ISSN:0975-9646

Securing the Clouds using OTP Technology

Sandeep Mali, Kishor Sawant, Nilesh Thombare

Computer Department,
Savitribai Phule Pune University
Dr. D Y Patil School Of Engg Academy, Ambi,
Pune,Maharashtra,India.

Prof. **Vinod Bharat**

HOD Computer Department,
Savitribai Phule Pune University
Dr. D Y Patil School Of Engg Academy, Ambi,
Pune, Maharashtra, India.

***Abstract* — One of most important revolution in data storage and it's retrievability in IT world is emerged in the form of Cloud Computing. Cloud computing have large impact over IT industry. But as the need increases in storage capacity the multi-cloud comes in action. Multi-cloud gives better facility in storage or security about the data. But there are still many problems which are arriving in today's world over cloud computing.**

As we all know One-Time Password is latest authenticating process used for recognizing the accurate user to optimizing its own facilities. OTP gives much better secure environment to user while using clouds. Our research is going to take place on what kind of problem users are facing while using cloud in the form of storing data or its security and how OTP can help to solve such kind of problems.

***Keywords*—Cloud Computing, OTP (One Time Password), Storage Security, Genetic Algorithm.**

I. INTRODUCTION

Cloud storage system is becoming the world's one of simple, fine and popular technology because of data storage on one point from anywhere and we can interact with that data easily from everywhere [1][2]. Cloud computing is used upon huge amount of data and processing over that data by various application because cloud computing provides such environment to user [4]. Use of cloud computing is increasing day by day in many industrial areas [3]. Cloud Storage Service (CSS) gives benefit over managing and maintaining data manually [4].

A Cloud Storage System ensures that user gets the file which user has demanded for i.e. user is able to retrieve the data they want [5]. Cloud computing is the internet based development in which a centre has been found for the storing the data [6].

Basically, In Cloud Computing environment the user can store and can manipulate its own data from ant where at any time which we called remote access. Cloud storage system provides the service like SAAS (Software As A Service), PAAS (Platform As A Service).

Because of facilities provided by the Cloud, Cloud Computing covers very wide area of computation. Cloud computing is used in each and every field.

There are 3 main entities involved in Cloud Computing environment [1,4]-

1. User – This is one who responsible for uploading and manipulating a data.

2. Cloud Server – These are provided by Cloud Service Provider for storing data in huge amount.

3. TPA (Third Party Auditor) – Auditing of the data is done by this entity. It verifies the query fired over data which is on Cloud.

Cloud computing is important area it provides the online storage to the user. So user can get on demand and cost effective services from cloud but it requires user to trust on cloud because of full authority, otherwise it may be lead to misuse or changing crucial data by private cloud in multi-cloud environment.

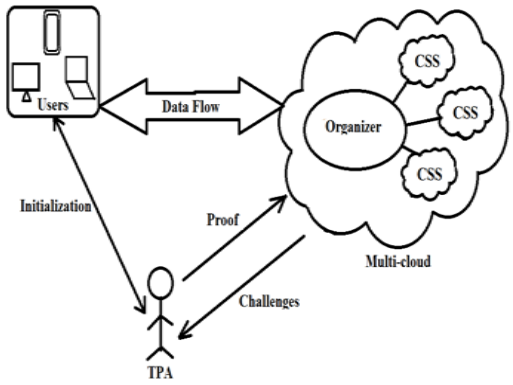

Fig. 1 Multi-cloud Architecture

In recent time Security over Cloud data has become the biggest issue about the cloud storage service. Cloud Storage service having problems like Data integrity, Data intrusion, Service availability, Hackers attack over data [3]. So, as per our research OTP is the way to solve the hacking problem.

II. RELATED WORK

Our survey describes the following major factors. These factors having the large impact on Cloud Security:

A. One-Time Password(OTP)

Authentication is process in which authorized user has rights to access particular resource. Only authorize user can access this resource.

There are various types of methods available for authentication.

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

In Knowledge based authentication password is very important. Password is used for authentication.

There are two types of password.

1. Alphanumeric password
2. Graphical password

In Alphanumeric password, there is sequence of alphabets, numbers and special characters. So this useful for create password. This password should not guesswork but hard to remember. For example Most people combines there name with birth date or numbers related to them. Such password can be easily cracked. If we set passwords with random character like "Nilu59Nryz3" is strong password but hard to remember. To overcome this problem pictures are used for password. This password is called as graphical password. These passwords are easy to remember but shoulder surfing attack is possible.

In Token based authentication user has token is more important. Token is used for authentication. For example Credit card.

In Biometric authentication user is authenticated using users behavioural and personal properties. This is unique for each other. For example face recognition, fingerprint, and voice recognition.

One time password is very simple and more popular forms of two factor authentication today. It is valid for only one time login session. One time password is strong authentication provides much better protection to corporate networks, online banks account and other systems containing sensitive data. This algorithm makes use of randomness. This is necessary otherwise it would be easy to find future OTPs from observing previous ones.

In today's world of internet we have to deal with many security issues like virus, spyware, phishing, outdoor theft, etc. It leads to the compromise our authentication system so new popular system which gives you a unique authentication password key to minimize the security problem is nothing but a One-Time Password in short OTP. It used in image authentication, transaction, mobile verification and other areas which require authenticate the user [7].

In multi cloud environment authentication issues like user identity, data security, physical security, application security, continuous data availability, piracy, compliance, governance, etc. are occurs [8].

For authentication of user password used widely in many applications and systems, but in one unique password system get weak due to reasons like unique password can guess easily by observing the users nature, or lack of care about worker or users. Once the password is hacked it is easy to theft to use again and again. So other approach which is gives user each time one of kind new password through OTP for granting permission to user in cloud [9].

It also free user from remembering password or reuse of same key headache. Every time login session new password is generated to authenticate user, also OTP ensure safety and it user friendly. There are many algorithms to generate OTP. Now a day's most popular is the generic algorithm to generate OTP.OTP typically generate from prediction of successor OTP and hash function.

B. Techniques to generate OTP

1. Time-synchronized OTP
2. A counter-synchronized OTP

Time synchronized OTP password is must be used in specific time interval after generation of password. It used in specific time otherwise it gets expired & generate new OTP. In other counter synchronized OTP techniques counter is synchronized to user device and OTP generation server in which each time login counter advanced or increases.

There are two modes to deliver OTP through mobile Messaging service or other is instant messaging service and email [10].

III. GENETIC ALGORITHM

Cloud computing is use of the internet and distributed servers to storing the lot of data of the users. Cloud computing is a type of online computing that believes in processing power, sharing computing resources and storage based on demand rather than dependent on local servers. Cloud computing is highly growth in every area of organization.

Cloud computing has become an entire and most important part of many developing education area and organizations. The necessary role of the cloud comes from its ability to provide easily bent, online and on time support for using its platform, services and infrastructure as a resources. A cloud computing resource includes security, data, storage, infrastructure and software which are delivered to the user.

Cloud computing is classified into four category model.

1. Public Cloud
2. Private Cloud
3. Hybrid Cloud
4. Community Cloud

Public cloud can everyone access and private cloud access only private users. Hybrid cloud is combination of private and public cloud. Community cloud is access by specific organization like company or education.

Genetic algorithm is the research field of John Holland. It is based on the principal of natural genetics. Genetic algorithm maintains initial population and generates a solution from that population. For that solution, population apply operators of selection, crossover and mutation to find a optimize solution.

In proposed system, we are using genetic algorithm for obtaining dynamic password. These passwords are dynamic in nature. Genetic algorithm based on different variation and selection. Genetic algorithm uses an evaluation function means a fitness function. Genetic algorithm is use a heuristics optimization algorithm for dynamic password [12].

Genetic algorithm uses the variables in the form of binary string {0, 1}. Population is choosing called as chromosomes. This population offspring is produced by applying the mutation and crossover operator. Population for producing offspring are according to their fitness value and parents choose from that value. Fitness value of offspring is calculated and less fit offspring is compulsory deleted [11].

Genetic algorithm obtained five following steps:

1. Initialization
   In Genetic Algorithm first step is to select the population of chromosomes. Apply fitness function and calculated of all these value of chromosomes. Initial population size should be random. “Seeding” is another possible solution of initial population. Means initial population of Genetic Algorithm should be same other heuristic technique produces good results.
2. Selection
   Fitness function is important in Genetic Algorithm. Using fitness function, produced the chromosomes value. The chromosomes that are to be select for reproduction select according to fitness value. So that more fit chromosomes has more chance for reproduction.
3. Cross-over
   After choosing the chromosomes fitness value next step is to perform the crossover operation. Few chromosomes of one parent is replace with other parent. So new offspring generated having characteristics similar to that of their parents.
   Example we have two parents P1 and P2 as:
   P1=11011000
   P2=10010001
   And after crossover the offspring’s are as:
   X1=11010001 and X2=10011000
4. Mutation
   After performing crossover, the next step is mutation. In some cases crossover is not used. Mutation is directly performed. Mutation is a common operator used to help preserve diversity in the population by finding new points in the search pace to evaluate. When a chromosome is chosen for mutation, a random change is made to the values of some locations in the chromosomes.
5. Termination

In last step in finding genetic algorithm, the all values and data is get erased. All values get terminated.

We can provide security to multi cloud and user for transaction of data by one time password generated. Genetic algorithm will give each time dynamic password and this password is deal with as a one-time password for transaction of data between cloud and user. It is one time password so that each time of transaction, the password is going to change. Even one time password is hacked but next time it is not possible to use for transactions because it is going to dead for transaction. For new OTP is generated. STATIC password is easy to crack but dynamic password is not easy to crack. One time password is time oriented and attempt based. It means one time password is time limited password. Over the time of password then password become invalid or expired.

Following figure shows the constructional architecture as how the Genetic algorithm works:-

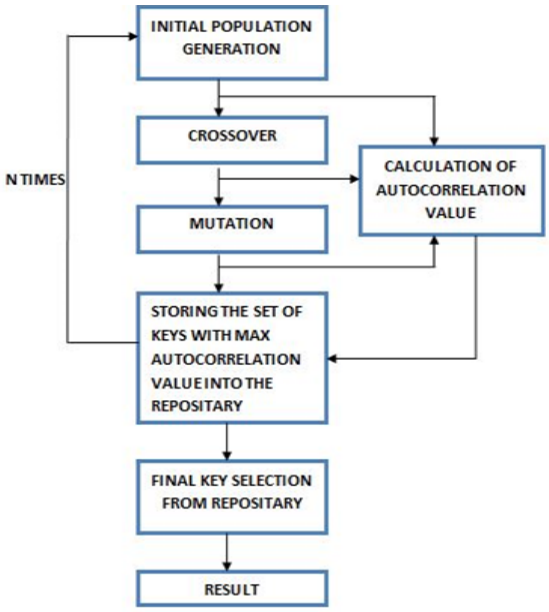

Fig. 2 Architecture of Genetic Algorithm

If unauthorized user enter wrong one time password then after three time’s wrong attempt the system will automatically logout. Genetic algorithm performs great work of obtaining dynamic one time password on each request of user. Then user can access data from cloud. Genetic algorithm will produce optimum random values. This random values used as a dynamic password. Each time it will mutate different values. So that is not giving to be same produce password. So Genetic algorithm is not reversible [12].

IV. Conclusions

Hence as describe in paper the Cloud technology is widely adapting technology because of its features. But security problems occurred in Cloud data is the issue while using the Cloud system by any user. OTP is one of the ways to solve the data security. Using OTP for user can access his own data in secured environment. Genetic algorithm for use of OTP is beneficial. In future more techniques like cryptography can be applied for more secured environment to user.

Acknowledgment

We would like to acknowledge our guide and HOD of our computer department Mr.Vinod Baharat sir for guiding and providing the helpful information in this paper. We would also like to thank to our staff teachers to give us support in various way.

REFERENCES

[1] He Kai, Huang Chuanhe+, Wang Jinhai, Zhou Hao, Chen Xi, Lu Yilong, Zhang Lianzhen, Wang Bin, "An Efficient Public Batch Auditing Protocol for Data Security in Multi-Cloud Storage",8th ACGC, 978-0-7695-5058-9/13, DOI 10.1109,IEEE,2013.

[2] R. H. Katz, A. Fox, R. Griffith, A. D. Joseph, A. Konwinski,G. Lee, M. Armbrust, D. A. Patterson, A. Rabkin and M. Zaharia, "A view of cloud computing,"Commun. ACM, vol. 53, no. 4, pp. 50-58, 2010.

[3] M.A. AlZain, E. ardede, B.Soh, J.A. Thom, "Cloud Computing Security: From Single to Multi-Clouds,"inProc of the 45th Annual Hawaii International Conference on System Sciences, 2012, pp. 5490-5499.

[4] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds,"in Proc. ACM Symposium On Applied Computing, 2011, pp.1550-1557.

[5] Juels and B. S. Kaliski, "PORs: Proofs of Retrievability for Large Files,"in Proc. ACM CCS, 2007, pp. 584-597.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing,"in Proc. of ESORICS, 2009, pp. 355-370.

[7] Kenneth G. Paterson,Information Security Group, Douglas Stebila, Information Security Institute "One-time-password-authenticated key exchange" September 4, 2009.

[8] Richa Chowdhary and Satyakshma Rawat "One Time Password for Multi-Cloud Environment" 2013, IJARCSSE March - 2013, pp. 594-597.

[9] W.B.Hsieh, J.S.Leu: "Design of a time and location based one time password authentication scheme", 7th IEEE International Conference,2011.

[10] Himika Parmar,Nancy Nainan and Sumaiya Thaseen "Generation of secure one-time password based on image authentication" CS & IT-CSCP 2012.

[11] Neha Sharma, Kiran Gautam,Pravin nagar "One Time Password System for Security over Clouds" ,vol no 4, Issue 7, July 2014.

[12] Nilesh Khankari, Geetanjali Kale, "Survey on one time password", vol 9, issu3, march 2015.

[13] Prajakta sadafule, Kumud Wasnik ,"Multi cloud security using one time password (OTP) by Genetic Algorithm",2014.