Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 10, Issue, 05(F), pp. 32512-32518, May, 2019

ISSN: 0976-3031

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

HYBRID AND ADAPTIVE AUTHENTICATION MECHANISM USING IMAGES

Himani Thakur and Anand Rajavat

Department of CSE, SVVV, Indore

DOI: http://dx.doi.org/10.24327/ijrsr.2019.1005.3487

ARTICLE INFO

Article History:
Received 4th February, 2019
Received in revised form 25th March, 2019
Accepted 23rd April, 2019
Published online 28th May, 2019

Key Words:

Authentication; Digital Data; Security; Single Phase Authentication; Two Phase Authentication.

ABSTRACT

Cloud computing is a globalized concept and there are no borders within the cloud. Computers used to process and store user data can be located anywhere on the globe, depending on the availability of required capacities in the global computer networks used for cloud computing. Because of the attractive features of cloud computing many organizations are using cloud storage for storing their sensitive data. The information can be stored remotely in the cloud by the clients and can be accessed using thin clients as and when required. One of the major issue in cloud today is data security in cloud computing. Storage of information in the cloud can be dangerous in view of utilization of Internet by cloud based services which means less power over the stored information. One of the significant concern in cloud is how would we snatch all the advantages of the cloud while keeping up security controls over the organizations resources.

This paper proposes a new approach for security of the data storage in clouds by using images. The authentication provided using image will be an efficient technique which provides more security to the data storage in clouds. The idea is to develop a mechanism for authentication where data possession is dynamic and whenever any of the clients wants to access the data stored in cloud then he has to authenticate for the public access of the data. The approach proposed in the paper is practically implementable and easy to use for the clients.

Copyright © Himani Thakur and Anand Rajavat, 2019, this is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

Cloud computing can be a model for facultative ubiquitous, convenient, on-demand network access to a shared group of computing resources that are configurable (e.g., networks, servers, storage, applications, and services) that will be rapidly provisioned and discharged with lowest management effort or service provider interaction[1].

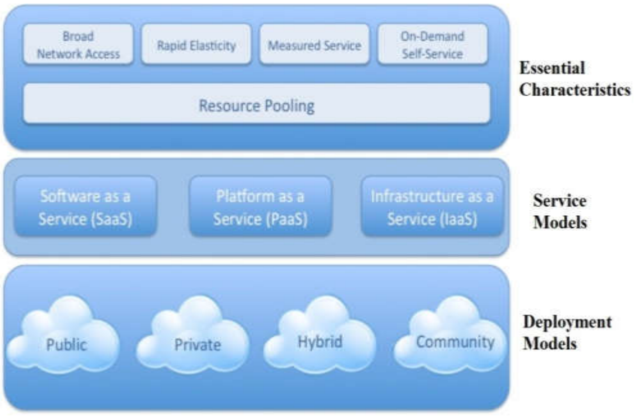

Figure 1 NIST Visual Model of Cloud Computing Definition

Characteristics of Cloud Computing [1]

This cloud model consists of 5 essential characteristics, 3 service models, and 4 deployment models. Cloud computing is using World Wide Web to access someone else's computer code running on someone else's hardware in someone else's information center. Essential Characteristics of a clod computing includes:

On-demand self-service:A client can unilaterally provision computing capabilities like server time and network storage as needed automatically, whereas not requiring human interaction with a service provider.

Broad network access: Capabilities are procurable over the network and accessed through commonplace mechanisms that promote use by heterogeneous thin or thick consumer platforms (e.g. Laptops, mobile phones, and PDAs) more as various ancient or cloud primarily based software system services for use.

Resource pooling: The computing resources of provider are pooled to serve multiple customers using a multi-tenant model, with utterly totally different physical and virtual resources

*Corresponding author: **Himani Thakur**
Department of CSE, SVVV, Indore

dynamically assigned and reassigned in step with consumer demand.

Rapid elasticity: Capabilities are rapidly and elastically provisioned - in few cases automatically - to quickly scaled out; and discharged rapidly to quickly scale in. To the patron, the capabilities procurable for provisioning typically appear to be unlimited and will be purchased in any quantity at any time.

Measured service: Cloud systems automatically management and optimize resource usage by leverage a metering capability at some level of abstraction acceptable to the kind of service. Resource usage are monitored, controlled, and reported - providing transparency for every the supplier and consumer of the service.

Authentication

Authentication is a mechanism to assure whether or not somebody or one thing is, that what it itself declares to be. This mechanism provides management of accessof systems by checking to ascertain if a user's user id and password match the credentials in exceedingly stored information of approved users present at information authentication server.

Users are typically known having a personal user ID and password. Authentication is competed once the user provides anID and password, as an example a password and user ID that matches therewith ID and password stored on the database of authentication server. Most of the users are most aware of employing a password, which, as a chunk of data that ought to be well-known solely to the user, is termed a data authentication factor.

Authentication is vital as a result of it permits organizations to maintain their networks sheltered by allowing solely genuine users (or processes) to access its sheltered resources, which can include computer systems, databases, websites, networks and services or different network-based applications.

Once genuine, a method or user is sometimes subjected to an authorization method as well, to see whether or not the genuine individual ought to be permissible right to use to a sheltered system or resource. A resource user may be genuine however not succeed to be resource access if that user of it wasn't approved authorization to access it.

Literature Review

In this paper [2] authors provided a novel and efficient authentication system which uses the cloud data centers and mobile phone to discover the uniqueness of the item. The system uses fast Response codes to spot the item details. The project when enforced within the reality can offer a simpler authentication system that the people will use to search out the originality of the item before shopping for it. They will conjointly ensure that the item that these obtain is originally manufactured by the various manufacturer and not from any cheat. The system conjointly reduces the value of the authentication method as there's no want for adding up any expensive tags to every product. Printing the QR codes is a lot of economical than different authentication systems. The foremost necessary advantage of the system is that the authentication is completed by the user itself and there's middleman within the method that will increase the trustiness and security of the system.

In this paper [3], authors used principal curves approach for fingerprint trivialities extraction then these keep them in an exceedingly database on a cloud, then authors used the Bio-Hash operate to secure the biometrics templates. additionally they compared there method with the method given in previous researches, and intended the error rates for his or her approach and verified that these increase the system performance by twenty fifth.

In this paper [4], authors present some advances system on offline signature identification system. Type the analysis of the recent literature within the field a number of the foremost valuable approaches is given and also the most fascinating directions for more analysis are highlighted.

In this paper [5], authors propose the implementation of a voice-based Fuzzy Vault authentication mechanism, for secure access and encryption support at intervals Cloud platforms and Cloud shared storage. The experimental outcome, stress on assessing the performances of the biometric intermediary, have shown FRR rates variable from 1/3 to thirty second and much rates variable from 2.5% and 11.3%.

In this paper [6], authors propose a brand new image integrity authentication method supported fixed point theory. within the proposed scheme, the subsequent three criterions square measure considered for selecting an acceptable transform fk (•) whose fixed points are used for image integrity authentication. 1) Fragility: the fixed points of fk (•) should be sparse; 2) straightforward calculation: a fixed point is simply found by few iterations; 3) transparence: a fixed point is found in a very little neighborhood of a given image function. They construct an acceptable transform fk (•) satisfying these criterions, based on the Gaussian Convolution and De-convolution, known as GCD transform. once establishing a theorem for the existence of fixed points of the GCD transform fk (•), these provide algorithms for a fast calculation of a fixed point image that is extremely on the point of the given image, and for the complete image integrity authentication scheme mistreatment the obtained fixed point image. The semi-fragility drawback is additionally mathematically thought-about via the commutatively of transforms. Experimental results show that the proposed method has superb performance.

In this paper [7], authors developed an iris recognition algorithm supported Fisher algorithm which may be run in a very lighter computing platform. Experiments conducted with CASIA information shows exciting results wherever the system achieves a awfully high accuracy. Iris recognition may be a biometrics authentication system mistreatment iris image. It's one in all the foremost reliable biometrics systems. The systems but need substantial computing power. Therefore it's not been able to penetrate the market however.

This paper [8] discusses the various ICA based mostly techniques that are utilized in last decade. This paper reviews the comparative study of various face recognition techniques that is predicated on ICA. The vital a part of this survey is that the discussion of previous work of face recognition associated with ICA. There are totally different strategies obtainable associated with ICA. Also, compare the various strategies in tabular kind. During this survey paper offer the transient summary of "How to recognition face using image processing".

In this paper [9] the human behavior is recognized from a collection of video samples and therefore the features are extracted victimization HOG transform. KNN classifiers are accustomed classify the features extracted from the videos. The HOG feature primarily based analysis has achieved higher recognition and accuracy of 93%compared to the prevailing ways. There are many factors affects this Gait Authentication which may be classified into 2 classes. They're (i) External factors: angles, lighting atmosphere, garments that have same color as background and alternative external objects. (ii) Internal factors: changes in gait because of natural effects like illness, ageing, pregnancy, gaining or losing weight.

In this paper [10] authors projected a sturdy face recognition technique by victimization native binary pattern and bar graph of adjusted gradient feature extractor and descriptors. During this study author have found that LBP feature extractors have virtually simple fraction higher accuracy result than the HOG feature extractors that doesn't have that a lot of distinction. They need tested it for authentication purpose to register to their device by taking one label as an administrator and it gave important results.

In this paper [11], authors present a completely unique security framework for NFC Secure Element-based Mutual Authentication and Attestation for Io T access with a user device like a mobile device using NFC based mostly.

Host Card Emulation (HCE) mode for the primary time. The recently framework for NFC Secure Element-based Mutual Authentication and Attestation for IoT access provides a completely unique on-demand communication and management of IoT devices with security, privacy, trust and proof-of-locality using the NFC-based HCE mode and secure tamper-resistant SE and TPM modules. This method cannot verify the dynamic device state like Control-Flow Integrity.

Author proposes a noisy vibration method for cloaking vibration sounds throughout pairing against such attacks. The method only needs a speaker for emitting the masking sound throughout key transmission [12]. They conjointly study motion sensor exploits against this scheme and compliment it with extra measures to mask vibration effects on motion sensors. There analysis shows that whereas vibration pairing could seem to be a beautiful mechanism for guaranteeing the protection and trust in an IoT network, it must be protected against acoustic aspect channel attacks by defensive measures like masking signals that are low price and straightforward to implement.

In this paper [13], author studied the ensemble performance of biometric authentication system that is supported secret key generation. Bearing on an ensemble of codes supported Slepian–Wolf binning, we've provided elaborate, sharp analyses of the false–reject and false–accept chances, in terms of error exponents, for a large category of stochastic decoders that covers the optimum MAP decoder, in addition as many extra decoders, as special cases. Converse bounds are derived in addition.

Author propose a physical-layer challenge-response authentication approach during this paper [14] supported combined shared secret key and channel state information (CSI) between 2 legitimate nodes in an orthogonal frequency division multiplexing (OFDM) system. The projected approach used although the correlation of channel coefficients exists, which might be exploited to extract the shared secret key in standard approaches. Moreover, channel coding is utilized to mitigate the distinction between the 2 calculable channels in addition as channel fading and background noise. Thus, they ascertained that within the projected approach as a physical-layer authentication approach, the decoder's output are often used for authentication and provided a reliable decision below active attack.

Proposed architecture

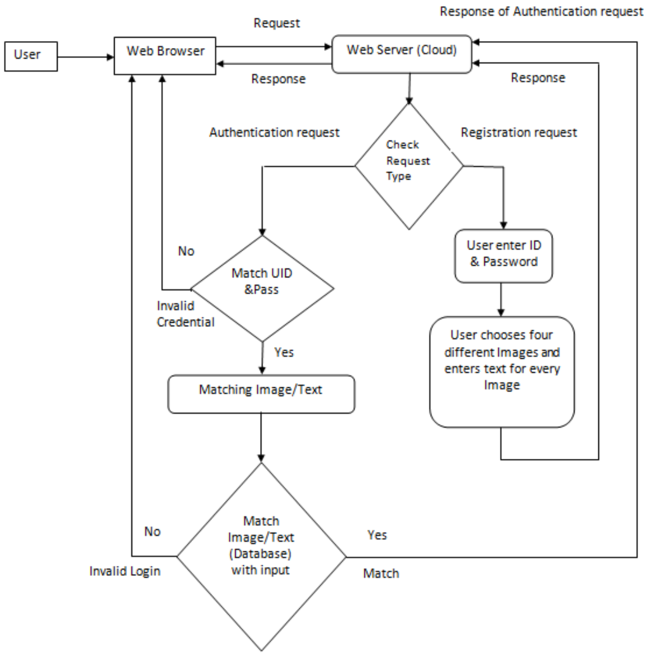

Figure 2 Proposed Architecture of Hybrid and Adaptive Authentication Mechanism using Image

The functional flow of the algorithm is given in the figure 2. The architecture mentioned above contains two main components:

Registration

First the user have to register with the required details along with the user ID and Password which is then stored in a database. Cipher values are generated based on the user's choice along with the usual registration process for the authentication mechanism. The users choice of cipher value is then also stored in the database. These cipher values are responsible for dynamic & advance security implementation in the cloud.

Login

After the registration along with the layer 1 security mechanism i.e. user ID and password and layer 2 mechanisms i.e. cipher value choice, user can login with the required details. First a user have to enter the layer 1 security mechanism, if user is an authenticated user according to layer 1 then he or she will entered in layer 2. In layer 2 a random image will be displayed to the user. He or she has to enter the significant other in order to access the cloud after that cipher value will be displayed to user then user choose significant image. On successful attempt he or she is permitted to inter in the cloud otherwise after three unsuccessful attempts he or she will be blocked.

Algorithm

The algorithm can be separated in two sub parts Registration and Login.

Registration

1. User fills required details for registration like User Name, Password, Email, and Address and stores it in database.
2. After that user chooses one Image from list of images and inserts text value (It should be number or text) of its choice with respect to the Image.
3. To complete the registration, step II is repeated four times, every time Image chosen in previous steps is removed from Image list.

Login

1. User fills user name and Password.
2. Systems checks user name and password in database if match is found then step III is followed otherwise Go to Step I.
3. List of stored image patterns is retrieved from the database (4 elements as per registration phase i.e. 4 Images) then a random number is generated and divided by 4. Then a pattern is chosen from list based on the reminder that we got after dividing the random number by 4 i.e. if reminder is 3 then choose third element of list.
4. Check the Image pattern that are not used in last three times, if the current pattern matched any one of last three times then repeat step III, if no then go to step V.
5. User inserts value as prompted by system with respect to step III. If the input matches with database values then proceed to step VI or else Log out & Go to Step I.
6. List of stored cipher patterns is retrieved from the database (4 elements as per registration phase i.e. four text/number values) then a random number is generated and divided by 4. Then a pattern is chosen from list based on the reminder that we got after dividing the random number by 4 i.e. if reminder is 2 then choose second element of list.
7. Check the pattern that are not used in last three times, if the current pattern matched any one of last three times then repeat step V, if no then go to step VI.
8. User chooses an image as prompted by system with respect to step V. If the input matches with database values then Login Successful or else Log out & Go to Step I.

RESULT ANALYSIS

Comparison based various types of Dependency Parameters

Various types of dependency parameters which causes system to fail in certain circumstances like

- Internet
- Extra hardware required
- Mobile network
- Failure due to third party

Table 1 Comparison based on various dependency parameters

Dependency Parameter	OTP	Biometric	Proposed Approach	Face Recognition
Internet	1	1	1	1
Extra Hardware	1	1	0	1
Mobile Network	1	0	0	0
Failure due to third party	1	1	0	1

The result shows that OTP authentication mechanism depends on internet, it needs extra hardware, mobile network and also depends on third party. If the third party fails to do the work then the OTP system also fails. In case of finger Print Technique, is also depends on all the dependency parameters except Mobile Network. But the proposed work is depends only on the Internet. So the failure rate of proposed work is decreased as compared to other techniques as shown in Figure 3.

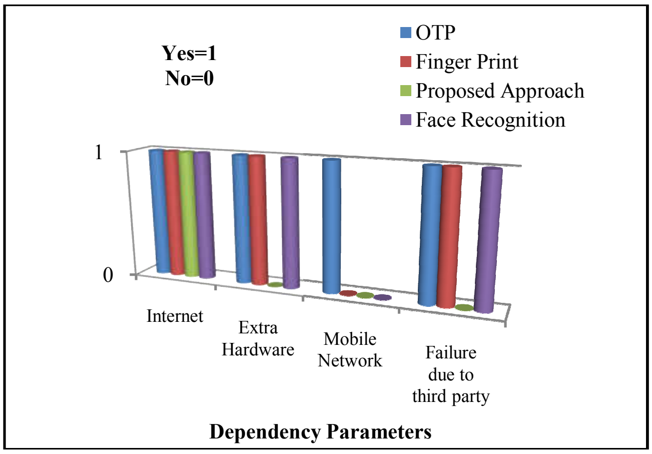

Figure 3 Comparison of Proposed Approach based on Dependency Parameters

Comparison Based on Various Attacks

Dictionary Attack

This is a kind of attack wherein a hacker/attacker tries to guess the password with the help of a dictionary – the collection of words. The attacker tries all possible combinations of words to crack the password. In this regard, graphical passwords provide more security than text-based passwords. If the password is present in the dictionary, then the hacker can easily crack it.

Table 2 Comparison based on Dictionary Attack

Approach	Possibility Yes=1 No=0
OTP	0 (Not possible as the OTP is changed every time)
Biometric	1 (Possible if the hacker has biometric impression)
Proposed Approach	0 (Not possible as the query is changed every time)
Face Recognition	1 (Possible if the hacker has users photo)

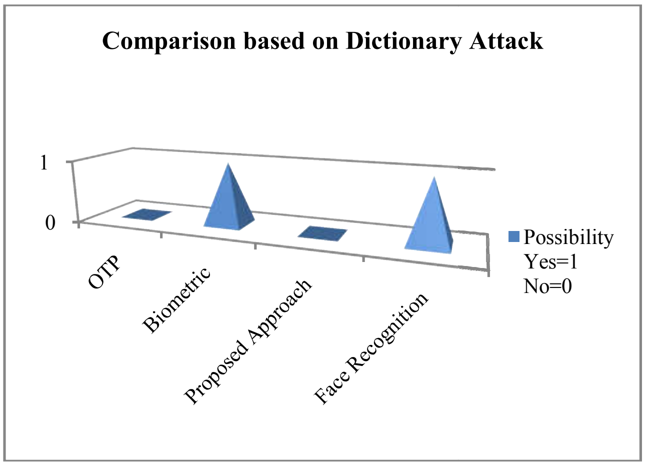

Figure 4 Comparison based on Dictionary Attack

Shoulder-Surfing Attack

Shoulder-surfing is also known as the peeping attack, which is a kind of attack where attackers watch the screen of the user's smart phone over a shoulder of the person to trace the password. This kind of attack usually happens in public places or if someone watches you on the camera.

Table 3 Comparison based on Shoulder-Surfing Attack

Approach	Possibility Yes=1 No=0
OTP	1 (Possible if the hacker is on the same OTP request page because OTP has time bounded validity)
Biometric	1 (Possible if the hacker saves user's biometric using some camera)
Proposed Approach	0 (Not possible as the query is changed every time on different screen)
Face Recognition	1 (Possible if the hacker captures users photo)

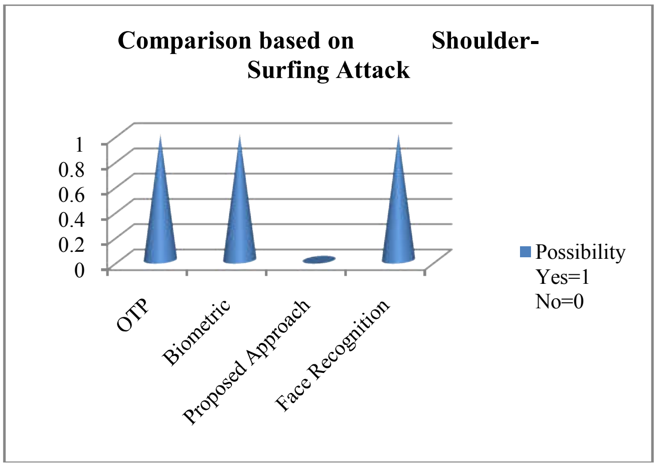

Figure 5 Comparison based on Shoulder-Surfing Attack

The password is always hard to remember and users choose their passwords which are easy to memorize and recall when needed. For this purpose, they use their personal information as a password, for example, house name. In most of the cases when an attacker tries to guess the password, s/he accesses users' personal information.

Table 4 Comparison based on Guessing Attack

Approach	Possibility Yes=1 No=0
OTP	0 (Not possible as OTP is not related to personal information)
Biometric	1 (Possible if the hacker has user's personal information and biometric is one of them)
Proposed Approach	0 (Not possible as the query is not dependent on personal information of user)
Face Recognition	1 (Possible if the hacker has user's personal information and photo is one of them)

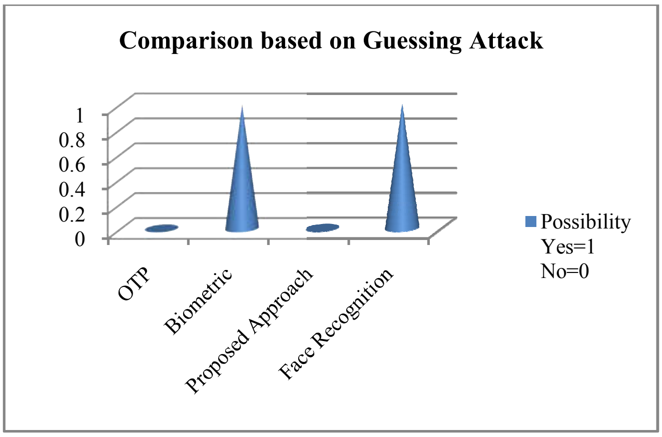

Figure 6 Comparison based on Guessing Attack

Spy-ware Attack

Spy-ware is a kind of attack in which malicious software is installed on the user's device secretly with the goal to steal users' information. There are two types of methods that the spy-ware can execute. The malware steals information about the user and leaks it to the attacker.

Table 5 Comparison based on Spy-ware Attack

Approach	Possibility Yes=1 No=0
OTP	1 (Possible if the hacker has installed Spy-ware software on device)
Biometric	1 (Possible if the hacker has installed Spy-ware software on device)
Proposed Approach	0 (Not possible as the query is changed every time)
Face Recognition	1 (Possible if the hacker has installed Spy-ware software on device)

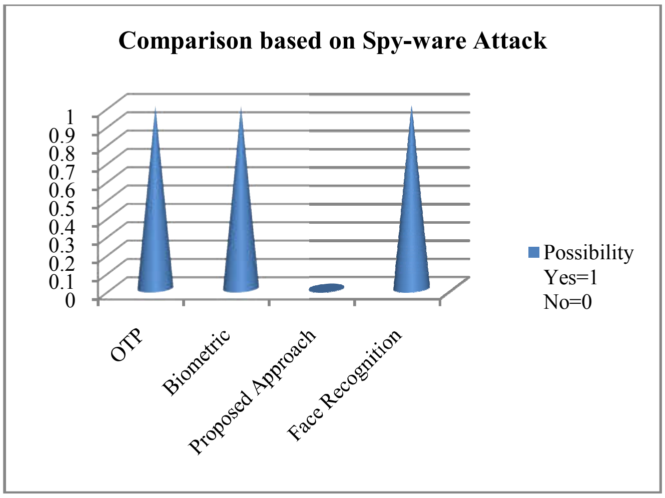

Figure 7 Comparison based on Spy-ware Attack

Social Engineering Attack

Social engineering attacks are very common for text-based passwords as well as for graphical passwords. In this kind of attacks, human interaction is involved. In addition, the attacker shows himself as an employee of a particular organization or company and tries to interact with the users to collect their personal or secret information.

Table 6 Comparison based on Social Engineering Attack

Approach	Possibility Yes=1 No=0
OTP	0 (Not possible as OTP is not part of personal information)
Biometric	1 (Possible as biometric is a part of personal information)
Proposed Approach	0 (Not possible as the query is changed every time)
Face Recognition	1 (Possible as Photo is a part of personal information)

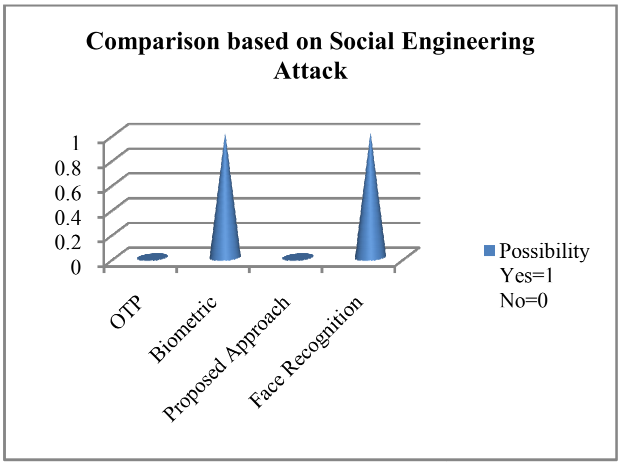

Figure 8 Comparison based on Social Engineering Attack

Brute Force Attack

In the Brute force attack, the attacker uses an algorithm that produces every combination of words to break a password. This type of attack is proven successfully on the traditional text-based password schemes.

Table 7 Comparison based on Brute Force Attack

Approach	Possibility Yes=1 No=0
OTP	1 (Possible as one of the combination may be same as OTP)
Biometric	0 (Not possible as biometric cannot be obtained from combination of words)
Proposed Approach	0 (Not possible as one of the query requests to select image)
Face Recognition	0 (Not possible as photo cannot be obtained from combination of words)

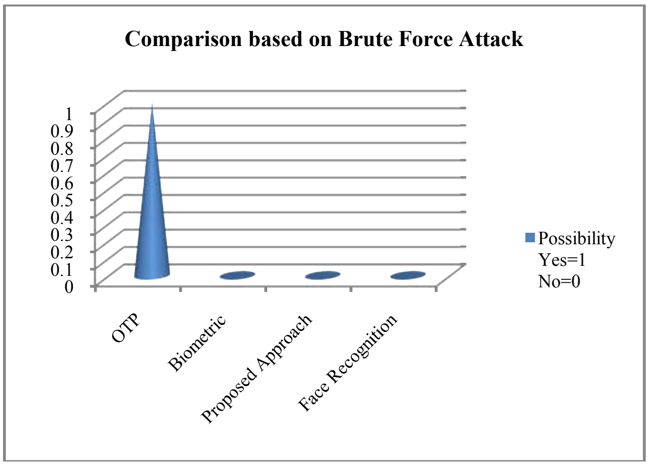

Figure 9 Comparison based on Brute Force Attack

CONCLUSION

In this paper the proposed approach is based on securing cloud by using Image cipher. Cloud security can also be enhanced by alphanumeric password but matter is that using alphanumeric password is not that much of secure. So we implemented new method for cloud authentication by using image cipher. Proposed approach enhances cloud storage security with minimum resources utilization. As discussed in result and analysis section, proposed approach gives comparatively better results when compared with various other authentication methods. Thus we present a new idea for the cloud storage security.

- The Proposed algorithm enhances password based security mechanism by adding one more layer for authentication. The proposed approach is so much secured that if intruder sees your username & password still he won't be able to login into the system.
- The proposed approach can also be used for authentication of the user from one cloud to another cloud.
- The Proposed approach uses combination of 4 images & its 4 names, i.e. it dynamically generates a query for authentication every time user wants to authenticate. This combination won't repeat for previous 3 queries.
- Proposed approach can be embedded with any existing authentication system without need of any extra hardware.

Acknowledgment

I am highly thankful to my guide Dr. AnandRajavat (Head of Department of Computer Science). His suggestion and interest have helped me in integrating the work. His accommodating nature tolerates my persistent queries and provided the best solution to my problem. I am also thankful to Department of Computer Science for providing all facilities and resources needed for this research paper.

Reference

1. Peter Mell and Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, September 2011.
2. Umanandhini .D, Latha Tamil Selvan, Udhayakumar .S &Vijayasingam .T presented paper entitled “Dynamic Authentication for Consumer Supplies in Mobile Cloud Environment” in IEEE conference at ICCCNT'12, Coimbatore, India.
3. Heba M. Sabri, Kareem Kamal A.Ghany, Hesham A. Hefny&NashaatElkhameesy presented paper entitled “Biometrics Template Security on Cloud Computing” at 978-1-4799-3080-7/14/$31.00 @ 2014 IEEE.
4. D. Impedovo, G. Pirlo & M. Russo presented paper entitled “Recent Advances in Offline Signature Identification” at IEEE 2014 14th International Conference on Frontiers in Handwriting Recognition.
5. Marius-Alexandru Velciu1, AlecsandruP˘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.

6. Xu Li, Xingming Sun &Quansheng Liu Patriciu presented paper entitled “Image Integrity Authentication Scheme Based on Fixed Point Theory” at IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 2, FEBRUARY 2015.
7. HermawanNugroho, Hamada Rasheed Hassan Al-Absi and Lee Pei Shan, “Iris Recognition for Authentication: Development on a Lighter Computing Platform”, in IEEE 978-1-5386-8369-9/18/$31.00 ©2018.
8. RajatNaik, Dr. DhirendraPratap Singh and Dr. JaytrilokChoudhary, “A Survey on Comparative Analysis of Different ICA based Face Recognition Technologies”, Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018), IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-09651.
9. S. JoulMonisha and G. Merlin Sheeba, “Gait Based Authentication with Hog Feature Extraction”, in IEEE 978-1-5386-1974-2/18/$31.00 ©2018.
10. MelkyeWeretaTsigie, RasikaThakare and Rahul Joshi, “Face Recognition Techniques Based on 2D Local Binary Pattern, Histogram of Oriented Gradient and Multiclass Support Vector Machines for Secure Document Authentication”, Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2.
11. DivyashikhaSethia, Daya Gupta and Huzur Saran, “NFC Secure Element-based Mutual Authentication and Attestation for IoT access”, JOURNAL OF TRANSACTIONS ON CONSUMER ELECTRONICS, VOL. 14, NO. 8, SEPTEMBER 2018, DOI 10.1109/TCE.2018.2873181, IEEE, Transactions on Consumer Electronics.
12. S Abhishek Anand and NiteshSaxena, “Noisy Vibrational Pairing of IoT Devices”, DOI 10.1109/TDSC.2018.2873372, IEEE.
13. NeriMerhav, “Ensemble Performance of Biometric Authentication Systems Based on Secret Key Generation”, DOI 10.1109/TIT.2018.2873132, IEEE.
14. Jinho Choi, “A Coding Approach with Key-Channel Randomization for Physical-Layer Authentication”, DOI 10.1109/TIFS.2018.2847659, IEEE.
15. https://searchsecurity.techtarget.com/definition/authentication

How to cite this article:

Himani Thakur and Anand Rajavat., 2019, Hybrid and Adaptive Authentication Mechanism Using Images. *Int J Recent Sci Res.* 10(05), pp. 32512-32518. DOI: http://dx.doi.org/10.24327/ijrsr.2019.1005.3487

****