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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Token Based Authentication Using *Hash Key, Session And Javamail Api*

Unnati Awasthi, Research Scholar

Dept. of Computer Science & Engg, Gyan Ganga Instt. of Tech.& Sciences, Jabalpur, India

Prof. and Head of Dept, Dept. of Computer Science & Engg, Gyan Ganga Instt. of Tech.& Sciences, Jabalpur, India

ABSTRACT*:* Cloud computing is a new generation of technology which is designed to provide the commercial necessities, solve the IT management issues, and run the appropriate applications. Another entry on the list of cloud functions which has been handled internally is Identity Access Management. Single sign-on (SSO) and OpenID have been discharged to take care of security and protection issues for cloud personality. Single Sign-On (SSO) is a verification system in which a cloud administration purchaser should be confirmed just once while getting to different administrations from numerous administration suppliers, or while getting to various administrations from the same administration supplier. The server-side encryption in a conniving situation such as open cloud is excessively unsafe. Then again, customer side encryption can undermine the advantages of cloud since it is a period devouring assignment for encryption and decoding. In such manner, we propose a solid client validation in light of computerized endorsements for distributed computing, clients are verified utilizing Session, JavaMail API and Public key foundation (PKI). The proposed system gives character control, shared verification, session key foundation between the clients and the cloud server to utilize better validation.

KEYWORDS: Session, JavaMail, PKI, SSO, Authentication, Public Cloud, Server-Side-Encryption

I. INTRODUCTION

Recently, cloud computing has gained a considerable acceptance as a promising model from both business and academic communities. It is a representation for empowering pervasive, convenient, on - request arrange right to use to a mutual pool of configurable registering assets (e.g., systems, servers, stockpiling, applications, and administrations) that can be quickly provisioned and discharged with ostensible administration exertion or administration supplier's cooperation. Cloud administration suppliers (CSP's) offer cloud stages for their clients to utilize and make their web administrations, much like network access suppliers offer costumers fast broadband to get to the web [3]. CSPs and ISPs (Internet Service Providers) both offer administrations. Distributed computing is a model that empowers advantageous, on-interest system access to a common pool of configurable registering assets, for example, systems, servers, stockpiling, applications that can be quickly provisioned and discharged with insignificant administration exertion or administration supplier's association.

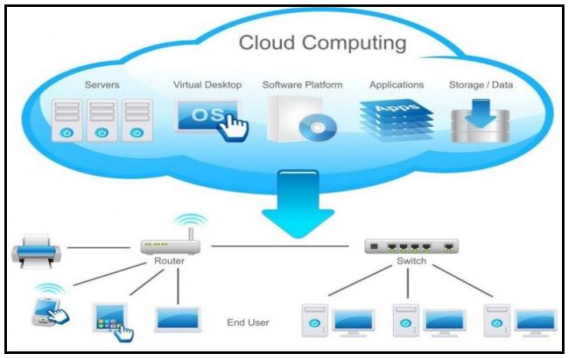

Fig 1.1 Cloud Computing

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

When all is said in done cloud suppliers offer three sorts of administrations i.e. Programming as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)[1]. Moreover, associations can without much of a stretch address the issues of quickly changing markets to guarantee that they are dependably on the main edge for their customers. The customers of business mists rent processing power (virtual machines) or storage room (virtual space) progressively, as per the requirements of their business. Furthermore, the distributed computing innovation accompanies a few issues and different security issues. In this way, conspires have been proposed, to give sufficient security to distributed computing. Be that as it may, these current security plans need efforts to establish safety. The significant issue comprises of multi-tenure, parcel transmission, putting away and scrambling client's information, application security, cloud respectability and security identified with outsider[6].

II. AUTHENTICATION ON THE WEB

2.1 HTTP Authentication

One alternative for actualizing the login framework is to utilize "HTTP Authentication". This system is a component of HTTP and is executed in verging on each web server and program [6]. At the point when the client tries to get to a secured zone, a pop-up dialog box shows up requesting the client name and secret word. This methodology is easy to code–most of the usefulness is incorporated with the web server and program. The primary drawback is that the web designer has little control over. This methodology is easy to code a large portion of the usefulness is incorporated with the web server. For instance, it is unrealistic to give a "tick here to make a record" join at the watchword brief. Additionally, this methodology is constrained to consistent secret key logins; it is impractical to do watchword challenges. HTTP confirmation comes in two principle variations: "essential" and "overview". With essential verification, the secret key is transmitted with a straightforward encoding recouping the watchword from sniffed system movement is trifling [8]. Digest validation is a "test reaction" convention where the secret key is never transmitted free. On the off chance that SSL is not SSL for all safe movement, fundamental confirmation is pretty much in the same class as condensation.

2.2 Forms Authentication

An option approach for verification is to utilize HTML shapes. Structures are a non specific instrument for clients to enter information into a site; they are bolstered by verging on each web program [7]. As a rule the web server does not by any stretch of the imagination touch the information; it is just gone to the web application. Shapes incorporate backing for a secret word box, which clouds the watchword as it is written. The genuine favorable position of this method is adaptability; web designers can make the structure and encompassing HTML show up anyway they like. The impediment is that the application must deal with the entire confirmation framework; the web server offers no help. This expansions multifaceted nature, which thusly builds the danger of bugs that cause security vulnerabilities.

III. PROPOSED WORK

In the proposed security model, one time token is utilized for validating the client. The token is utilized as key to confirm the client for secure record login. By and large utilized techniques for verification such as client characterized secret word can be traded off. To beat this trouble one time emit token is utilized as a part of the proposed security model. Consequently at whatever points a client login in the framework, he/she will be furnished with another watchword/token for utilizing it as a part of the following login. This watchword will be produced haphazardly by the confirmation power. Every time another secret word is made for a client, the past watchword for that client will be eradicated from the framework. New watchword will be overhauled for that specific client. A solitary secret word will be utilized for login just once. The secret word will be sent to the clients approved mail account. In this manner at a same time a check to decide the legitimacy of the client is likewise performed.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

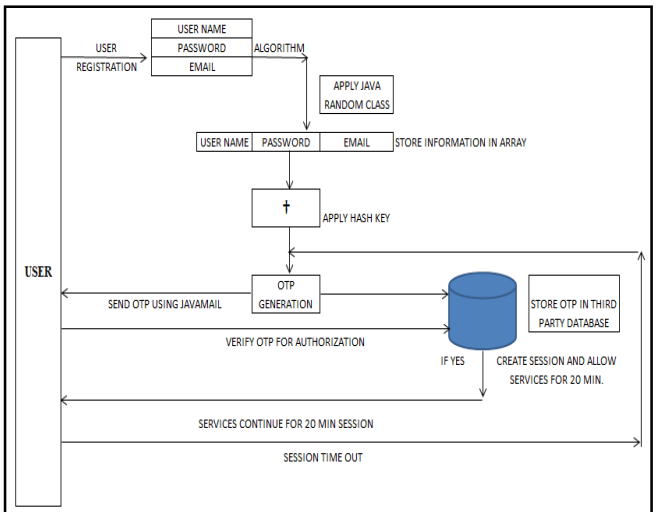

Fig. 1.2 Proposed Architecture for Authentication with OTP generation and verification

IV. RESULTS

Open ubuntu terminal with the help of alt+ctrl+t ,in this terminal we run ifconfig command. The "**ifconfig**" command with no arguments will display all the active interfaces details. The **ifconfig** command also used to check the assigned IP address of a server.

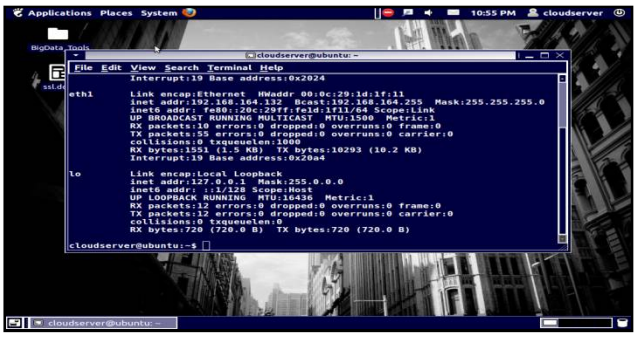

Fig. 1.3 Run ifconfig Command in Terminal

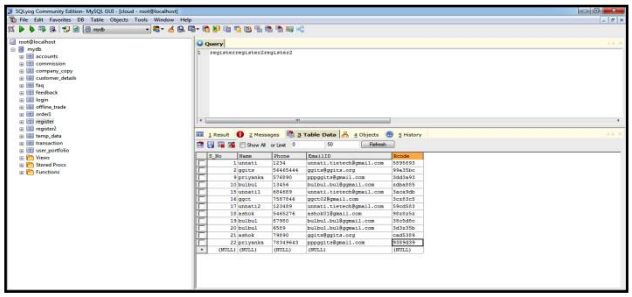

Fig. 1.4 SQLyog community edition-MySQL GUI

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Fig. 1.5 User Application Form

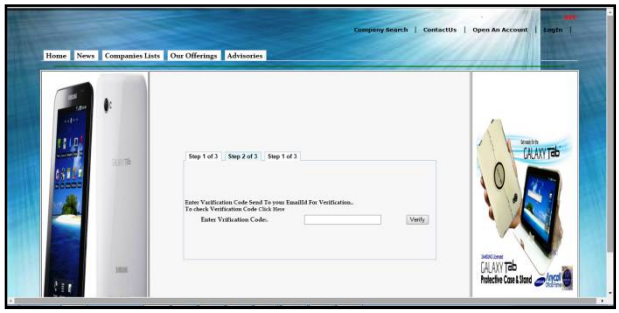

Fig. 1.6 Verification Code for Registration

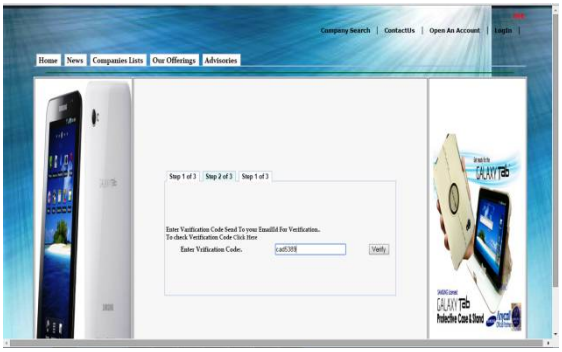

Fig. 1.7 Verification Code for Registration

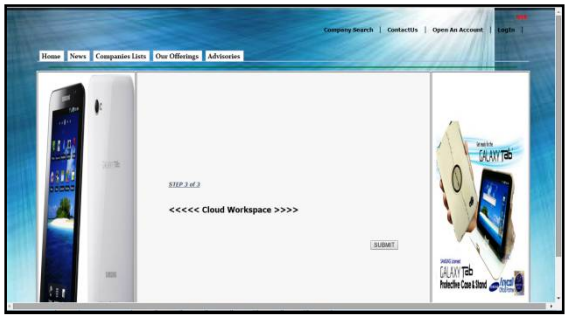

Fig. 1.8 Starting Cloud Workspace after User Verification

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

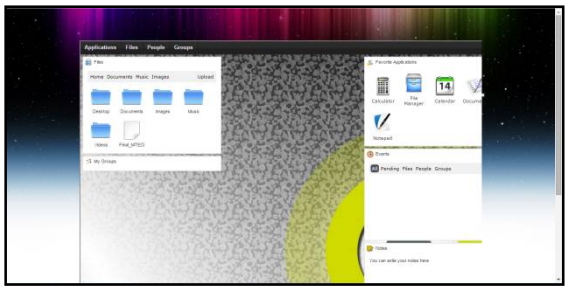

Fig. 1.9 Trusted Party Interface

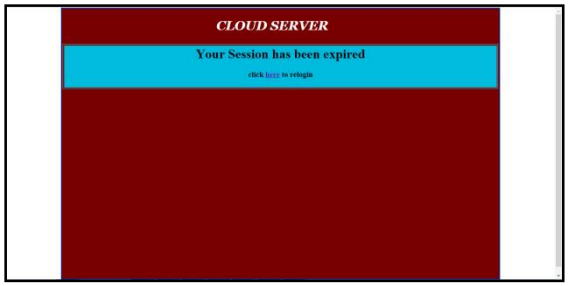

Fig. 1.10 User Session Page

V. COMPARISONS

5.1 Comparison among Non-Secure and Secure Web Applications

Comparison Criteria	Non-Secure	Secure
Authentication	Static User ID and Password	Dynamic User-ID and Password
Session	Session does not expire	Session expire
Security Limits	Secure those pages that collect data	Secure all pages
Deceptive links	Delicate with Deceptive links	Resistive with Deceptive links
Security Level	Low/Medium	Very High

Table 1.1 Security Comparisons

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

5.2 Security comparison results

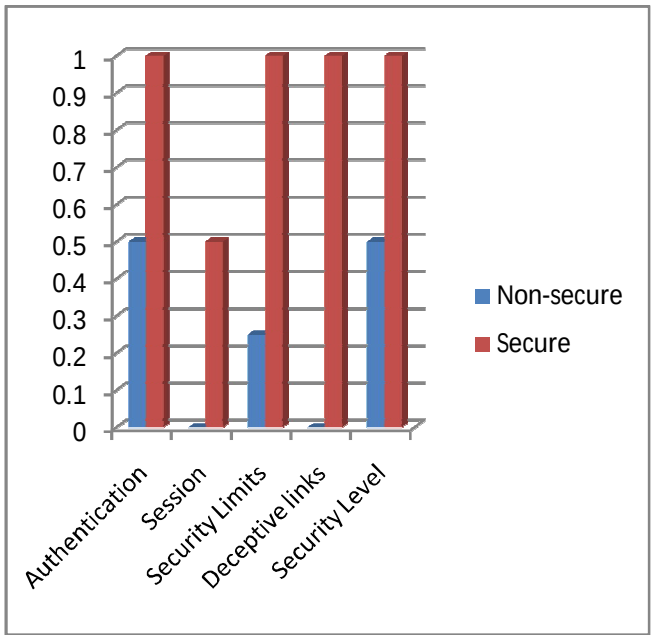

Fig. 1.11 Security Comparison between Secure and Non secure Web Applications

4.2.3 Existing and proposed method's security comparison results

Comparison Criteria	Existing Systems	Proposed System
Secure communication of credentials	Medium Security	Higher Security
User's Data Based Token	Traditional Key Based Token is Used	New Key Generation Method is Used
Email and Time Based OTP	Not Available	Available with Secure Data Transmission
Session Hijacking Attack	Attackable	Secure
Brute Force attack	Attackable	Secure against attack
Session Time Out Mechanism	Not Available	Available with User Notification and Re-login Facility

Table 1.2 Comparisons of Existing and Proposed Systems

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

4.2.4 Existing and proposed method's security comparison

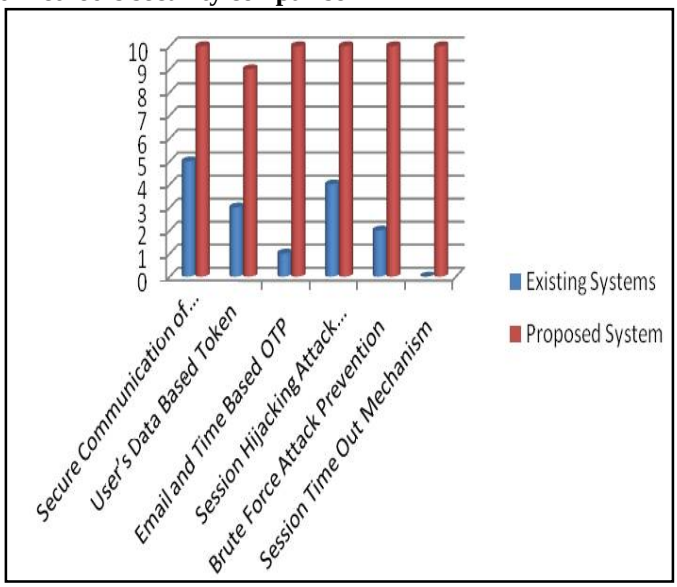

Fig. 4.14 Existing and Proposed Method's Security Comparison

VI.CONCLUSIONS

In cloud computing where multi-occupancy, virtualization and outsourcing qualities make it at danger of trading off security viewpoints and there is no physical control on information very still or information in movement, the information can be ensured by putting away cryptographically and giving the key administration to the approved party. In any case, finding a trusted gathering for doing the essential assignment in such a situation is exceptionally troublesome. Keeping in mind the end goal to take care of the issue, the cryptography strategies should be tweaked for the cloud environment. A few analysts with a mix of confirmation and cryptography have attempted to moderate the misuse of any untrustworthy gatherings in the cloud. The character based verification and characteristic based confirmation are the significant security issue in cloud environment.

So a novel and more secure verification arrangement have been proposed in the work. The verification depends on E-mail based OTP, which is secured by Java Mail API and hash key. This verification makes a Time Based Session, which will be recharged by rehashing client confirmation process. The outcomes demonstrate that our validation plan is more hearty and secure against numerous assaults and give better security to client confirmation. Future work for general model can be recommended that incorporate key administration process. Besides, a model of verification taking into account trait or personality can be proposed for the EaaS. The future work ought to concentrate on the better and proficient systems for client validation with lower unpredictability. The general execution time can be minimized in future examines and researches.

REFERENCES

[1] Chia-Ming Wu et al, Ruay-Shiung Chang, Hsin-Yu Chan :"A [1] Chia-Ming Wu et al, Ruay-Shiung Chang, Hsin-Yu [1] M. Armbrust et aI. Above the Clouds: A Berkeley View of Cloud Computing, technical report. Univ. of California, Berkeley; Feb 2009.
[2] Deepika Singh, Puran Gour, Rajeev Thakur, "User Security in Cloud Using Password Authentication", Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 6(Version 5), June 2014, pp.39-44.
[3] Hossein Rahmani, Elankovan Sundararajan, Zulkarnain Md. Ali, Abdullah Mohd Zin," Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud", The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013), 2212-0173 © 2013 The Authors. Published by Elsevier Ltd.
[4] Haibo Yang and Mary Tate, "Where are we at with Cloud Computing?: A Descriptive Literature Review" 20th Australasian Conference on Information Systems, 2-4 Dec 2009, Melbourne.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

[5] Manoj V. Thomas, Anand Dhole, K. Chandrasekaran, " Single Sign-On in Cloud Federation using CloudSim" *I. J. Computer Network and Information Security*, 2015, 6, 50-58, DOI: 10.5815/ijcnis.2015.06.06.
[6] My Abdelkader Youssefi, "Securing Cloud Computing Services Using Strong User Authentication With Local Certification Authority", (IJITR) International Journal Of Innovative Technology And Research Volume No.3, Issue No.6, October - November 2015, 2493 – 2497.
[7] Satheesh K S V A Kavuri, Dr.Gangadhara Rao Kancherla and Dr.Basaveswara Rao Bobba, "Data Authentication and Integrity Verification Techniques for Trusted/Untrusted Cloud Servers", 978-1-4799-3080-7/14/$31.00_c 2014 IEEE.
[8] Manish Kumar Sharma, Rasmeet S. Bali and Arvinder Kaur, "Dyanimc Key based Authentication Scheme for Vehicular Cloud Computing", 978-1-4673-7910-6/15/$31.00_c 2015 IEEE.
[9] Tamal Kanti Chakraborty, Anil Dhami, Prakhar Bansal and Tripti Singh, "Enhanced Public Auditability & Secure Data Storage in Cloud Computing", 978-1-4673-4529-3/12/$31.00_c 2012 IEEE.
[10] Ms.Vishnupriya.S, Ms.Saranya.P and Ms.Rajasri.A, " Secure Multicloud Storage with Policy based access control and Cooperative Provable Data Possession", ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE.