1. INTRODUCTION

The design of secure authentication protocols is quite challenging, considering that various kinds of root kits reside in PCs (Personal Computers) to observe user’s behavior and to make PCs untrusted devices. Involving human in authentication protocols, while promising, is not easy because of their limited capability of computation and memorization. Therefore, relying on users to enhance security necessarily degrades the usability. To that end, we propose two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol.

Our approach to solving the problem is to introduce an intermediate device that bridges a human user and a terminal. Then, instead of the user directly invoking the regular authentication protocol, she invokes a more sophisticated but user-friendly protocol via the intermediate helping device. Every interaction between the user and an intermediate helping device is visualized using a Quick Response (QR) code. The goal is to keep user-experience the same as in legacy authentication methods as much as possible, while preventing keylogging attacks. More specifically, our approach visualizes the security process of authentication using a smartphone aided augmented reality. The visual involvement of users in a security protocol boosts both the security of the protocol and is re-assuring to the user because she feels that she plays a role in the process. To securely implement visual security protocols, a smartphone with a camera is used. Instead of executing the entire security protocol on the personal computer, part of security protocol is moved to the smartphone. This visualization of some part of security protocols enhances security greatly and offers protection against hard-to-defend against attacks such as malware and keylogging attack, while not degrading the usability. However, we note that our goal is not securing the authentication process against the shoulder surfing attacker who can see or compromise simultaneously both devices over the shoulder, but rather to make it hard for the adversary to launch the attack.

QPass is a new challenge/response based on multi factor authentication.It stands for QR Code based Password. It provides a new cost effective method for multi factor user authentication. It is resistant against several attacks including key loggers.

1. PROBLEM DEFINITION

Existing systems we studied are RSAs SecureID and Googles Authenticator.Both of the SecureID and Google Authenticator are variations of the same idea, and they indeed implement the broader type of time based authentication using RFC 6238: TOTP: Time-Based One-Time Password Algorithm. Existing system of OTP’s relies on an external devices (RSA SecureID) or SMS. OTP’s send as SMS are prone to network delays and are not accessible .They are costly for small companies to implement.

The proposed system helps us to provide a universal economic secure solution. Proposed system not only help to find who took our phone, but also help as to keep our mobile phone secure from unknown persons. It help us to keep our personal data away from unknown person. Our approach visualizes the security process of authentication using a smartphone aided augmented reality. The visual involvement of users in a security protocol boosts both the security of the protocol and is re-assuring to the user because she feels that she plays a role in the process. To securely implement visual security protocols, a smartphone with a camera is used. Instead of executing the entire security protocol on the personal computer, part of security protocol is moved to the smartphone. This visualization of some part of security protocols enhances security greatly and offers protection against hard-to-defend against attacks such as malware and keylogging attack, while not degrading the usability. However, we note that our goal is not securing the authentication process against the shouldersurfing attacker who can see or compromise simultaneously both devices over the shoulder, but rather to make it hard for the adversary to launch the attack.

3.OBJECTIVES

QPass aims at providing an economical way to provide secure login to websites

It is secure against common password stealing attacks including key loggers.

We aim at realizations of protocols that not only improve the user experience but also resist challenging attacks, such as the keylogger and malware attacks. Our protocols utilize simple technologies available in most out-of-the-box smartphone devices. Our work indeed opens the door for several other directions that we would like to investigate as a future work. In future, we plan to implement our protocol on the smart glasses such as the google glass, and conduct the user study.

4. EXISTING SYSTEM

Some of the major companies like Google, Facebook,Twitter,Dropbox have implemented Two Step Authentication.Most of them have implemented two step verification using SMS suffering from disadvantages discussed before. Independent OTP devices like RSA SecureID and Google Authenticator uses Time Based OTP’s. This gives the attacker a window for replay attacks External devices like RSA SecureID need not be present with user at all times while phone is always available for authentication.

5. SOFTWARE REQUIREMENT SPECIFICATION

5.1. INTRODUCTION

**5.1.1 Purpose of this Document**

This SRS describes the function and the performance allocated to our product. It provides a reference for the validation of the final product.SRS provides an overview of the product including functional and nonfunctional requirements, abbreviations used, product and functions etc.

**5.1.2 Scope of the Development Project**

The name of our product is “QPass”. This application is mainly based on security and systems. Provides better protection for the users. It aims at giving a universal economical way for authentication.

**5.1.3Overview of Document**

This document provides a description of the requirements of the product. Section 2 of the SRS gives detailed description of the product including the data requirements. Section 3 provides specific functional requirements of the different components of the product and the performance criteria. Section 4 provides idea about the software and hardware requirements.

5.2 GENERAL DESCRIPTION

**5.2.1User Characteristics**

The user is registerd with QPass web site.He could login to other websites that registerd to QPass securely using QR Codes.He could choose any one of the two protocols discussed above.

**5.2.2 Product Perspective**

The software on been installed can be implemented on any android system or a device which has a camera.

**5.2.3General Constraints, Assumptions, Dependencies and Guidelines**

The system will work only if there is a smart phone. The user can add QPass as an extra security measure for logging in.

5.3 SPECIALREQUIREMENTS

**5.3.1 User Interface**

The user can interact with the system using graphical user interface. Using the screen, user can customize all settings the application.

**5.3.2 Detailed Description of Functional Requirements**

This section provides a requirement overview of the product. The project will be developed on java, and will run in an android operating system.

**5.3.3 Functional Requirements**

* Login only for valid user.
* Owner can change the password after login to application.
* Owner can customize the application settings.
* Users can select the protocols of their choice
* Companies could register with QPass and provide a secure login for their clients

**5.3.4 User Input Validation**

If the user leaves a mandatory field blank, he will be prompted to enter valid data in that particular field.The data is verified against common XSS and SQLi attack vectors.

**5.3.5 Performance Requirement**

The performance of our product is at its best if the users use a smartphoen with a camera of resolution 2 MP or above.

5.4 REQUIREMENTS

**5.4.1 Software Requirements**

Operating system : Android

Platform : Eclipse

Client Side : Android

Server Side : JSP

**5.4.2 Hardware Requirements**

Processor : 1.6 GHz or faster processor.

Memory size : 1GB RAM.

Storage : 10 GB Hard Disk.

Keyboard : Virtual keyboard with 102 keys.

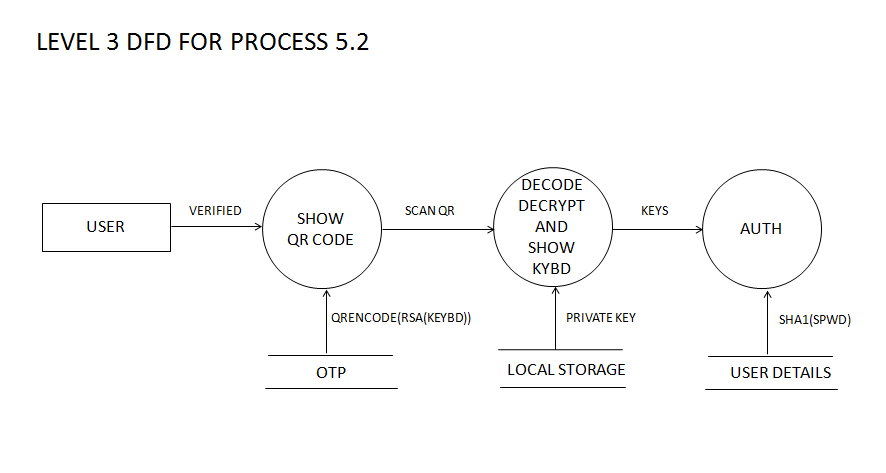
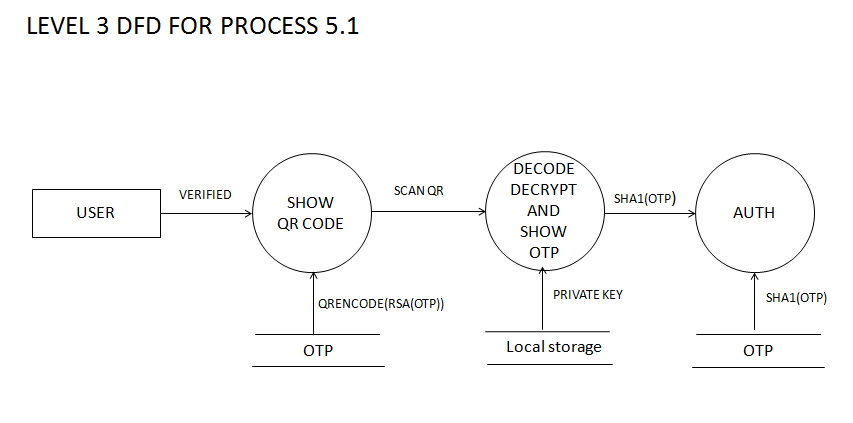
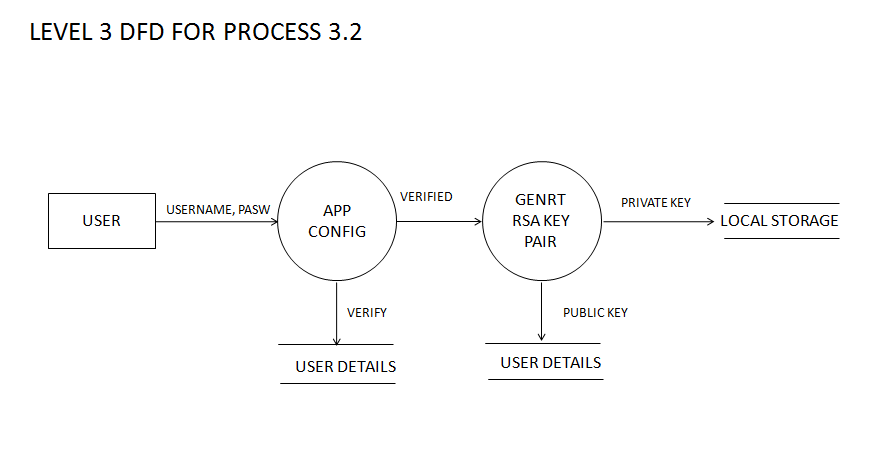
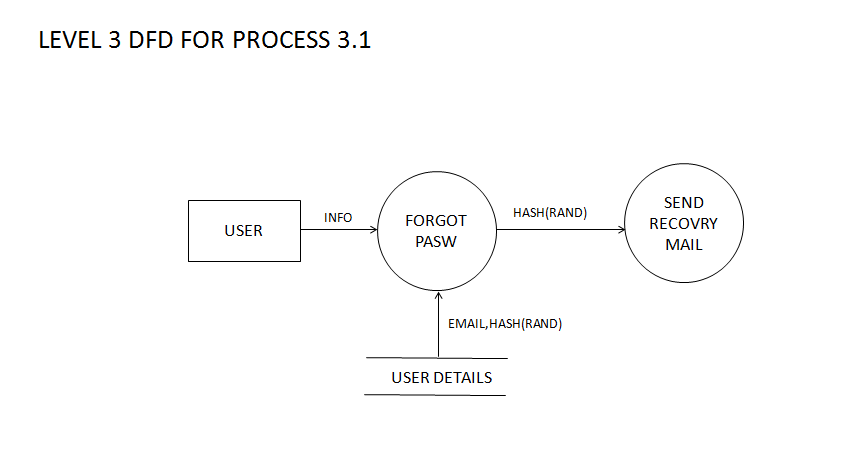
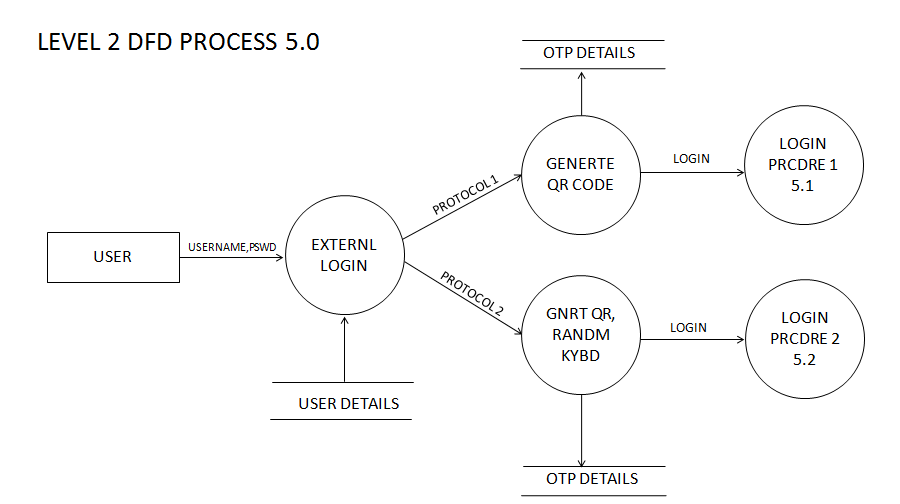
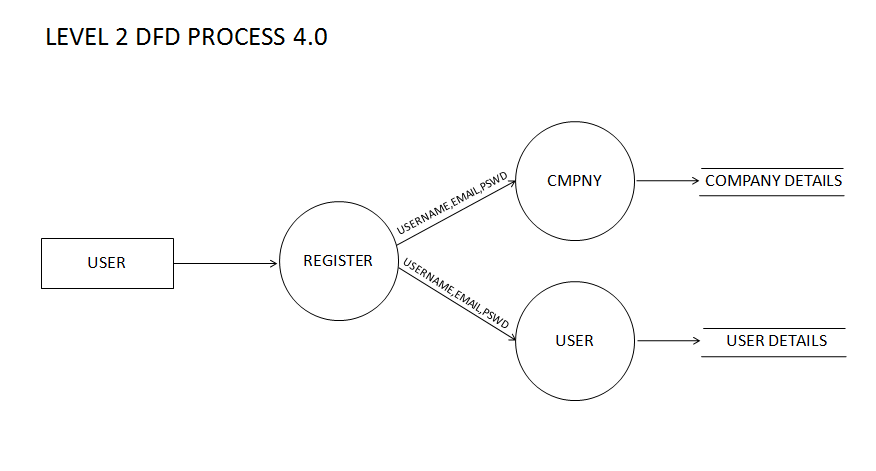
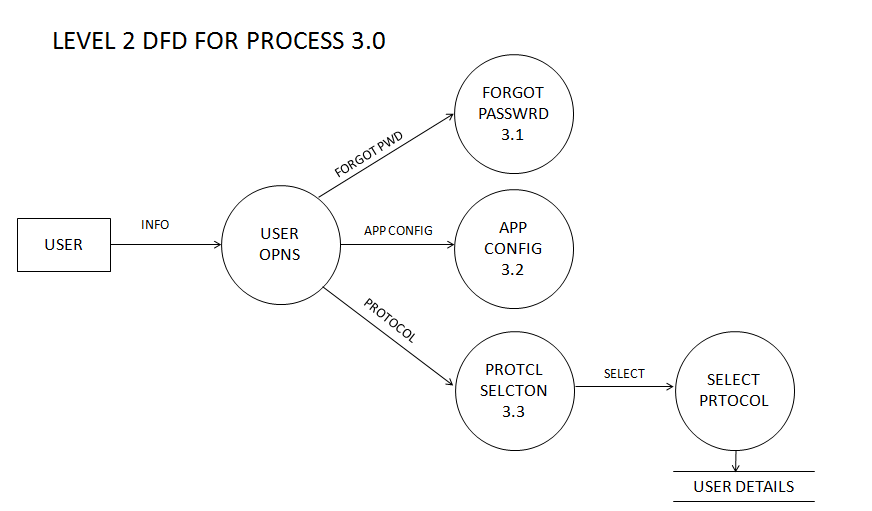
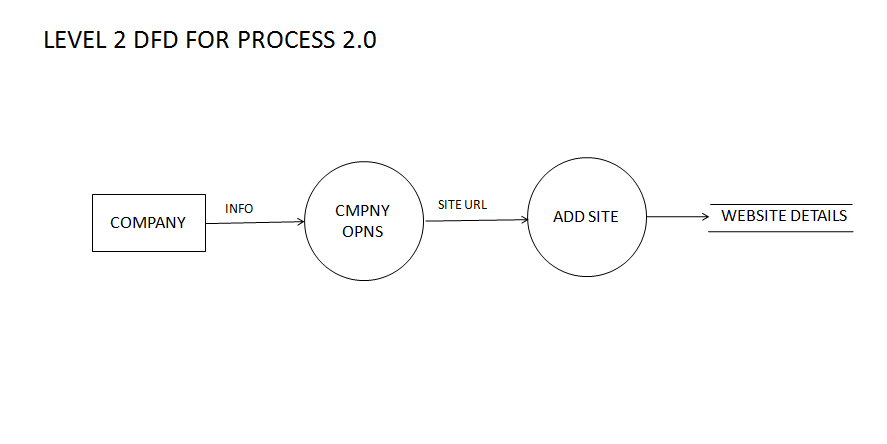
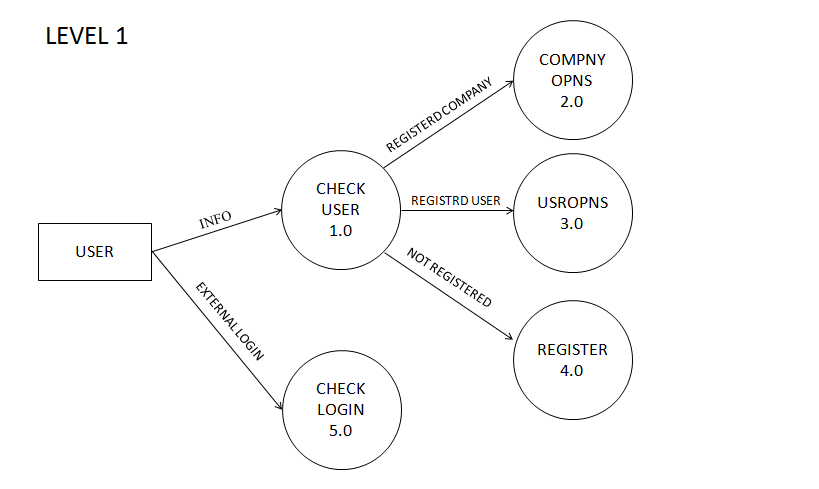
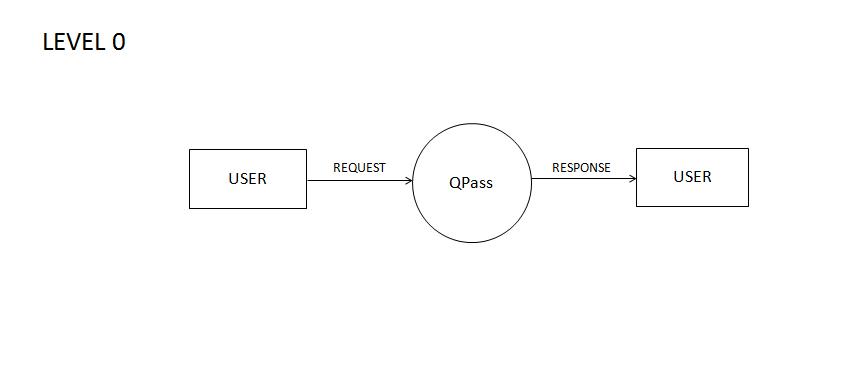
Device : Android Mobile with 2MP or higher camera.

6. MODULES

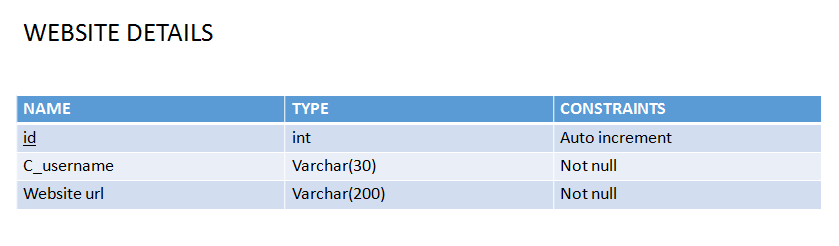
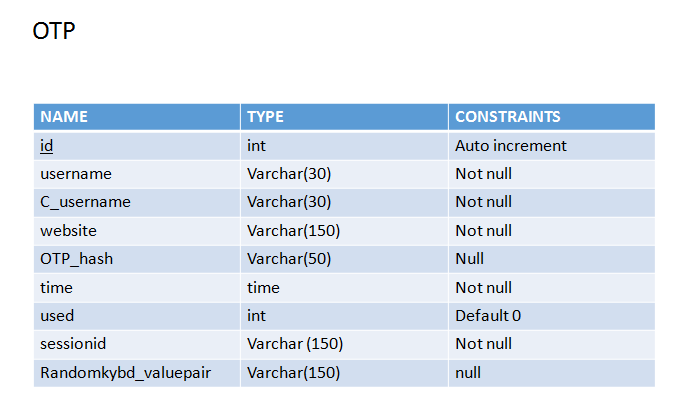
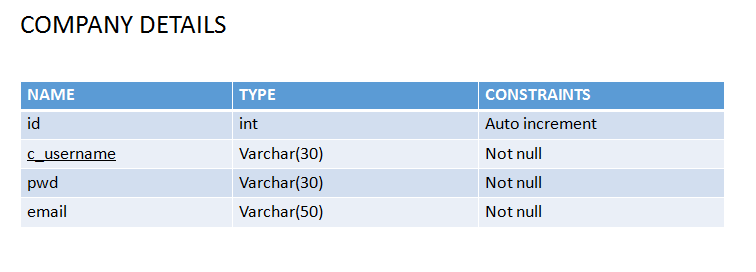
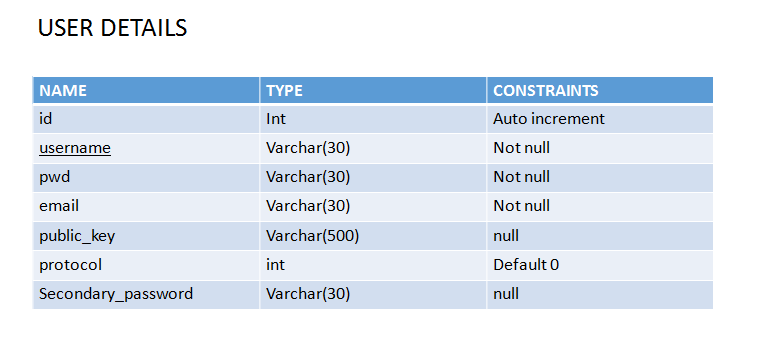
There are 4 modules in this project.

* REGISTRATION
  + Username, password and email address are collected from users and companies
  + Companies can enter their website details
  + User can select protocol and specify secondary password
* APPLICATION CONFIGURATION
  + Verified user can only use the system
  + RSA 2048 bit key pair generation
  + Public key is uploaded to server
  + Private key is saved to local storage
* QR CODE GENERATION
  + User is verified and protocol selected
  + For protocol 1 OTP is generated, encrypted and encoded to QR code
  + For protocol 2 random keyboard layout is created ,encrypted and encoded to QR code
* LOGIN PROCEDURE
  + User is verified , QR code is generated and displayed
  + User scans the QR Code
  + For protocol 1 OTP is decoded from QR code, decrypted and displayed
  + For protocol 2 Keyboard layout is decoded from QR code ,decrypted and displayed

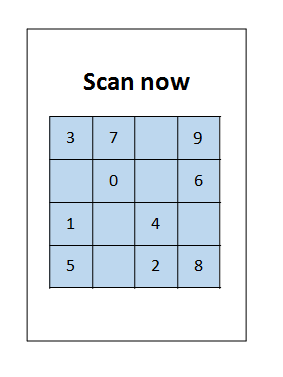
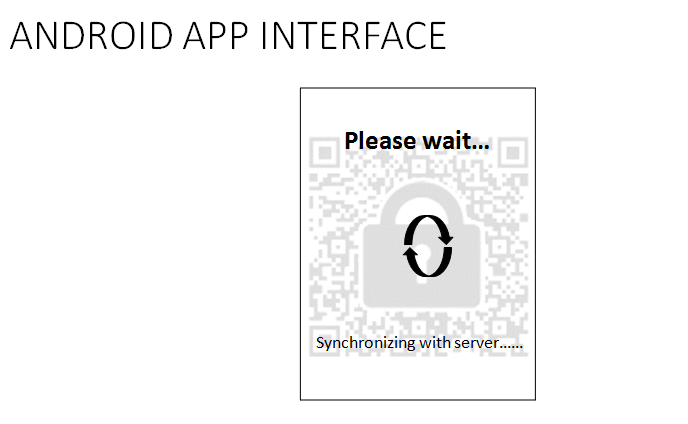
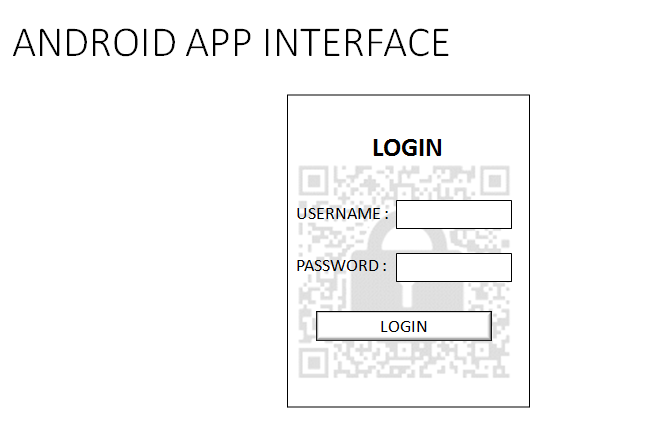
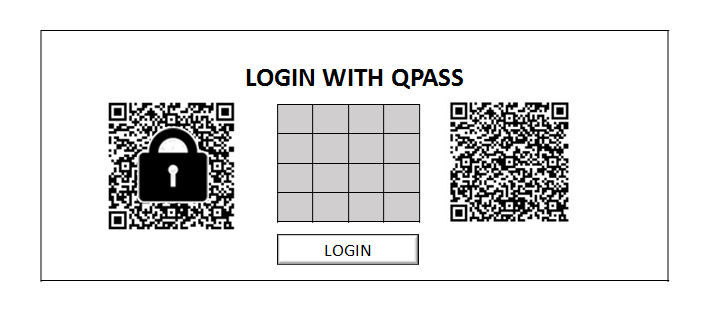
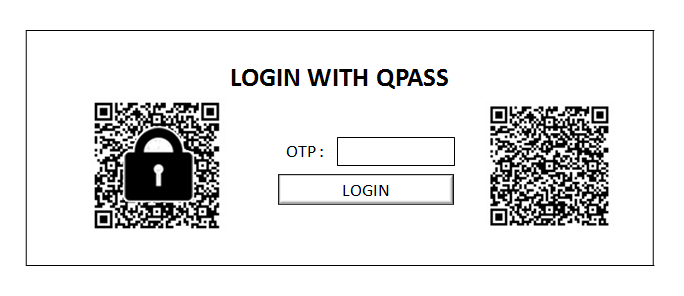
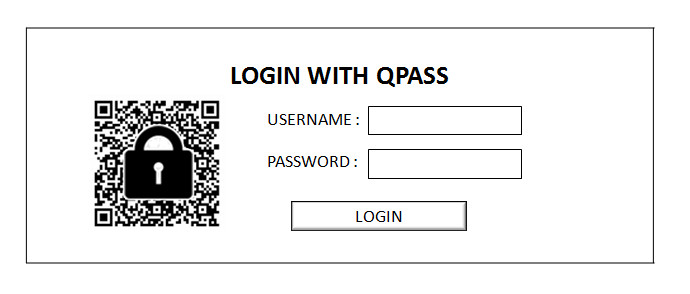
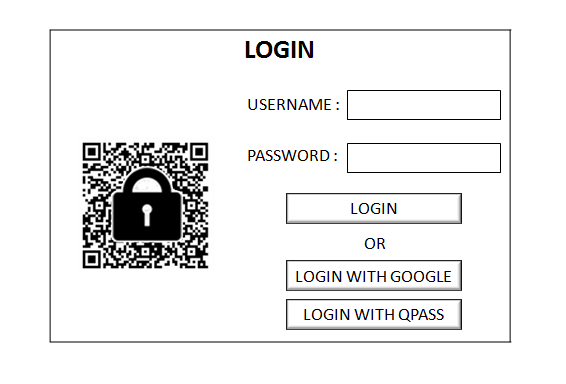
**7. DATA FLOW DIAGRAMS**



8.TABLE DESIGN



9. FORM DESIGN



10.CONCLUSION

Gotya will be a great security application which help as to find which unknown person took our smart phone. This application is mainly based on security and systems. Gotya provides better protection for the smartphones.The system will work only if there is a properly configured network connection.User get much protection than using other applications.Data encryption/decryption is included in this software, so that it guarantees the protection of the user.

Gotya also help as to erase all our personal data from the phone when some thief try to access our smart phone. . It also help as to encrypt our personal data in our phone. Gotya help as to set a strong password or a strong swipe pattern for our smartphone. It will also provide password expire technology.

11.REFERENCES

[1] —. Google authenticator. http://code.google.com/p/google-authenticator/

[2] —. Rsa securid. http://www.emc.com/security/rsa-securid.htm.

[3] Cronto. http://www.cronto.com/.

[4] —. BS ISO/IEC 18004:2006. information technology. automatic identiﬁcation and data capture techniques. ISO/IEC, 2006.

[5] —. ZXing. http://code.google.com/p/zxing/, 2011.

[6] D. Boneh and X. Boyen. Short signatures without random oracles. In

Proc. of EUROCRYPT, pages 56–73, 2004.

[7] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest

to replace passwords: A framework for comparative evaluation of web

authentication schemes. In Security and Privacy (SP), 2012 IEEE

Symposium on, pages 553–567. IEEE, 2012.

[8] J. Brown. Zbar bar code reader, zbar android sdk 0.2.

http://zbar.sourceforge.net/, April 2012.

[9] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. M. McCune, A. Studer,

A. Perrig, B.-Y. Yang, and T.-C. Wu. Gangs: gather, authenticate

’n group securely. In J. J. Garcia-Luna-Aceves, R. Sivakumar, and

P. Steenkiste, editors, MOBICOM, pages 92–103. ACM, 2008.

[10] S. Chiasson, P. van Oorschot, and R. Biddle. Graphical password

authentication using cued click points. In Proc. of ESORICS, 2008.

[11] D. Crockford. The application/json media type for javascript object

notation (json). http://www.ietf.org/rfc/rfc4627.txt?number=4627, July

2006.