Secure Data Platform For Mobile Cloud Computing

Dolly R Pawar[1], Priya Jambhulkar[2], Supriya Sawwashere[3]
[1, 2, 3] Dept of Information Technology
[1, 2, 3] G.N.I.E.T Nagpur, India

Abstract- *Due increase in the usage of cloud based systems there is an increase in the amount of information on the cloud and as a result there is need for confidentiality. Most common method used for authentication is textual password. But these passwords are susceptible to shoulder surfing, dictionary attack, eavesdropping. Generally the passwords tend to follow patterns that are easier for attackers to guess. A literature survey shows that text-based password suffer this security problem. Pictographic passwords are provided as replacement to text based passwords. In this paper we present a framework which can also be used for other cloud based application but we proposed a mobile cloud security solution. Which use Pictographic and Geo Graphic password. Pictographic passwords may prone to shoulder surfing. Pictographic passwords may suffer with the usability issue. This paper uses color code authentication which provides two step authentication to the user. Each time user signup in with generated one time password. With the rising popularity of cloud storage, and its ever-increasing versatility, it's no surprise that enterprises have jumped on the cloud bandwagon. This powerful tool not only meets storage and computing needs, but also helps saves business thousands of dollars in IT investments. This high demand for storage has nurtured the growth of a thriving cloud service industry that offers affordable, easy-to-use and remotely-accessible cloud services.*

But as with every kind of new technology, whether physical or virtual, IT experts have warned of the inherent security risks associated with using cloud storage and file sharing apps. In fact, security or the lack thereof has restricted universal adoption of cloud services. The main issue is that enterprises have to entrust the security of their sensitive business data to third-parties, who may or may not be working in their best interest.

Keywords- Security, privacy, mobile cloud, data security.

I. INTRODUCTION

Authentication system play an important role in every application. Its allow application to authenticate user and provide him access control for the application. A weak authentication system leads to various vulnerable attacks. When its come to user authentication, the first Scheme comes in minds is Text based authentication .In cloud computing to access data one has to authenticate the system. The common authentication method used to access data on cloud is password. The major drawbacks of text based passwords are weak password, forgot password, stealing of password etc. So it requires strong and secure authentication method for the protection of data on cloud. Cloud security mostly depends on authenticating the User by using passwords. The key requirements of password is, it should be easy to remember and secure. In case studies of password by Moris it is found that users are not selecting and handling text based passwords in insecure manner. Dhamija et al concluded that humans can only memorize very few passwords due to this fact user are writing down, share or User the same passwords for many accounts. The solution to this may be the pictographic password. The first graphical password is described by Greg Blonder.In this scheme user requires to click on selected regions in image that is displayed on screen. The user has to select the same regions for login. But such scheme suffers from stability problem due to its static image selection. Text based password are susceptible to dictionary attack, shoulder surfing, eavesdropping. To overcome some of these problems pictographic password are introduced. The dictionary attack is not possible with such password. But it suffers from shoulder surfing. Man et al. added a small layer of patter graphics along with alphanumeric characters to prevent shoulder surfing.
Today, authentication is achieved through the use of password technique. To prove and maintain the identity every user uses a password authentication. The traditional method of password is a textual (alphanumeric) password. It is the combination of alphabets, digits and special symbols. But it has various limitations.

Computer/network security hinges on two very simple goals:

- Keeping unauthorized persons from gaining access to resources
- Ensuring that authorized persons can access the resources they need

II. AUTHENTICATION AND SECURITY

Authentication is an absolutely essential element of a typical security model. It is the process of confirming the identification of a user (or in some cases, a machine) that is trying to log on or access resources. There are a number of

different authentication frameworks, but all serve this same purpose.

Authentication vs. authorization:

It is easy to confuse authentication with another element of the security plan: authorization. While authentication verifies the user's identity, authorization verifies that the user in question has the correct permissions and rights to access the requested resource. As you can see, the two work together. Authentication occurs first, then authorization.

Forms of Authentication (combinations are possible):

- password-based
- address-based
- cryptographic
- Scenario

Security system plays a vital role in any system where user id is a matter of concern, security systems are essential for any computerized or digital access control.

Authentication system have already been implanted for almost all the fields such as defense, information systems and even in physical buildings (camera implantation).The strength of authentication system lies in the password. Passwords are simple alpha-numeric strings shared between server and the user.

Important factor to note here is that alphanumeric passwords are not stored ―as it is‖ on the server but rather are saved in encrypted form after hashing. Later many studies were done on authentication system and researchers discovered graphical password authentication system which later proved as the best alternative to text based passwords.

.

III. LITERATURE SURVEY

Susan Wiedenbeck Jim Waters, Jean-Camille Birget and Alex Brodskiy Nasir Memon in their work "Authentication Using Graphical Passwords: Basic Results" designed a new and more secure graphical password system, called PassPoints. In this work they describe the PassPoints system, its security characteristics, and the empirical study we carried out comparing PassPoints to alphanumeric passwords. In the empirical study participants learned either an alphanumeric or graphical password and subsequently carried out three longitudinal trials to input their passwords over a period of five weeks.

In the work "Secure Authentication" presented by Jyothi P Joy and Jyothi P Joy enhanced security schemes have been presented.The enhancements show the existence of a strong tradeoff between security and usability, indicating that the safety of cognitive authentication methods comes in a non-negligible usability cost. For this reason, the design of a new cognitive authentication method should not ignore possible threats induced by side-channel timing attacks.The paper "Graphical Password-Based User Authentication with Free-Form Doodles " presented by Marcos Martinez-Diaz, Julian Fierrez, and Javier Galbally discusses Authentication with free-form sketches Verification systems using dynamic time warping and Gaussian mixture models are proposed, based on dynamic signature verification approaches.

The most discriminant features are studied using the sequential forward floating selection algorithm. The effects of the time lapse between capture sessions and the impact of the training set size are also studied. Development and validation experiments are performed using the DooDB database, which contains passwords from 100 users captured on a smartphone touchscreen. Equal error rates between 3% and 8% are obtained against random forgeries and between 21% and 22% against skilled forgeries. High variability between capture sessions increases the error rates

A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme presented by Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao discusses an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Next, we analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login.

IV. PROPOSED SYSTEM

We design a authentication framework for mobile cloud based application. The normal cloud based apps use Text based password which are susceptible to dictionary attack, shoulder surfing, eavesdropping. To overcome some of these problems pictographic password are introduced. We provide two security Scheme for authentication. In this paper we proposed pictographic based authentication Scheme which includes

- Color Code Authentication Framework
- Geographic Authentication Framework

We also integrated geographic authentication Scheme in which user requires to choose a place on a digital map to

authentication with (a location password). In this we use GeoPass and allow user to annotate that location with some keywords (an annotated location password). In geographic Scheme, users are authenticated by correctly entering both a location and an annotation. We provide a robust and secure authentication framework for

- Online banking
- E-Commerce sites
- Social Networking sites
- Government organizations
- Cloud Storage
- Medical Applications
- Insurances Application

V. MODULES

In the proposed system we are going to implement following modules

There two main modules in this project

Web Application

It's basically a cloud storage application in which we implement following modules

1. Color Code Authentication Framework (CCA)
2. Geographic Authentication Framework (GAS)
3. OTP (One time password)
4. Challenge Response System (CRS)
5. DAO (Data access object)
6. AES (Advance Encryption System)
    - Encryption
    - Decryption

ABOUT WEB APPLICATION :

Fig 1. Once application is started through Eclipse it will open the application in the system default browser and display following page.

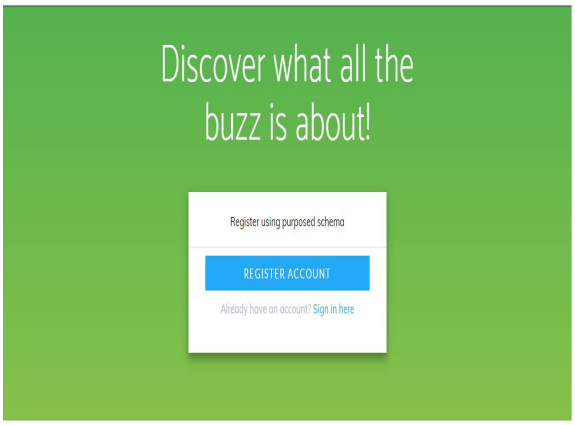

Fig 2. In this page we have to click on the register button which open the another page where user can register there account .

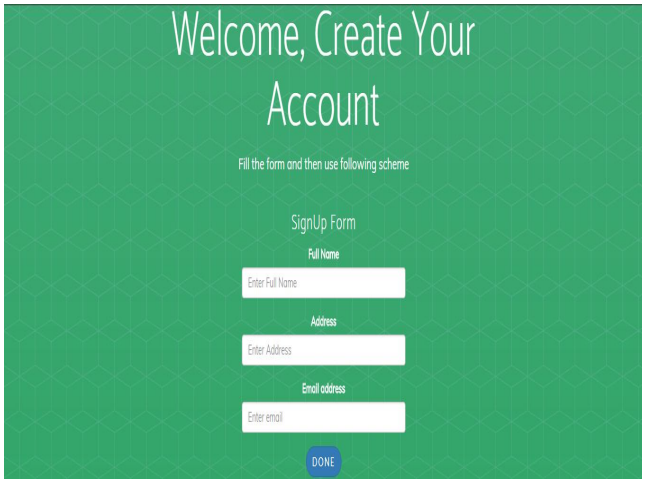

Fig 3. In this page user need to give following information regarding there name and address.

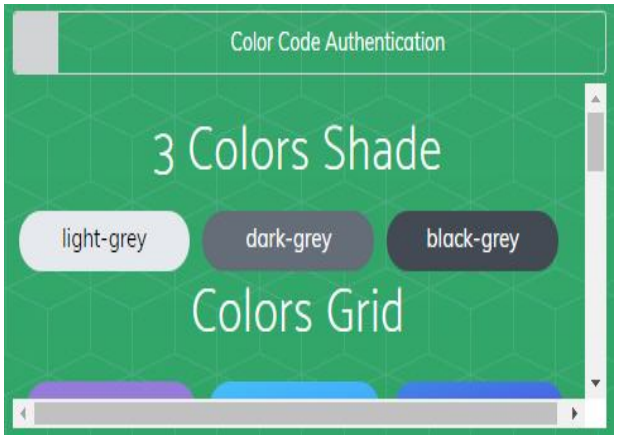

Fig 4. In this page user have to choose one shade from 3 color shade for authentication.

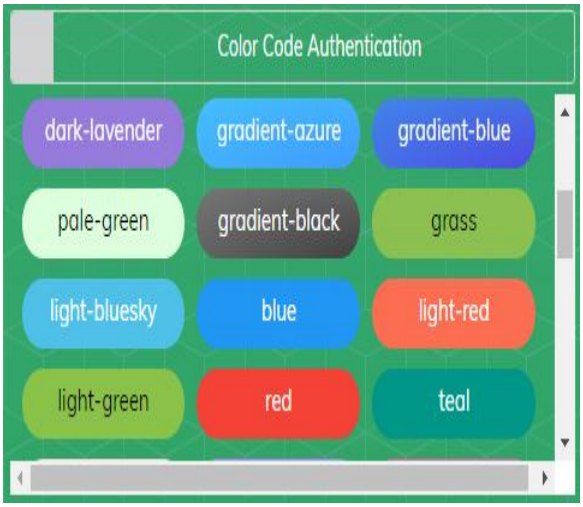

Fig 5. In this page the user has to choose 6 colors for authentication

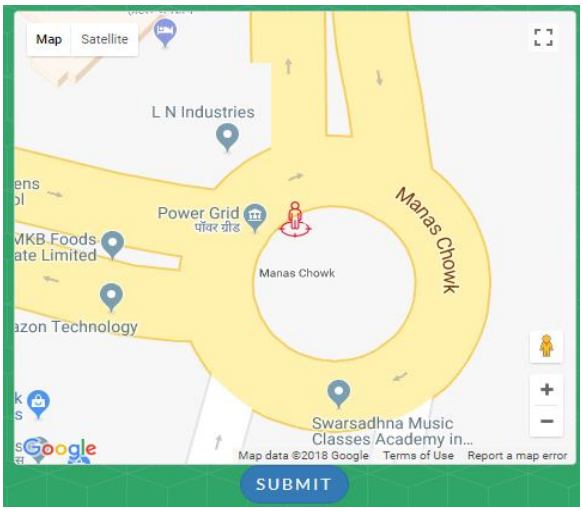

Fig 6. User have to give one address which is the password for the account.

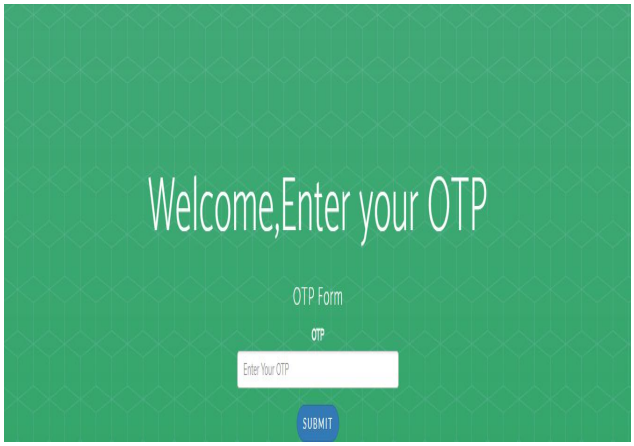

Fig 7: .In the Given mail address the user will receive OTP for the validation.

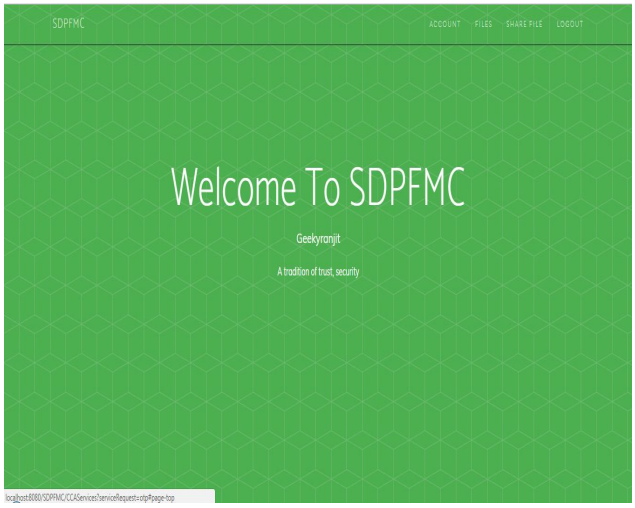

Fig 8: . This the account page:

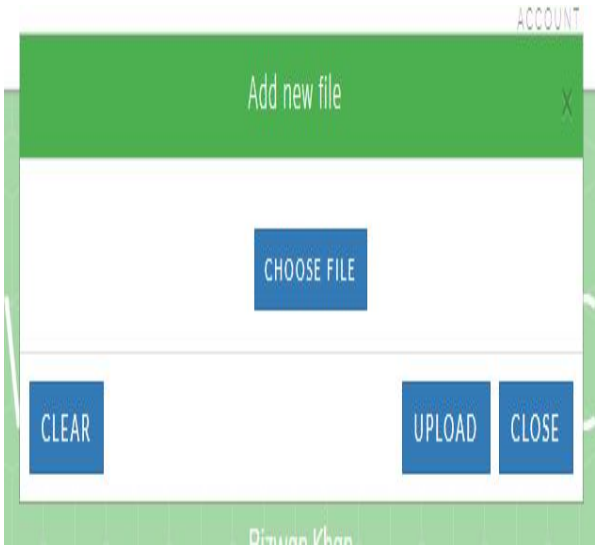

Fig 9: In this user can Upload a file.

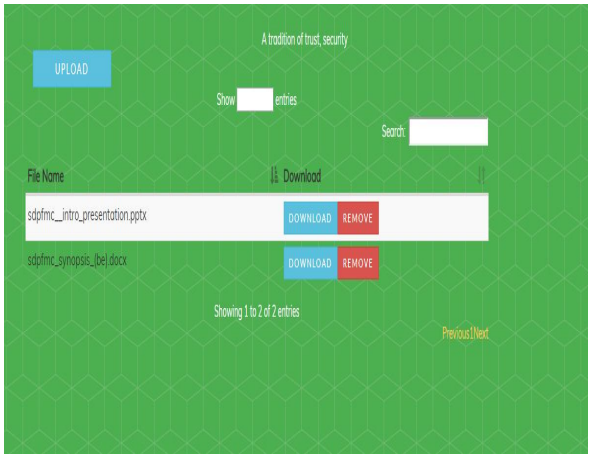

Fig 10: . Here user can download or delete the file.

VI. CONCLUSION AND FUTURE SCOPE

We conclude that we have been able to present a 3 level pictographical scheme for authentication system. We have been able to improve the security of graphical password systems by integrating color code and geographical approach which can be demonstrated by building and testing a fully functional prototype on localhost.

We also conclude that in this work the color code & geographical authentication will conserve the beneficial properties of graphical passwords while increasing their security.

As compare to plain text authentication scheme, the proposed scheme provides more robust and secure framework. We have integrated color code and geographical functionality to build this system. This system still need few updates to provide a complete authentication framework for cloud based application.

In future work we implement fingerprint, face recognition using iris sensor of android smartphone.

Currently this scheme is suitable for user authentication only, in future we can provide this scheme for payment, ticketing system, and other form of security application where authentication system is needed.

REFRENCES

[1] D. Huang, X. Zhang, M. Kang, and J. Luo, "Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication," in Proceedings of 5th IEEE International Symposium on Service-*Oriented System Engineering, 2010*.

[2] N. Santos, K. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," Proceedings of USENIX HotCloud, 2009.

[3] P. Barreto, B. Libert, N. McCullagh, and J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," Advances in Cryptology-ASIACRYPT 2005, pp. 515–532, 2005.

[4] Secure Networking And Computing Research Group (SNAC), "MobiCloud," available at http://mobicloud.asu.edu, 2010.