An Adaptive Sign-in mechanism for cloud

*Nilesh D. Katre

**Dr. Varsha Namdeo

ABSTRACT

Cloud computing is the most popular methodology in the present world. Most of the organization and people uses cloud storage for data and information storing because cloud storage is cost effective and easy to access anytime and anywhere. But security on the cloud is the most important thing. Most important are the authentication security because traditional id & Password base authentication has not the fully secure today. Various researchers made many types of authentication security based algorithm and methods. But most of those methods are not satisfactory because some methods need third party dependency and some method needs extra hardware. So in this paper, we present a new adaptive sign-in mechanism for authentication on cloud based on image cipher. Also, we study the various types of attacks and previous research.

Keywords: Cloud Computing, Security on Cloud, Authentication on Cloud, Images, Cipher.

*Nilesh D. Katre, Dept. CSE, RKDF Institute of Science and Technology, Bhopal, nileshmailbook@gmail.com

**Dr. Varsha Namdeo, Associate Professor (Dept. CSE), RKDF Institute of Science and Technology, Bhopal, Varsha_namdeo@yahoo.com

INTRODUCTION:

Cloud computing is a model for convenient, on-demand network access to a shared pool of configurable computing resources (e.g., net- works, servers, storage, applications, and services) that can be provisioned and out with service provider interaction or minimal management effort. In cloud computing data and applications are maintained with the use of central remote server and internet and allow consumers to use the applications without installing and also with the help of internet cloud computing allows customers to access their personal files which are stored on the different computer. Gmail, Yahoo email or Hotmail etc are examples of cloud computing. The email management software and the server are fully managed and controlled by the CSP like Google, Yahoo etc and are all on the cloud (internet).

The architecture comprises of many loosely coupled cloud components. Cloud can be broadly classified into two parts front end and the back end. Client part of the cloud computing system is referred to as front end which consists of the applications and interfaces that are needed for accessing cloud computing, e.g., Browser. Back end alludes to the cloud itself and comprises of every last one of resources that are obliged to give cloud computing services. It comprises of virtual machines, security mechanism, huge data storage, services, deployment models, servers and so forth. These ends are typically connected through a network, normally connected to the Internet. Back end is liable to provide traffic control, protocols and built-in security mechanism. The server employs certain protocols, known as middleware that helps the devices that are connected to communicate and correspond with each other.

The authentication security on the cloud is the very important because the various type of attacks are made by intruders for gathering important data and information of cloud users. Figure 1 shows the Classification of Authentication Attacks in the Cloud Environment**.** The various types of attacks describe below:

Man-in-the-Middle Attack (MITM): the attacker intercepts the communication channel established between legitimate users and modifies the communication between client and server without their knowledge [1].

Password Discovery Attack: Attacker adopts several mechanisms to retrieve passwords stored or transmitted by a computer system to launch this attack.

Guessing Attack: Most often people use easy to remember passwords which make them vulnerable to guessing attack.

Brute Force Attack: This attack is launched by guessing passwords containing all possible combinations of numbers, letters, and alphanumeric characters until the invader get the accurate password.

Dictionary Attack: Here the attacker tries to guess a password from a pre-computed dictionary of passwords [1].

Video Recording Attack: In such type of attack launched in public places, the attackers with the help of camera-equipped mobile phones or miniature camera capture the password while the victim enters the same.

Stolen Verifier Attack: The attacker performs this attack by accessing the password table stored at the verifier. Then he launches an offline guessing attack by attempting a script which applies hash on each entry of the phrase book and compares the generated message digest with the stored digest of the verifier until a match is found [1].

Session Hijacking: Session hijacking is possible if the Session ID issued to the authenticated users is not protected properly, which in turn can be used for spoofing identity [1].

Denial-of-Service (DOS Attacks): The main objective of DOS attack is to overload the target machine with bogus service requests to prevent it from responding to legitimate requests. Unable to maintain all its own service requests, it transfers the workload to other similar service instances which ultimately lead to flooding attacks.

Cloud Malware Injection Attack: The attack target at inserting a malicious service execution or virtual machine instance, which appears as one of the valid service instances running in the cloud [2].

Distributed Denial of Service Attacks: Distributed Denial of Service called an advanced version of DoS in stipulations of denying the important services running on a server by flooding the destination server with large numbers of packets such that the target server is not able to handle it [3].

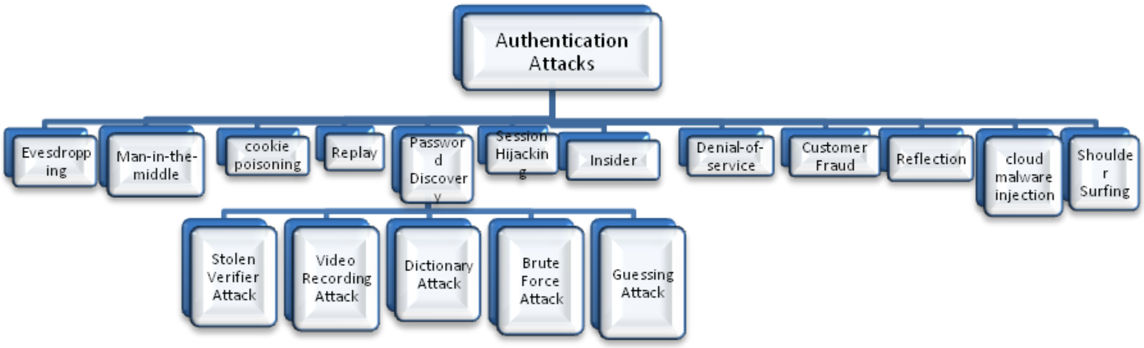

Figure 1: Classification of Authentication Attacks [4]

LITERATURE REVIEW

In this paper [5], authors demonstrated however Cloud-Trust is wont to assess the security status of IaaS CCSs and IaaS CSP service offerings, and the way it's accustomed compute probabilities of APT infiltration (high-value data access) and possibilities of APT detection. These quantify two key security metrics: IaaS CCS confidentiality and integrity. Cloud-Trust additionally produces quantitative assessments of the worth and contribution of specific CCS security controls (including many optional security controls currently offered by leading industrial CSPs), and may be accustomed conduct sensitivity analyses of the incremental value of adding specific security controls to an IaaS CCS, once there's uncertainty relating to the value of a particular security management (which could also be no mandatory and increase the price of CSP services).

In this paper [6], authors propose the implementation of a voice-based Fuzzy Vault authentication mechanism, for secure access and cryptography support among Cloud platforms and Cloud shared storage. The experimental results, targeted on evaluating the performances of the biometric matcher, have shown FRR rates variable from 0% to 32% and far rates varied from 2.5% and 11.3%.

In this paper [7], authors propose a new image integrity authentication scheme based on fixed point theory. In the proposed scheme, the following three criterions are considered for selecting an appropriate transform *fk (·)* whose fixed points are used for image integrity authentication. 1) Fragility: the fixed points of *fk (·)* must be sparse; 2) easy calculation: a fixed point can be easily found by few iterations; 3) transparence: a fixed point can be found in a very small neighborhood of a given image function. They construct an appropriate transform *fk (·)* satisfying these criterions, based on the Gaussian Convolution and Deconvolution, called GCD transform. After establishing a theorem for the existence of fixed points of the GCD transform *fk (·)*, these give algorithms for a quick calculation of a fixed point image which is very close to the given image, and for the whole image integrity authentication scheme using the obtained fixed point image. The semi-fragility problem is also mathematically considered via the commutatively of transforms. Experimental results show that the proposed scheme has very good performance.

In this paper [8], authors present a survey of recent trends to automatic recognition of human facial behavior using soft computing. Soft computing is the most attractive field nowadays. Soft computing proves effective techniques to the problem of classification, prediction, optimization, pattern recognition, image processing, etc. The facial behavior recognition processes in three steps in general. Face detection is the process of identifying a face from images. Feature extraction is a process of highlighting the facial part that takes part in the identification of expression and lasts a classifier is a design that identifies the expression. There are a lot of effective methods are there to detect face expression, but no method performs best in all types of situation. Each method has their limitations. The future of human facial behavior recognition system is to make a robust system that will perform efficiently under any circumstances.

Application developers may face with an adverse set of scenarios, each with its own identity solution without claim-based identity. Claim-based identity helps in providing a consistent answer across a wide range of scenario of cloud services. By building and deploying claim-based applications besides existing application result in simpler migration. Claim-based identity is not for only Microsoft vendors-many vendors are involved. In this paper [9], authors show why claim-based identity solutions are required and how to use the cloud service provider in cloud applications.

In this paper [10], authors identified a brand new privacy challenge throughout data accessing within the cloud computing to realize privacy-preserving access authority sharing. Authentication is established to ensure data confidentiality and data integrity. Data obscurity is achieved since the wrapped values are changed throughout the transmission. User privacy is increased by anonymous access requests to in private inform the cloud server regarding the users' access desires. Forward security is accomplished by the session identifiers to stop the session correlation. It indicates that the presented system is possibly applied for privacy preservation in cloud applications.

For obtaining correct results iris shouldn't be so much than a number of meters from the camera and it should be ensured that the iris should be stationary [11]. Totally different procedures are accustomed ensure that the image is real rather than a photograph. The image will be obscured if the contact lens is being employed. Make sure that reflections mustn't be made by the light source. If it happens image will be unclear. They analyze biometric authentication in cloud computing, it's numerous techniques and the way they're helpful in reducing the security threats.

Cloud computing is an emerging technology which is used by enterprises and companies for making their business more collaborative. Also, it faces major challenges on its way. The data security is a serious matter of concern since the data has to be entrusted to a third party. There is a need for strong authentications on the data put on the cloud, to prevent intrusions, leakage or loss of critical information. The gaze-based authentication model discussed by the authors, they provide an efficient, feasible, cost effective procedure which has high scalability, usability and security [12].

Cloud is an open environment to host the data of users. It has many benefits at the same time it also has some security problems. It is necessary to have the proper security framework to address the authentication issues in a cloud environment. In this paper [13] authors propose a framework namely VEAR AaaS which strongly protects the cloud services from the unauthorized users. The users can choose their authentication service based on their wish. Once the user selects the specific authentication service then the user is authenticated by that service only. User's details are encrypted by the symmetric encryption algorithms which are specifically designed and adopted in the cloud authentication service. This framework protects the cloud environment using its components Authenticator, Encryptor and Key Generator.

Cloud providers offer cloud services to the consumer as per their demand with different benefits of cloud computing, like reducing run time and response time, minimize infrastructure risk, lower cost of entry, increased the pace of innovation. Many security issues are coming with the cloud infrastructure which leads to an impediment to the growth of cloud computing in the IT industries. Although there are various authentication schemes have been implemented for the security of these data but either they are too much complex or they require huge network resources. Objective to improve the data security in cloud computing based on advanced image authentication algorithm. Our proposed method helps to give better fault tolerance against attacks, intrusion and data modification attacks.

PROPOSED WORK

The proposed work functional flow is given in figure 2. The whole work divided into two phases; the first one is the registration phase and second is the Authentication phase. In registration phase user register itself in the system, furthermore registration phase also divided into two parts, first is the basic information registration like Name, Address, Contact number and Login credential after that second part is the cipher registration in this part user choose cipher image from list of various image and enter cipher value respect to this image. This second part is repeated in four times means user selecting four images and entering four cipher values. The second phase (authentication phase) also divided into two parts, Firstly user entering ID and password, system match this ID & password to the stored ID & password in the database. If a match is found then go to the next phase of authentication otherwise login is a field. After the match is found then the system calculates which cipher is shown for verification means eight ciphers is stored in the database, four cipher Images and four cipher value. Our system calculates the random number in between 1 to 8 and according to this number image or cipher value prompted to the user for verification. If the image shows then the user enters its cipher value otherwise, cipher value is shown then user select image according to cipher value. If a match is found then authentication is completed otherwise authentication is failed and start from the beginning.

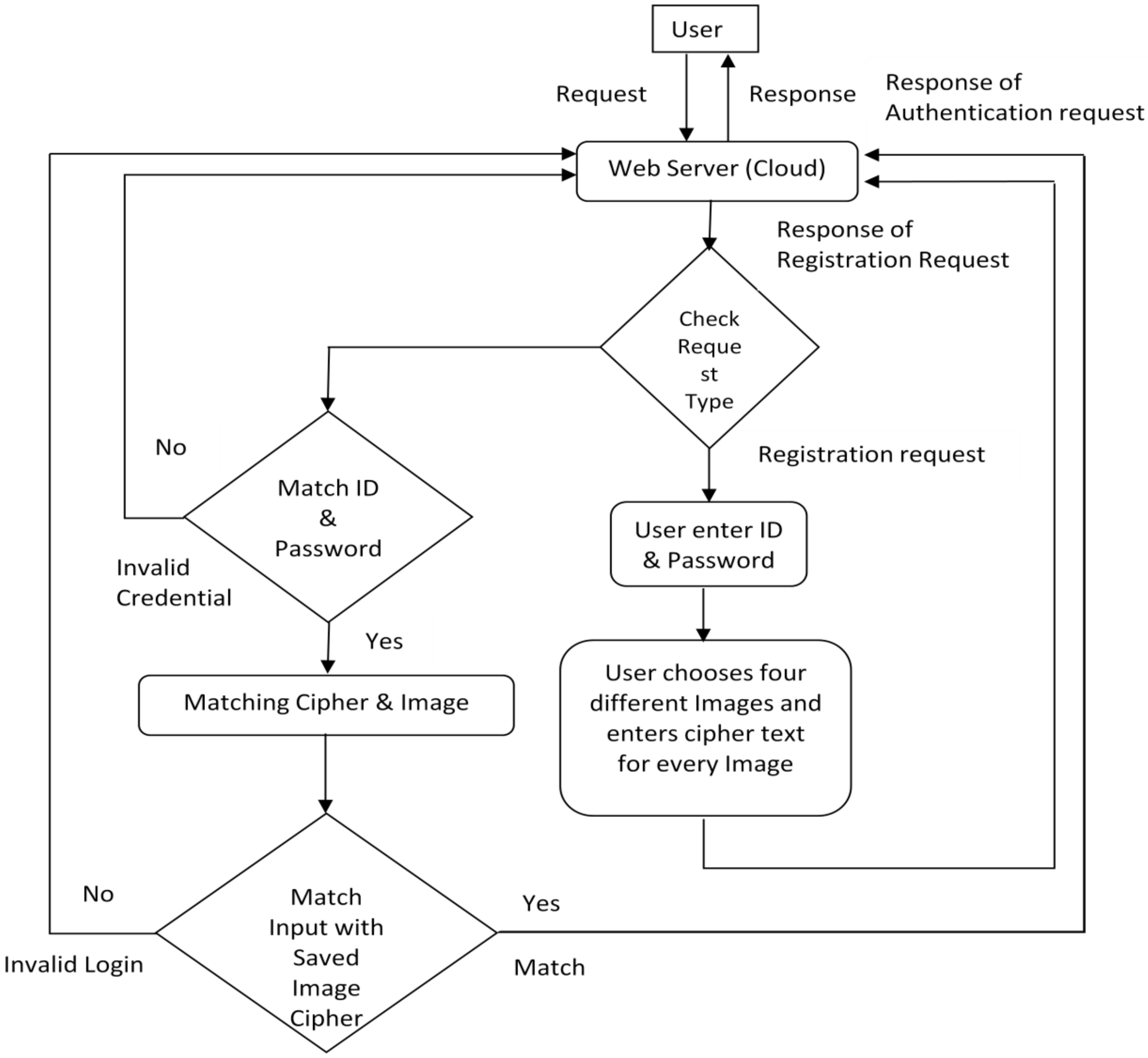

Figure 2: Proposed Architecture of Image Cipher Sign-in mechanism

ALGORITHM

The algorithm can be divided in two phase: Registration & Authentication.

1. **Registration Phase: -** The registration phase divided into two subparts first is the basic information registration and the second one is the cipher value registration.

I. **Basic Information Registration:** User fills required details for registration like User Name, Password, Email, Address and stores it in the database.

II. **Cipher Value Registration:** After basic information registration in next step user chooses one Image cipher from the list of images and inserts cipher value (It should be number or text) of its choice with respect to the Image. To complete the registration, this step is repeated four times, every time Image cipher chosen in previous steps is removed from the Image list.

2. Authentication Phase: - The authentication phase also divides into two subparts first one is the Credential based authentication after that second is the cipher authentication.

Credential based Authentication:

I. The user fills username and Password.

II. Systems check username and password in the database if a match is found then step III is followed otherwise Go to Step I.

Cipher Authentication:

III. List of stored image cipher patterns is retrieved from the database (8 elements as per registration phase i.e. 4 Images & their four text values) then a random number is generated and divided by 8. Then a pattern is chosen from a list based on the reminder that we got after dividing the random number by 8 i.e. if the remainder is 4 then choose the fourth element of the list.

IV. Check the Image cipher pattern that is not used in last three times, if the current pattern matched any one of last three times then repeats step III, if no then go to step V.

V. The user inserts cipher value or chooses an image cipher as prompted by the system with respect to step III.

VI. If a match is found then authentication is successful otherwise the user is sent back to step I to try again.

SIMULATION AND RESULT

For the results, we had implemented the proposed approach using .NET & SQL server. Refer table 1 and figure 3 for result analysis.

Table 1: Prevention from various attacks

Attacks	Status
Identity Spoofing	**YES**
Insider attack	**YES**
Eavesdropping	**YES**
Man-in-the middle attack	**YES**
Outsider attack	**YES**
Password based attack	**YES**
Identity disclosure attack	**YES**
Replay attack	**YES**

As shown in table 1 is the prevention of our proposed work from various attacks in the attack.

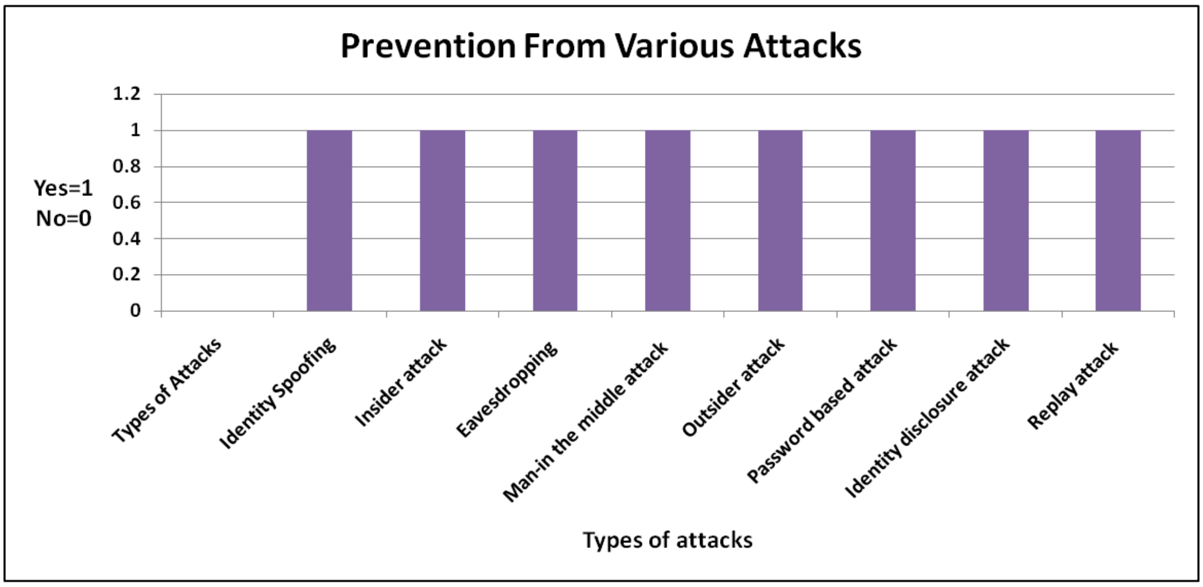

Figure 3: Prevention from various attacks.

CONCLUSION

In the real world, every people are work online and saved its important data in the cloud. So security is the measure concern today. Various researches are made for data and authentication security. In literature review section we study various authentication technique most of the techniques are Id & password based and extra hardware are required for authentication like Thumb expression based authentication, Retina scan based authentication, Mobile OTP-based authentication etc. But in our proposed methodology no extra hardware needed and also it provides security from various types of attacks. The result analysis section in above describes that our proposed mechanism provide prevention from various type of attacks like Password attacks, Insider attack, Outsider attacks etc.

REFERENCES

1. B. Sumitra, C.R. Pethuru, M. Misbahuddin “A Survey of Cloud Authentication Attacks and SolutionApproaches”http://www.ijircce.com/upload/2014/october/36_A%20Survey.pdf
2. M. Misbahuddin, “Secure Image Based Multi-Factor Authentication (SIMFA): A Novel approach for Web Based Services, Ph.D. Thesis, Jawaharlal Nehru Technological University, [Online], http://shodhganga.inflibnet.ac.in/handle/10603/3473, 2010.
3. X. Yu and Q. Wen, “A view about Cloud data security from data life cycle,(2010),” in Proc. IEEE Intl. Conference on Computational Intelligence and Software Engineering, pp. 1-4, 2010.
4. Meiko Jensen, J¨org Schwenk, Nils Gruschka, Luigi Lo Iacono (2009) “On Technical Security Issues in Cloud Computing” IEEE International Conference on Cloud Computing.
5. Dan Gonzales, Jeremy Kaplan, Evan Saltzman, Zev Winkelman & Dulani Woods presented a paper entitled “Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds” at IEEE TRANSACTIONS ON JOURNAL GONZALES, TCC-2014-03-0102.
6. Marius-Alexandru Velciu1, Alecsandru P˘atra¸scu & Victor-Valeriu Patriciu presented paper entitled “Bio-cryptographic authentication in cloud storage sharing” at 9th IEEE International Symposium on Applied Computational Intelligence and Informatics • May 15-17, 2014 • Timişoara, Romania.
7. Xu Li, Xingming Sun & Quansheng Liu Patriciu presented a paper entitled “Image Integrity Authentication Scheme Based on Fixed Point Theory” at IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 2, FEBRUARY 2015.
8. Khyati Kantharia & Ghanshyam I Prajapati presented paper entitled “Facial Behavior Recognition using Soft Computing Techniques: A Survey” at IEEE 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
9. Ashish Singh & Kakali Chatterjee presented a paper entitled “Identity Management in Cloud computing Through Claim-Based Solution” at IEEE 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
10. Hong Liu, Huansheng Ning, Qingxu Xiong & Laurence T. Yang presented a paper entitled “Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing” at IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 1, JANUARY 2015.

11. Ghazal Naveed and Rakhshanda Batool presented a paper entitled “Biometric Authentication in Cloud Computing” at JBMBS, Volume 6, Issue 5, 2015.
12. Ayushi Gahlot and Umesh Gupta presented a paper entitled “Gaze-based Authentication in Cloud Computing” at International Journal of Computer Applications, Recent Trends in Future Perspective in Engineering & Management Technology 2016.
13. N. Veeraragavan and Dr. L. Arockiam presented a paper entitled “A Novel Framework for Authentication as a Service (AaaS) in Public Cloud Environment” at International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016.