Cloud Computing Security Framework

Privacy Security

Nassreldeen Ibrahim Eltayb
Information And Documentation Center, Africa City Of Technology
Act, Khartoum, Sudan
Naseros@Hotmail.Com

Prof. Osama Abdalwahab Rayis
General Manger Act
Act, Khartoum, Sudan
Rayis @Hotmail.Com

Abstract—Cloud computing is an emerging style of IT delivery that intends to make the Internet the ultimate home of all computing resources-storage, computations, and accessibility. It has an important aspect for the companies and organization to build and deploy their infrastructure and application. It changed the IT roadmap essential from service seeking infrastructure to infrastructure seeking services. It holds the promise of helping organizations because of its performance, high availability, least cost and many others. But the promise of the cloud cannot be fulfilled until IT professionals have more confidence in the security and safety of the cloud. Data Storage service in the cloud computing is easy as compare to the other data storage services. At the same time, cloud security in the cloud environment is challenging task. Security issues such as service availability, massive traffic handling, application security and authentication, ranging from missing system configuration, lack of proper updates, or unwise user actions from remote data storage. It can expose user's private data and information to unwanted access. It consider to be biggest problem in a cloud computing. The focus of this research consist on the secure cloud framework and to define a methodology for cloud that will protect user's data and highly important information from malicious insider as well as outsider attacks by using Kerberos, and LDAP identification.

Keywords-*cloud computing, cloud computing security, LDAB, Kerberos.*

*****

I. Introduction

Cloud computing is one of the important and hot research area. Companies such as Google, IBM, saleforce.com, and Microsoft are the biggest player of cloud computing environment. Cloud computing contains to services, applications, and data storage delivered online. Through cloud computing IT-related capabilities are provided as services to multiple external customers using Internet technologies. It allows users to consume services without knowledge and control over the technology and infrastructure supporting them. Today's businesses are very complicated, and agile fatly whenever there is a new need and change we need to purchase new hardware, software licenses etc. Also organizations need experts to install, configure, test and run them. Cloud computing reduces this entire burden as organizations need not to own all these resources. Resources are owned by the third party cloud provider. The best idea behind this is reusability of IT resources, and related capabilities. Therefore, cloud computing platforms are smart solution for the users to handle complicated IT infrastructures.

Deployment of cloud computing depends on whether the cloud is a private, community, public, or hybrid one. Private clouds are operated for a particular organization, whereas community clouds are mutual by a number of organizations. Public clouds are available to the common public or large groups of Industries, while hybrid clouds combine public and private elements in the same data center, each type need different type and limit of security. There are three types of models for providing the services of cloud. These three models are often referred as the SPI (Software as service, Platform as service and Infrastructure as service) model. These services are known as SaaS, PaaS and IaaS. These services are used to make IT Infrastructure scalable, reliable and cost effective.

The important advantages of cloud computing are: Fast delivery of resources, lower entry cost, agility, device independency, services independency, location independency and scalability. Services are provided like utilities in Cloud computing, so end users only pay according to the type and amount of usage. It facilitates on-demand service delivery and also quality of service. Cloud computing is usable in several applications areas such as education, banking, medical and health and several financial applications. But as cloud is a distributed and shared environment there are several issues related to its security.

In this paper, we explore the security issues and challenges for the cloud computing and suggested a cloud computing framework to secure user's private data, messages and highly important information. The rest of the paper is organized as follows:

II. Related work

Recently cloud computing security received significant attention from IT industries and research communities as there are still several unresolved issues which needed to be addressed before important development take place, due to large tries number of hacking and interrupting cloud computing services. each client stores its own user data in cloud storage, which is not only burdens the applications with storing, managing, and securing user data but also dispossess users from controlling their own data [1][5].

To improvement in security, analyst have their different view as privacy is an important issue in Cloud computing in terms of user trust and need to be considered at every phase of design [6]. Sometime it happens that without awareness of organization's detail user record their data; companies may send user's sensitive information to other companies for economical reason, from transformation of data cyber-criminal may steal the user email and bank's detail etc. The awareness is also increases for the need for design for privacy from both companies and organizations, it needs big efforts and time to be spend with the user to minimize the risk [7]. Authenticationmay the required user name or password or any of the authentication techniques include hardware token, software token, digital certificates on smart cards and USB Tokens, out-of-band authentication and biometric [8]. It is observed that everyday new security advisors are published [9] [10].

Many research had been done in cloud security, Aniesh Krishna K, Balagopalan A S have discussed using Kerberos as single sign-on authentication model for an open environment that combines the platform trust in user systems and trusted module security . Minqi Zhou, Rong Zhang and others have discussed several security and privacy issues related to cloud. They investigated several Cloud Computing system providers and their concerns on privacy and security issues. Santosh Khamitkar, Yasir Fuad AL-Dubai, Pawan Wanik have designed the Kerberos Authentication with Role Based Access Control (KARBAC) framework for cloud computing applications. Kevin Hamlen, Murat Kantarcioglu and et al. Have followed bottom up approach to security and worked on small problems in the cloud environment in the hope that it will solve the larger problems of cloud security. They discussed security issues for cloud middleware security, storage security, network security, data security and application level security. Richard Chow, Philippe Golle et al. characterize the problems and their impact on adoption of cloud computing. They have proposed to extend control measures through the use of Trusted Computing and by applying cryptographic techniques. B.Meena, Krishnaveer Abhishek Challa identifies all the possible security attacks on clouds including: Authentication attack, Denial of Service attack, Wrapping attacks, Man-in-the Middle attack, Flooding attacks, Malware-Injection attacks, Browser attacks, and also Accountability check problems. They mentioned the root causes of these attacks and also proposed specific solutions for all of these attacks. Farhan Bashir Shaikh and Sajjad Haider identifies top security concerns of cloud computing, these concerns are Leakage of Data, Data loss, User‘s Authentication, Client‘s trust, Malicious users handling, risk management, Wrong usage of Cloud services and Hijacking of sessions while accessing data. They propose to use new release of governance

The Cloud Security Alliance (CSA) and compliance stack for cloud computing counter these kinds of attacks, Chi-Chun Lo, Chun-Chieh Huang and Joy Ku have proposed a framework of cooperative intrusion detection system (IDS)[]. This system could reduce the DDOS attacks impacts[]. This cooperative IDS send the alert messages to other IDSs, if detected any region suffers from DoS attacks [2].

In this paper, security concern of cloud computing will be analyzed and propose a secure framework for cloud computing.

III. Problem Statement

The cloud computing security has to be part of company’s overall security strategy. Security risks break and threats can come in so many forms. It comes from so various places that many organizations take a comprehensive approach to security management across IT and the business function. Organization must have IT tools to monitor, detect, prevent and trace the intrusion trying to get access corporate information, either from organizations perimeter or from any other external location [1][11]. An organization planning to secure cloud environment will generally focus on the broad range of potential vulnerabilities to its data center. It is also necessary that safeguard sensitive corporate, customer, and partners highly information whenever it is located. A company’s software application may include lots of built in application and data level protection, but there are many situations where these protections aren’t enough.

Currently, IT industries face a perimeter security problem because above 70 percent of security breaches are caused by the malicious insider. Whenever, companies are going to plan to deploy cloud services. They must have to deal with insider attacks as well as outside attacks (threats) [5].

The most important threads of cloud computing are abuse and nefarious use of cloud computing, insecure interface and API, malicious insider, shared technological issues, data loss or leakage, account on service hijacking, unknown risk profile etc [9]. Thus, we suggest a secure architecture to avoid abuse and nefarious use of cloud computing, design a framework to secure insecure interfaces and API, account on service hijacking and malicious insider with following consideration.

Authenticate all people to access network.

Frame all access permissions and roles so users can have access only to application and data that they have been granted.

Authenticate all the software of the company.

It monitors network activities.

Log all user activity and program activity and analyzed it for unexpected behavior.

Encrypt data, when there is need of some extra protection.

Regularly check all networks for vulnerabilities in all cloud software. [1]

IV. Proposed Solution

The basic idea of cloud computing is that it describes a new enhancement, utilization and delivery model for IT services based on Internet protocols. The best feature of cloud computing is that it has made access to computing resources a lot effortless way, but with that convenience has come a whole new universe of threats and vulnerabilities. Our work focus is to provide a solution for these threats that are the major issue for anyone when they want to adopt cloud model and services for their work. For this purpose, a framework should be designed for execution of data and information securely in cloud computing environment. It will protect user’s data, information from various attacks. In this paper, we explore the security issues and challenges for the cloud computing and suggested a cloud computing framework to secure user’s private data, messages and highly important information.

A. Designed Frame Work

IT After an analysis of the relevant existing work, and cloud design we have designed the Kerberos Authentication with LDAP Role Based Access Control (KLDAP) framework for cloud computing applications. Figure 1 shows the design of the KLDAP it’s easy for clients to protect their resources in accordance with its security and access control requirements. The designed framework provides a policy, permission, and role specification module to cloud computing clients to define access control on its resources using LDAP-RBAC policy, then the Kerberos authorization server component stores and generate access control decisions based on the LDAP-RBAC policy and permissions [8].

when user U logs on to a web service to check his or her data or asking for service on a cloud data server, U must supply a password to get a ticket for the data server. If U needs to verify the data several times during the day, each attempt requires re-entering the password in traditional authentication systems. Nitin, Santosh improved their system by allowing tickets to reused. For a single login session, the web service can store the data server ticket after it is received. It useson behalf of the user for multiple accesses to the data server. However, under this scheme it remains the case that a user would need a new ticket for every different service. If a user wished to access a print server, a mail server, a file server, etc. each access would require a new ticket and hence require the user to enter the password.

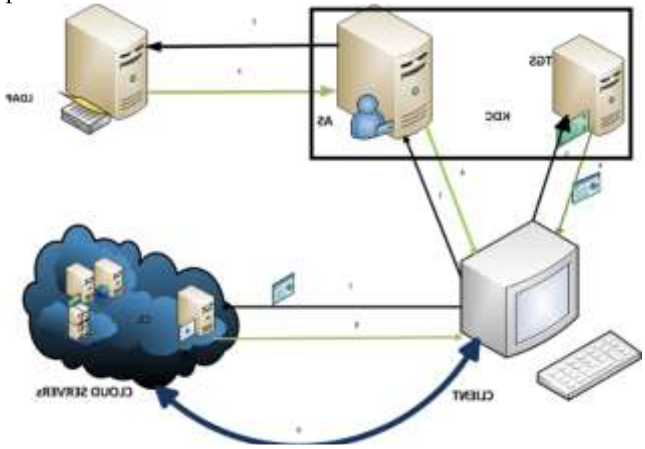

Figure 1. Show the system KLDAP component and the interactive between them

Kerberos main purpose is securing authentication service in a network and cloud. In the Kerberos authentication model, AS shares a unique secret key with each server. These keys have been distributed physically or in some other secure manner such as ticket [8]. the following communication for User login session:

U→ AS: IDU || PU || IDCDS
AS → LDAP IDU || PU
LDAP→ PRAC
AS→ U: Ticket
U →CDS: IDU || Ticket

Ticket = E (KCDS, [IDU || ADU || IDCDS])
Where,
U = User, IDCDS = Identifier of Cloud server
AS= Authentication server, PU = Password of user
CDS = Cloud Data Server, ADU = Network address of user
PRAC = Policy and Role Access Control
IDU = Identifier of user, KCDS = Secret encryption key shared by AS and CDS

when user U logs on to a web service to check his or her data on a cloud data server or asking for service, U must supply a password to get a ticket for the data server. If U needs to verify the data several times by using traditional systems during the day, each attempt requires re-entering the password. Nitin, Santosh improved systems by tickets reused. For a single login session, the web service can store the data server ticket after it is received. It uses it on behalf of the user for multiple accesses to the data server. However, under this scheme it remains the case that a user would need a new ticket for every different service. If a user wished to access a print server, a mail server, a file server, etc. each access would require a new ticket and hence require the user to enter the password. [2][3]

The service, TGS, issues tickets to users who have been authenticated to AS. Thus, the user first requests a ticket-giving ticket (Ticket) from the AS. Each time the user requires access to a new service, the user applies to the TGS, using the ticket to authenticate itself. TGS grants a ticket for the particular service. Here, only the correct user knows the password and can recover the ticket. Ticket consists of the ID and network address of the user and the ID of the TGS. The idea is that the user can reuse this ticket to request multiple service giving tickets. [3]

Consider the following scenario, an opponent captures the login ticket and waits until the user has logged off his or her cloud services. Then the opponent either gains access to that web services.

U → TGS: IDU || IDCDS || TicketTGS
TGS → U: TicketCDS
U → CDS: ID U || Ticket CDS

Ticket TGS = E(KTGS ,[IDU || AD U CDS || ID TGS ||TS 1 ||Lifetime1])
TicketCDS =E(KCDS,[IDU||ADU||IDCDS||TS2 | Lifetime2])

The opponent would be able to reuse the ticket to send-up the TGS. To counter this, the ticket includes a timestamp, indicating the date and time at which the ticket was granted, and a lifetime, indicating the total time for which the ticket is valid. Thus, the user now has a reusable ticket and need not bother the user for a password for each new service request. [2]

B. Proposed Frame components

The framework implements identification and separation of duty constraints or that is effective to perform well even in minimalist situations. It explained the detailed of the components and Kerberos protocol required for communication between these components.

I. Cloud Client

A cloud computing client is a person or entity who uses various cloud computing applications deployed by vendors of various cloud computing services to its client. Cloud computing client creates stores and shares resources with other applications or clients. Module specifications policy exists on the client's computer to provide client interface and tools to create, edit and manage access control to resources. And policies are dynamically formed in back end using LDAP-RBAC policy.

II. Kerberos Protocol

Kerberos authentication protocol is responsible for verifying client identities. Authentication is provided as a guest service in the system design, and can be achieved via any standard authentication protocol. Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all their communications to assure privacy and data integrity, as they go about their business [9, 10]. The KDC contain of two main steps as we illustrate as the following:

Authentication Server (AS): The first step of the KDC is AS. Cloud computing client (principal) initially requests a ticket to the KDC by giving it is name, an expiration time until when the authentication will remain valid, the cloud computing service required (tgs) and some other information, is not mentioned here for clarity the KDC if found the cloud computing client in it is database, replies with two steps:

cloud computing client ticket contains a session key SA, KDC, the expiration time and it is tgs cloud computing service name, all encrypted using the secret key of the principal KA.

The expiration time usually working day or eight hours, gives a period of time during which the tickets will be valid.

Granting ticket contains the session key SA, KDC, the expiration time and the name of the cloud computing client/user, all encrypted using the secret key for the KDC. This is what is known as a TGT. The principal unable to decrypt the TGT, and will be used later to request tickets for the other cloud computing services.As it is encrypted the cloud computing client/user cannot read the data inside. If tries to modify it, the KDC will not be able to decrypt it and it will be refused.

Task for each client/server interaction, server can be required to undertake this. But in a cloud computing like open and shared environment, this places a substantial burden on each server. AS handling the client server interaction on behalf of cloud server, who knows the passwords of all users and stores them in a centralized database.

User login session:

U → AS: ID U || ID tgs
AS → LDAP: ID U
LDAP→ RPAC
AS → U: E (KUtgs, Ticket tgs)

TICKET GRANTING SERVER (TGS): The second step of the KDC is the distribution of tickets it called the TGS. Once authenticated the cloud computing client who requests a specific application such as telnet or FTP first asks the KDC. It does not query the cloud computing service directly. This request to the KDC it contains several fields:

An authenticator consists of a timestamp and checksum encrypted with the session key SA, KDC, which was obtained earlier in the KDC, shared between the cloud computing client/user and the KDC. This proves the identity of the cloud computing client/user since he is the only one to know this session key. The checksum proves the authentication message has not been modified during the transiting. The timestamp confirms the message is recent, and is used to prevent "reply" attacks, since anyone can Interception of data across the network and use it at a later time. Typically, the KDC must responds within five minutes for a message to be accepted. This is why it is important to have a good time synchronization across your network where is implemented the Kerberos AS to the cloud computing. Consider the use of Protocol such as NTP (Network Time Protocol) to keep it accurate.

TGT received during the authentication exchange with the KDC. It is used by the KDC to verify the cloud computing client/user's name. If the cloud computing client name present in the TGT does not match with related the session key and this means the cloud computing client has been impersonated and the KDC is unable to decrypt the authenticator. Also the KDC verifies the validly by checking the expiration time of the authentication.

U → TGS: IDU || IDCDS || TICKETTGS
TGS → U: TICKETCDS

THE CLOUD COMPUTING SERVER name to which the cloud computing client wants to establish a connection.

An expiration time for the TGT. The KDC responses to the cloud computing client (principal) with two tickets:

The cloud computing client ticket contains a new session key SA, that the cloud computing client/user and the cloud computing server will be used to verify each other's identity and to encrypt their sessions. The ticket also encloses the cloud computing service name and the expiration time of the new ticket. All of these items encrypted using the key SA, KDC shared between the cloud computing client and the KDC, known only to the cloud computing client.

The server ticket that contains the same session key SA,B as mentioned above , the cloud computing client's name and time of the expiration of the ticket. The server ticket being encrypted with the cloudcomputing service's secret key KB, only known to the server. It is then under the responsibility of the cloud computing client to send a server ticket to the cloud computing server.

U □ CDS: ID U || TICKET CDS
TICKET TGS = E(KTGS ,[ID || AD U CDS || ID TGS TGS ||TS 1 ||LIFETIME])
TICKETCDS =E(KCDS,[IDU||ADU||IDCDS||TS2 | LIFETIME1])

III. LDAP SERVER

LDAP Authorization server stores access control policies defined by the clients of cloud computing (in terms of resources) and cloud computing applications (regarding registered clients). It also generates access control decisions based on those policies stored using LDAP-RBAC policy engine. It consists of a policy storage module that stores and manages access control policies, and working as a Policy Administration Point (PAP) and Policy Retrieval Point (PRP) in System Designer. LDAP Authorization server also contains a policy decision module which is a Policy Decision Point (PDP), it creates access control decisions by evaluating access request against the stored policies. It also implements various time-based semantics of temporal hierarchies and separation of duty constraints or SoD that is effective to perform well even in minimalist situations.

As well as it handling the authorization roles, LDAP works as second authentication factor, given strong authentication mechanism.

IV. CLOUD CONTROL NODE

Control Node component acts as a gateway between the clients of cloud computing and the cloud services. It manages connections and sessions for cloud computing clients and deal with access requests to the cloud computing applications and gets access control decisions from the authorization server. Since this component intercepts all messages between the various components, so we also added Policy Enforcement Features in it.

V. CLOUD COMPUTING APPLICATION

The cloud computing application provides cloud computing client's different services. It allows them to create, upload and share resources (documents, files, images, etc.) with other clients or applications. The designed framework the cloud computing application has a delegated it access control functionality to the client and authorization server. All access control decisions are created by authorization server on behalf of a cloud computing application. It contains a repository of resources, and is only responsible for storage resources that are created or uploaded by clients.

In our research we found that Kerberos and LDAP together make for a great combination in cloud computing environment. Kerberos is used to manage credential securely (authentication) while LDAP is used for hold authoritative information about the account such as what they're allowed to access (authorization). Fig. 2 represents the working of AS.

C. SEQUENCE DIAGRAM EXCHANGING MASSAGES

Figure below shows sequential or interactive diagram for the whole working. It shows the sequential process of messages transmission for accessing the Cloud Services. The solid arrow lines here depict message transmission for messages from 1) to (10). The vertical lines depict the timeline and text in boxes represents objects interacting with each other. Such as client interacting with AS, TGS etc.

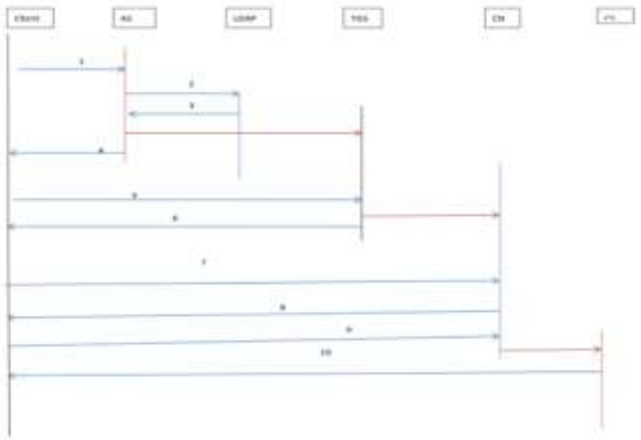

FIGURE 2. SEQUENTIAL OR INTERACTIVE DIAGRAM

Client request for a ticket-granting ticket to access cloud service. It includes the user's ID, TGS's ID and timestamp 1.

Authentication server sends to LDAP server after initial authentication asking for authentication and permission and authorized services.

LDAP response to AS with the policy and permissions regarding the user, and the access that allow.

AS responds back the client with ticket to TGS, client ID, timestamp 2 etc. These all are in encrypted form and this encryption is done using the key generated from the client's password.

Client sends the TGT along with its authentication and ID of TGS to get TGT.

TGS sends the ticket to cloud server along with client ID to client.

Client sends the cloud control node ticket and its authentication to cloud server.

Control Node response the client with granting access the service.

Client send the control node to connecting to the service, control node reserves the service to the client and establish connection. Cloud may either request authentication from client or client can directly start accessing service from cloud.

Client encrypt data and send it to the cloud. And when need it and get it from the cloud, decryption process will be implement. And then client can deal with it. Section (4.4) give more detail.

Cloud may either request authentication -depending on the mechanism used- from client or client can directly start accessing service from cloud.

V. CONCLUSION

In this paper we have developed Kerberos with LDAP Frame work to secure cloud from malicious insider or outsider, DDoS, and others threats. the major concerns for companies to adopt cloud computing environment. also we discuss about some of the top threat of cloud security concerns, and also provide a simple and efficient secure framework for privacy, the Kerberos Authentication with LDAP (Role Based Access Control) with encryption with AES algorithm. The proposed framework provides a policy specification module to cloud computing clients to define accesscontrol on its resources using LDAPRBAC policy format, this leads to solved the Kerberos limitation when been used alone.

Then the Kerberos authorization server component stores and generate access control decisions based on the RBAC policy. Also we are developed an authentication framework for cloud based on the Kerberos V5 protocol to provide single sign-on and to prevent against malicious and DDOS attacks in the access control system. Although benefit by filtering against unauthorized access and to reduce the burden, computation and memory usage of cloud against authentication checks for each client. It acts as a trust third party between cloud servers and clients to allow secure access to cloud services.

As authentication server is the main entity that stores complete database of login details, it will be worst if in any case its security is compromised. AS must be physically protected.

Kerberos protocol can only authenticate a client's identity; it cannot authorize the accesses of users once they got ticket to access services from cloud.

Kerberos and LDAP together given strong authentication and access control, the system named KLDAP. The rest of work regarding the integrity will be by using powerful encryption keys AES. Confidentiality is also provided by the vendor Online Tech which obtains confidentiality in the cloud computing using encryption methods that encrypt stored data on hard disk encrypting the data with the AES (Advanced Encryption Standard) algorithm. If client data lost or stolen there is data is encrypted and no one else than the client can used it.

Cloud computing also involves several security and management risks and concerns. Cloud involves virtual machines that are very prone to attacks. malicious and DDOS attacks can be easily influence the cloud resources. These issues have made the adaptation cloud a bit difficult. These hurdles have several management issues. Still many new providers are stepping into this business. So choices for customers are increasing day by day. But there are always threats of attacks, data leakage and security breach. The solutions proposed here can be implemented in future to prevent cloud from direct access, DDOS attacks and to produce satisfactory improvements in cloud security. This will help to enhance the client's interest and satisfaction.

A TGT can be misused by attacker for accessing cloud services until the session expires, in case if TGT is stolen this issue is need more investigate and trying to find solution without affecting the performance of the system.

Although these issues are rare but need special attention. Once satisfactory care is taken for all these, and then this solution can be able for better detection and filtration of DDOS attacks.

REFERENCES

[1] Nitin Nagar, and Pradeep k. Jatav, "A Secure Authenticate Framework for Cloud Computing Environment" International Journal of Advanced Computer Research (ISSN (print): 2249-

7277 ISSN (online): 2277-7970) Volume-4 Number-1 Issue-14 March-2014.

[2] ANIESH KRISHNA K, and BALAGOPALAN A S "AUTHENTICATION MODEL FOR CLOUD COMPUTING USING SINGLE SIGN-ON" IRF International Conference, October-2014, Bengaluru, India, ISBN: 978-93-84209-56-8.

[3] Santosh Khamitkar, Yaser Fuad AL-Dubai, Parag Bhal Chandara, and Pawan Wasink "KERBEROS AUTHENTICATION WITH CLOUD COMPUTING ACCESS CONTROL" IIER International Conference, Bangkok, Thailand, 4th April 2015, ISBN: 978-93-82702-89-4.

[4] Raja Shree S. "Secure Substantiation in Cloud Computing Environment", National Conference on Architecture, Software systems and Green computing (NCASG), Chennai 600 117 India.

[5] Farhan Bashir Shaikh and Sajjad Haider, "Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, IEEE, 11-14 December 2011

[6] Harold C. Lim et al, "Automated Control in Cloud Computing: Challenges and Opportunities", ACDC'09, June 19, 2009, Barcelona, Spain, pp 13-18.

[7] B.Meena, Krishnaveer Abhishek Challa, "Cloud Computing Security Issues with Possible Solutions", IJCST Vol. 3, Issue 1, Jan. - March 2012

[8] D. Catteddu and G. Hogben, "Cloud Computing:Benefits, risks and recommendations for information security", http://www.enisa. europa.eu/activities/riskmanagement/files/deliverables/Cloudcomputing risk-assessment/at download/fullReport, ENISA2009,

[9] B. Clifford Neuman and Theodore Ts'o (September 1994). "Kerberos: An Authentication Service for Computer Networks". IEEE Communications.

[10] "Security Guidance for Critical Areas of Focus in Cloud Computing", April 2009, presented by Cloud Security Alliance (CSA).

[11] Minqi Zhou, Rong Zhang and others, "Security and Privacy in Cloud Computing: A Survey", Sixth International Conference on Semantics, Knowledge and Grids, IEEE, 2010

[12] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), April-June 2010

[13] B.Meena, Krishnaveer Abhishek Challa, "Cloud Computing Security Issues with Possible Solutions", IJCST Vol. 3, Issue 1, Jan. - March 2012

[14] Nitin, Durg Singh Chauhan et al, "Security Analysis and Implementation of *JUIT–Image Based Authentication System using Kerberos Protocol", Seventh IEEE/ACIS International Conference on Computer and Information Science, 2008.

[15] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0", Proceedings of Nineteenth TheIIER International Conference, Bangkok, Thailand, 4 http://www.Cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf. 2011.

[16] Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing" NIST, NIST Special Publication 800-144; December 2011.

[17] John E. Canavan ―Fundamentals of Network Security‖, Library of Congress Cataloging-in-Publication Data ISBN 1-58053-176-8 (alk. paper)

[18] Gawali M. B., R. B. Wagh, S. P. Patil ―Enhancement for data security in cloud computing environment‖, international journal of internet computing.

[19] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security and Privacy, Vol. 8, No. 6, pp. 25-31, 2010.

[20] S. M. Bellovin and M. Merritt. "Limitations of the Kerberos Authentication System". Usenix Conference. URL:http://academiccommons.columbia.edu/download/fedora_content/download/ac:127107/CONTENT/kerblimit. usenix. pdf. January 1991.

[21] Kai Hwang ,Deyi Li ―Trusted Cloud Computing with Secure Resources and Data Coloring‖ ,Published by the IEEE Computer Society 1089-7801/10/$26.00 © 2010

[22] Mandeep Kaur, Manish Mahajan ― Using Encryption Algorithms to enhance the Data Security in Cloud Computing‖, International Journal of Communication and Computer Technologies Volume 01 – No.12, Issue: 03 January 2013

[23] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/, December 2009

[24] B. Clifford Neumann,Theodore Ts'o ―Kerberos: An Authentication Service for Computer Networks‖,IEEE Communications Magazine, Volume 32, Number 9, pages 33-38, September 1994.