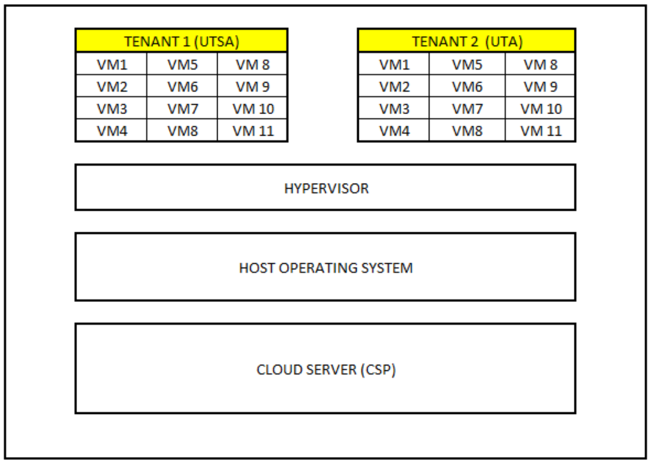
FINAL PROJECT REPORT

NAME: RUSHIKESH JAGDALE
SAWANI SOMAN

Cloud Infrastructure as a Service using Kerberos

The project proposes implementation of Kerberos authentication for Cloud Infrastructure as a Service for Role Based Access Control (RBAC) protocol. It is necessary to identify the possible cloud threats in order to implement better security mechanisms to protect cloud computing environments. Different attacks on Cloud Infrastructure as a Services like Openstack may face are brute force attack, privilege escalation attack, side channel attack and replay attack. These attacks may lead of entire cloud breach. This can be improvised by mutual authentication protocol named Kerberos which is based on Needham Shroeder Protocol. This gives strength to cloud identity services like Keystone in Openstack.

The basic working of Needham Shroeder protocol is dependent on Key Distribution Center (KDC). In real world keys are not directly shared between entities. So in order to communicate and have a session key; key distribution center is required. KDC generates session key maintaining all the user ID and their respective keys.



TENANT 1 (UTSA)		
VM1	VM5	VM 8
VM2	VM6	VM 9
VM3	VM7	VM 10
VM4	VM8	VM 11

TENANT 2 (UTA)		
VM1	VM5	VM 8
VM2	VM6	VM 9
VM3	VM7	VM 10
VM4	VM8	VM 11

Fig (1) Basic Cloud IaaS Architecture

Different threats that need to be addressed in Cloud IaaS are explained below:

(1) Side Channel Attack: - In Cloud IaaS, it is possible to identify the particular target VM (virtual machine) in internal cloud infrastructure and then placed new VM with targeted VM and extract confidential information from targeted VM on same physical machine called as simple side channel attack. In side channel attack, attacker takes advantage of a shared physical component (e.g. the processor cache) in order to steal information (e.g. a cryptographic key) from the victim.[1]

Side channel attack requires two main steps: Placement and Extraction. Placement refers to the adversary or attacker arranging to place their malicious VM on the same physical machine. Extraction: After successfully placement of the malicious VM to the targeted VM extract the confidential information, file and documents on the targeted VM.

Following figures shows the side channel attack: -

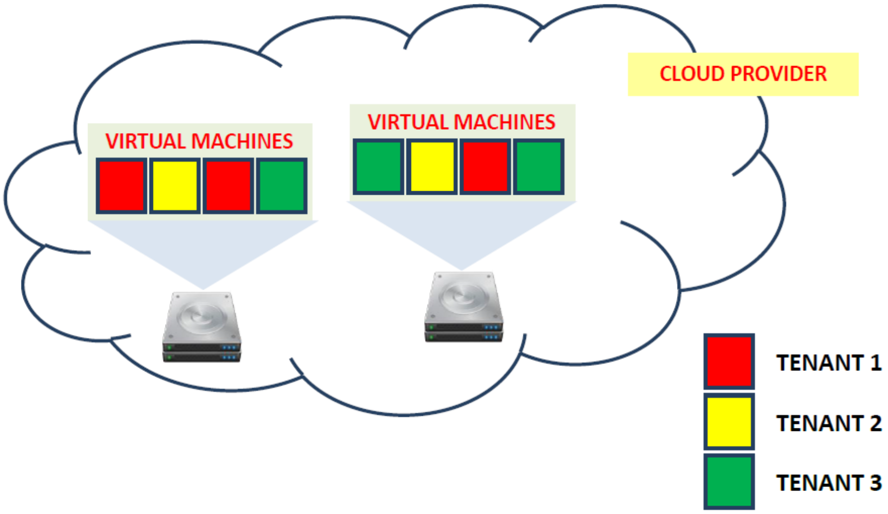


Fig (2) Side Channel Attack [5]

(2) Brute Force Attack: - A brute force attack is a technique used to break passwords. The success of this attack is greatly reliant on powerful computing capability because thousands of possible passwords are needed to be sent to a target user's account until it finds the correct one to access. Cloud computing system provides a perfect platform for hackers to launch this type of attack.

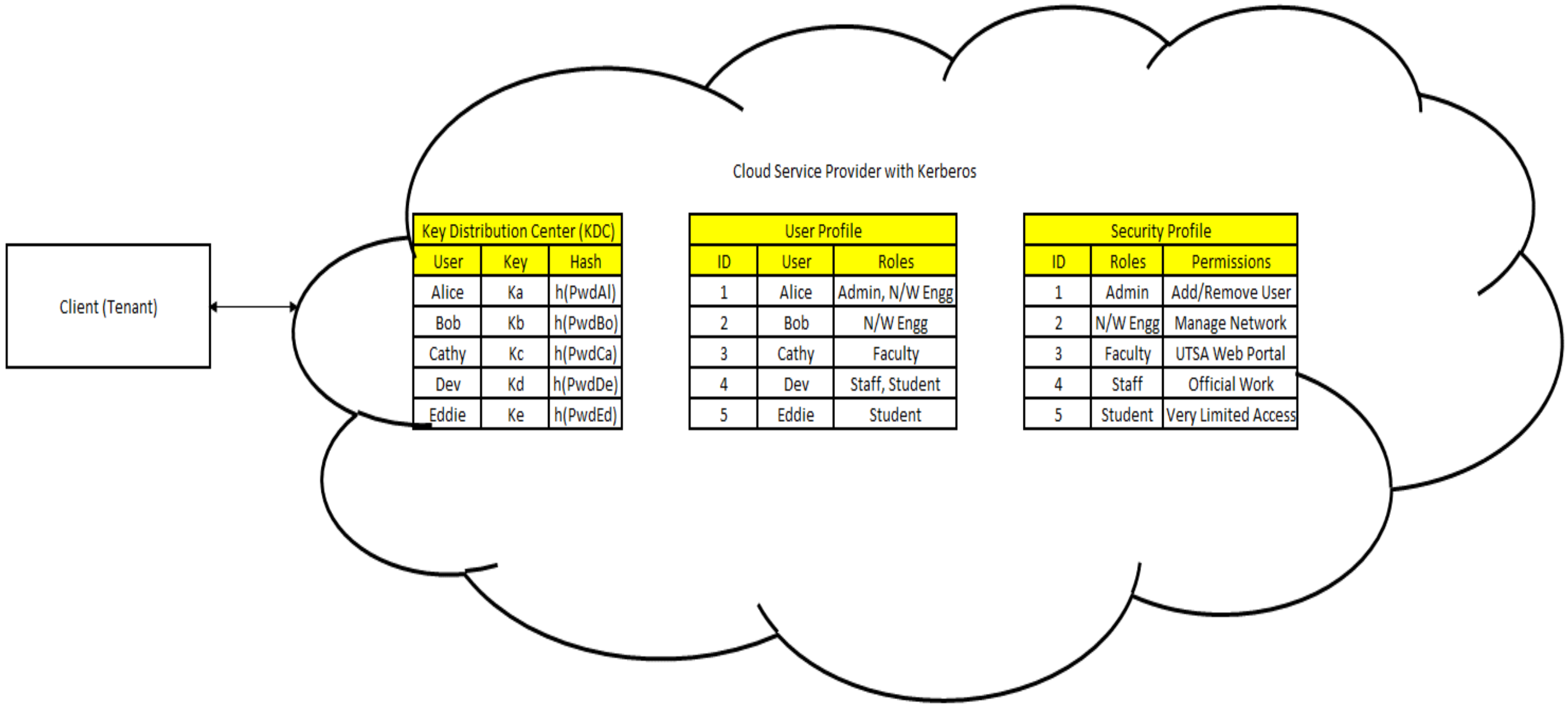
(3) Privilege Escalation Attack: - A privilege escalation attack is a type of network intrusion that grant the attacker elevated access to the network and its associated data and applications. There are two kinds of privilege escalation attacks: - Vertical and Horizontal.

Vertical privilege escalation: - It requires the attacker to grant himself higher privileges. This is typically achieved by performing kernel-level operations that allow the attacker to run unauthorized code.

Horizontal privilege escalation: - It requires the attacker to use the same level of privileges he already has been granted, but assume the identity of another user with similar privileges. For example, someone gaining access to another person's online banking account would constitute horizontal privilege escalation.

(4) Replay Attack: - A replay attack occurs when an attacker copies a stream of messages between two parties and replays the stream to one or more of the parties.

(5) Active Directory Password Breach: -In openstack the password is stored in openrc file and also required while login. When using the command line clients, the users had the choice of storing their password in environment variables such as with the local openrc script or re-typing their password with each OpenStack command. Passwords in environment variables has significant security risks since they are passed to any sub-command and can be read by the system administrator of the server you are on. [2]



Key Distribution Center (KDC)		
User	Key	Hash
Alice	Ka	h(PwdAl)
Bob	Kb	h(PwdBo)
Cathy	Kc	h(PwdCa)
Dev	Kd	h(PwdDe)
Eddie	Ke	h(PwdEd)

User Profile		
ID	User	Roles
1	Alice	Admin, N/W Engg
2	Bob	N/W Engg
3	Cathy	Faculty
4	Dev	Staff, Student
5	Eddie	Student

Security Profile		
ID	Roles	Permissions
1	Admin	Add/Remove User
2	N/W Engg	Manage Network
3	Faculty	UTSA Web Portal
4	Staff	Official Work
5	Student	Very Limited Access

Fig (3) Proposed Cloud IaaS Architecture

Solution to previously mentioned threats in Cloud IaaS: -

(1) How to avoid Side Channel Attack?

Firewall is a set of related programs that protects the resources of users from other networks and intruders or adversaries. It is possible to adversaries or intruders identify the targeted VM in cloud infrastructure and then instantiate new VM to targeted VM and extract confidential information but virtual firewall prevent this placement step of side channel.

Random encryption and decryption can be implemented to prevent side channel attack. Random encryption and decryption implements AES, 3DES and DES algorithm in order to encrypt client's confidential data.

Combination of virtual firewall and random encryption-decryption algorithm provides security against side channel attack

(2) How to avoid Brute Force Attack?

Brute force attack can be avoided by implementing account lockout threshold policy. The Account lockout threshold policy setting determines the number of failed sign-in attempts that will cause a user account to be locked. A locked account cannot be used until it is reset by an administrator or until the number of minutes specified by the Account lockout duration policy setting expires.[6]

Brute Force attack can also be prevented by implementing a Completely Automated Public Turing test to tell Computers and Humans Apart, or CAPTCHA. It is a program that allows you to distinguish between humans and computers. [4]

(3) How to avoid Privilege Escalation Attack?

RBAC, system administrators create roles according to the job functions performed in a company or organization, grant permissions (access authorization) to those roles, and then assign users to the roles on the basis of their specific job responsibilities and qualifications

A role can represent specific task competency, such as that of a physician or a pharmacist. A role can embody the authority and responsibility of, say, a project supervisor. Authority and responsibility are distinct from competency. A person may be competent to manage several departments but have the responsibility for only the department actually managed. Roles can also reflect specific duty assignments rotated through multiple users—for example, a duty physician or a shift manager. RBAC models and implementations should conveniently accommodate all these manifestations of the role concept.

Roles define both the specific individuals allowed to access resources and the extent to which resources are accessed. For example, an operator role might access all computer resources but not change access permissions; a security-officer role might change permissions but have no access to resources; and an auditor role might access only audit trails. Roles are used for system administration.

Thus in the above shown Cloud IaaS architecture different tables are stored in the cloud service provider database also known as security profile catalog are used to check the user roles and the permissions or operations user has. Also CSP has the user profile catalog that defines the roles of the user.

(4) How to avoid Replay Attack?

A replay attack can be eliminated by using time stamps instead of nonce while authenticating a user. This can be achieved by using Kerberos authentication protocol which also provides mutual authentication. Kerberos can be used by the cloud service provider as security server for authentication and authorization of a client.

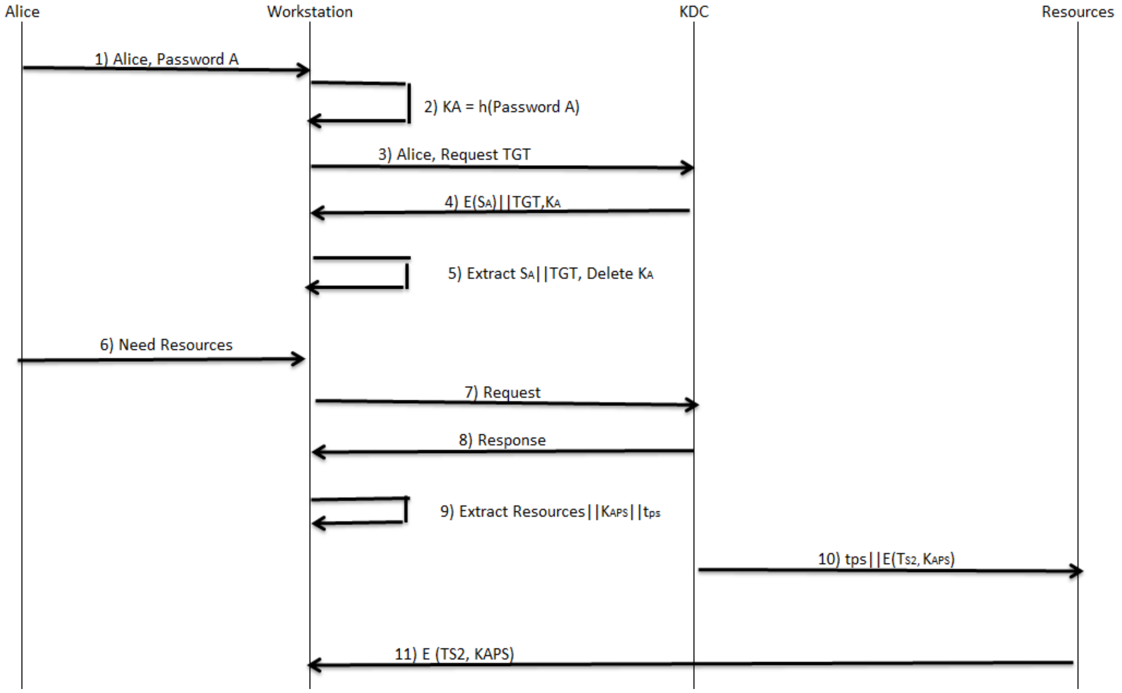


Fig (5) Working of Kerberos Authentication Protocol

In the architecture when a client ask a request to KDC for communication to a resource server on a CSP, KDC will generate TGT and provide a session key to communicate with the server. Before providing the session key security server will also check the role of the client and if the permissions are available to the client KDC will provide the session key.

(5) How to avoid Active Directory Password Breach?

Active Directory Password Breach can also be prevented using the Kerberos protocol. This can be achieved by implementing session key between the cloud service provider server and client. In this way system administrator will not be able to breach into the VM of a client.

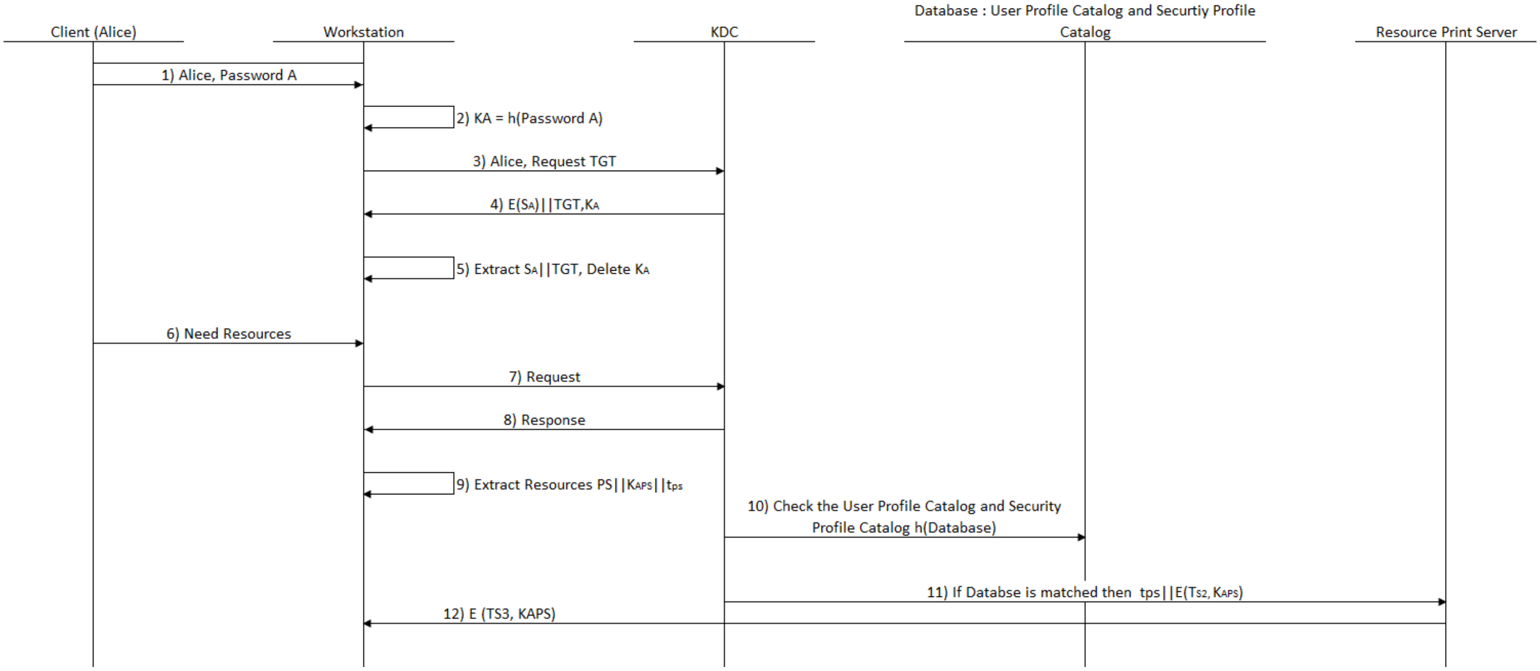

Client (Alice)
Workstation
KDC
Database : User Profile Catalog and Securtiy Profile Catalog
Resource Print Server
1) Alice, Password A
2) KA = h(Password A)
3) Alice, Request TGT
4) E(SA)||TGT,KA
5) Extract SA||TGT, Delete KA
6) Need Resources
7) Request
8) Response
9) Extract Resources PS||KAPS||tps
10) Check the User Profile Catalog and Security Profile Catalog h(Database)
11) If Databse is matched then tps||E(TS2, KAPS)
12) E (TS3, KAPS)

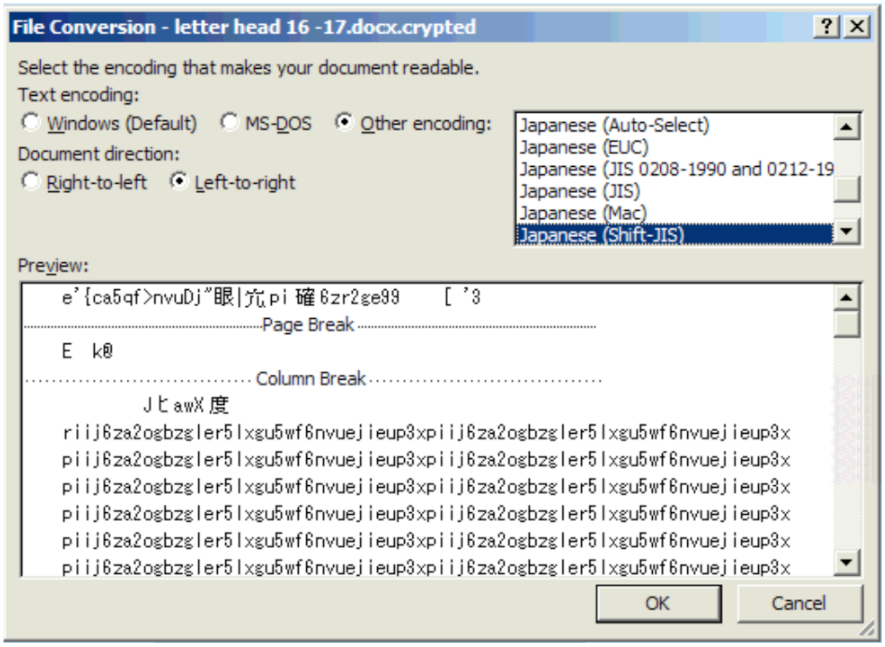
Fig (6) Working of Cloud IaaS with Kerberos Authentication Protocol

Pseudo Code for implementing proposed Cloud IaaS with Kerberos Authentication Protocol

1. Alice Enters password in her workstation.
2. When her password is matched with hash value of her password, she can access her work station
3. Alice request CSP for TGT in order to establish communication between other resources available on CSP
4. Security server of CSP will ask KDC to generate session key S_A and provide TGT to Alice
5. Alice will extract the message received from KDC using her key K_A and delete K_A
6. Upon establishing connection between KDC and Alice, she can ask for resources of CSP
7. Alice will request KDC to access some resources like print server to KDC
8. Security server will check the user profile and security profile database before giving any access to Alice.
9. If Alice requested for resources according to her capabilities, KDC will send appropriate ticket to Alice or else will not allow her to access the resources.
10. If the database matches with the requirements of Alice, KDC will send ticket to respective resource server along with the session key between Alice and Resource Server
11. Resource server can challenge Alice using session key in order to have mutual authentication.

Other threats observed in the cloud architecture are as follows:

1. Ransomware attack: - In this attack, all the files of the victim server are encrypted using public key system. This kind of attack takes place due to malware injection in the system



File Conversion - letter head 16 -17.docx.crypted

Select the encoding that makes your document readable.

Text encoding:

○ Windows (Default) ○ MS-DOS ● Other encoding:

Document direction:

○ Right-to-left ● Left-to-right

Japanese (Auto-Select)
Japanese (EUC)
Japanese (JIS 0208-1990 and 0212-19
Japanese (JIS)
Japanese (Mac)
Japanese (Shift-JIS)

Preview:

```
    e’{ca5qf>nvuDj”眼|宂pi 確6zr2ge99    [ ’3
..........................Page Break..........................
    E  k@
.........................Column Break.........................
           JヒawX度
    riij6za2ogbzgler5lxgu5wf6nvuejieup3xpiij6za2ogbzgler5lxgu5wf6nvuejieup3x
    piij6za2ogbzgler5lxgu5wf6nvuejieup3xpiij6za2ogbzgler5lxgu5wf6nvuejieup3x
    piij6za2ogbzgler5lxgu5wf6nvuejieup3xpiij6za2ogbzgler5lxgu5wf6nvuejieup3x
    piij6za2ogbzgler5lxgu5wf6nvuejieup3xpiij6za2ogbzgler5lxgu5wf6nvuejieup3x
    piij6za2ogbzgler5lxgu5wf6nvuejieup3xpiij6za2ogbzgler5lxgu5wf6nvuejieup3x
    piij6za2ogbzgler5lxgu5wf6nvuejieup3xpiij6za2ogbzgler5lxgu5wf6nvuejieup3x
```

Fig (7) Ransomware Attack

2. DOS (Denial of Service Attack): This attack happens due to flooding of request to the system and flooding of resources. When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more virtual machines, more service instances) to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power), but actually to some extent even supports the attacker by enabling him to do most possible damage on a service’s availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service. [3]

3. Malicious Injection Attack: - A first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system. A promising countermeasure approach to this threat consists in the Cloud system performing a service instance integrity check prior to using a service instance for incoming requests. This can e.g. be done by storing a hash value on the original service instance’s image file and comparing this value with the hash values of all new service instance images. Thus, an

attacker would be required to trick that hash value comparison in order to inject his malicious instances into the Cloud system. [3]

References:

[1] Bhrugu Sevak (December 2012). Security against Side Channel Attack in Cloud Computing", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-2,

[2] http://openstack-in-production.blogspot.com/2014/10/kerberos-and-single-sign-on-with.html

[3] Singh, A., & Shrivastava, M. (2012). Overview of security issues in cloud computing.*International Journal of Advanced Computer Research*, *2*(1), 41-41.

[4] https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

[5] https://elastic-security.com/2013/09/11/how-to-detect-side-channel-attacks-in-cloud-infrastructures/

[6] Chou, T. (2013). security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology, 5(3), 79-79.