International Journal of System and Software Engineering
Volume 5 Issue 1, June 2017
ISSN.: 2321-6107

Multi-Factor Authentication for Net Banking

Neenu Ann Shaji[1], Sumitha Soman[1]
[1]Computer Science and Engineering Sree Buddha College of Engineering, Pattoor, Alappuzha, Kerala, India
E-mail: neenuannshaji@gmail.com

Abstract: Today's mobile devices come incorporated with biometric security features. In this paper, we explain about how to use this feature to develop a web login authentication mobile application. Our application uses Redmi Xiaomi note 3 fingerprint recognition feature to login to the application and only using this interface we can carry on any online transactions. On the web side, we enable the user to login and thus proceed with the transaction. The user has to enter a valid OTP send to his phone within a limited time frame. On the successful completion of that, a QR code will be generated which is encrypted with the registered IMEI and the OTP generated. When all these three authentication procedures fall into place, a transaction proceeds to fulfillment. As the production of mobile devices with fingerprint recognition continues to increase, biometric authentication apps, like the one introduced here, will become a prevalent security measure.

Keywords: Index Terms-biometric, fingerprint, online transactions

I. Introduction

Mobile devices have paved their way right into the routine of human life. As they have a significant role in the daily life, users access their social networks, bank accounts and many other websites via these devices. With the increasing use of mobile devices, security problems also arise. The followed way of authentication is by providing a security password, username etc. This method of authentication is vulnerable, as anyone having our personal details can easily carry out actions in our name. Mobile hardware manufacturers, operating system and application developers take a variety of security measures due to the personal, private and/or sensitive nature of the information stored in mobile devices. Biometric authentication is now the emerging trend. The fingerprint login feature is becoming increasingly popular as it provides high level of security in a very user friendly manner.

In this paper, we come up with an application developed using the fingerprint security feature of Redmi Xiaomi note 3. We will discuss the importance of fingerprint security applications and the development stages of our fingerprint web login authentication program.

A. Biometric Security in Net Banking

Biometrics is the way of authenticating based on the physiological or chemical traits of a person. These traits will be unique for each individual. As they can never be stolen or replicated, they prevent dictionary attacks (It is a way of trying hundreds and sometimes even millions of combinations as in a dictionary so as to find the correct one), phishing attacks (fraudulent acts that try to acquire our personal information by gaining faith in us) etc. While making online payments or transferring money from one account to another, the online bankers are always concerned about the hackers and anti-social elements. The followed way of authentication is vulnerable, as anyone having our personal details can easily carry out actions in our name. Mobile hardware manufacturers, operating system and application developers take a variety of security measures due to the personal, private and/or sensitive nature of the information stored in mobile devices. Considering all the advantages of biometric recognition, mobile device manufacturers have started to include different biometric sensors on mobile devices. The fingerprint authentication feature is used here as it has a high accuracy and is the front-runner for mass-market biometric-ID systems. Goode Intelligence predicts that 3.4 billion users will use biometric systems on their mobile devices by 2018 [4].

II. The Developed System

With the increase of mobile devices that accommodate the fingerprint recognition feature, it is possible to use this feature for security. Many security measures have been adopted in the areas of e-governance, e-banking and e-learning for verifying the user identity.

The proposed system enhances the current authentication system in e-banking by adding two additional layers of security, specifically a biometric scan and IMEI verification. Proposed system uses finger print feature for authentication of the user. Our Android based Web Login Authentication application has been developed to use the mobile biometric feature.

A. Operation of the Application

The application is divided among two phases, the web phase and the android application phase.

The user has to register with the bank his IMEI, phone number and the basic information at the time of the account creation.

The operation of Web Side is as follows:

1) The login page of the banking site will be asking the username and password form the user. The user can also update the password, provided he should know the IMEI of the device. We use the IMEI for security purpose else any intruder knowing the username and password can update the user account. From the login page, the user is directed to the payment page.
2) The payment asks for the payee details and the amount to be transferred. If the amount exceeds the account balance, the transaction fails.

   After providing the correct details, a 4 digit OTP is send to phone. The 2 digits of OTP will be any combination of 0-9 and A-B and the next 2 digits will be a combination of current timestamp and User ID. If the OTP entered matches with the one send to the registered number, a QR code will be generated.
3) This QR code is encoded with IMEI registered and the OTP generated, using the Message Digest 5(MD5) algorithm. This QR code has to be scanned within the time limit using our android application. When the IMEI matches, the transfer proceeds to success.

The user has to register with the bank his IMEI, phone number and the basic information at the time of the account creation.

Fig. 1: Login in using Username and Password

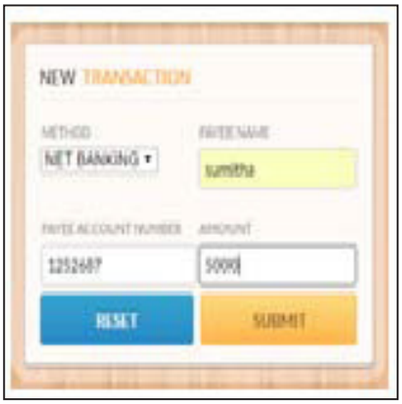

Fig. 2: Entering the Transaction Details

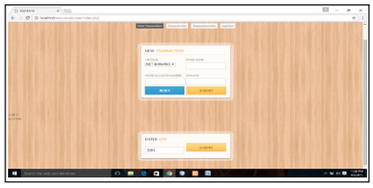

Fig. 3: OTP generated and Send to User's Phone

Fig. 4: QR Code Generated when OTP is Matched

The operation of the Android Application is as follows:

1) Initially, the user is presented with the screen shown in Figure 1, here the user will be asked to login with any of the registered fingerprint in the device. If the fingerprint is not registered, the user can do the same by getting into the device settings (Android devices support up to 5 fingerprints). After the successful authentication, the user is directed to the next interface.
2) In second interface, we use a cam scanner to scan the QR code generated at the web side. The QR code will be having the IMEI number of the registered device. During the scanning process, the device compares the IMEI number of the device with the one in the QR code.

After the successful completion of authentication process, the verified user will be allowed to proceed with the banking transaction.

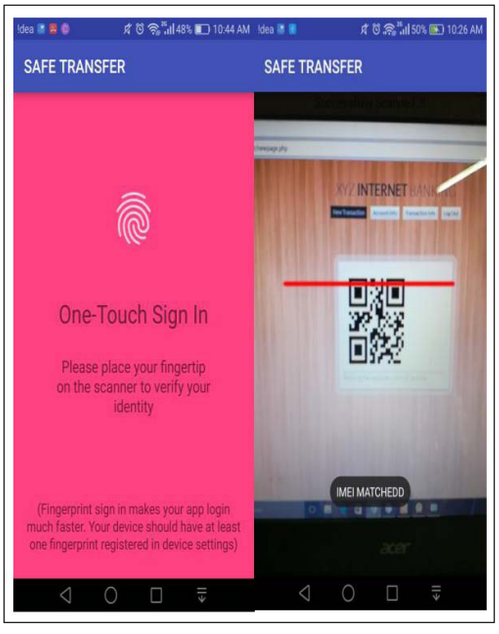

Fig. 5: Android Side Working

B. Main Components

Before discussing about the components of the application, we will talk about the phone used. We use a Xiaomi Redmi Note3. It has inbuilt fingerprint recognition feature and it allows third party application developers to create applications using the fingerprint sensor API. The user application runs on the device and it needs to be authenticated with any one among the five registered fingerprints in the phone. We will have the IMEI number of the phone registered into the database along with the customer details. The user can only use the registered device for a transaction. Up to four different fingerprints can be registered on the phone. The owner has to verify each time a new fingerprint is added. Thus even if the intruder passes all other steps on the web side, he won't be able to access the phone without a proper fingerprint match.

After the user provides all the details about the transaction, an OTP will be generated, which is based on a shuffle method. Two of the characters will be the timestamp and the other two will be any combinations of alphanumeric characters.

The OTP will be send to the registered device and it will have a lifespan of 3minutes. The user has to enter the valid OTP within the time frame else the entire transaction will come to fail. If the user manages to enter the correct OTP, a Quick Response code will be generated which is encoded with the IMEI number of the registered device and the OTP.

And now comes the android part. The user opens the application using any one of the registered fingerprint and then the user will be treated by the scanning interface. The QR code generated at the web side is scanned and the IMEI is verified across the current device's IMEI and if found the same, the user is notified and the transaction comes to a successful end. QR code scanning is also having a time frame.

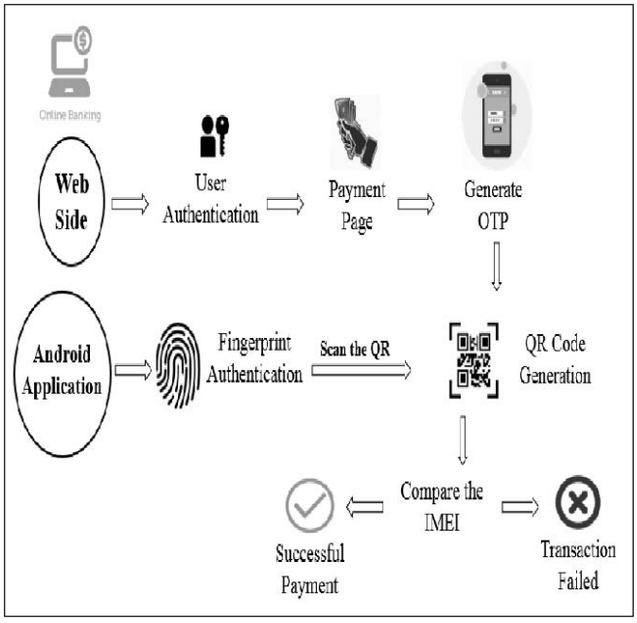

Fig. 6: Components of the Application

III. Conclusion

Internet banking now a days tend to be exposed to different types of security threats. With the growth of e-banking, new forms of security risks arise.

Today most of the mobile devices come with the biometric authentication feature. Here, we use this authentication mechanism for improving the security of web based application and can thus ensure the user, a well-protected online transaction.

In this paper, an innovative system is implemented which uses OTP, IMEI and finger print verification for authentication. Thus user authentication as well as device authentication is achieved. So security is not compromised by fraudulent calls and other kinds of phishing attacks. The developed system is capable to overcome different forms of phishing attacks including vishing. Limitation is that it requires both desktop/laptop and a mobile device with finger print sensors and camera for a transaction to get accomplished.

References

[1] A. C. Grivei, "Touch based biometric authentication for android devices," *ECAI 2015 - International Conference on (7thEd), Electronics, Computers and Artificial Intelligence*, Bucharest, June 2015.

[2] M. Umamaheswari, S. Sivasubramanian, and B. H. Kumar, "Online credit card transaction using finger print recognition," *International Journal of Engineering and Technology*, vol. 2, no. 5, pp. 320-322, 2010.

[3] W. Yang, J. Hu, J. Yang, S. Wang, and L. Shu, "Biometrics for securing mobile payments: Benefits, challenges and solutions," *6th International Congress on Image and Signal Processing*, 2013.

[4] "Goode Intelligence forecasts that the market for mobile biometric security products and services is set to grow and will generate over $S.3 billion revenue by 201S," 2013, Available: Goodeintelligence.com

[5] Q. Tao, and R. Veldhuis, "Biometric authentication system on mobile personal devices," *IEEE Transactions on Instrumentation and Measurement,* 2010.

[6] F. S. Lesani, F. F. Ghazvini, and R. Dianat, "Mobile phone security using automatic lip reading," *9th International Conference on e-Commerce in Developing Countries: With focus on e-Business (ECDC)*, 2015.

[7] D. Mahto, and D. K. Yadav, "Enhancing security of one-time password using elliptic curve cryptography with biometrics for e-commerce applications", *IEEE 3rd International Conference on Computer, Communication, Control and Information Technology*, 2015.

[8] W. Yang, Y. Wu, and G. Chen, "Application of voice recognition for mobile e-commerce security", *3rd Pacific-Asia Conference on Circuits, Communications and System (PACCS),* 2011.

[9] S. Easwaramoorthy, "Biometric authentication using finger nails," *International Conference on Emerging Trends in Engineering, Technology and Science*, 2016.

[10] T. Barbu, A. Ciobanu, and M. Luca, "Multimodal Biometric Authentication based on Voice, Face and Iris," *Conference on E-Health and Bioengineering (EHB)*, 2015.

[11] Y. Li, J. Yang, M. Xie, D. Carlson, H. G. Jang, and J. Bian, "Comparison of PIN- and pattern-based behavioral biometric authentication on mobile devices," *Military Communications Conference, MILCOM*, 2015.