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. 3, Issue 12, December 2015

Multi-Cloud Security using One Time Password(OTP) by Genetic Algorithm(GA)

Prajakta S.Sadafule, Kumud Wasnik

M.Tech Scholar, Dept. of CST, Usha Mittal Institute of Technology, SNDT, Mumbai, India

Asst. Professor, Dept. of CST, Usha Mittal Institute of Technology, SNDT, Mumbai, India

ABSTRACT: Cloud and this will avoid the problem low rate of data availability. So for providing high rate of availability of data in Multi-cloud we need to consider security issues. The security Cloud computing is typically defined as a type of online computing that believes in sharing computing resources, processing power and storage based on demand rather than dependent on local servers or personal devices to provide such facility. "Cloud of Clouds" known as Multi issues till now solve by static password generation algorithms e.g RSA,DEA,AES but these password are easy to guess and can be further used for malfunction, so the proposed system state optimized algorithm that is Genetic algorithm which produces each time new dynamic password. This dynamic password called as One Time Password(OTP).So guessing for dynamic password is difficult and even if it has been guessed it will not usable for next session.

KEYWORDS: Multi-cloud, Static passwords, Dynamic Passwords, Genetic Algorithm, One Time Password (OTP).

I. INTRODUCTION

Cloud Computing is a technological facility that makes use of the internet and distributed servers to storing the huge amount of data of the users and for helping them to provide environment to run their application programs. Cloud computing is typically defined as a type of online computing that believes in sharing computing resources, processing power and storage based on demand rather than dependent on local servers or personal devices to provide such facility. Cloud allows running the applications and storing the file on cloud data storage without accessing user's personal files from their computer with continuous internet access. As use of cloud computing is achieving growth rapidly in every area of organization i.e public, private, hybrid and community but same times bring the fear of problems along with it. Some problems like data loss and high availability of data. Solution for data loss and high rate of available cloud mash -ups is a recent trend; mash-ups combine services from multiple clouds into a single service or application, possibly with On-premises (client-side) data and services [3]. Another trend is to be "Cloud of Clouds"; the mixing combines services from multiple clouds into a single "Cloud of Clouds" to avoid the problem of single Cloud Computing.

II. LITERATURE REVIEW

Cloud computing has become a integral and necessary part of many developing education area and organizations. The most important role of the cloud comes from its ability to provide flexible and on-line as well as on-time support for using its services, platform and infrastructure as a resources. Cloud computing resources includes infrastructure, software, storage, security, data, etc which are delivered to the user as per request on the basis of pay as per use.

Cloud Computing is classified into four category models such as Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud depending upon requirements. Public Cloud can be used by everyone and Private cloud is accessible only to private users. Hybrid is combination of Public and Private Cloud. Community cloud is used by some specific organization like education or company, etc.

As we are using MULTI-CLOUD facilities i.e. 'Cloud of Clouds' now a days it provides high rate of availability and good performance by taking the advantage of multiple cloud providers to users at a time. An important issue is the security part and one more important part is that a organization that is thinking of Navigating services to the Multi cloud. Organization need to know that their data is safe, both at the provider's side and during transmissions between the one points to another point. However the authentication stage must be very secure and strong; the best security encryption algorithms in the worldwide will not protect the data loss or leakage if anyone has crack out or guess your

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. 3, Issue 12, December 2015

password because these best security encryption algorithms provides STATIC passwords.

III. EXISTING SYSTEM

Existing cloud and multi-cloud computing uses some algorithms i.e. RSA, AES, DES and BLOWFISH for security and these algorithms provides STATIC passwords. As discussed in forgoing paragraphs the security algorithms try to secure the multi-cloud and till now it gives good performance but still at certain stage these algorithms fail to provide strong security to multi-cloud. Because static passwords are venerable to get leaked easily so it faces the problems of data loss and data leakage. These issues cause a reason of low availability in multi-cloud environment. If there is high availability rate of data not achieved in multi-cloud then using of 'Clouds of Cloud' is of no use.

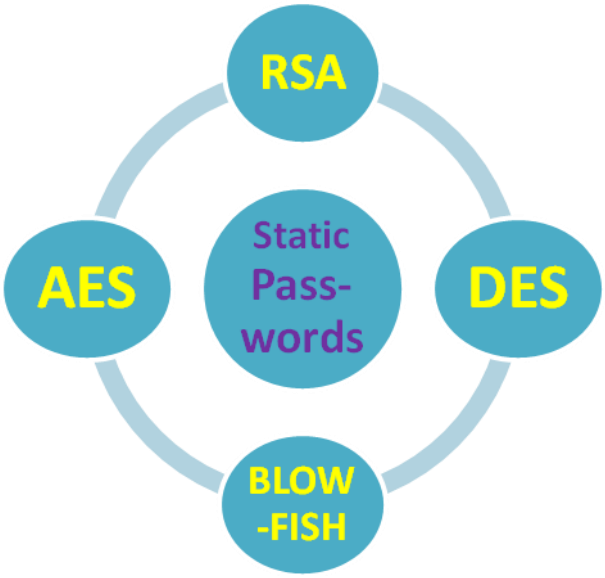

Fig 1.Static password generation algorithms

IV. PROPOSED SYSTEM

Fastest access is also a benefit of Multi-cloud in this, if one cloud is not able to serve the request of the user, cloud service provider can use other cloud from multi-cloud to serve the user instead of waiting for that particular cloud to get free and serve the user [12].

Also relying a single cloud is risky and facing problems of security threats, there could be some malicious user or software who may be trying to make attack on the data being exchanged in transaction. So to avoid attacks and leakage of data from cloud we require an algorithm which gives strong security for uploading and downloading of cloud data. In existing systems, RSA, AES, DES and BLOWFISH algorithms gives good security mechanism but with STATIC passwords it faces security problems particularly in a situation when static password get leaked or hacked, the cracker can get easy access to cloud data. Static passwords are easy to guess by using permutations and combinations. Cracker can guess it and can steal or make changes in cloud data. So to reduce such problems we need one optimize algorithm that can provide password which are DYNAMIC and difficult to guess and also time based.

V .OPTIMIZATION ALGORITHMS

Optimization gives various methods to achieved optimum output from minimum input. Multi-cloud computing environment needs optimization algorithms to get optimum utilization of the resource and data usage from cloud to user with a security. Optimization algorithms are mostly comprises into types deterministic, probabilistic and heuristic algorithms. So in the proposed system we are considering heuristics algorithm to get dynamic passwords for accessing cloud data.

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. 3, Issue 12, December 2015

V.1 GENETIC ALGORITHM

In proposed system, we are using genetic algorithm for obtaining password. Genetic algorithm passwords are dynamic in nature. Genetic algorithm based on variation and selection. This algorithm uses an evaluation function (a fitness function) Genetic algorithm is a heuristics optimization algorithm.
Genetic algorithm gives approximately closest optimal solution to problem. The working of Genetic algorithm can be obtained into 5 following steps:-
(i) Initialization
(ii) Selection
(iii) Cross-Over
(iv) Mutation
(v) Termination

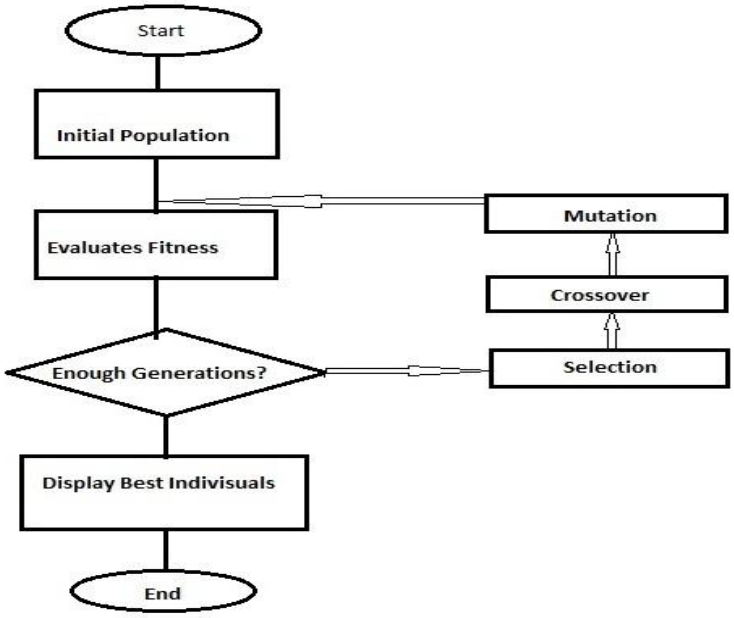

Fig 2. Flow chart of Genetic Algorithm

1. Initial Population of GA:-Select the population of chromosomes.
2. Selection Chromosomes:-The parents are selected for reproduction according their fitness value and fitness value is calculated using fitness function.
3. Crossover:-Few Chromosomes of one parent is replaced with other parent so that new offspring should be generated.

   P1=10010001
   P2=11011000
   X3=10011000
   X4=11010001
4. Mutation:-If we want to mutate 4 and 8 bit of X3 then X5=10001001
5. Terminate when we have a satisfactory solution (or we run out of time).

V.2 GENETIC ALGORITHM USED TO OBTAINING OTP

In proposed system, we are providing security to user and multi-cloud for transaction of data by One Time Password (OTP).Each time Genetic algorithm will give dynamic password and this dynamic password is treat as a OTP for transaction of data between user and Cloud. It is OTP so that each time of transaction of data it is going to change so that even though OTP is cracked but next time it is not able to use for transactions because it is going to expire for transaction. Next time transaction only can be done by newly obtained OTP. Cracking OTP is as not easy as like cracking STATIC passwords.OTP is also time based and attempt based it means after particular time span OTP is

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. 3, Issue 12, December 2015

become invalid or expired and if unauthorized user wrongly enter wrong OTP then after three attempt the system automatically logout.

So that Genetic algorithm performs great job of obtaining OTP on each request of user for accessing data from cloud. By using Genetic algorithm it will optimize random values. These random values can be used as a Password. Each time it will mutate different values so that it is not going to be same password. That's why it is not reversible. So here Genetic algorithm for obtaining OTP makes security level to Cloud stronger.

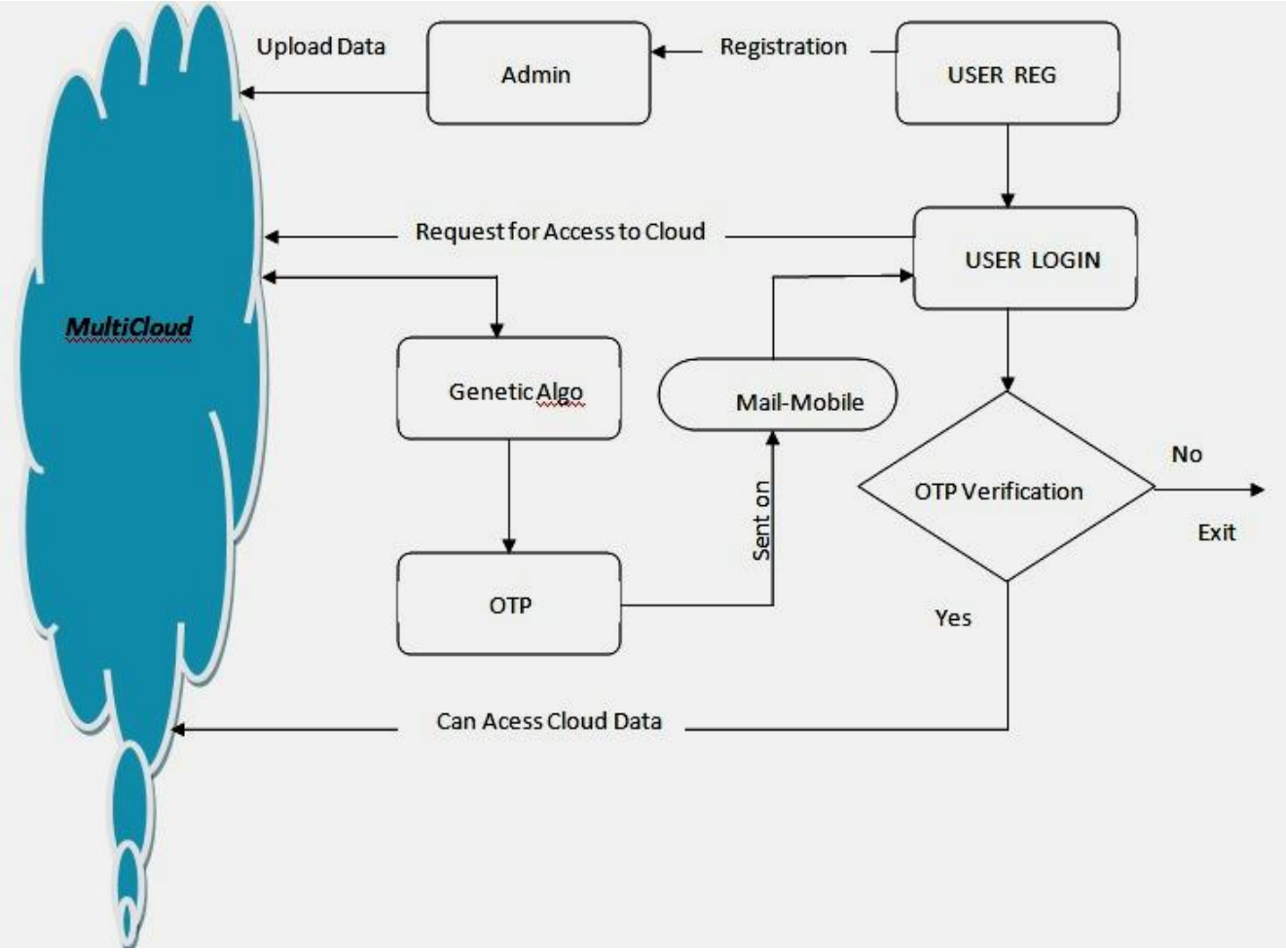

Fig.3 Proposed System Architecture

As the proposed system architecture shows multi-cloud security using OTP by Genetic Algorithm. Firstly Admin upload the data on multi cloud so that each register user can access that data. For accessing data user need to do two things those are Registration and OTP submission by user. In the system architecture user register in system after this user login in system and user gets OTP on his/her mobile and/or mail which is registered at the time of registration.OTP is formed by using Genetic algorithm. When user got OTP then it should be enter in the system and if OTP is entered correctly then system allows user to access data or else it will ask for correct OTP for maximum three attempts to enter correct OTP in available time and if user fails to enter correct OTP then system will automatically exit. One more care is taken for OTP is that it is time based. After certain amount of time OTP get expired and cannot used after expiration for accessing data from cloud, so that proposed system architecture provides strong password security with dynamic in nature so that cracker or intruder not able to crack it easily or access data.

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. 3, Issue 12, December 2015

VI. RESULTS

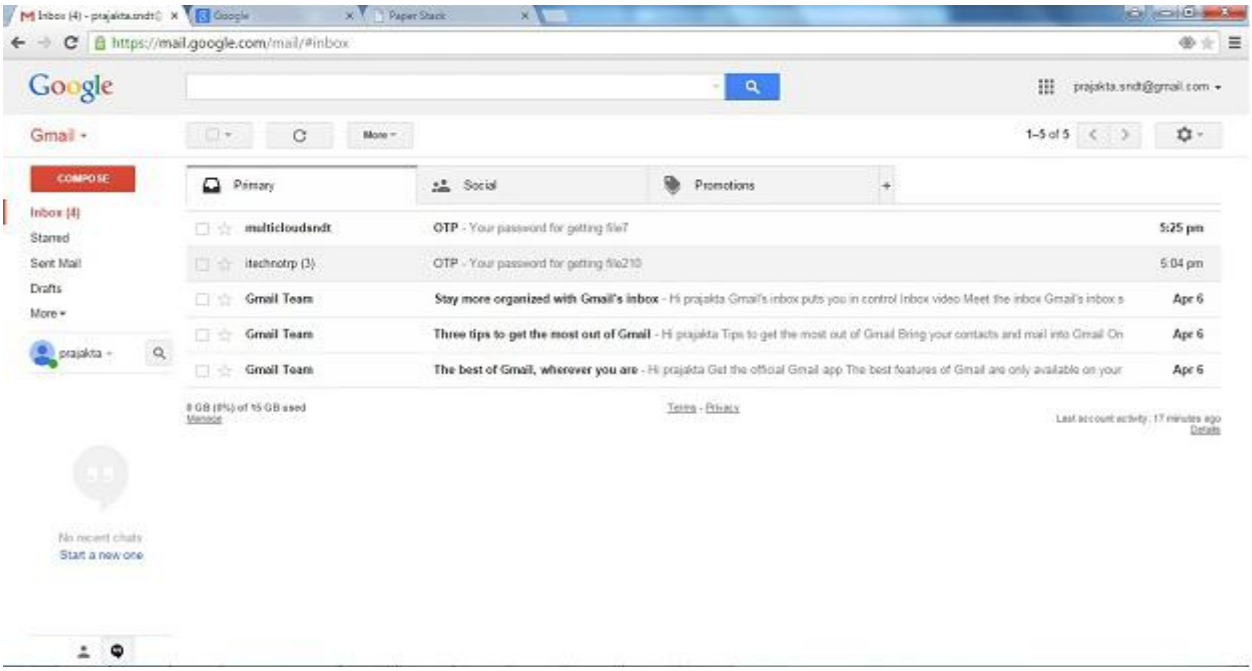

Fig 4.OTP Received via Mail

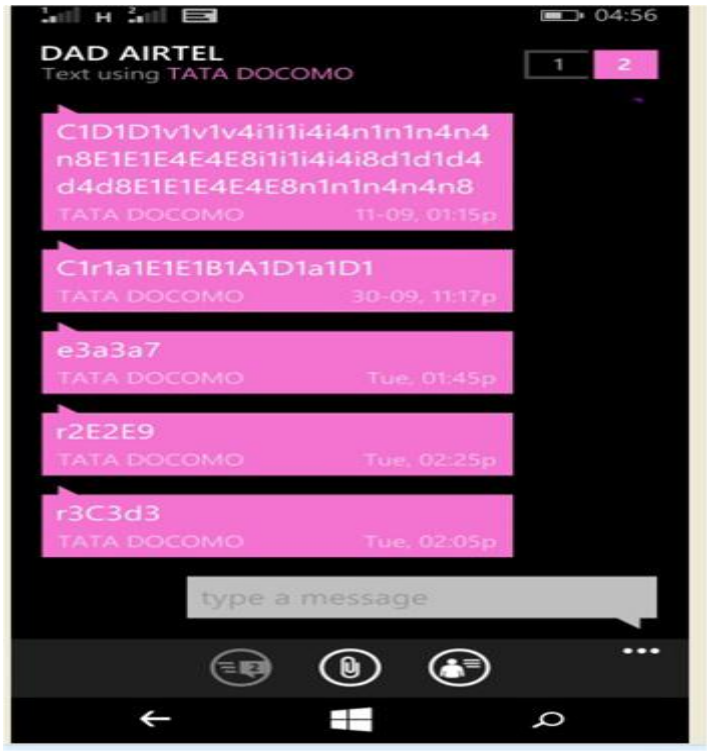

Fig 5.OTP Received via Message on mobile Number

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. 3, Issue 12, December 2015

Parameters	Existing System Static Password	Proposed System Dynamic Password
Operation	Generate static Key	Generate new key Every Time OTP
Life of KEY	Can be use for Longer time	Only valid for that instance
Strongness	Sometimes guessed or cracked	if cracked cannot be used for next time
Reversibility	Yes	Never
Algorithms	AES,DES and RSA	Genetic Algorithm
Performance	Low if password is cracked	High
Cost	High	Comparatively Low
Availability	Not fixed data may be loss	High Rate

Table 1. Analysis of Existing and Proposed System

VII.CONCLUSION

Existing system till now gives static password and it may be easily to crack or guess. Once the password gets leaked then cloud cannot be consider as safe. So proposed system overcome these problems in multi cloud by providing dynamic password. Genetic Algorithm is one of best optimization algorithm for obtaining one time password (OTP).OTP is time based so that even if gets cracked it cannot used for accessing data after some time, thereby allowing authorized user to access data which provides more secure environment for cloud or multi-cloud computing environment.

REFERENCES

[1] NIST,"NIST.gov -Computer Security Division –Computer security resource center, http://csrc.nist.gov/publications /nistpubs /800-145 /SP800-145.pdf, 2011
[2] M. Malathi "Cloud Computing Concepts", Bangalore, Karnataka, India., 2011, IEEE.
[3] MunwarAli Zardari, Low Tang Jung, Mohamed Nordin B.Zakaria, "Hybrid Multi-cloud data security (HMCDS) model and data classification",2013IEEE TRANSACTION.
[4] K.S. Suresh, K. V .Prasad, Andhra Pradesh, "Security Issues and Security Algorithms in Cloud Computing", 2013
[5] Swapnila S Mirajkar, Santoshkumar Biradar, "Using secret sharing algorithm for improving security in cloud computing", 2014.
[6] Mukesh Singhal and Santosh Chandrasekhar, Merced Tingjian Ge, l Ravi Sandhu and Ram Krishnan, "Collaboration in Multicloud Computing Environments: Framework and security issues"-2013IEEE TRANSACTION
[7] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member,IEEE,Luigi Lo Iacono, and Ninja arnau,"Security and Privacy -Enhancing Multicloud Architectures",2013 IEEE TRANSACTION.
[8] Swapnila S Mirajkar, Santoshkumar Biradar "Secret Sharing Based Approach to Enhance Security in Cloud Computing", 2014
[9] Shaik.Aafreen Naaz, Pothireddygari.Ramya, P.Vishunu Vardhan Reddy and S.Vinay kumar "CLOUD COMPUTING: USE OF MULTI-CLOUDS",2013
[10] Sunita Sharma, Amit Chugh,Ajay Kumar," ENHANCING DATA SECURITY IN CLOUD STORAGE",May-2013
[11] Shakeeba S. Khan, Prof.R.R. Tuteja," Security in Cloud Computing using Cryptographic Algorithms",Jan-2015
[12] Prajakta S. Sadafule, Kumud Wasnik," A Survey on Security Issues and Security Schemes for Cloud and Multi-Cloud Computing",2015
[13] Shaik.Aafreen Naaz, Pothireddygari.Ramya, P.Vishunu Vardhan Reddy and S.Vinay kumar CLOUD COMPUTING: USE OF MULTI-CLOUDS,2013