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. 4, Issue 12, December 2016

Strong Authentication for Cloud using Image Based OTP & User Profile

Anjali Singh[1], Prof. Prateek Gupta[2]

M.Tech Scholar, Dept. of Computer Science & Engineering, Srist, Jabalpur, MP, India

Asst. Professor, Dept. of Computer Science & Engineering, Srist, Jabalpur, MP, India

ABSTRACT: Cloud Computing is a rising field in the history of computing. It is a way to maximise the capacity and capabilities without spending a lot to buy a new infrastructure and software. Although it seems highly reasonable and usable, there is always the protection, security and privacy concerns related to cloud as the information and data could be accessed by cloud service providers at any time. Authentication is a vital and indispensable technology for data and information security. It is a mechanism to find proof of identities to get entry and access to the data and information in the system. Conventional password authentication mechanisms do not provide sufficient security measures for data and information in the cloud computing environment to the most modern ways of phishing and attacks. Therefore, we suggest a new authentication and integration framework for cloud computing to secure data and information hacks. User authentication in proposed work is performed on the basis of secure OTP & user profiles. It is verified on the basis of several security aspects and is verified to be available, accessible, feasible, secure, and user-friendly and provides strong authentication system. The proposed framework shows the close agreement with the standard criteria for security.

KEYWORDS: Authentication, Image OTP, Cloud security, SHA-512, Multifactor Authentication

I. Introduction

Ever since its genesis, cloud computing has been revolutionizing the way data storage and processing mechanisms are envisioned and implemented. It enabled the on-demand availability of services such as Software, Platform, Infrastructure (through SaaS, PaaS, IaaS respectively) and thus formed an economic solution to meet the ever-fluctuating demand for storage and computational resources by growing businesses. Cloud computing as a business paradigm has gone a long way from the early innovations of Salesforce.com and Amazon web services [**1**]. Today, in 2016, a whopping $32 billion is calculated to be spent on cloud IT infrastructure per year, according to International Data Corporation, the market intelligence firm [**2**]. This accounts for 33 percentage of the total IT infrastructure spending. Further, cloud infrastructure spending is expected to reach $52 billion in 2019 which is 43 percentage of the total IT expenditure.

The cloud is responsible for providing real time services such as storing the data, giving application and processing the data for consumers through the internet. The consumers can remotely store their data into the cloud and can enjoy the scalable services pay-on-demand [**3**]. Fig. 1 shows the basic structure of cloud computing where users access cloud services via the internet. As an emerging technology, it holds great potential albeit with its fair share of issues, perhaps the most prominent among which is ensuring security and privacy. As in traditional paradigms, authentication plays a major role in security in cloud computing. User authentication is an important scheme to ensure only the authorized users can access the server. This paper summarizes the existing authentication methods in CC, presents a classification system for the various methods and points out the advantages and disadvantages of each.

DOI: 10.15680/IJIRCCE.2016. 0412089

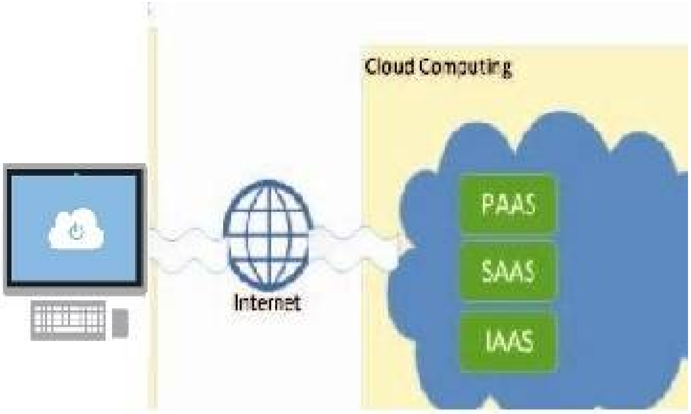


FIG 1. Basic architecture of Cloud Computing

II. SECURITY IN CLOUD COMPUTING

Nowadays, cyber warfare is arguably the most complex challenge in a distributed and multi- tenant environment. It is a complex job within the client-server architecture. When the data transfer to the cloud services, the requirements of security should be the most important. The European Network Information Security Agency (ENISA) enumerated the risks, recommendations and benefits for cloud computing [**4**]. It also lists the infection on confidential document, loss of governance, malicious insider, and insecure incomplete data. The Elastica 2015 shadow data report [**5**] it focuses on unauthorized apps discovered in an organization. It examines which type of data typically found in sharing apps, riskiest exposure, and what steps take to mitigate these security problems.

In this section, we briefly introduce about the major security concerns of cloud computing.

- *Software security:* It provides basic idea of software security come from the engineering software department that it continues to function correctly under the malicious activities. To build a cloud environment a central and critical problem is software security problem. It defects with security including implementation bugs, buffer overflow, designed flaws, error handling promises and much more [**6**].
- *Infrastructure security:* The most common and fundamental challenges is to demonstrate that the virtual and physical infrastructure of the cloud can be trusted. The attestation of the third party is not enough for the critical business process. It’s absolutely essential for the organization to be able to verify business requirements that the underlying infrastructure is secure.
- *Storage security:* In cloud storage system, end user stores the data in the cloud and no longer owns the data and where it's stored. This always has been an important aspect of quality of service. It ensures the correctness of user’s data in the cloud and by utilizing homomorphic token with distributed verification of erasure-coded data [**7**].
- *Network security:* In cloud computing, communication is via the internet and it is the backbone of the cloud environment.

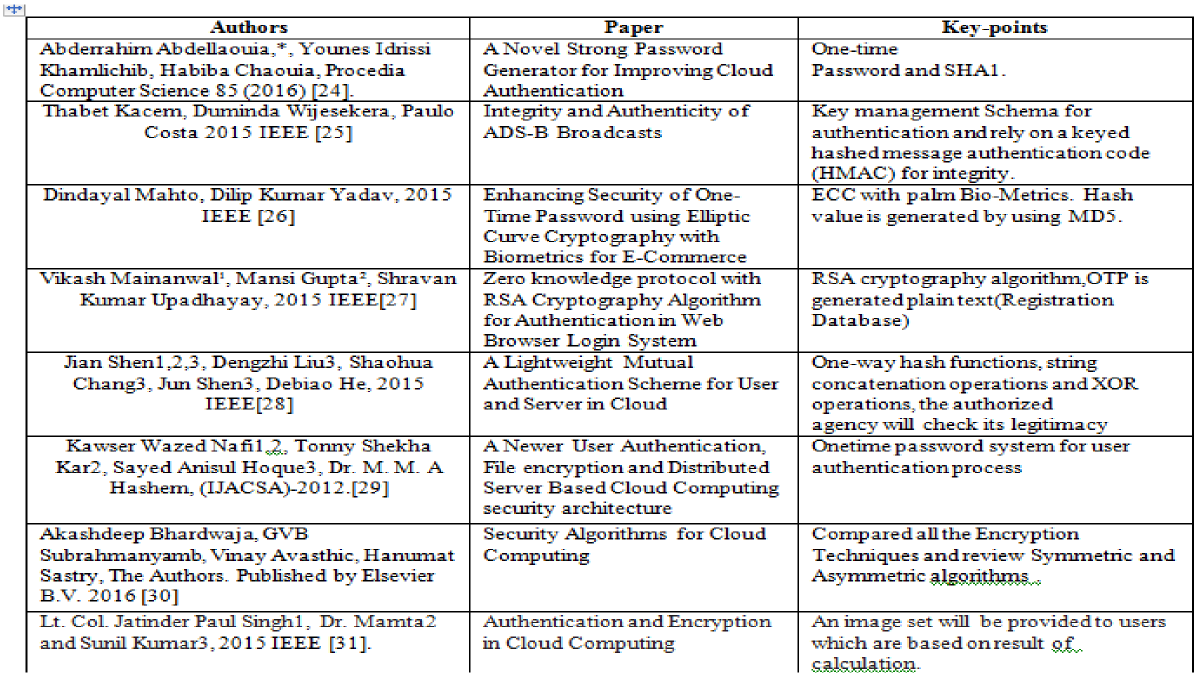
Network security concerns about both internal and external attacks. These attacks in the network can either occur in the virtual or physical network. Hanqian W., et al. [**8**] focuses on the virtual network in a Xen platform by discussing and analyzing its security problems.

III. LITERATURE SURVEY

This survey **encompasses** most of the major authentication schemes proposed in cloud computing so far. We briefly discuss the principles behind each authentication method. Further, based on the authentication criteria, we propose a classification scheme for the surveyed methods.

Table I summarize and compare the surveyed methods for authentication, highlighting the advantages, disadvantages and implementation stage of each.

DOI: 10.15680/IJIRCCE.2016. 0412089



Authors	Paper	Key-points
Abderrahim Abdellaouia,*, Younes Idrissi Khamlichib, Habiba Chaouia, Procedia Computer Science 85 (2016) [24].	A Novel Strong Password Generator for Improving Cloud Authentication	One-time Password and SHA1.
Thabet Kacem, Duminda Wijesekera, Paulo Costa 2015 IEEE [25]	Integrity and Authenticity of ADS-B Broadcasts	Key management Schema for authentication and rely on a keyed hashed message authentication code (HMAC) for integrity.
Dindayal Mahto, Dilip Kumar Yadav, 2015 IEEE [26]	Enhancing Security of One-Time Password using Elliptic Curve Cryptography with Biometrics for E-Commerce	ECC with palm Bio-Metrics. Hash value is generated by using MD5.
Vikash Mainanwal^1, Mansi Gupta^2, Shravan Kumar Upadhayay, 2015 IEEE[27]	Zero knowledge protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System	RSA cryptography algorithm,OTP is generated plain text(Registration Database)
Jian Shen1,2,3, Dengzhi Liu3, Shaohua Chang3, Jun Shen3, Debiao He, 2015 IEEE[28]	A Lightweight Mutual Authentication Scheme for User and Server in Cloud	One-way hash functions, string concatenation operations and XOR operations, the authorized agency will check its legitimacy
Kawser Wazed Nafi1,2, Tonny Shekha Kar2, Sayed Anisul Hoque3, Dr. M. M. A Hashem, (IJACSA)-2012.[29]	A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture	Onetime password system for user authentication process
Akashdeep Bhardwaja, GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastry, The Authors. Published by Elsevier B.V. 2016 [30]	Security Algorithms for Cloud Computing	Compared all the Encryption Techniques and review Symmetric and Asymmetric algorithms.
Lt. Col. Jatinder Paul Singh1, Dr. Mamta2 and Sunil Kumar3, 2015 IEEE [31].	Authentication and Encryption in Cloud Computing	An image set will be provided to users which are based on result of calculation.

TABLE I: Comparison of related work

Authentication is a security architecture that requires numerous methods of attestation from independent classes of credentials to check the identification of the user for login or other activities. It encircles two or more independent credentials: password - what the user recognizes and security token – what the user retains and biometric verification – who the end user is. The intention of Authentication is to form a covered shield and make it extra tiresome for an unauthorised user to access the object such as a location, computing device, network or database. If any one of these factor is compromised or damaged then the hacker is still required to successfully break the add-on authentication factor for breaching into the target [9].

IV. PROPOSED METHOD

The Figure 2 shown below represents architecture of proposed work. In cloud computing cloud application will be stored on cloud server. Client or User accesses these applications by sending request to server. Security is the major concern for cloud computing. Presented model represents a secure client authentication methodology for access the services of cloud.

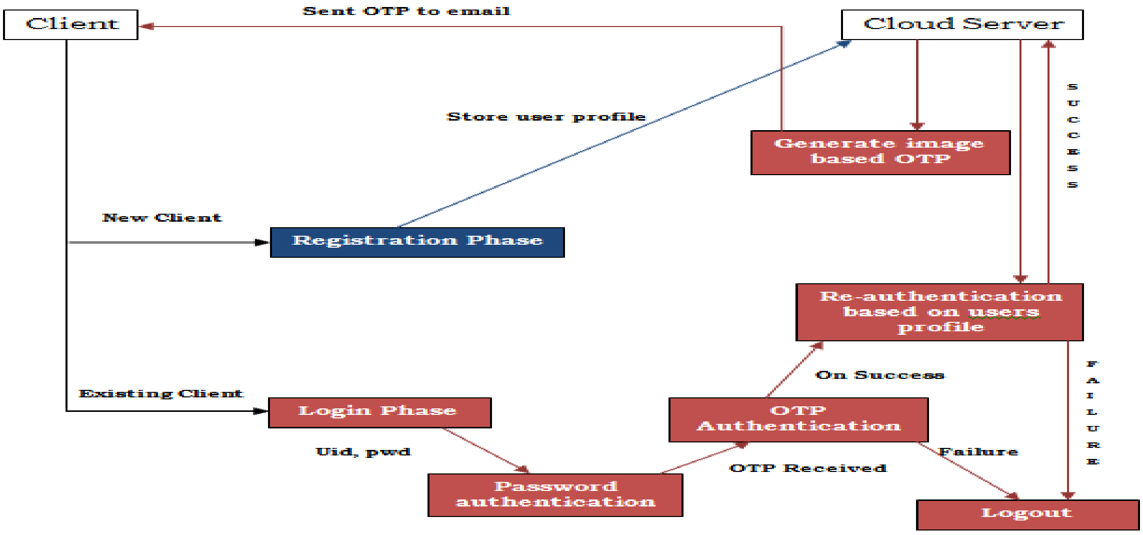


Fig 2: Proposed Model

Proposed method uses the concept of user profile based multifactor authentication. Firstly client should register in the system. In first step text based authentication is processed. In next step time synchronized OTP (One Time Password) will be generated using image based encryption with SHA512 and sent to client email. If this is valid, than re-authentication will be processed. For this user profile based three questions will be asked randomly in fixed time interval, if any one answer get wrong than client will be logout. If all three answers are correct than system will assume that client is authorized so client continues the work.

Our proposed model contains four phases:

1. User Registration
2. Text Based Authentication
3. OTP Generation & Authentication
4. Re-authentication

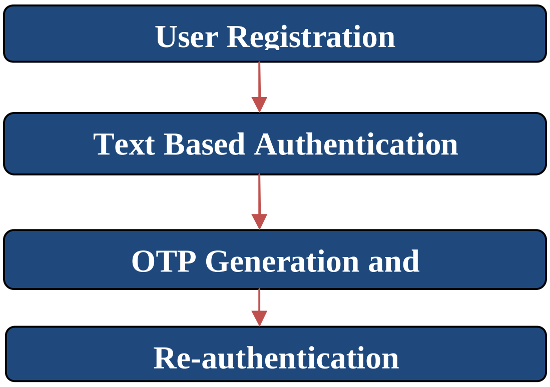
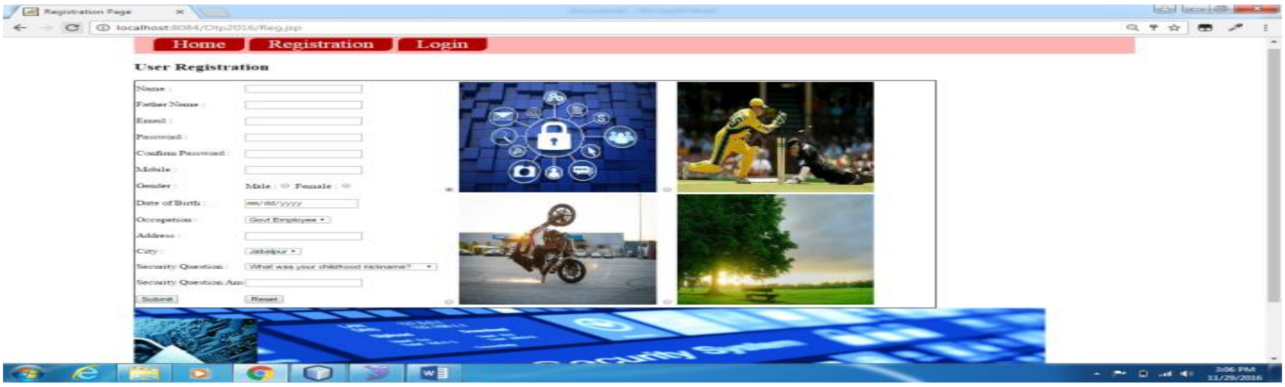


Fig 3: Proposed Model

V. RESULT

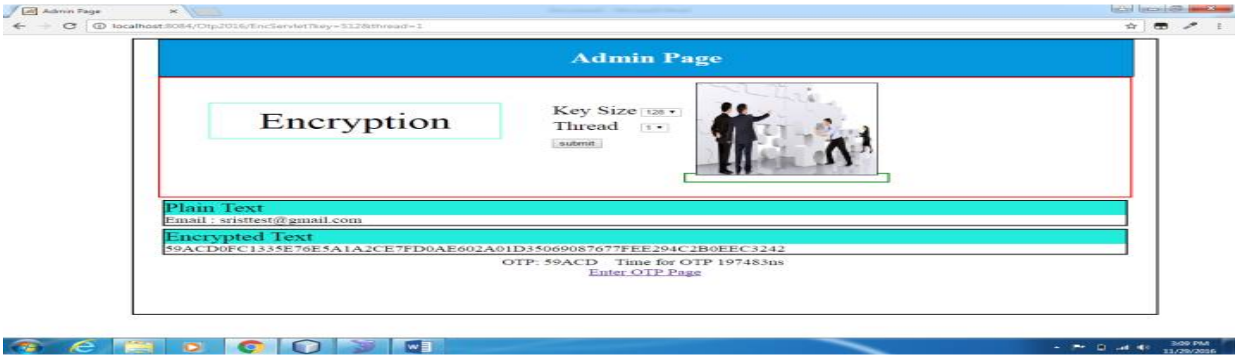
Figure below represents snapshots of proposed work.



User Registration

Name :	
Father Name :	
Email :	
Password :	
Confirm Password :	
Mobile :	
Gender :	Male : ○ Female : ○
Date of Birth :	mm/dd/yyyy
Occupation :	Govt Employee ▾
Address :	
City :	Jabalpur ▾
Security Question :	What was your childhood nickname? ▾
Security Question Ans:	

Fig 4: Registration Page



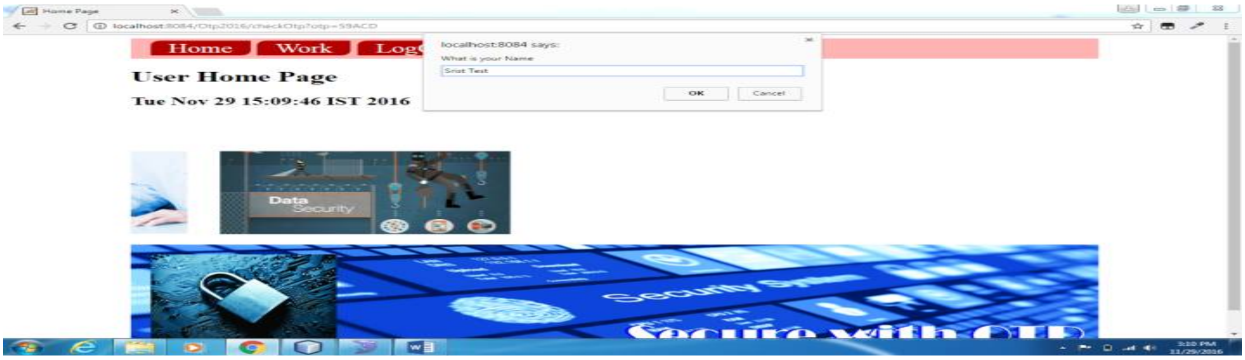
Key Size 128 ▾
Thread 1 ▾

Plain Text
Email : sristtest@gmail.com

Encrypted Text
59ACD0FC1335E76E5A1A2CE7FD0AE602A01D35069087677FEE294C2B0EEC3242

OTP: 59ACD Time for OTP 197483ns

Fig 5: OTP Generation Page



User Home Page

Tue Nov 29 15:09:46 IST 2016

localhost:8084 says:

What is your Name

Srist Test

Fig 6: Re-authentication Page

In proposed method, authentication will be on three layers-text based, OTP based and user profile based. OTP is generated by image as a key with using SHA512, so it will provide more security. Re-authentication is based on user's profile given at the time of signup. If OTP will be hacked by someone than re-authentication checks authenticity again so improves security.

VI. CONCLUSION

The hype of cloud paradigm is changing the IT industry; it brings many benefits to companies, organizations and even countries. Despite bringing several advantages, the cloud still is vulnerable to many security challenges. This is why security is the major challenge in the adoption of the cloud. The proposed model for authentication of a client on a cloud server solves following issues for authentication using multifactor approach. It keeps resistance against -token theft, token duplication, replay attack, eavesdropping, and man-in-the-middle attack.

REFERENCES

[1] X. Wang, A. V. Vasilakos, M. Chen, Y. Liu, and T. T. Kwon, “A survey of green mobile networks: Opportunities and challenges,” ACM/Springer MONET, vol. 17, no. 1, pp. 4–20, Feb. 2012.

[2] M. Chen, “MM-QoS for BAN: Multi-Level MAC-Layer QoS Design in Body Area Networks,” in Proc. IEEE Globecom, Atlanta, GA, USA, Dec. 9–13, 2013.

[3] RSS 2.0 Specification, Advisory R. S. S. Board, Jun. 2007.

[4] Power Law. http://en.wikipedia.org/wiki Power_law

[5] X. Li, J. Yan, Z. Deng, L. Ji, W. Fan, B. Zhang, and Z. Chen, “A Novel Clustering-based RSS Aggregator,” in Proc. 16th Int. Conf. World Wide Web, 2007, pp. 1309–1310.

[6] M. Chen, Y.Wen, H. Jin, and V. Leung, “Enabling technologies for future data center networking: A primer,” IEEE Netw., vol. 27, no. 4, pp. 8–15, Jul. 2013.

[7] C. Lai, H. Chao, Y. Lai, and J. Wan, “Cloud-assisted real-time transrating for http live streaming,” IEEE Wireless Commun., vol. 20, no. 3, pp. 62– 70, Jun. 2013