users. To overcome such kind of problems the users identification is must. In this paper we are proposing a new security mechanism based on asymmetric key cryptography Based technique to detect and isolate a zombie attack in cloud Architecture The proposed work has been implemented on Ubuntu Operating system with Network simulator (NS2).

Keywords— Cloud Computing , Zombie, Asymmetric Key Cryptography.

I. INTRODUCTION

Cloud Computing is a biggest-scale distributed computing paradigm that is driven by economies of scale i.e. a pool of managed computing power, abstracted, dynamically-scalable, virtualized, storage, platforms and services are delivered on demand to external customers over the Internet. As we know Cloud Computing has become the hottest technology in IT world and is the research also focus in academic. User retrieved data and modified data which is stored by client or an organization in centralized data called cloud. Cloud is a design, where cloud service provider provides services to user on demand and it is also known as CSP stands for "Cloud Service Provider. It means that the user or the client who is using the service has to pay for whatever he/she is using or being used and served. It is a technique which gives a huge amount of applications under different-different topologies and each topology gives some new specialized services.

There are different types of clouds –The cloud which is available publically over the internet is a public cloud and which might be restricted to the one organization and group of organizations is private cloud or which is shared by a number of organizations is hybrid cloud security is a major concern in the cloud environment from various attacks or illegitimate access. There is an special attention is required on the authentication of users before the communication link between user and server. Which can be achieved by using a novel asymmetric key cryptography based improved RSA technique.

1.1 Motivation & Research Problem

Now a days a number of peoples or a organizations are moving towards clouds for using a various types of services which are provided by the cloud service provider security is a major issue in a cloud environment due to its virtualized nature. There are various types of security vulnerabilities like access control, authentication and authorization , attacks ,integrity and confidentiality etc. A virtual machines are targeted by the attackers on a behalf of legitimate user because some illegitimate user spoof the credentials of legitimate users and act as a real user and CSP denied the services of its legitimate user. This problem is arrived due to a improper identification mechanism . There are many verification techniques are available in cloud computing but there are some vulnerabilities are exist in these techniques. Some of these techniques are based on the identification of packets there is no identification of user. Identification of user is must .There is an need to propose a technique based on the proper verification of user. A asymmetric key cryptography based technique improved RSA algorithm is solve the problem of security from malicious attacks in cloud environment.

1.2 Cloud Computing Architecture

Cloud computing is a paradigm that focuses on sharing the information and computations over a scalable network of nodes. Examples are like nodes include end user computers, , and Web Services ,data centres and such a network of nodes as a cloud. An application based on these clouds is taken as a cloud application. In architectural considerations, This infrastructural models that are require to evaluate the cloud computing architectures. Cloud Computing Architecture refers to the components and sub components needed for a cloud computing. These collective components r communicating with each other on application programming interfaces, usually web services.

There are two main components in a cloud computing architecture are front end and back end. Users of the computer are come under the category of front end and back end is "cloud" Itself which provides a various services to its users as cloud service provider. It comprises of virtual machines, deployment model, service model, virtual servers etc. There are several types of cloud deployment models that are differentiated on the basis of infrastructure's provider and physical location. Cloud provides two types of models service model and deployment models. The cloud computing architecture is shown in following figure:

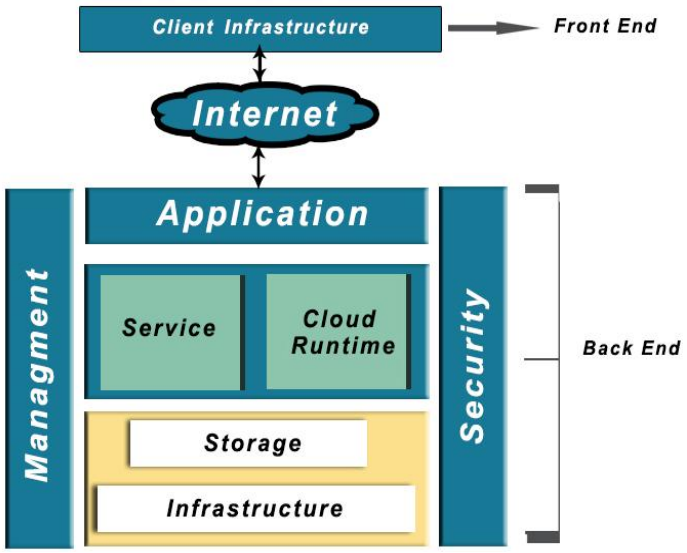

Fig :1 Cloud Computing Architecture

1.2.1 Cloud Deployment Model

Cloud is a allegory for internet and is an abstraction for the complex infrastructure it conceals. The main idea is to use the existing infrastructure in order to bring and deploy all feasible services to the cloud and make it possible to access those services regardless of time and location. Each organization choose a unique deployment model depend on their specific requirements. There are four deployment models in a cloud environment:

1. Public cloud – Public clouds are provided by third party i.e. all the facilities are provided by some third party with all information technology resources residing in their datacenter, such cloud is shared among many customers and all customers have equal chance of utilizing those resources. The public cloud infrastructure is owned and operated by third party. This model provide an elastic, cost effective means to deploy solutions .

2. Private cloud – private cloud computing resources are only available to finite group of consumers, typically it may be an organization. The cloud infrastructure runs in the organization's physical data center or it may be third party co-location. Private clouds are designed and managed by an IT department within an organization. This model gives a high level of control over the cloud services and the cloud infrastructure

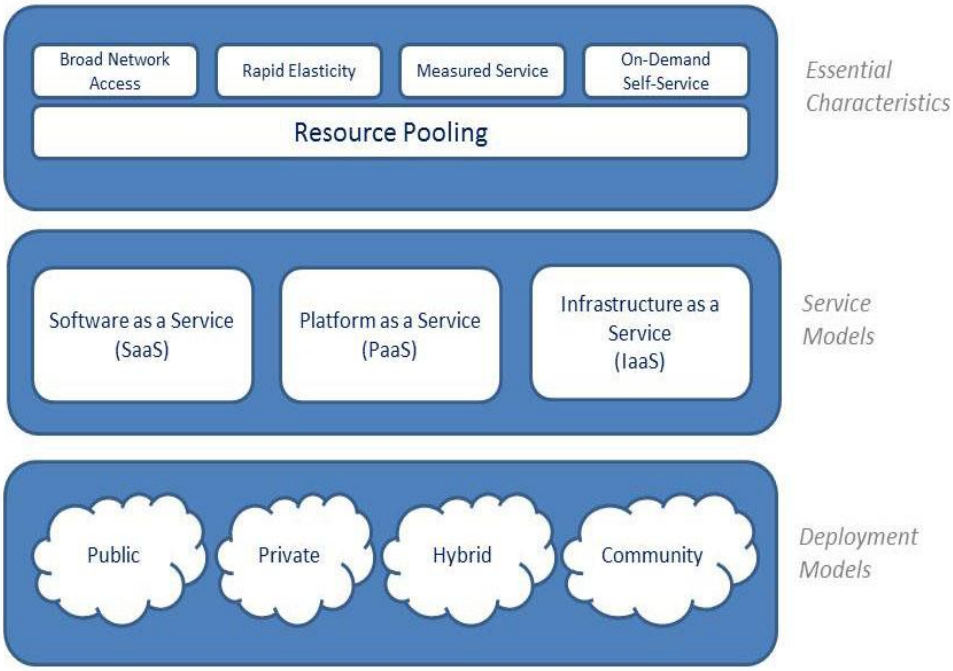

Fig: 2 Cloud Service & Delivery Model

3. Hybrid cloud – Hybrid cloud is the combination of public and private clouds. Hybrid cloud is basically used when the service providers or the cloud owners do not want to invest in datacenters and to extend cloud services to accommodate more and more user's requests. Thus public cloud providers borrow facilities of private cloud to extend services.

4. Community cloud -- Community clouds are also provided by third party and they service organizations having similar interest e.g. hospitals .The community generally restricts a participants from the same industry or with a similar needs. Specific software are developed which could be used by all hospitals under community cloud umbrella.

II. SECURITY ON CLOUD

Security is the Major anxieties when planning to adopt the cloud. Providing a security of data in cloud is important to achieve users trust on cloud provider. This involves virtualization security, distributed computing, application security, identity management, access control and authentication. The most critical part is authentication among the client. So, the proper user authentication is critical for cloud computing to ensure that only valid user have to access to the server. There are number of security issues in a cloud computing due to these vulnerabilities attacks are possible in cloud :

i. **Denial of service attack-**Many security professional have argued that the cloud is more vulnerable to dos/ddos attack because this is shared by large number of users which can make dos attack much more harmful.
ii. **Side channel attack-** An attacker could attempt to compromise the cloud through placing a malicious virtual machine in close proximity to target the cloud server and then exploiting a side channel attack.
iii. **Man in middle attack-** This type of attack is performed when attacker placed himself between two communication parties there is the possibility that they can intercept and modify a communication msg. In the working of this attack the attacker intercepts some or all traffic coming from the client & collect the information and proceeds it to the destination the user was originally intended to visit.

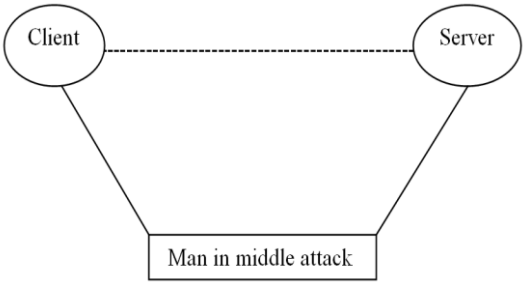

Fig: 3

iv. **Inside attack-**Such type of attack is performed when the staff, person , or employees or who is knowledge of how the system runs from client to server then he can implant a malicious code to damage every thing in the cloud system.

III. REVIEW OF LITERATURE

A. Akinbi (2013)[1] they discussed security requirements for identity and access -+8in PaaS cloud infrastructure as a yardstick for measuring security frameworks and identification of security controls. they proposed an technique for identifying security controls needs in secured PaaS cloud environments by separating its individual components. They identified threats to each component and possible industry standard security scheme which can be applied to mitigate such threats like distributed systems and virtualization. An IAM security framework was drafted from the holistic technique and security strategy to find security controls needs for a secured PaaS.

Chen Danwei (2011) [2]This paper mainly discussed cloud service security. Cloud service is based on Web Services and it will face all kinds of security issues including what Web Services face. The development of cloud service closely relates to its security therefore the research of cloud service security is a very important theme. This paper explain cloud computing and cloud service firstly and then gives cloud services access control model based on UCON and negotiation technologies and also designs the negotiation module.

Logica Banica, Emil B urtescu , Cistian Stefan (2014)[3] This paper has been proposed to focussed on the analysis of several security methods applied in cloud computing environment. In a cloud computing Public key infrastructure certificates are released by a trusted organization, A certificate authority that verifies the identify and validates the server involved in communication. The contents of PKI certificates, which involves a pair of public and private key . Asymmetric algorithm is applied in this. There is an so many cloud infrastructure security methods and protection models, but there is no perfect solution for all kinds of use-cases . In future work they aiming to continuous the cloud environment security investigation by testing and comparing a performance of the encryption scheme in public cloud system presented.

Dr. Santosh Lomte, Sharddha Dudhani (2015)[4] in this paper authentication model is proposed using Kerberos technique and threshold cryptography. Kerberos and threshold cryptography scheme minimize the problem of exchanging of Key. In future work they can enhance this work for identification and detection of cheater among share holder that the part of secret.

Priti Bali(2014) [5] This review describes the comparison of private and public key algorithms. For providing a better solution combination of private and public key is used . Hybrid scheme is used to provide a better security in network. This combination of private and public key algorithms often capitalize on the best futures of each

IV. ZOMBIE ATTACK IN CLOUD ENVIRONMENT

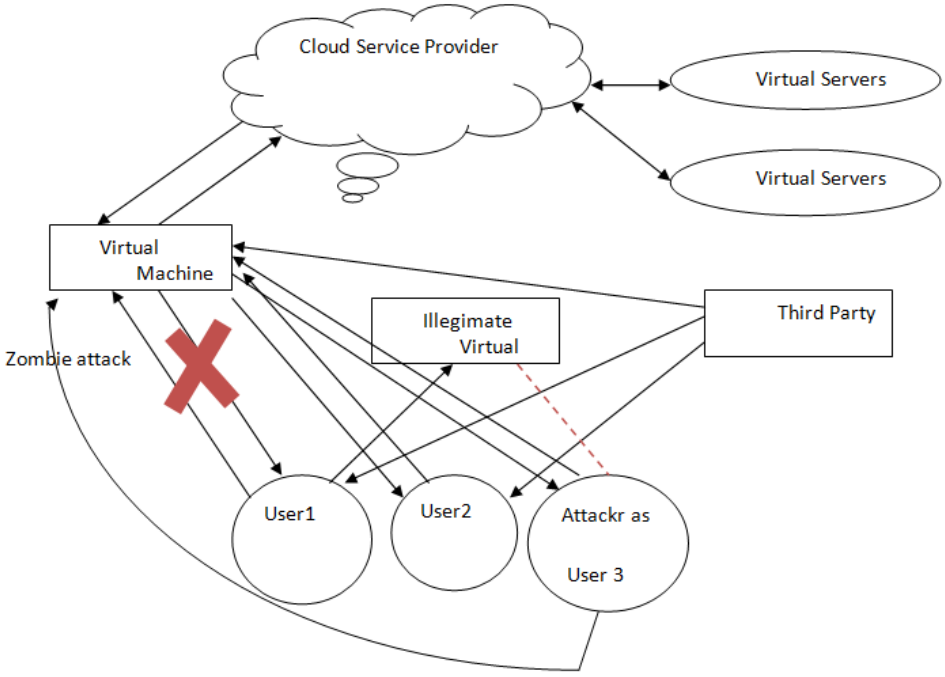

Fig: 4 Zombie attack In a cloud Environment

A zombie attack is performed by a malicious attackers or illegitimate users ,a group of malicious users across the internet can be turned into zombies and used to attack the another system or website. In the above figure a cloud service provider is present which is associated with virtual servers bidirectional. It is also associated with virtual machines. There are numbers of user are present in a network. These users are associated with virtual machines to exchange data between them. Third party is also present in the network. This party is attached or linked with virtual machines, users and cloud service provider. But there is also a user 3 which is attacker. This attacker first of all associated with legitimate virtual machine and as a response this virtual machine gives credential to the attacker or we can say attacker steal credential from legitimate virtual machine. Now user 3 force user 1 to link up new virtual machine which is similar to legitimate user. When User1 associates with illegitimate virtual machine, its information goes to attacker i.e. user 3. This is called zombie attack which is performed by a malicious attacker. In this attack illegitimate users which act as a legitimate user and effect the services of legitimate user.

Security from attacks is an important issue in a cloud computing & , attackers can explore vulnerabilities of a cloud system such as , the detection of zombie exploration attack is extremely difficult. For a better attack detection NICE employees a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, they preventing a zombie VMs. In this technique the (NICE-A) Network intrusion detection Agent is installed on each cloud server to capture and analyze the network traffic. The Proposed solution can significantly reduce the risk of the cloud system. NICE only investigates the network IDS approach to counter a zombie explorative attack . In order to improve the detection accuracy, host based IDS solutions spectrum of IDS in cloud system.[6] the identification of user is must , there is no identification of user in this there is an incoming packets are verified for checking a intrusion.

V. PROPOSED METHODOLOGY

In proposed methodology, A communication between user and server a secure connection is needed between them to protect a users confidential data from attacks. The illegitimate users trigger the zombie attack on targeted system and degrade the network performance also and denied the services of its legitimate user . Improved RSA based asymmetric key cryptographic technique is used for the identification of user. In this technique senders data is converted into encrypted form of non readable form and at receiver end again decrypt it using its on key. There are two types of keys are used in this technique public which is distributed to a public and private key is secret only by the user. The user login on virtual machine then it will send a query message to user. In cloud network the zombie attack is triggered by the malicious attacker , illegitimate user steal the credential of legitimate user and act like a authorized user. So the novel technique is proposed which is based on the both side verification process . when user enter there credential are verified by the server and server ask for a ticket id then if user prove there identity then further process is proceed otherwise user is detected as a malicious user and isolated. And same as at user side before communication legitimate client will ask the sever for its credentials. If the sever credentials are verified by the client then further process will proceed otherwise algorithm will be halt.

Pseudocode: Deploy the network with uses and ask for credentials
User input ‘user name’
User input ‘password’
Set the flag B=0;

Set the array with resisted user and virtual machines
Do {
The user send Query message about the MAC ID of the virtual machine
If " mac_id" of virtual machine is equal to registered MAC ID
{
Set B=1;
Else
{
1. Ask for the secret number of virtual machine, NONCE number and identity of machine
If (Secret number of the virtual machine matched with user secrete number)
Ask for MAC ID of the machine
If (MAC ID Machine matched)
{
User access the assigned data
}
Else
Isolate the machine
}

5.1 Experimental Results

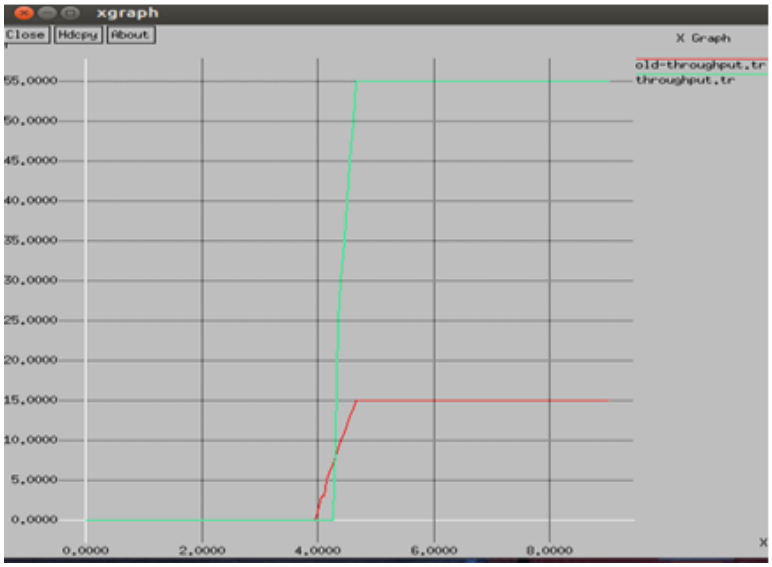

Fig: 5 Throughput Comparison at the time of attack and after avoidance of attack

X axis represented the time in milliseconds and Y axis represents the no. of packets. Above figure represents that throughput is increased after the avoidance of attack as compared to the time of attack. In this green line represents the increased level of throughput after the removal of attack and red line represents lesser throughput at the time of attack.

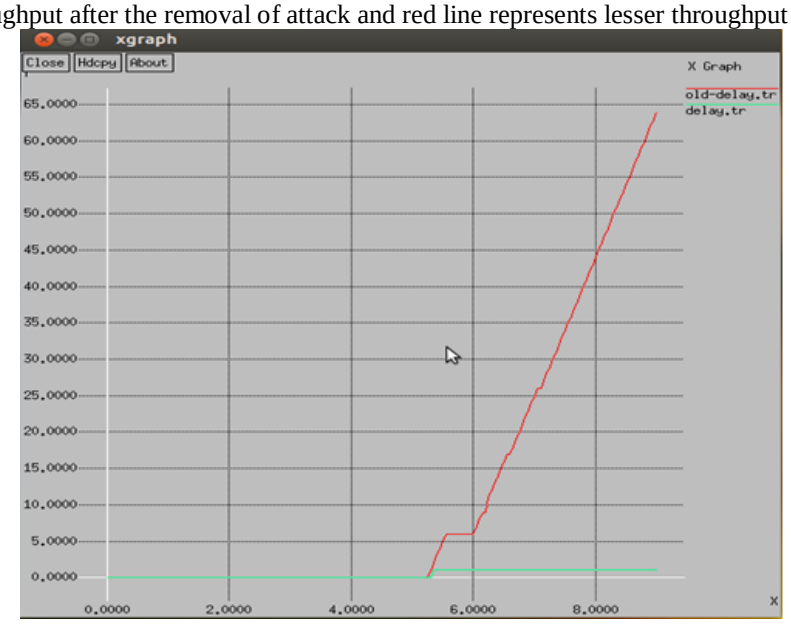

Fig: 6 Comparison of Delay at the time of attack and after the avoidance of attack

X axis represents the time in mili seconds and Y axis represents the no. of packets. Above figure represents that Delay is lessor after the avoidance of attack as compared to the time of attack. In this green line represents the lesser delay after the removal of attack and red line represents more or highest delay at the time of attack.

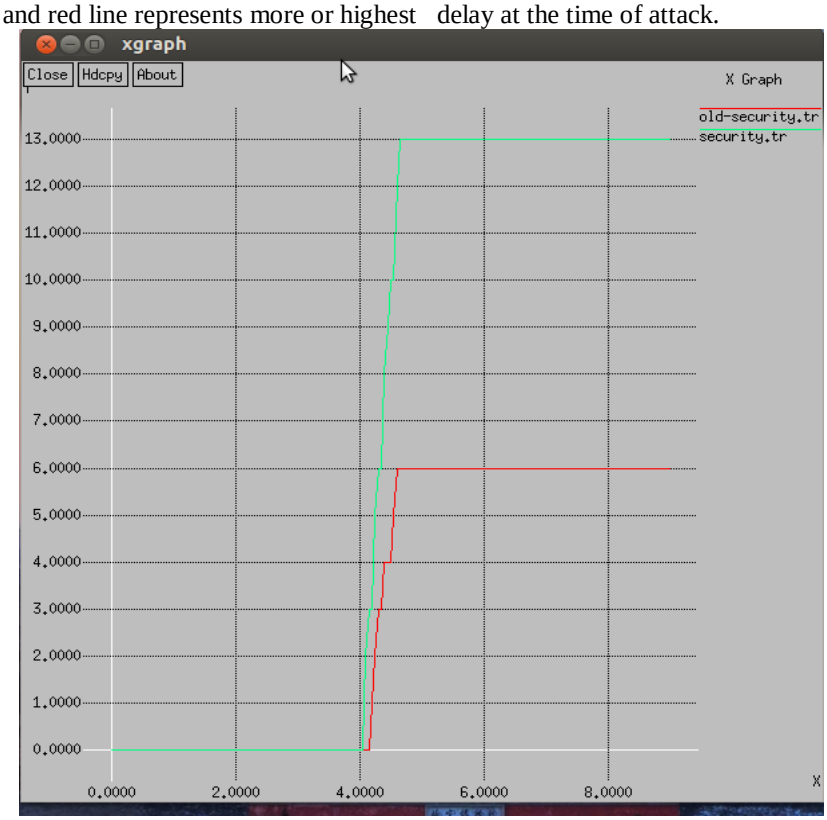

Fig: 7 Security levels comparison at the time of attack and after avoidance of attack

X axis represents the time in mili seconds and Y axis represents the Levels of security (no of vulnerabilities). Above figure represents that Security level is increased after the avoidance of attack as compared to the time of attack. In this green line represents the increased level of security after the removal of attack and red line represents more lowest level of security at the time of attack.

VI. CONCLUSION AND FUTURE SCOPE

Cloud computing provides a many types of services and benefits to its users but there are some security issues are there which makes the user unstable about the efficiency , safety and reliability in cloud computing. A proposed technique is asymmetric key cryptography based improved RSA technique. In a proposed work only the legitimate user can access there services. This technique is based on the both side verification process. In this technique illegitimate users are detected and isolate from the network to prevent the zombie attack in a cloud architecture. In this paper a novel technique is proposed which is more efficient as it increases the performance of system. In a future work such algorithm with hybrid message authentication code technique is can be applied on integrity of data to prevent a man in middle attack for multi tenants.

REFERENCES

[1] **A Akinbi, E. Pereira, C. Beaumont (2013)** *"Identifying Security Methods and Controls for Secure PaaS Cloud Environments"* International Journal of Emerging Technology and Advanced Engineering.

[2] **Chen Danwei, Huang Xiuli, and Ren Xunyi (2011)** "Access Control of Cloud Service Based on UCON" Nanjing University of posts & Telecommunications.

[3] **Logica Banica, Emil Burtescu, Cristian Stefan (2014)** "Advanced Security Model for Cloud Infrastructures", Journal of Emerging Trends in Computing & Information Science,(Vol 5, June 2015) ISSN NO: 2079-8407

[4] **Dr. Santosh Lomte , Shraddha DUdhani (2015)** " Secure Key for Authentication & Secret Sharing In Cloud Computing " , International Journal of Advance Research in Computer science and Software engineering, (vol 5, June 2015) ISSN NO: 2277428X.

[5] **Priti Bali (2014)** "Comparative Study of Private and Public Key Cryptography Algorithms A Survey" , International Journal of Research in Engineering & Technology, (vol 3, Sep 2014) ISSN NO: 23191163.

[6] **Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun & Dijiang Huang (2013)** "Network intrusion detection and counter measure selection in virtual network systems" August 2013

[7] **Chirag N. Modi and Dhiren Patel (2013)** "A Novel Hybrid-Network intrusion detection system in cloud computing" 2013

[8] **Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013)** *"An analysis of security issues for cloud computing"*2013

[9] **Jian Yu, Quan Z. Sheng, Yanbo Han (2013)** *"Introduction to special issue on cloud and service computing"* 26 April 2013

[10] **Joel Gibson, Darren Eveleigh, Robin Rondeau and Qing Tan (2012)** *"Benefits and Challenges of Three Cloud Computing Service Models"*2012 IEEE

[11] **Mohammed A. AlZain #, Eric Pardede #, Ben Soh #, James A. Thom* (2012)** *"Cloud Computing Security: From Single to Multi-Clouds"* 2012 45th Hawaii International Conference.

[12] **Anas BOUA Y AD, Asmae BLILA T, Nour el houda MEJHED, Mohammed EL GHAZI (2012)** "*Cloud computing : security challenges"*2012 IEEE.

