Bank Authentication for Mobile Payment Services

Sanjana Reddy B, Smitha H B, Priyanka Aryan M P, Shradha Janib, Vishwesh J*

Department of Computer Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, India

DOI: https://doi.org/10.21467/proceedings.1.32

* Corresponding author email: vishweshj@gsss.edu.in

Abstract

In our project we ensure the authentication for the applied customer. We use the mobile payment service. Mobile payment method is a user friendly than other payment methods. The RSA algorithm is used to ensure the security of the proposed method. In this process Bank, Visa center and the mobile center plays the main role. Customer request the services from the bank. Than bank should contact the visa center to give a authorization for the mobile. Bank should inform the mobile center that the services is authorized by sending information. Mobile center sends a message to the customer. The customer receives the pin from the bank. The bank will generate a computed public and private key and send public key to market. Then the market generates a computed public and private key and send customer can use the services.

Keywords— Encryption, Security, Cryptography, Mobile payment;

1 INTRODUCTION

The definition of a mobile payment is the payment for goods between two parties for which a mobile device plays a key role in the realization of the payment, Mobile payment can be categorized into two main types based on the geographical position between customers and merchant; these are Remote payment: The customer initiate payment remotely from the merchant, and POS (Point of Sale) or Proximity mobile payment: The customer is near the merchant or retail. These types have a variety of different technologies that can be widely applied especially in the Middle East where there is a high mobile device concentration. The following are some of these technologies: SMS (Short messages Service), USSD (Unstructured supplementary service data), NFC (Near field communication), RFID (Radio frequencies identification). The security in mobile payment is divided since it relies on different players or stakeholders. One of the top industries worry about different attacks that can be launched in retail payment such as; mobile, and Credit card payment methods. One of the methods that can be used to secure communications in presence of hackers is cryptography. Moreover, the cryptanalysis and attacking, protocols speed, and performance evaluation are the core elements in building a secure mobile payment system. Therefore, this paper focuses its attention on these concerns by presenting a mobile payment system which is based on public key cryptography.

2 PROPOSED APPROACH

Generally, the proposed method describes three processes for mobile payment system (refer to Figure1). Whereby, the proposed method is based on the integer factorization problem for RSA public-key cryptosystem. Meanwhile, RSA cryptosystem is typically divided into three sub-algorithms; key generation, encryption, and decryption algorithms. However, the proposed method processes are: the authentication process, the member recognition process, and payment process.

3 Authentication Process

This process is the first step in the proposed mobile payment system that prepares the customer to be able to use the mobile for payment. In this phase, the Bank, the Visa Center, and the Mobile Center plays the main role, whereby confirmation can be given to the customer. As illustrated in Figure 1, the customer should request the mobile payment service from the bank. Once the Customer requested the service from the bank, the following steps should have been done by the bank. As shown in Figure 1, the bank should contact the visa center depending on the customer's request to give authorization for the mobile. Following these two steps, the bank should notify the mobile center that the service is authorized by sending the customer information as shown in Figure 1. The mobile center, in turn, confirms this process by sending a message to the customer as shown in Figure 1. Figure 3 step 6 shows that the customer gets the service by receiving the PIN from the bank. Once the customer gets the PIN, the bank will generate a computed RSA public-key and private-key (refer to Figure 1) and then pass the public-key to the market (refer to Figure 1) After that the market will generate a computed RSA public-key and private-key (refer to Figure 1) and then pass the public-key to the bank (refer to Figure 1). Finally, the customer can go to the market and use the mobile for Payment. The diagram shows the process of the authentication.

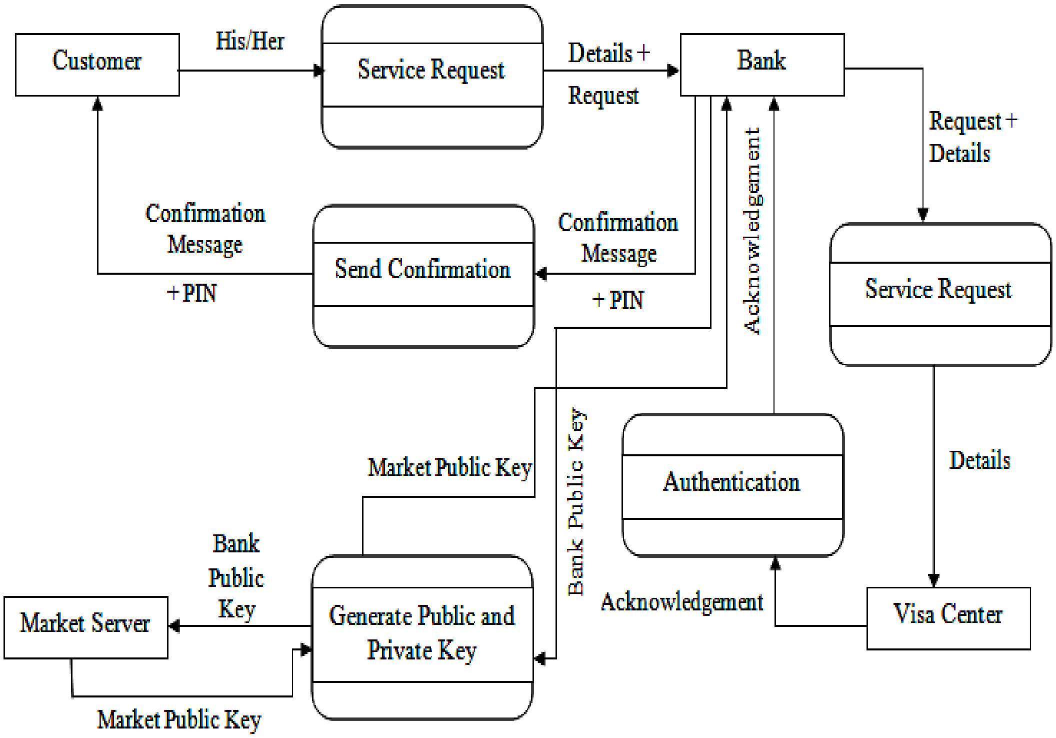
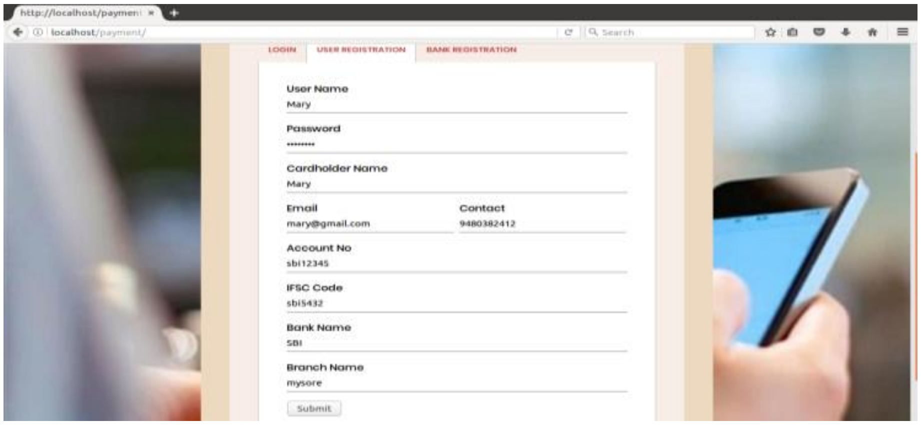


Figure 1: Authentication process

4 SIMULATION RESULTS

Firstly the users register shown in fig 1, bank registration shown in fig 2, user login shown in fig 3, authentication request, confirmation message, bank login, services request sent to visa center, visa center login, confirmation of authorization, bank login, user has been authorized successfully, mobile login, notification added, request for mobile payment confirmation, bank login, pin sent to mail id, user receive the pin shown in fig 4.



User Name
Mary

Password
••••••••

Cardholder Name
Mary

Email
mary@gmail.com

Contact
9480382412

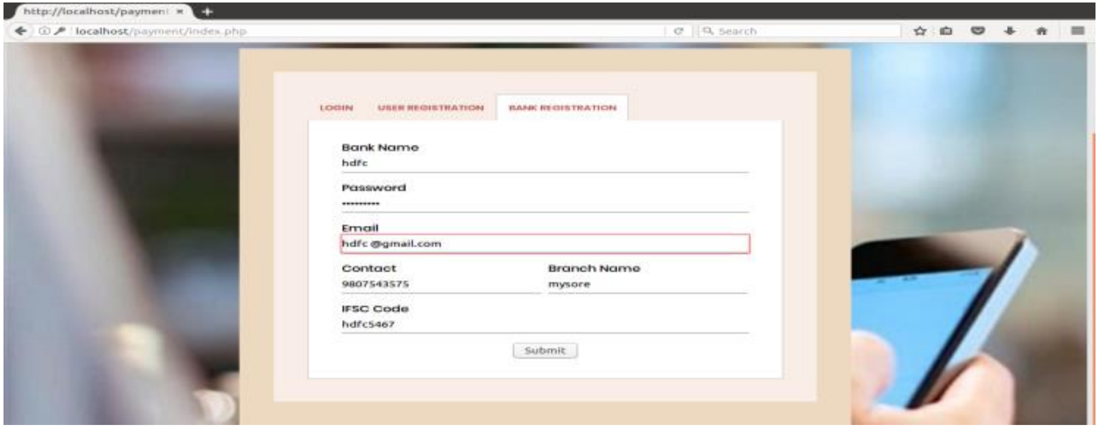
Account No
sbi12345

IFSC Code
sbi5432

Bank Name
SBI

Branch Name
mysore

Fig 1 : User Registration



Bank Name
hdfc

Password
•••••••••

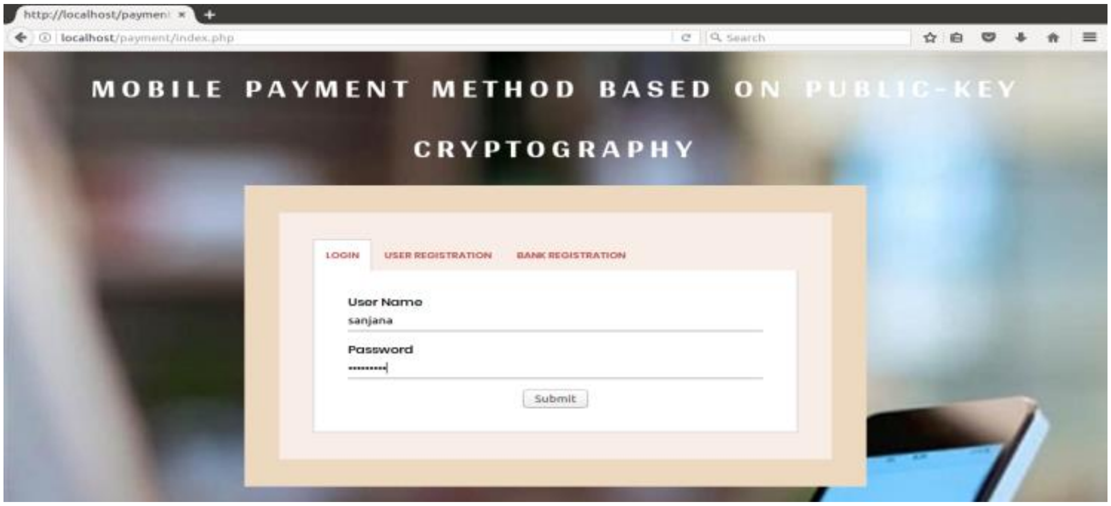
Email
hdfc@gmail.com

Contact
9807543575

Branch Name
mysore

IFSC Code
hdfc5467

Fig 2 : Bank Registration

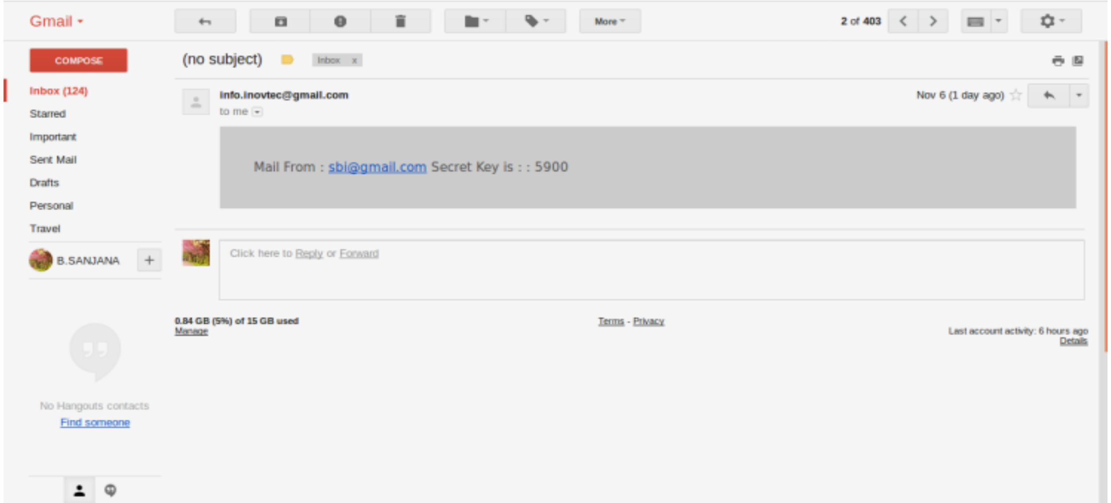


MOBILE PAYMENT METHOD BASED ON PUBLIC-KEY CRYPTOGRAPHY

User Name
sanjana

Password
•••••••••

Fig 3 : User Login



(no subject)

info.inovtec@gmail.com
to me

Nov 6 (1 day ago)

Mail From : sbi@gmail.com Secret Key is : : 5900

Click here to Reply or Forward

0.84 GB (5%) of 15 GB used
Manage

Last account activity: 6 hours ago
Details

Fig 4 : User receive the pin

5 CONCLUSION AND FUTURE WORK

This paper shows the security of the proposed mobile payment depends on RSA public key encryption protocol. This method is more efficient than the other methods. It enables the customer to pay money from the mobile without any effort. A new technology as introduced such as mobile payment services, Since the customer can use mobile for payment easily. This method involve few requirements such as; mobile phone, mobile center, market server and visa center. So, in future we also provide some new features such as avoiding the people from standing in the queue and customer scans the barcode instead of the shopkeeper. This project uses SHA1 algorithm which ensure the safety of the entire process.

ACKNOWLEDGEMENT

We gratefully acknowledge the help & cooperation offered by Dr. Meenakshi sundaram, Professor and Head, Department of Computer Science Engineering, our project coordinator Rummana Firdaus Asst. Professor and our project guide Vishwesh J, Department of computer science and Management of GSSSIETW, Mysuru for providing help and support to carry out the project.

REFERENCES

[1]. M. J. Arnold, K. E. Reynolds, N. Pondere, and J. E. Lueg. "Customer delight in a retail context: investigating delightful and terrible shopping experiences". Journal of BusinessResearch,58(8):11321145.Doi:10.1016/j.jbusres.2004.01.006, 2012.

[2]. E. Hardcastle. "Ericsson launches mobile phone banking services". Thomson Reuters, 2012.

[3]. Ericsson Money. "Ericsson Money Services brings connected mobile money toEurope".Ericsson.com.2014.

[4]. R. Englund, and D.Turesson. "Contactless mobile payments in Europe: Stakeholder' perspective on ecosystem issues and developments". KTH Industrial Engineering and Management. SE-100 44 STOCKHOLM, DIVA, 2012.

[5]. S. Bhawan and J.L. Nehru Marg. "USSD-based Mobile Banking Services for Financial Inclusion". Telecom Regulatory Authority of India. 2013.

[6]. Ericsson, "western Union partner to push mobile financial services". Mobile Payment Today, 2013.

[7]. G. Kamonzo. "Mobile Money Exchange", WordPress.com. The Pilcrow Theme, 2011.

[8]. L. Chaix, and D.TORRE. "FOUR models for mobile payments". University Nice Sophia-Antipolis, JEL Classification: E42, O33, 2011