International Journal of Research in
Engineering & Technology (IJRET)
ISSN 2321-8843
Vol. 1, Issue 2, July 2013, 1-10
© Impact Journals

A SURVEY ON SECURITY ISSUES AND COUNTERMEASURES IN CLOUD COMPUTING STORAGE AND A TOUR TOWARDS MULTI-CLOUDS

A. PRIYADHARSHINI

PG Scholar, Department of CSE, Shreenivasa Engineering College, Dharmapuri, Tamil Nadu, India

ABSTRACT

Cloud Computing is an agile, reliable, cost effective and scalable method for delivery of computing and delivery of data. End users access cloud based applications through a web browser or a lightweight desktop or mobile app while the business software and data are stored on servers at a remote location. Cloud Computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. This paper focus on security issues and the countermeasures in cloud computing storage. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions introduce a heavy computation overhead. This paper eliminates the computation overhead in countering the security issues in cloud storage by using Kerberos authentication mechanism and address the need for moving to multi-clouds.

KEYWORDS: Clouds, Multi Clouds, Kerberos, Kerberos Realms

INTRODUCTION

The use of cloud computing has increased rapidly in many organizations. Cloud computing is a resource delivery and usage model, it means get resource(Hardware, Software)via network. The network of providing resource is called ‘cloud’. The hardware resource in the ‘cloud’ seems scalable infinitely and can be used whenever. Cloud computing is an emerging technology which play a vital role in effective implementation of a lower cost. Today’s dynamic environment of changing needs require on demand location independent computing services which include software, platform and scalable infrastructure. The cloud computing can provide such an environment for optimum utilization of resources.

Types of Clouds

In providing a secure cloud computing solution, a major decision is to decide on the type of cloud to be implemented. Cloud Deployment Models

Public Cloud

A public cloud is one which allows user’s to access the cloud via interface using mainstream web browsers. It is based on pay-per-use model, similar to a electricity metering system. Public clouds are less secure than the other cloud models because it places an addition a burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

Private Cloud

A private cloud is set up within an organization’s internal enterprise data center. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud.

Hybrid Cloud

A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. Hybrid clouds provide more secure control of the data and applications and allows various parties to access information over the Internet.

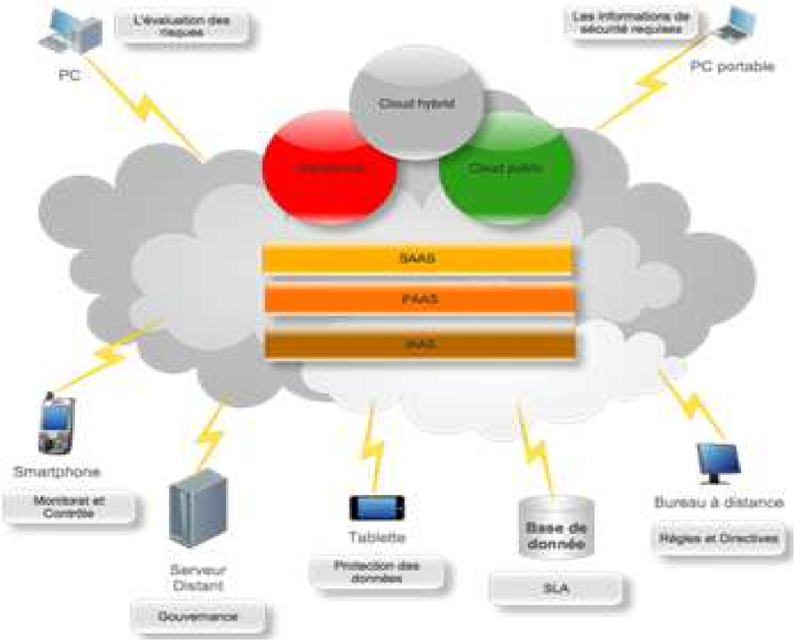


Figure 1: Cloud Computing Map

Cloud Computing Delivery Models

Cloud computing can be categorized according to three types of delivery models, namely Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS).

Infrastructure as a Service (IaaS)

IaaS is a single cloud layer where the cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee.

Software as a Service (SaaS)

SaaS also operates on the virtualized and pay-per-use costing model whereby software applications are leased out to contracted organizations by specialized SaaS vendors SaaS applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Web Services(WS) security, Extensible Markup language(XML) encryption, Secure Socket Layer(SSL) and available options which are used in enforcing data protection transmitted over the Internet..

Platform as a Service (PaaS)

PaaS works like IaaS but it provides an additional level of "rented" functionality Virtual machines are used. Virtual machines must be protected against malicious attacks.

INFORMATION SECURITY REQUIRMENTS

Figure 2 describes various information security requirements for both cloud delivery models and cloud deployment models.

Identification and Authentication

In cloud computing, depending on the type of cloud as well as the delivery model, specified users must firstly be established and supplementary access priorities and permissions may be granted accordingly. This process is targeting at verifying and validating cloud users by employing usernames and passwords to their cloud profiles.

Authorisation

It is an important information security to ensure referential integrity is maintained. It is maintained by the system administrator in a private cloud.

Confidentiality

In cloud computing, confidentiality plays a major part especially in maintaining control over organisation's data situated across multiple distributed databases.

Integrity

ACID (Automicity, Consistency, Isolation and Durability) properties of the cloud's data should without a doubt be robustly imposed across all cloud computing delivery models.

Non-Repudiation

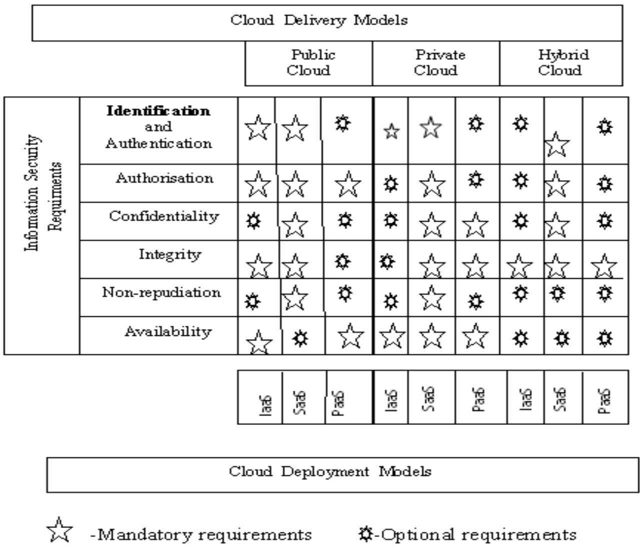
Non-repudiation can be obtained by applying e-commerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services.

Availability

The service Level Agreement (SLA)is the most important document which highlights the availability in cloud services and resources between the cloud provider and client.

Key Issues in Cloud Computing

- Where is the data?
- Who has access to the data?
- What are the regulatory requirements?
- Whether the user have the Right to Audit?
- What type of training does the provider offer their employees?
- What type of data classification system does the provider use?
- What are the Service Level Agreement(SLA) terms?
- What is the Long-term viability of the provider?
- What happens if there is a security breach?
- What is the disaster recovery/Business continuity plan?



		Cloud Delivery Models								
		Public Cloud			Private Cloud			Hybrid Cloud		
Information Security Requirments	**Identification** and Authentication	☆	☆	✲	☆	☆	✲	✲	☆	✲
	Authorisation	☆	☆	☆	✲	☆	✲	✲	☆	✲
	Confidentiality	✲	☆	✲	✲	☆	☆	✲	☆	✲
	Integrity	☆	☆	✲	✲	☆	☆	☆	☆	☆
	Non-repudiation	✲	☆	✲	✲	☆	✲	✲	✲	✲
	Availability	☆	✲	☆	☆	☆	☆	✲	✲	✲
		IaaS	SaaS	PaaS	IaaS	SaaS	PaaS	IaaS	SaaS	PaaS
		Cloud Deployment Models								

☆ -Mandatory requirements ✲-Optional requirements

Figure 2: Cloud Computing Security Requirements

THREATS TO SECURITY IN CLOUD COMPUTING

The chief concern in cloud environments is to provide security around multi-tendancy and isolation, given customers more comfort besides “trust-us” idea of clouds.

Basic Security Issues

- **SQL Injection Attacks:** Are the one in which a malicious code is inserted into a standard SQL code and thus the attackers gains unauthorized access to the database and can able to access sensitive information.
- **Countermeasure:** Avoiding the usage of dynamically generated SQL code, using filtering techniques to sanitize the user input etc.

Cross Site Scripting (XSS) Attacks

Which injects malicious scripts into web contents.

- **Countermeasures:** Active content filtering, Content based data leakage prevention technology, Web application vulnerability detection technology.

Man in the Middle Attacks (MITM)

k, an intruder tries to intrude in an ongoing conversation between a sender and a client to inject false information and to have knowledge of the important data transferred between them.

- **Countermeasure:** Evaluation software as a service security, separate end point and server security processes.

Network Level Security Issues

- **DNS Attacks:** A Domain Name Server(DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible.

Countermeasures

Domain Name System security extensions reduces the effects of DNS threats.

- **Sniffer Attacks:** These attacks are launched by applications that can capture packets flowing in a network and if the data is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured.

Countermeasures

A malicious sniffing detection platform based on ARPC(Address resolution protocol) and RTT(Round trip time) can be used to detect a sniffing system running on a network.

- **Issue of Reused IP Addresses:** Each node of a network is provided an IP address and hence an IP address is basically a finite quantity. When a particular user moves out of a network then the IP address associated with him (her) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time la between the change of an IP address in DNS and the clearing of that address in DNS caches.

- **BGP Prefix Hijacking:** BGP (Border Gateway Protocol) prefix hijackin is a type of network attack in which a wrong announcement related to the IP addresses associated with an Autonomous systems(AS) is made and hence malicious parties get access to the untraceable IP addresses.

Application Level Security Issues

- **Security Concerns with the Hypervisor:** Cloud computing rests mainly on the concept of virtualization. In a virtualized world, hypervisor is defined as a controller popularly known as virtual machine manager (VMM) that allows multiple operating systems to be run on a system at a time, providing the resources to each operating system such that they do not interfere with each. As number of operating systems running on a hardware unit increase, the security issues concerned with those that of new operating systems also need to be considered.

- **Denial of Service Attacks:** A DOS attack is an attempt to make the services assigned to the authorized users unable to be used by them. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user.

Countermeasure

Intrusion Detection System is the most popular method of defence against this type of attacks.

- **Cookie Poisoning:** It involves changing or modifying the contents of cookie to make unauthorized access to an application or to a webpage.

Countermeasure

This can be avoided either by performing regular cookie cleanup or implementing an encryption scheme for the cookie data.

- **Hidden Field Manipulation:** While access in a web-page, there are certain fields that are hidden and contain the page related information and basically used by developers. However, these fields are highly prone to a hacker attacker as they can be modified easily and posted on the web-page. This may result in severe security violations.

- **Backdoor Attacks:** A common habit of the developers is to enable the debug option while publishing a web-site. This enables them to make developmental changes in the code and get them implemented in the web-site. Since these debug options facilitate back-end entry to the developers, and sometimes these debug options are left enabled unnoticed, this may provide an easy entry to a hacker into the website and let him make changes at the web-site level.

- **Distributed DOS Attacks:** DDOS may be called an advanced version of DOS in terms of denying the important services running on a server by flooding the destination server with number of packets such that the target server is not able to handle it. In DDOS the attack is relayed from different dynamic networks which have already been compromised unlike DOS. The attackers have the power to control the flow of information by allowing some information available at certain times. Thus the amount and type of information available for public usage is clearly under the control of the attacker.

Countermeasure

Intrusion Detection System.

- **CAPTCHA Breaking:** CAPTCHA's were developed in order to prevent the usage of internet resources by bots or computers. They are used to prevent spam and over exploitation of network resources by bots. Even the multiple web-site registrations, dictionary attacks etc by an automated program are prevented using a CAPTCHA. But recently, it has been found that the spammers are able to break the CAPTCHA, provided by the Hotmail and G-mail service providers.
- **Google Hacking:** Google has emerged as the best option for finding details regarding anything on the net. Google hacking refers to using Google search engine to find sensitive information that a hacker can use to his benefit while hacking a user's account.

KERBEROS AUTHENTICATION MECHANISM

To overcome all the attacks and the computation overhead caused by the above solution the service providers must allow only authenticated users Kerberos authentication mechanism is used.

Kerberos

Kerberos is an authentication service that enables clients and servers/cloud service providers to establish authenticated communication.

Requirements

- **Secure:** Kerberos should be strong enough to protect weak link from opponent.
- **Reliable:** Kerberos should be highly reliable with one system able to back up another.
- **Transparent:** The client/user should not be aware that authentication taking place, expect to enter a password for login.
- **Scalable:** The system should be capable of supporting large number of clients and service providers.

Kerberos Authentication Dialogue

This is the actual Kerberos protocol .Kerberos consists of

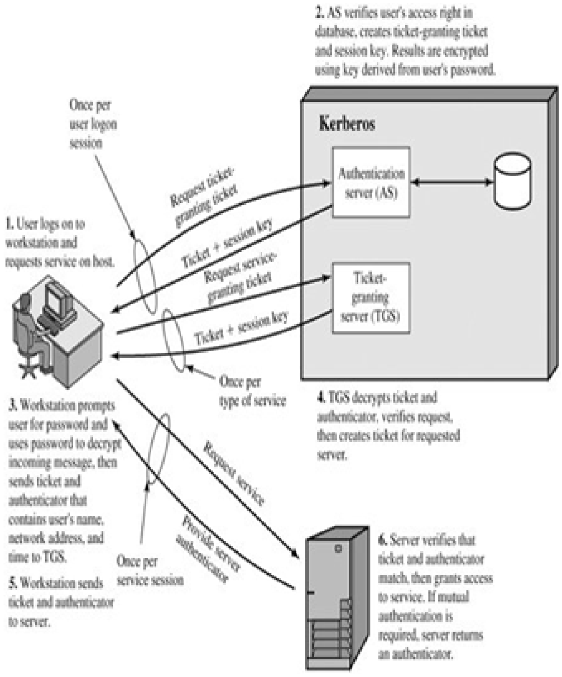
- **Authentication Server (AS):** AS checks whether the user/client is authenticated by searching the user name and password in the database. It provides ticket to access TGS.
- **Ticket Granting Server (TGS):** The client who needs the service from the cloud service provider request service granting ticket from the TGS using the ticket obtained from the authentication server.

An efficient way of accomplishing this is to use an encryption key as the secure information. This is referred to as session key in Kerberos.

Figure 3 provides a simplified overview of the action. The actions to be performed by Kerberos are as follows.

Step 1: Client/User logs on to workstation and requests service on cloud.

Step 2: AS verifies users access right in its database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.


2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
Kerberos
Authentication server (AS)
Ticket-granting server (TGS)
Once per user logon session
Request ticket-granting ticket
Ticket + session key
Request service-granting ticket
Ticket + session key
1. User logs on to workstation and requests service on host.
Once per type of service
3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.
4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.
Request service
Provide server authenticator
Once per service session
5. Workstation sends ticket and authenticator to server.
6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

Steps 1 and 2-Once per user logon session
Steps 3 and 4-Once per type of service
Steps 5 and 6-Once per service session

Figure 3: Overview of Kerberos

Step 3: Workstation prompts user/client for password and uses password to decrypt incoming message, then sends ticket and authenticator that contain client's name, network address and time to TGS.

Step 4: TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.

Step 5: Workstation sends ticket and authenticator to server.

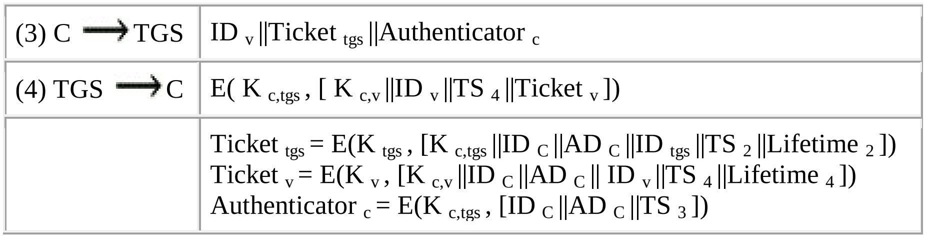
Step 6: Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

The dialogue is as follows,

Authentication Service Exchange: to obtain ticket-granting ticket

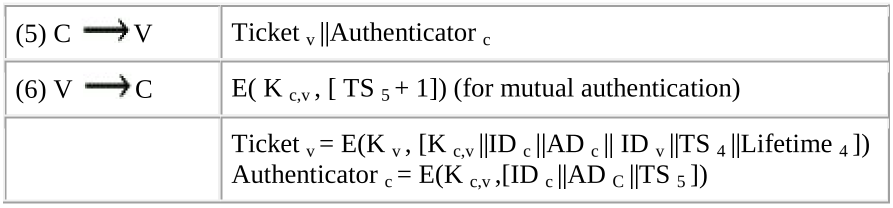
(1) C $\longrightarrow$ AS	$ID_c \| ID_{tgs} \| TS_1$
(2) AS $\longrightarrow$ C	$E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$
	$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_c \| AD_c \| ID_{tgs} \| TS_2 \| Lifetime_2])$

Ticket-Granting Service Exchange: to obtain service-granting ticket



(3) C ⟶ TGS	ID $_{v}$ ||Ticket $_{tgs}$ ||Authenticator $_{c}$
(4) TGS ⟶ C	E(K $_{c,tgs}$, [K $_{c,v}$ ||ID $_{v}$ ||TS $_{4}$ ||Ticket $_{v}$])
	Ticket $_{tgs}$ = E(K $_{tgs}$, [K $_{c,tgs}$ ||ID $_{C}$ ||AD $_{C}$ ||ID $_{tgs}$ ||TS $_{2}$ ||Lifetime $_{2}$]) Ticket $_{v}$ = E(K $_{v}$, [K $_{c,v}$ ||ID $_{C}$ ||AD $_{C}$ || ID $_{v}$ ||TS $_{4}$ ||Lifetime $_{4}$]) Authenticator $_{c}$ = E(K $_{c,tgs}$, [ID $_{C}$ ||AD $_{C}$ ||TS $_{3}$])

Client/Server Authentication Exchange: to obtain service



(5) C ⟶ V	Ticket $_{v}$ ||Authenticator $_{c}$
(6) V ⟶ C	E(K $_{c,v}$, [TS $_{5}$ + 1]) (for mutual authentication)
	Ticket $_{v}$ = E(K $_{v}$, [K $_{c,v}$ ||ID $_{c}$ ||AD $_{c}$ || ID $_{v}$ ||TS $_{4}$ ||Lifetime $_{4}$]) Authenticator $_{c}$ = E(K $_{c,v}$,[ID $_{c}$ ||AD $_{C}$ ||TS $_{5}$])

where

C	= client
AS	= authentication server
V	=service provider
ID $_{C}$	= identifier of C
ID $_{V}$	= identifier of V
ID $_{tgs}$	= identifier of TGS
AD $_{C}$	= network address of C
K $_{c ,v}$	= secret encryption key shared by C and V
K $_{c,tgs}$	=secret encryption key shared by C and TG

The steps are

Step 1: Client requests AS to access TGS.

Step 2: Now AS responds with a message encrypted with a key derived from the user’s password (K_C) that contains Ticket$_{tgs}$ and session key $K_{c,tgs}$. So the user C can only able to read this message. The Ticket$_{tgs}$ is encrypted by K_{tgs}. This Ticket $_{tgs}$ is reusable per user logon session.

Step 3: C requests TGS to obtain service granting ticket. This requests consists of ID $_{V}$, Ticket$_{tgs}$ and Authenticator$_{C}$. This authenticator is not reusable and has a very short lifetime and encrypted by $K_{c,tgs.}$

Step 4: TGS responds to C, to issue Ticket$_{V}$, for access server V, encrypted with K $_{c,tgs}$. The Ticket$_{V}$ consists of session key $K_{c ,v}$.

Step 5: Now the user C sends the request to V to obtain service. This request includes Ticket$_{V}$ and Authenticator$_{C}$. (which is encrypted using K $_{c ,v}$)

Step 6: For mutual authentication, the a ender V sends a message to C which is the value of timestamp from the authenticator incremented by 1 and encrypted with the session key K $_{c ,v}$.

In steps 1and 2,the session key K $_{c ,tgs}$ has been securely delivered to both C and the TGS. In step 3 and 4,the session key K $_{c ,v}$ has been securely delivered to both C and Server V.

All of the messages from step 1 through step 6 use timestamp and lifetime values to prove that the messages is timely and not expired.

MULTICLOUDS

Dealing with “single cloud” providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards “multi-clouds”, “inter cloud” or “cloud-of-clouds”.

To provide authentication in multi-clouds Kerberos realms and multiple kerberi are used.

Kerberos Realms and Multiple Kerberi

A full service Kerberos environments consisting of a Kerberos server, a number of clients and a number of application servers requires the following,

- The Kerberos server must have user ID(UID) and hashed password of all participating user in its database. All users are registered with the Kerberos server.
- The Kerberos server must share a secret key with each server. All servers are registered with the Kerberos server.

Such an environment is referred to as a Realm. Networks of clients and servers under different administrative organizations typically has different realms. The user in one realm may need access to server in other realm. Some servers may be willing to provide service to users from other realms provided that those users are authenticated.

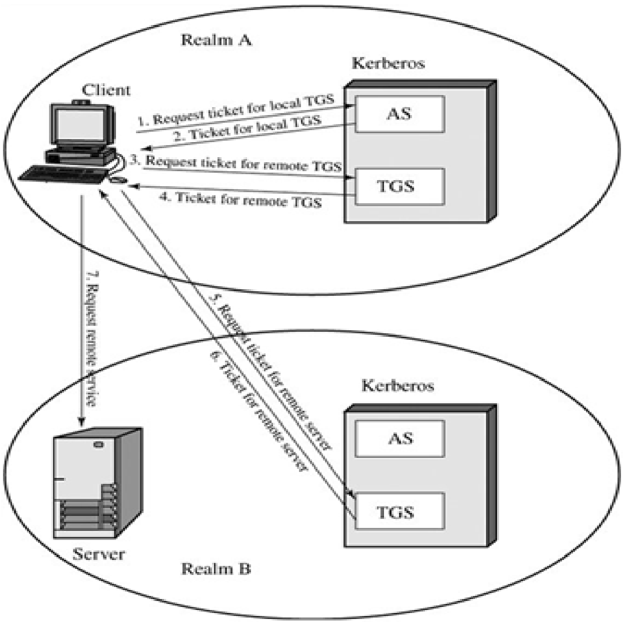

Realm A
Kerberos
Client
1. Request ticket for local TGS
2. Ticket for local TGS
3. Request ticket for remote TGS
4. Ticket for remote TGS
AS
TGS
7. Request remote service
5. Request ticket for remote server
6. Ticket for remote server
Kerberos
AS
TGS
Server
Realm B

Figure 4: Request for Service in another Realm

(1) $C \rightarrow AS$	$ID_c \Vert ID_{tgs} \Vert TS_1$
(2) $AS \rightarrow C$	$E(K_c, [K_{c,tgs} \Vert ID_{tgs} \Vert TS_2 \Vert Lifetime_2 \Vert Ticket_{tgs}])$
(3) $C \rightarrow TGS$	$ID_{tgsrem} \Vert Ticket_{tgs} \Vert Authenticator_c$
(4) $TGS \rightarrow C$	$E(K_{c,tgs}, [K_{c,tgsrem} \Vert ID_{tgsrem} \Vert TS_4 \Vert Ticket_{tgsrem}])$
(5) $C \rightarrow TGSr_{em}$	$ID_{vrem} \Vert Ticket_{tgsrem} \Vert Authenticator_c$
(6) $TGS_{rem} \rightarrow C$	$E(K_{c,tgsrem}, [K_{c,vrem} \Vert ID_{vrem} \Vert TS_5 \Vert Ticket_{vrem}])$
(7) $C \rightarrow V_{rem}$	$Ticket_{vrem} \Vert Authenticator_c$

CONCLUSIONS

A new approach is proposed that resolve security issues in cloud computing storage. It eliminates the computing overhead caused by other cryptographic methods. And this paper describes the reason for moving from single cloud to multiclouds. And the same Kerberos approach is used for multiclouds. And hence the computing overhead in countering security issues in cloud computing storage is minimized.

REFERENCES

1. “Toward Secure and Dependable Storage Services in Cloud Computing” Kui Ren, Senior Member, Cong Wang.
2. “Optimization of Resource Provisioning Cost in Cloud Computing” Sivadon Chaisiri, April-June 2012.
3. “A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems”, Journal of Emerging Trends in Computing and Information Sciences, June 2012.ion detection in wireless ad-hoc networks,”
4. “Information security Issue of Enterprises Adopting the Application of Cloud Computing”, Chang-Lung, Tsai Uei-Chin, Chin Lin Allen Y.Chang, Chun-Jung Chen.
5. “Ensuring Data Storage Security in Cloud Computing” Cong Wang and Kui Ren.
6. “The Management of Security in Cloud Computing”, Ramgovind S, Eloff, Smith E.
7. “A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding”, Hsiao-Ying Lin, Wen-Guey Tzeng,In Proceedings of IEEE Transaction on Parallel and Distributed Systems,pp.995-1003,Vol.23,Issue No.26,June 2012.
8. “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, In Proceedings of IEEE Transactions on Parrallel and Distributed Systems, Vol.22,Issue No.5,pp.847-859,May 2011.
9. “Toward Publicly Auditable Secure Cloud Data Storage Services”, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, In Proceedings of IEEE Network Magazine,Vol.24,Issue No.4,pp.19-24,July-August 2010.