ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A Framework for Preservation of Cloud User's Data Privacy

Kratika Ingle, Prof. Bharat Solanki, Prof. Nitin Shukla, Dr. Samar Upadhyay

Research Scholar, Dept. of Computer Science & Engineering, Shri Ram Institute of Technology, Jabalpur, India

Dept. of Master of Computer Application, Shri Ram Institute of Technology, Jabalpur, India

HOD, Dept. of Master of Computer Application, Shri Ram Institute of Technology, Jabalpur, India

HOD, Government Engineering College, Jabalpur, India

ABSTRACT: Cloud computing is a new generation technology which resourcefully support the client oriented services. Now in these days there are a number of applications which consumes the cloud storage service for storing and retrieving information. In such conditions the data owner management and privacy preservation cryptographic techniques are utilized frequently. But due to cryptographic technique of security implementation the data leave their own format and converted into other unreadable format. Due to this retrieval of required information becomes complex. Therefore in this work we proposed solution have as a feature the hash table encryption and salted md5 techniques which may facilitate for encrypting user data and identifying the user data and privacy.

KEYWORDS*:* Cloud computing, MD5, Cloud storage, Salted MD5, Hash key**.**

I. INTRODUCTION

Cloud computing is a new generation technology that offers on - demand, network access to a shared pool of configurable computing resources on a pay per use basis. This new computing paradigm differs from other similar computing technologies in that, the cloud computing services follow a self – service model. Cloud computing offers software, platform and infrastructure over the Internet and this constitutes the three flavours of cloud viz., Software as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). This computing model enables the Cloud users to increase their capacity and capability dynamically without investing in new infrastructure, training new personnel, licensing new software etc.[1]. Cloud computing technology enables users to remotely access shared resources stored in cloud servers using web services via the Internet. Hence the cloud resident resources are viable to the security threats applicable to Internet and web services. The fact that the resources should be accessible only to legitimate user's points out to the requirement of deriving a secure, user authentication mechanism for the cloud environment. Authentication involves the process of ensuring that a person who presents a set of credentials is whom he or she claims to be. The cloud service providers need to tackle the issues faced by user authentication mechanisms carried out prior to providing access to the shared resources. The architectural features of cloud such as Multi-tenancy and Virtualization allow the users to achieve better operating costs and be very agile by facilitating fast acquisition of services and resources on a need basis. However, to achieve the full benefits of cloud, the service providers need to tackle the security concerns raised by the fast growing cloud consumers. Among the various security concerns, data security, trust and privacy are the major ones that make potential customers think multiple times before adopting cloud services. In a survey conducted by International Data Corporation (IDC), to understand challenges of Cloud computing,87.5 % of the masses belonging to varied levels starting from IT executives to CEOs have said that security is the top most challenge to be dealt with in every cloud service [2]. Amongst the various threats faced by the different cloud services, security threat is considered to be of high risk [3] and hence the cloud service providers need to consider security as a serious issue to be addressed immediately for the whole he started adoption of cloud services. These threats can be thwarted in an application by the introduction of some suitable elements based on the goals of information security paradigm. The goals include Confidentiality, Data-Integrity, Authenticity, Authorization, Non-Repudiation, Availability, Audit and Control [4, 5, and 6].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

II. AUTHENTICATION METHODS

The n today's world to access critical resources authentication is required. To secure our critical resources more secure authentication is necessary. Authentication is process in which authorized user (i.e user which has rights to access particular resource) will be given access to resource. During authentication only authorize user will get access to resources. There are various types of methods available for authentication. These methods basically classify into following 3 types.

1. Knowledge based authentication
2. Token based authentication
3. Biometric authentication

In knowledge based authentication password is used for authentication. There are two types of password for authentication, alphanumeric password and Graphical password. Alphanumeric password is sequence of alphabets, numbers and special characters. So in alphanumeric password characters are used to create password. This password should not guessable. But alphanumeric password which is not guessable is hard to remember. For example most people combines there name with some number related to them. Such passwords can be easily guessed. To solve this problem pictures are used for password such passwords are called as graphical passwords. Graphical passwords are easy to remember. But shoulder surfing attack is possible in graphical password [1].

In token based authentication user has token which is used for authentication. For example Credit card, ATM card. Disadvantage of this method is when token is lost or stolen.

In biometric authentication user is authenticated using user's physical and behavioural properties which are unique for each user. Face recognition, Fingerprint, voice recognition etc. are example of biometric authentication. Biometric authentication is costly as it requires hardware device for recognition of physical property of user [2].

Each above method has some disadvantage to overcome these disadvantages combination of more than one technique of authentication is used to authenticate user. This phenomenon called as multi-factor authentication. Multi-factor authentication uses the combination of more than one type of authentication. More than one form of authentication used in multi-factor authentication that's why multi-factor authentication. Multi-factor authentication provides extra layer of authentication which minimises risk in risk based authentication.

III. AUTHENTICATION ATTACKS IN CLOUD

Research studies reveal that any authentication mechanism related to web applications and cloud should provide high security, easy to use interface and support user mobility. The customers prefer to access their applications from different locations and different devices such as desktop, laptop, PDA, smart phones, cell phones etc. Those needs pose significant requirements to the security of applications. The broad range of user requirements introduces wide range of attack vectors in the cloud that makes the security of cloud applications a thought provoking matter. Cloud service providers need to ensure that only legitimate user are accessing their services and this points out to the requirement of a strong user authentication mechanism. But there exists numerous attacks that can create loop holes in the authentication mechanism and hence identifying the most secure authentication mechanism with high user acceptability is a big challenge in the cloud environment.

Thus an in-depth idea of attacks on authenticity and corresponding prevention techniques are required to draft a fool proof authentication mechanism for cloud environment. Figure 1 gives a pictorial representation of the attacks on authenticity and in the sections that follows, a detailed description of the attacks and the possible solutions are given.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

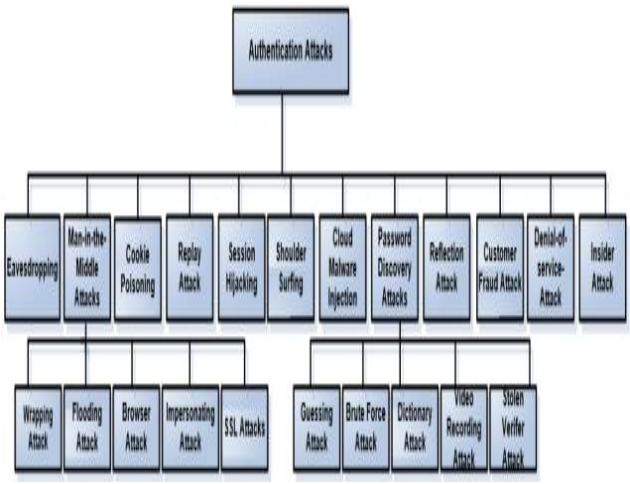


Fig 1.1 Classification of Authentication Attacks in the Cloud Environment

3.1 Eavesdropping: Eavesdropping involves the act of listening to the communication channel established between two authorized users. In a cloud environment, a traffic eavesdropper passively intercepts the data transferred within a cloud by loading a bit of code on a cloud server [7] or listens to data moving from a cloud consumer to provider and makes an unauthorized copy of the message [8]. The attacker can use the illegally gathered information to get valid credentials of an authorized user which can be user to launch impersonating attack. Eavesdropping attack, in a cloud environment which results in information disclosure can be minimized by enforcing proper authorization procedures and by transmitting the data over a secure connection such as HTTPS. Encrypting the transmitted data and attaching a signature to the same can help the destination to ensure the integrity and authenticity of data. Adopting privacy-enhancing protocols which minimize the requirement of transmitting identity credentials from the cloud service user to the verifier will discourage the illegal activity of eavesdroppers. Authentication Protocols that protect secrets, ensures user anonymity and Password Authenticated Key exchange (PAKE) protocols are much preferred in a multi-tenant cloud environment.

3.2 Man-in-the-Middle Attack (MITM): Since the inception of Web 2.0, MITM has become quite popular in the SaaS environment. Here the attacker intercepts the communication channel established between legitimate users and modifies the communication between client and server without their knowledge [9]. The following paragraphs discuss the various types of MITM attacks.

i) Wrapping Attack: A XML Signature wrapping attack applicable to web services is applicable to cloud as well, since cloud consumers use web services as a tool to access cloud services. This attack is launched by duplicating the credentials in the login phase by modifying the Simple Object Access Protocol (SOAP) messages exchanged between the browser and the server during communication set up [10]. The attacker modifies the signed request of a legitimate client by moving the original message body to a newly inserted wrapping element inside the SOAP header. A new body containing the unauthorized operation the attacker wants to perform with the original sender's authorization is inserted in the position of original message. The service executes the modified request since it contains the signature of a legitimate user. As a result, the adversary is able to intrude in the cloud and can run a malicious code to interrupt the usual functioning of the cloud servers.

ii). Flooding Attack: In a cloud environment, all the computation servers work in a service specific manner, with internal communication among themselves [10]. A successfully authorize adversary can easily send bogus request to the cloud. The cloud server before providing the requested service, checks for the authenticity of the requested jobs and the process consumes CPU utilization, memory etc. Processing of these bogus requests, make legitimate service requests to starve, and as a result the server will offload its jobs to another server, which will also eventually arrive at the same situation. The adversary is thus successful in engaging the whole cloud system, by attacking one server and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

propagating the attack further by flooding the entire system. Flooding attack can be handled by organizing all the servers providing a specific cloud service as a fleet and these servers communicating among themselves regarding the incoming requests by message passing [17]. Again a hypervisor can be used to schedule the requests among the fleets, determine the authenticity of the requests and prevent the fleets from being overloaded with bogus requests from an adversary.
This attack can be controlled by data transfer throttling, fool proof authentication mechanisms and mechanisms that filter out bogus requests.

iii) Browser Attack: This attack which results in data stealing is committed by sabotaging the signature and encryption during the translation of SOAP messages in between the web browser and web server, causing the browser to consider the adversary as a legitimate user and process all requests, communicating with web server [10]. For authenticating the clients, current web browsers rely upon SSL/TLS as they are not able to apply WS-Security. Nevertheless, SSL/TLS only supports
Point-to-point communications and this makes the authentication process insecure. Also SSL/TLS has been broken by Marlin Spike using "Null-Prefix Attack" and attackers are able to perform this technique in order to request services from cloud systems without a valid authentication [7].

iv) Impersonating Attack: Here the adversary pretends to be a valid server or user valid entity to reveal the authenticating credentials which in turn is used to gain unauthorized access to the resources. Verifier Impersonation attack, Phishing attack etc. can be categorized as impersonation attacks. Most of the times, in Phishing attacks the users are made to believe that they are communicating with valid server by creating a web page that look similar to the valid server page. In verifier impersonation attack, the attacker pretends to be the verifier and lure the customer to share the authentication keys or data, which may then be used to authenticate falsely to the verifier.

v) SSL Attacks: Secure Socket Layer (SSL) is a fundamental security mechanism that encrypts the information transmitted between client and server. SSL provides an authenticated environment for running a cloud service by verifying the identity of the communication parties [14].

3.3 Cookie Poisoning: In cookie poisoning, the identity related credentials stored in the cookies of an authorized user are modified by the attacker to gain unauthorized access to resources. Cookie poisoning attacks in cloud can be mitigated to a certain extent by using Intrusion prevention products that examines each HTTP request sent to the web server [16]. This attack which involves tampering with data can be handled by attaching the hash values of the data stored in the cookies and recalculating the same at the destination. Use of Message authentication codes, tamper resistant protocols and Digital signatures can also aid in the detection and prevention of modifying the cookies.

3.4 Replay Attack: In capture-replay attack the authentication message contains the same authentication tokens previously exchanged between an authorized user and sender and was sniffed by the attacker. The key to handle replay attack, which involves identity spoofing, is to ensure that something in the message changes each time. Considering this aspect, many protocols use time stamps or randomly generated nonce values to resist replay attack, which enables the verifier to check the freshness or the authenticity of the message. The usage of time stamps demands synchronization of timing at both the cloud service user and verifier end, which may not be feasible in a distributed cloud environment. Hence randomly generated nonce values are more preferable in a Cloud environment and since these values are unique for each session the receiver will be able to identify a replay of the previously send message containing an old nonce value.

IV. PROPOSED WORK

This section includes involved work and identified issues in system in addition to that an optimum solution is also provided. The cloud environment provides support for efficient computing and enables to provide the storage solutions at the remote end. The main aim is to address the following issues in the existing cloud storage.
Data security: the data is placed on the cloud which is not much secured due to third party access and treads therefore the data security in cloud storage is required

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Data owner and client privacy management: the data owner and client in not distinguishable using the data additionally the privacy on such data is access is required.

Searchable data space: the cryptographic manner of data security converts the formats and not a bit of data recovered during the information retrieval.
We have discussed above, about the issues and challenges now we will provide the solution steps that are described below. In order to provide end to end solution for the cloud storage the following solution steps are included.

Authentication management: in authentication management the system and user attributes are recovered additionally the one time password is included to manage the secure authentication.

Cryptographic data security: in this phase the salted MD5 cryptographic algorithm is consumed for providing the security.

V. IMPLEMENTATIONS AND RESULTS

First we need to create virtualization and need to allocate infrastructure unit for secondary operating system

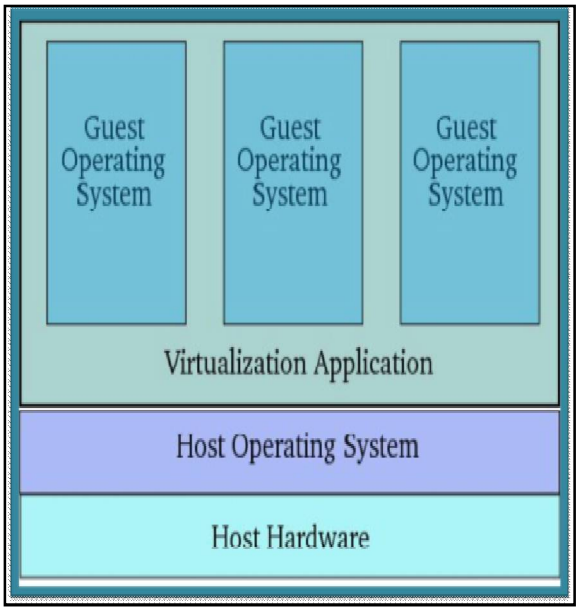


Fig.1.3 Virtualization Framework

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

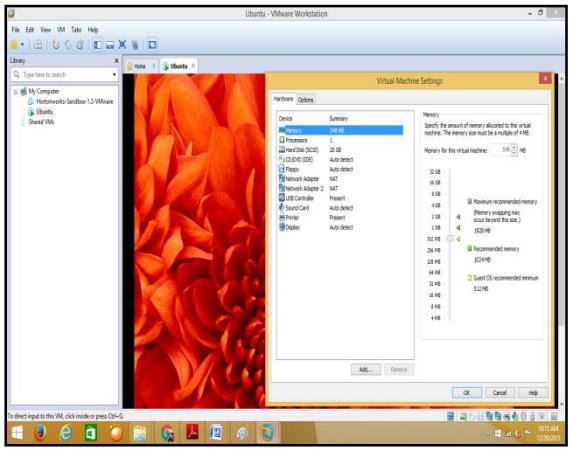
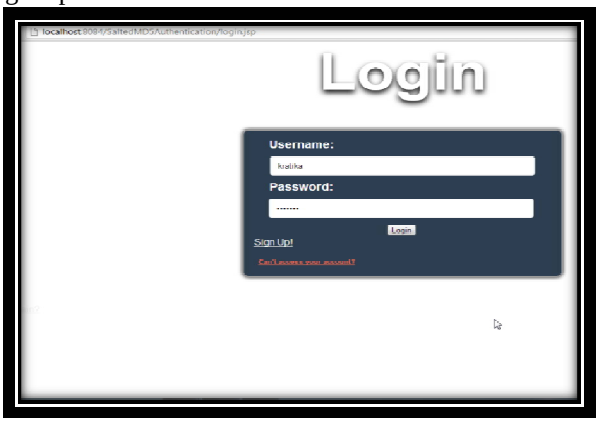
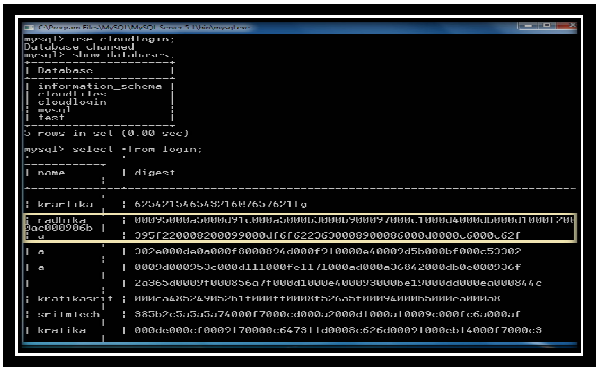


Fig. 1.4 Virtualization Implementation

1. Login section to perform login operation



2. After login all login credentials will be stored at database in secure format with the help of salted md5.



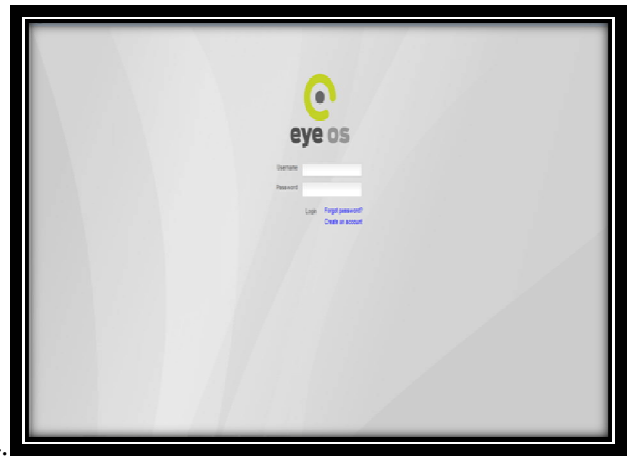
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

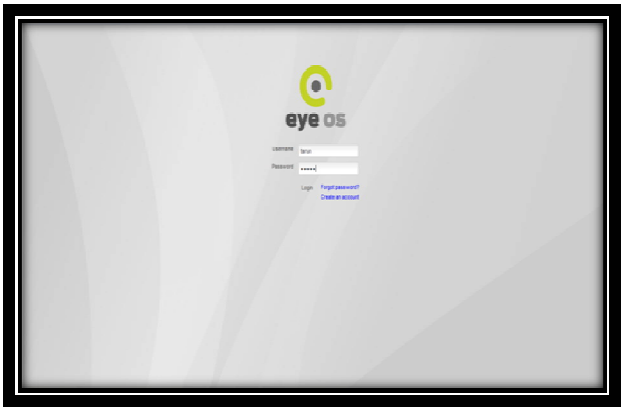
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

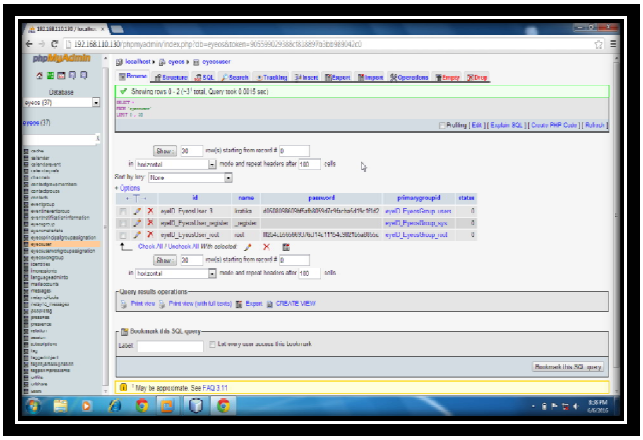
3.Cloud Server Web page will be access by user for to upload their data in the Cloud Environment

4. 

4. Login in Cloud Environment using Username and Password.



5. Same user credential will be stored at cloud sever end using MD5



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

6. Cloud Environment Home Page where we can Upload Our Data in Cloud Server.

7 Click to the Home → After Open it clicks in Upload Option.

VI. COMPARISONS OF EXISTING AND PROPOSED SYSTEM

Comparison of Existing System and Proposed System Techniques

Comparison Factors	Existing System	Proposed System
Portability	Low	High – Can be implemented on multiplatform environment
Deployment Complexity	Medium	High
Different Attacks	Vulnerabilities to prevent attacks	Prevent all major attacks
Replace Cost	Medium	Low
User Authentication	Not Available	It makes system secure from network attacks and authentication factor attacks
User authentication framework	Weak	Strong

Table 4.1 Comparisons of existing and proposed techniques
Comparison of Existing System and Proposed System Techniques.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

VI. CONCLUSIONS AND FUTURE WORK

In this work we discussed various method of encryption to secure the data in cloud storage. Also we discussed about cryptography methods which helps to convert the data from readable to unreadable form so our data could be saved in cloud storage from challenger. By studying all these survey papers and our proposed work we can conclude that the essence of security for cloud storage is very necessary so that client could feel secure while accessing the cloud storage services. In this work we proposed a scheme for secure data accessing with maintaining its privacy by using strong cryptographic algorithm.

Future work should focus on improving availability and quality of services provided. We are currently in the process of researching the development of extended security by cloud certificates that provide information to end users.

REFERENCES

[1] S. Subashini and V.Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications , vol. 34, ,no.1, pp. 1 -11, 2011.
[2] H. Lv and Y. Hu,"Analysis and Research about Cloud computing security protect policy", in Proc. IEEE Int. Conference on Intelligence Science and Information Engineering. pp. 214-216, 2011.
[3] A. Bakshi and B.Yogesh,"Securing Cloudfrom DDOS Attacks using Intrusion Detection System in VM," in Proc. IEEE Second Int. Conference on Communication Software and
Networks., pp. 260-264,2010.
[4] N.S Chauhan and A.Saxena,"Energy Analysis of Security for
CloudApplication," in Proc. Annual IEEE India Conference, pp. 1-6, 2011.
[5] W.Liu, "Research on Cloud Computing Security Problem and Strategy," inProc. IEEE 2nd Int. Conference on Consumer Electronics, Communications and Networks, pp. 1216-1219, 2012.
[6] X. Yu and Q. Wen, "A view about Cloud data security from data life cycle, (2010)," in Proc. IEEE Intl. Conference on Computational Intelligence and Software Engineering, pp. 1-4,
2010.
[7] Larry Hardesty,"Thwarting the Cleverest attack", May 1,[online]web.mit.edu/newsoffice/2012,thwarting -
eavesdropping-data-0501.html,2012.
[8] Maventek, CloudSecurity Consulting [WWW] Available from:www.maventek.com/services/Cloud - security-consulting, 2012.
[9] M.Misbahuddin,"Secure Image Based Multi-Factor Authentication (SIMFA): A Novel approach for Web Based Services, Ph.D Thesis, Jawaharlal Nehru Technological University, [Online], http://shodhganga.inflibnet.ac.in/handle/10603/3473, 2010
[10] B.Meena and K.A. Challa , "Cloud Computing Security Issues with possible solutions," Int, Journal of Computerr Science and Technology, vol.2, Issue: 1, Jan–
March, 2012
[11]Kazi Zunnurhain and Susan V. Vrbsky,,"Security Attacks and Solutions in Clouds, [Online] http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf, 2010
[12] Danish Jamil & Hassan zaki, " Security Measures in Cloud computing and Counter measures", International Journal of Engineering Science and Technology(IJEST), Vol.3 No.4 ,2011
[13 19]Y.Andree,"Implications of Salesforce Phishing Incident", [Online] http://www.ebizq.net/blogs/security_insider/2007/11/implications_of_salesforce_phi.php, 2007
[14] Abel Wike, "SSL Encryption –A Protocol that Authenticate Cloud Computing", [Online] comluv.com/ssl-encryption-a-protocol-that-authenticate-
Cloud-computing, Feb 5, 2013.
[15] Larry Seltzer,[Online] Spoofing Server-Server communication: How can you prevent it" https://otalliance.org/resources/EV/SSLStrip_Whitepaper.pdf, 2009.
[16] Imperva(2013), Cookie Poisoning[WWW], Available from: http://www.imperva.com/resources/glossary/cookie_ poisoning.html 2013

BIOGRAPHY

Kratika Ingle, Research Scholar, Dept. of Computer Science & Engineering, Shri Ram Institute of Technology, Jabalpur, India

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Prof. Nitin Shukla Presently working as H.O.D , Deptt. of Master of Computer Application at Shri Ram Institute of Techology Jabalpur, India

Prof. Bharat Solanki Presently working at Shri Ram Institute of Technology,Jabalpur (as Asst. Prof.) since 2001. Published more than 10 research papers in International /National Journals/conferences. Attend more than 12 conferences/seminar/short term training program at various organisation.

Dr. Samar Upadhyay Presently serving at Government Engineering College, Jabalpur, (as Head of the Department) since 1994. Published more than 15 research papers in International and National Journals organised more than 15 national conferences/seminars/short term training programs at Govt. Engineering College, Jabalpur (M.P.).