© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Secure Data Platform for Mobile Computing

Dolly R Pawar, Priya Jambhulkar, Supriya Sawwashere
Student, Information Technology G.N.I.E.T Nagpur, India

ABSTRACT

Cloud provides the environment for the mobile users called mobicloud to performs computationally intensive operation such as searching, data mining, and multimedia processing. Addressing the trust management, secure routing, and risk management issues in this framework are notable. To this end, we present a secure mobile cloud data access framework through trust management and private data isolation.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 android application which utilize our framework design using Pictographic , Geo Graphic passwords. Our Android app act as a client application for our web app. The web application With the rising popularity of cloud storage, and its ever-increasing versatility, it's no surprise that enterprises have jumped on the cloud bandwagon. We go with Android SDK because its offers a unified approach to application development for mobile devices which means developers need only develop for Android, and their applications should be able to run on different devices powered by Android. We will provide cloud storage functionality for end user using our security framework.

Keywords: Security, Privacy, Mobile Cloud, Data Security.

I. INTRODUCTION

Cloud computing has grown rapidly in the past few years due to the increasing network bandwidth, mature virtualization techniques, and emerging cloud based business demands. What is more, by 2013, mobile devices will overtake PCs as the most common web access entities worldwide as predicted by Gartner [1]. Thus, a mix of cloud computing with mobile technologies is highly expected. Mobile Cloud Computing (MCC) is a term that refers to an infrastructure where both data storage and data processing are done outside of mobile devices from which an application is launched. Besides that, a mobile entity is not limited to only a mobile device; more importantly, it could also be cloud resources, infrastructure, services, and human beings. Hence, with this understanding, MCC further refers to a cloud system where mobility happens in infrastructure, resources, services, user devices and even human beings. The trend of the MCC system is not just aimed to providing fixed services for users in certain areas, but is especially to look forward to establishing connections among mobile users all over the world. Due to the mobility of MCC users, a geographically distributed cloud system is a natural choice that allows users to connect to cloud resources that are geographically "close" to their mobile devices, which usually means less communication delay compared to the centralized approach.This research article is presented as a position paper to highlight research directions and possible solutions for enhancing secure mobile computing using cloud computing. MobiCloud transforms traditional

MANETs into a new service-oriented communication architecture.In MobiCloud, a mobile device can outsource its computing and storage services to its corresponding ESSI and Secure Storage (SS). Moreover, the device will send its sensed information such as moving trajectory to the cloud. As a return, the cloud can provide better location-based services according to the mobility information provided by the mobile device. In MobiCloud [2], mobile users must trust the cloud service provider to protect the data received from mobile devices. However, it is a big concern for storing their privacy sensitive information in a public cloud. This paper targets to address this privacy issue.The new secure mobile cloud framework .The mobile cloud is composed by three main domains: the cloud mobile and sensing domain, the cloud trusted domain, and the cloud public service and storage domain.

II. PROBLEM DEFINITION

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. The mobile devices are facing up with many struggles in their resources such as storage, security, communication and so on. A large number of security vulnerabilities and threats such as malicious codes Which affects the different mobile devices such as cellular phones, smartphones, laptops etc. These challenges have great affect in the improvement of the service qualities .Customer have expressed an interest in a common solution that can be used by cloud , mobile , web and components like API management , that enables simple discovery and secure access to OS business and infrastructure assets using REST technology .Infrastructure providers (cloud based IaaS and SaaS provider) and mobile services registers (i.e API management) require a uniform way to interact with middleware for discovery , provisioning , data transformation and service invocation .The fast advancing worlds of mobile and cloud computing are putting more and more pressure on the applications and business logics .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 spite of the hype achieved by mobile cloud computing, the growth of the mobile cloud computing subscribers is still below expectations due to the risks associated with the security and privacy. This study is based on existing literature, highlights the current state of the work proposed to secure mobile cloud computing infrastructure.Itani et al. proposed an energy efficient integrity verification scheme for mobile clients to verify the integrity of the files stored on a cloud server using an incremental message authentication code. The proposed scheme offloads most of the integrity verification jobs on a cloud service provider and trusted third party to minimize the processing overhead on the mobile client. The cloud service provider redirects the stored files towards the coprocessor when instructed by a mobile client. The coprocessor computes incremental MAC on received files for integrity verification. Jia et al., proposed a secure data service that outsources data and security

management on cloud without disclosing any user information with the help of proxy re-encryption and identity based encryption schemes. Although the proposed secure data service has removed security management overhead from mobile users, still mobile users have to perform cryptographic operations before uploading a file on cloud. The cryptographic operations involve massive pairing evaluations and exponential calculations. The cryptographic operations consume a considerable amount of energy that needs to be considered while designing a secure framework for mobile cloud computing. Secondly, the cloud is responsible for performing the security management and re-encryption on behalf of the mobile user.Hsueh et al. proposed a scheme for smart phones that ensures the security, integrity, and authentication of mobile user data. The mobile user encrypts the files using traditional asymmetric encryption techniques. The encrypted files are stored on cloud servers along with mobile user name, signature, and password. The encrypted files along with user credentials may be stored on a cloud server hosted by an adversary. The adversary can utilize credentials to impersonate the user later on. Secondly, the proposed scheme ignored the processing and storage limitations of the device. The encryption and decryption and even hash function applied on an entire file are performed on the mobile device. Yang et al. proposed a public provable data possession scheme for a resource constrained mobile device that ensures privacy and confidentiality. Trusted third party is responsible for handling encoding/decoding, encryption/decryption, signature generation, and verification on behalf of the mobile user. Although the offloading of mobile user's jobs on trusted third party saves energy, an increase in the number of mobile users results in performance degradation.Huan et al. proposed a new mobile cloud computing framework that not only provides conventional computation services but also improves the functionality of MANET in terms of risk management, trust management, and secure routing. In spite of the advantages provided by the MobiCloud to MANET, the MobiCloud framework did not consider the trust worthiness of the cloud node. There should be a mechanism to store mobile user information on cloud servers in a secure manner.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 implement an android application which uses our color code and geographic authentication framework for mobile cloud based application. The android app act as a client application for our Web application which will run on an local server for testing. 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 on Android application 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

MODULES

- Android Application
  It's basically an android based cloud storage application in which we utilize following modules

1. Color Code Authentication Framework (CCA)
2. Geographic Authentication Framework (GAS)

ABOUT ANDROID APPLICATION :

Figure 1. Once application is Installed we can start using it.Firstly it will show thw homepage of the app.

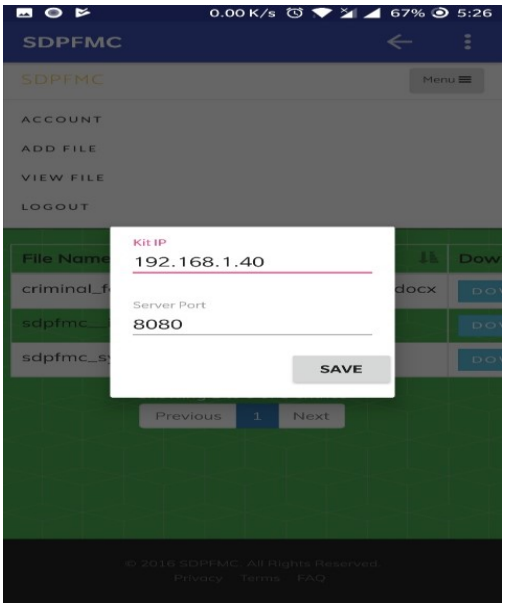

Figure 2. In this page user need to give the Server ip and Port address as we are using local hosting .

Figure 3. This page shows the application menus.. The account page will have following menus

- View FIles
- Upload File
- Logout

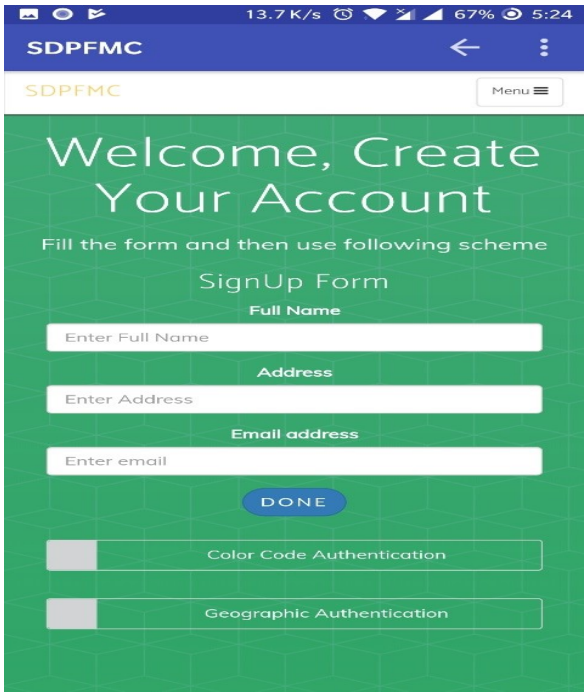

Figure 4. In this page user have to Fill the form .Where the user will have to provide the information related to there name , address and Email_ID.

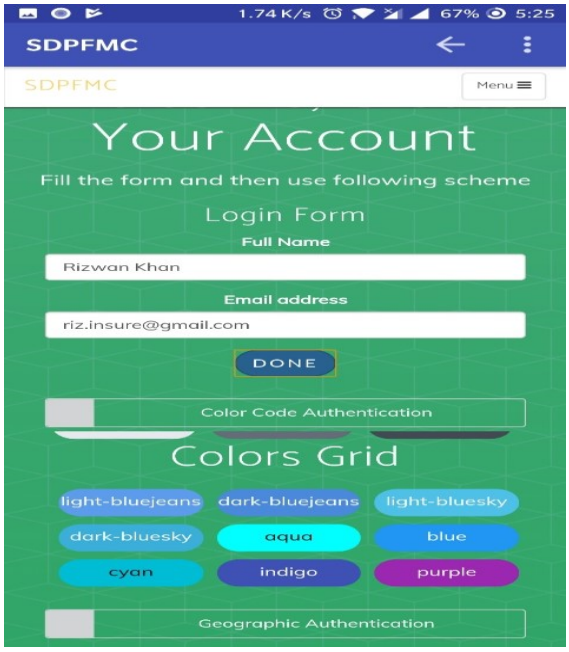

Figure 5. In this page the user has to choose 6 colors for authentication

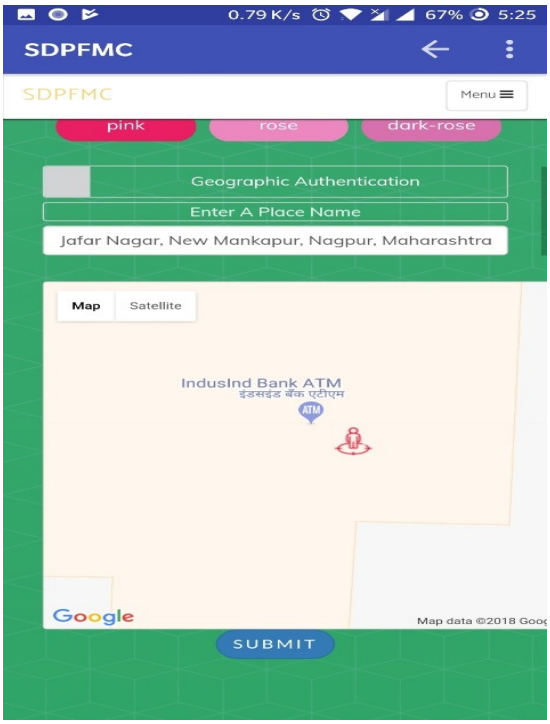

Figure 6. User have to give one address which is the password for the account.

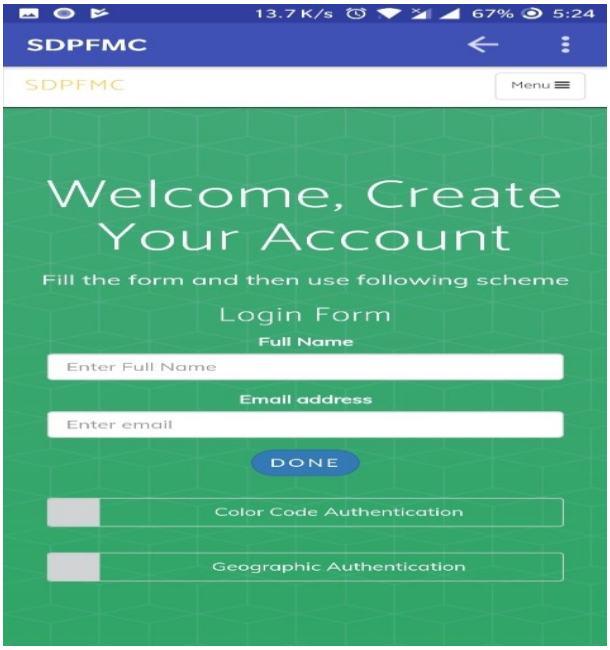

Figure 7. .User Need to remember the colors and address for the login that he gave at the time of registration .

Figure 8. This the account page:

Figure 9. In this user can Upload a file.

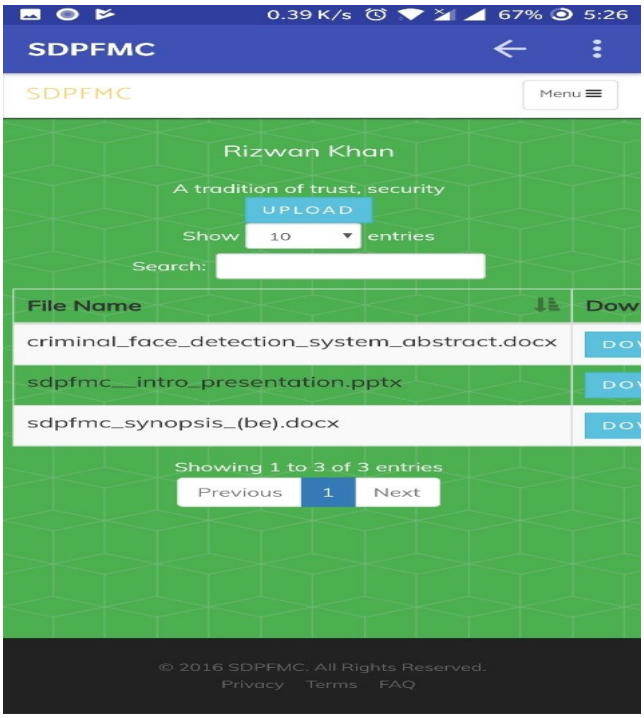

Figure 10. Here user can download or delete the file.

V. CONCLUSION AND FUTURE SCOPE

In this work we have been able to provide a new and more secure graphical password system based on Android application. Our Android app act as a client application. We conclude that we have been able to implement a 3 level pictographical scheme for authentication system on Android Application. We also conclude that we can use this application for cloud storage. Ultimately, we conclude that in this work the color code & geographical authentication will conserve the beneficial properties of graphical passwords while increasing their security for android as well as web applications.

As compare to plain text authentication scheme, the proposed scheme provides more robust and secure framework and it will also improve cloud storage security for android application. In future we can 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.

VI. REFERENCES

[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.