Access Control for Cloud Computing Through Secure OTP Logging as Services

Priyanka Patel
Samrat Ashok Technological Institute Department of Information Technology,Vidisha,India

Nirmal Gaud
Samrat Ashok Technological Institute Department of Information Technology,Vidisha,India

ABSTRACT
And non-linear interpolation. The empirical evaluation shows that the proposed system is better than current Access control mechanism is very important phase over internet based services. Cloud computing is internet based service application provide variety of services such as IaaS, PaaS and SaaS. For the accessing of cloud services cloud service provider provide user login information in terms of username and password. The login information is easy hacked and cracked by other party and the security strength of cloud computing is decreases. Now days some authors used dual authentication mode in terms of mail conformation and one time password. The one time password increase the security strength of access control over cloud computing. In this paper proposed a secured authentication system based on secured OTP based logging system in cloud computing environment. The proposed algorithm is a combination of hash algorithm system.

Keywords
Cloud Computing, OTP, Hash Function, Access Control

1. INTRODUCTION
Security and access control over internet based services always a challenging issue. The internet based services offer various services over internet such as ecommerce, web based application and cloud computing. Now days the utility of cloud computing based services are increase and the growth of cloud market is approx is 100$ billion. The increasing market and utility compromised the security issue of cloud computing in terms of data tampering, account hacking and many more man in middle attack. For the protection of user account and data cloud computing provide the primary level security in terms of username and password[1]. The username and password process is easily trapped and hacked by some predefined tool and normal user faced a security threats. For second level authentication cloud service provider used third party auditor. The concept of third party auditor also used primary authentication concept and compromised same scenario of security threats. And the processing of TPA is costly and not provide it complete secured environment. Now a day's used second level authentication technique based on one time password (OTP). The generation and transmission of OTP password is also a serious issue, some organization used mail facility for transmission and some are used mobile phone device[2]. The mobile phone device used SMS facility for receiving an OTP password. The SMS facility used a standard template for the processing of password. The generation of OTP password used cryptography algorithm and hash function. Some authors linear and non-linear interpolation with hash function. The authentication of OTP process increases the security strength of cloud access model. The static authentication system of cloud computing overcome the limitation of dynamic login and authentication system over cloud computing. The main weakness static password is that if it is simple it can be easily attacked by Trojan attacks, password attacks, or by simply guessing it. A static password is the usual way that a user authenticates when log in to a service is needed. The password is usually a secret word or phrase picked by the user and used together with the user's username.[3,5] It can be used when logging in to your own personal computer, an e-mail system, an online community etc. Cloud computing security should be very secure and reliable otherwise the people confidential information will get Compromise. People Still Using the same passwords to access the different accounts on the cloud which is very insecure and third party cloud computing service providers are not providing proper security about static passwords. This is the big disadvantage of the cloud computing environment because static password can be attacked by unauthorized user and account information can be easily taken by hackers. In this paper proposed a langrage's interpolation based one time password generation with MD5 hash algorithm[6,7]. The proposed algorithm is very efficient in terms of computational complexity and very complex in terms of security strength. In section II discuss the related work. In section III discuss the OTP MD5 and AES algorithm. In section IV discuss the proposed methodology. In section V discuss experimental result analysis and finally discuss conclusion & future work in section VI.

2. RELATED WORK
In this section discuss the related work in the field of secured one time password generation and authentication mechanism by different author

In this paper [1] authors describe the generation of one time password based on MD5 algorithm. the MD5 algorithm basically used for the process of hash generation. The hash code send along with OTP password for the process of protection for any type of man in middle attack. The authors method tested on various online tools such as kill will and some other tools such as key logger and password guessing tool for the braking the strength of algorithm. Authors also test the cryptography analysis tool for the measurement of strength of one time password.

In paper this paper [2] authors used the concept of MD5 hash function for the purpose of hashing of one time password and some other password. The authors derived the table for allocation and distribution of password. The allocated and distributed password tested over local area network for the validation purpose. The authors also analyzed the cryptography analysis test for the time and differential attack analysis.

[3] In this paper authors describe the process of website authentication system based on the concept of primary and

secondary authentication system. In primary authentication system the website provide the username and password for the authentication and secondary the website provide the facilitation of dynamic password generation for the purpose of authentication.

[4] In this paper, authors describe the method of secured login system over cloud computing environment. The secured login system provides primary as well as secondary login system for user authentication process. The secondary user authentication system is more reliable and secured than primary authentication system. The authentication policy also provides the trust level for the transmission of data over cloud network.

[5] In this paper authors discuss the multi-authority system for the authentication of user. The multi-authentication system based on different key cryptography technique. the multiple key cryptography technique used the concept of private and public key system.

[6] In this paper author studies the security management methods of cloud computing authorized user, analyzes the vulnerabilities of OTP and proposed security authentication scheme based on OTP authentication. This authentication enables two-way authentication between the user and the service provider, effectively prevent middleman attack, reduce information leakage and relies secure communications. OTP is a simple authentication technology that can be quickly loaded onto the system without the need for any additional hardware. It uses a one-time pad method can effectively guarantee the security of user identity, at the same time, it does not require third-party notarization low cost, suitable for network environment is not yet mature, but its existence decimal vulnerable to attack, middle attack security vulnerabilities, therefore, requires the use of certain methods to make it safe and reliable.

[7] Here they have proposed new approach to access cloud using login credential and OTP (one time password) for secure access of cloud storage. Cloud computing based applications has many benefits but it has several security problems like Authentication and Access Control, Trust, Legal Issues, Confidentiality, Data Encryption, Early Approaches, Querying Encrypted Data, Denial of Services, Malicious Insiders, Data Breach, Vulnerability in virtualization, etc. To access cloud based application user need to login, but many users don't know about whether their login is secure or not, and providing login credentials to correct site etc.

[8] In this paper author focus on authentication and transmission encryption in cloud services. The current solutions used today to login to cloud services have been investigated and concluded that they don't satisfy the needs for cloud services. They are insecure, complex or costly. It can also be concluded that the best encryption algorithm to use in a cloud environment is AES, which is secure algorithm. This paper have resulted in an authentication and registration method that is both secure and easy to use, therefore fulfilling the needs of cloud service authentication. The method use a regular mobile phone to generate one time passwords that is used to login to cloud services. All of the data transmissions between the client and the server have been configured to use AES encryption. The conclusions that can be drawn is that the security proposal implemented in this paper functions very well, and provide good security together with an ease of use for clients that don't have so much technical knowledge.

[9] In this paper they describe the design and implementation of a semantic web based framework for secure information integration. In particular, we have evaluated Amazon's Simple Storage Service's ability to provide storage support for large-scale semantic data used by a semantic web-based framework called Blackbook. They describe cryptographic techniques for enforcing the protection of published data on Amazon S3. We also explore access control issues associated with such services and provide a solution using Sun's implementation of eXtensible Access Control Markup Language (XACML).

In this paper [10] authors describe the security models of security threats in cloud computing environment. The proposed model describes the utilization of EIGamal algorithm for the process of encryption and description. The proposed security model used for the dual authentication of software as service application over cloud network.

3. OTP AND LANGUAGES INTERPOLATION

The one time password (OTP) is concept of dynamic authentication and verification module in cloud security system. The generation and transmission is major issue of OTP in cloud environment. For the generation for OTP algorithm used various cryptographic algorithms such as RSA, DES, RC4 and other hash based algorithm. Some authors used random OTP password generation technique. The Random OTP password generation technique is easily predictable for hacker and man in middle attack. For the generation of OTP used langrage's polynomial equation along with AES cryptographic technique along with MD5 algorithm. The AES algorithm is very efficient in terms of RSA, DES and RC4. The calculation and multiplication of key is generated by interpolation derivates for the processing of password. The length of password is generated in terms of iteration manner and never fixed but length of message is fixed.

3.1 Languages Interpolation

a. A set of data points (x_i, y_i), i= $0, 1, \ldots, n$ obtained from a function $f(x)$ so that$y_i = f(x)$, $i = 0, 1, \ldots, n$. A suitable function for interpolation $I(x)$ is expressible as

b. $I(x) = \sum_{i=0}^{n} L_i\ (x).f(x_i)$ (1)

c. $= L_0\,(x).f(x_0) + L_1(x).f(x_1) + \cdots + L_n(x).f(x_n)$ (1a)

d. The functions $L_i(x)$, $i = 0, 1, \ldots, n$ are chosen to satisfy

e. $L_i(x) = \begin{cases} 0 & x=x_0, x_1, \ldots x_{i-1},\ x_{i+1}, \ldots x_n \\ 1 & x=x_i \end{cases}$ (2)

f. Before we actually define the $L_i(x)$ functions, let's be certain we understand the implication of Equations (4.1) and (4.2). The best way to accomplish this is simple to choose a value for "n" and write out the resulting equations. Suppose we have the four data points $[x_i, f(x_i)]$, $i = 0, 1, 2, 3$. From Equations (4.1) with $n = 3$, the interpolating function $I(x)$ becomes

g. $I(x) = \sum_{i=0}^{3} \mathrm{L_i(x).\,f(x_i)}$ (3)

h. $= L_0(x).f(x_0) + L_1(x).f(x_1) + L_2(x).f(x_2) + L_3(x).f(x_3)$ (3a)

i. And it remains to be shown that $I(x)$ at x_0, x_1, x_2 and x_3,

j. $I(x_0) = L_0(x_0).f(x_0) + L_1(x_0).f(x_1) + L_2(x_0).f(x_2) + L_3(x_0).f(x_3)$ (4)

k. $I(x_1) = L_0(x_1).f(x_0) + L_1(x_1).f(x_1) + L_2(x_1).f(x_2) + L_3(x_1).f(x_3)$ (4a)

l. $I(x_2) = L_0(x_2).f(x_0) + L_1(x_2).f(x_1) + L_2(x_2).f(x_2) + L_3(x_2).f(x_3)$ (4b)

m. $I(x_3) = L_0(x_3).f(x_0) + L_1(x_3).f(x_1) + L_2(x_3).f(x_2) + L_3(x_3).f(x_3)$ (4c)

n. According to Equation (2), $L_0(x_0) = 1$ and $L_1(x_0) = L_2(x_0) = L_3(x_0) = 0$.

o. Equation (4) is simplified as shown below.

p. $I(x_0) = L_0(x_0).f(x_0) + L_1(x_0).f(x_1) + L_2(x_0).f(x_2) + L_3(x_0).f(x_3)$

q. $= 1.f(x_0) + 0.f(x_1) + 0.f(x_2) + 0.f(x_3)$

r. $= f(x_0)$

s. By the same reasoning, $I(x_1) = f(x_1)$, $I(x_2) = f(x_2)$ and $I(x_3) = f(x_3)$ which means the interpolating function $I(x)$ passes through the given set of data points.

t. The analytical from of $I(x)$ depends on the functions $L_i(x)$, $i = 0, 1, \ldots, n$ that satisfy Equation (4.2). They are called Lagrange coefficient polynomials and are defined as follows:

u. $L_i(x) = \prod_{j=0,\ 1,\ldots,i-1,\ i+1,\ldots\ldots,n} \cdot \left(\frac{x-x_j}{x_i-x_j}\right)$ $i = 0,1,2,\ldots\ldots n$ (5)

4. PROPOSED METHOD

In this section discuss the modified algorithm of OTP generation using the interpolation derivatives and MD5 hash algorithm. the interpolation derivates derived the input massage in terms of username and password and create a variable size matrix for the processing of input data of hash algorithm and randomly select the 6 bit data for OTP transmission.

- Let x is the input size of username and password (x1,…….xn).
- Let m is the no. of vector input point for the processing of data(v1,v2,……., vm)
- Compute the value of round integer data for the processing of randomization.
- For each random data manipulated as interpolation nominator and dominator.
- For each estimate value for the minimization factor.
- $Minimize \sum_x L(x) = J(x), B(x) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (a)$

  Here j is total message and B is hash function input value
- $B(x) = C(x) + L(x) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (b)$

  Here C is cost interpolation
- $B(x) \leq \sum_{i=1}^{k} Mi \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (c)$

  Total meassage passes through MD5 algorithm.
- $F(x) \leq \sum_{i=1}^{k} MD5(i,k) \ldots\ldots\ldots\ldots\ldots (d)$
- The processing of hash byte data

  $otp(Li, Rj) = \begin{Bmatrix} Allocated(Ta, tready(Li, ai)) if\ Li \neq Ai\ empty \\ 0\ otherwise \end{Bmatrix} (e)$
- Finally send the mobile
- $ROTP = Max_{Li \in Ai(MD5(i,k)) + \sum Bi} \ldots\ldots\ldots\ldots\ldots (f)$

  Process is authenticated

5. EXPERIMENTAL ANALYSIS

For the validation of modified process of one time password generation used JAVA development software for the purpose of implementation. In java implementation phase create cloud server provider for initial login information such as username and password. After the authentication of login and password, the server generates the OTP password and sends to user mobile phone via standard SMS template. The generation time of OTP with MD5 is high in terms of AES and interpolation derivates. For the security verification also measure the time session of OTP message send and receive by the user for the authentication.

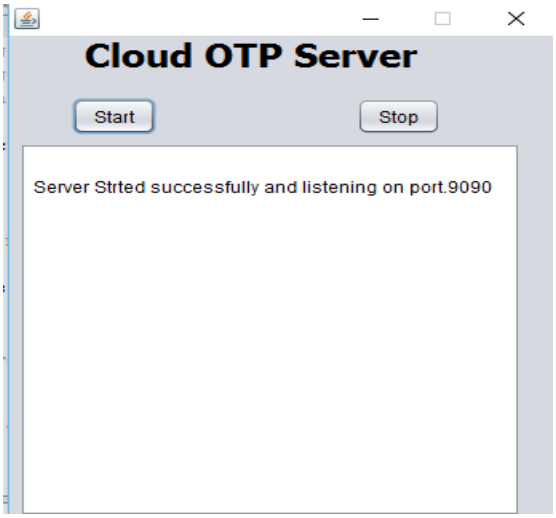

Figure 1 show that window of cloud server OTP center. The cloud OTP center mange the primary information of user in terms of username and password.

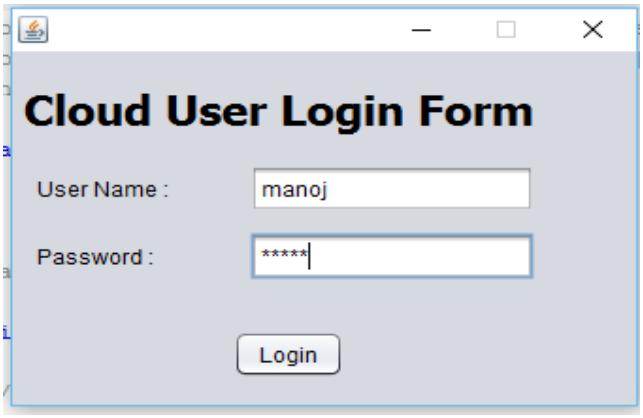

Figure 2 shows that the client login from for the processing of user login system.

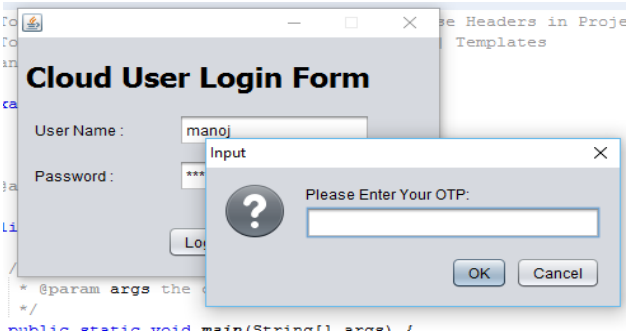

Figure 3 shows that input of one time password login window for the processing of OTP password receive by user mobile phone.

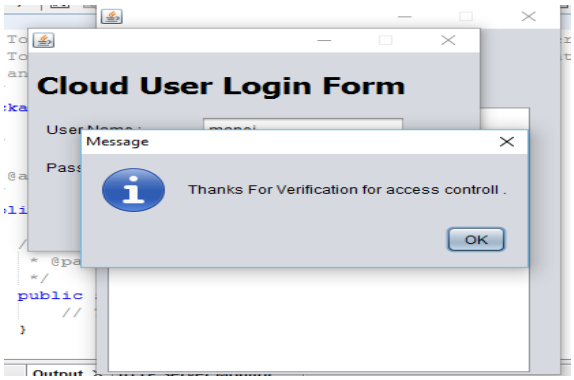

Figure 4 shows those verification windows of OTP password and validation of user in two level authentication modes.

Table 1 shows that the user authentication time in two different mode of algorithm.

Method	User	Time in millisecond
OPT+MD5	MANOJ	2.32
LD+MD5	MAOJ	1.829
OPT+MD5	PRIYANKA	1.89
LD+MD5	PRIYANKA	1.78

6. . CONCLUSION & FUTURE SCOPE

In this paper proposed an OTP based cloud access control model for enhancing the security of cloud computing environment. The proposed OTP generation algorithm used AES encryption algorithm and interpolation derivates for the processing of mathematical operation. The proposed algorithm takes minimum key generation time from other OTP generation algorithm. The proposed algorithm reduces the security risk over cloud based services. For the validation and verification of proposed algorithm used Cain and Abel tool for password cracking and recovery. The proposed algorithm OTP is not hacked and cracked over this tool. The derivates of interpolation is very complex in terms of guessing and predictability. In future used another Oder of polynomial for the generation of OTP password for increase more reliable verification system

7. REFERENCES

[1] Eko Sediyono , Kartika Imam Santoso ,Suhartono "Secure Login by Using One-time Password Authentication Based on MD5 Hash Encrypted SMS" IEEE 2013 PP1604 -1608.

[2] Antony G. Robertiello, Kiran A. Bandla "Attacks on MD5 Hashed Passwords" ECE GMU 2005 PP 1-14.

[3] Vimmi Pandey "Securing the Cloud Environment Using OTP" International Journal of Scientific Research in Computer Science and Engineering PP 38-43.

[4] Shams Zawoad, Amit Kumar Dutta, and Ragib Hasan "Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL-13, 2016. Pp 148-162.

[5] CHEN Yanli, SONG Lingling, YANG Geng "Attribute-Based Access Control for Multi-Authority system with constant size ciphertext in cloud computing" China communication, 2016. Pp 146-162.

[6] Yuan BaoLi "Research on the Security Management Method of Cloud Computing Authorized User Based on Anonymous OTP" 5th International Conference on Computer Sciences and Automation, 2015. Pp 1-4.

[7] Ankush Kudale, Binod Kumar "Protected Authentication by Login Credential and OTP for Cloud Based Application" International Journal of Computer Application, Vol-5, 2015. Pp 42-48.

[8] Indrajit Das, Ria das "Mobile Security (OTP) by Cloud Computing" , IJIET, 2013. Pp 284-300.

[9] Pranav Parikh, Murat Kantarcioglu, Vaibhav Khadilkar, Bhavani Thuraisingham, Latifur Khan "secure information integration with a semantic web-based framework" IEEE, 2012. Pp 659-666.

[10] Mohd Fawzi Al-Hunaity, Jawdat Alshaer, Osama Dorgham, Hussam Farraj "Security Model for Communication and Exchanging Data in Mobile Cloud Computing" International Journal of Computer Trends and Technology, Vol-30, 2015. Pp 138-146.

[11] Vishal Paranjape, Vimmi Pandey "An Approach towards Security in Private Cloud Using OTP" International Journal of Emerging Technology and Advanced Engineering, Vol-3, 2013. Pp 683-687.

[12] Soorat Hussain "Access Control in Cloud Computing Environment" Int. J. Advanced Networking and Applications, Vol-5, 2014. Pp 2011-2015.

[13] Ankita Patil, Kiran Zambare, Preeti Yadav, Pankaj Wasulkar "Secure File Access Using Md5 For One Time Password Generation On Cloud" IJEEBS Pp 345-348.

[14] Kenneth G. Paterson ,Douglas Stebila "One-time-password-authenticated key exchange (full version)" 2010 IACR Pp 1-18.

[15] D.Parameswari , L.Jose "SET with SMS OTP using Two Factor Authentication JSA" 2011 Pp 106-112.

[16] Uma Tejaswi, Srilatha.B IJESC "Web Security with OTP by Using Android Mobile" 2015. Pp 831-835.

[17] Mohammed Alzomai Audun Jøsang "The Mobile Phone as a Multi OTP Device Using Trusted Computing" IEEE 2010. Pp 75-82.

[18] T.Venkat Narayana Rao, Vedavathi K "Authentication Using Mobile Phone as a Security Token" IJCSET 2011. Pp 569-574.