

Near Field Communication Based Digital Transaction Card

Ravichandran¹, M. Krishnamurthy²

¹Department of Information Technology, AMET University, Chennai

²Department of Information Technology, KCG College of Engineering and Technology, Chennai

Article Info

Article history:

Received Nov 21, 2017

Revised Jan 29, 2018

Accepted Feb 17, 2018

Keywords:

NFC

E-Paper Display

Bluetooth and Digital

Transaction

ABSTRACT

Our paper aim is to design a reprogrammable smart payment card that replaces all other cards in the wallet assembled using an ultra-low power e-paper display, Bluetooth Communication, capacitive touch sensor and NFC. The controllers used in this project based on ARM Cortex-M architecture. The main advantage of this paper is the card will be in constant communication with the smartphone. In case if the connection was lost, after a certain time interval the card interprets it as lost or stolen and will automatically disable itself. The user can re-enable the card only by entering the authentication password on the card and from the smartphone app.

*Copyright © 2018 Institute of Advanced Engineering and Science.
All rights reserved.*

Corresponding Author:

Ravichandran,

Department of Information Technology,

AMET University, Chennai

India

1. INTRODUCTION

Some research and development efforts were being conducted simultaneously to this study in areas of direct relevance to the research. Much of this work falls within the NFC based Intelligent Transaction Systems [1]. Most of the people are taking all the cards. So in this project introduced by digital transaction card based on NFC [2]. The user can add a new card, erase a particular one or even delete all using a smartphone app [3]. The card is enabled with Bluetooth radio to communicate with the smartphone. The smartcard can store up to 30 different cards. The android app allows the user to see the current balance of their bank accounts in their cards [4]. It also allows viewing the history of the transaction. This eliminates the user from logging into different bank apps and maintaining them [5]. The systems and procedures in this study [6] are expected to process payment transactions done more quickly, easily and securely. The data accuracy is expected in implementing loyalty management based on utilising data mining of customer behaviour pattern toward the purchase of products everytime more efficient. In [7], they discussed a new proxy blind multi-signature scheme based on integer factorisation problem (IFP) and discrete logarithm problem (DLP). Digital image encryption has been achieved using hybrid (DES-RSA) cryptographic technique for applications over wireless communication networks. The overall simulation results yield useful information [8]. The technology gives an improved security of the selected images according to Shannon's definition of perfect safety. The method used in [9] would avoid any intrusion like phishing. This system can be evolved using Biometric-Kerberos based Authentication Protocol to provide security in Cloud Computing furthermore.

2. WORKING PRINCIPLE

All in one electronic digital transaction card replacing the present multi-card scenario based on NFC, E-Paper display, Bluetooth and Cap Touch Sense. As shown in Figure 1 & Figure 2 the user has to enter a four-digit secure PIN before switching cards or making changes to the card. Once the authentication

completed, the desired card can be selected by just swiping on the cap touch area and used for payment. If the card is already selected, only entering the secure PIN will unlock the card for payment, ensuring that no other can take the card and use it. Before handling the card to a merchant, the user will be able to lock it with only the last four digits of the card visible using a simple touch on the card. To enable this, the card has a capacitive touch input area that senses both button press as well as swiping gestures. Entering secure PIN and switching cards are thus intuitive and an easy one within a few seconds.

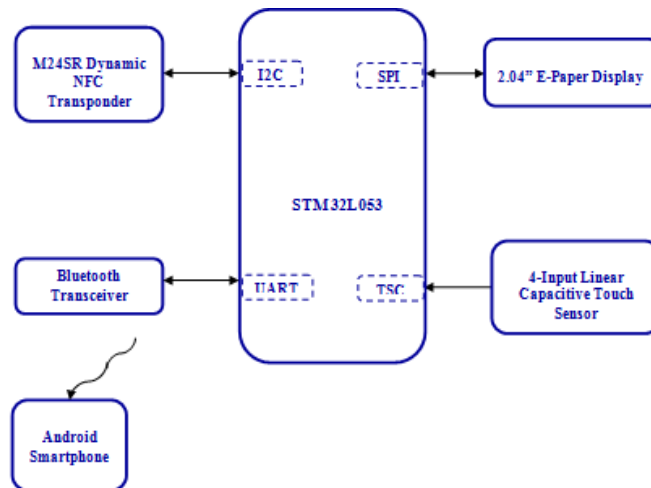


Figure 1. Card Unit

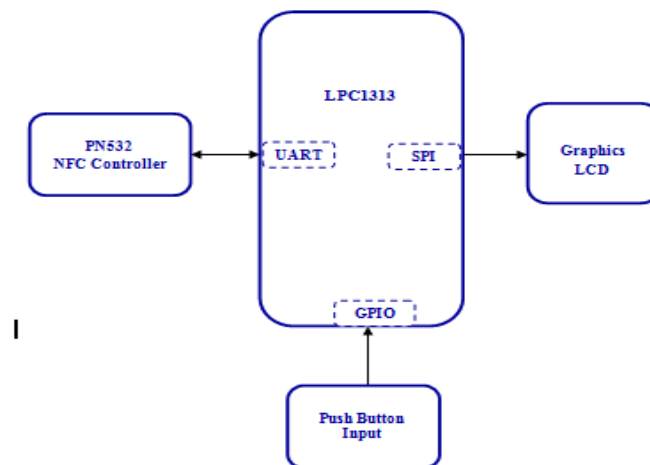


Figure 2. NFC Reader-Writer Unit

3. RESULTS AND DISCUSSION

An E-Paper display embedded on the card will show the details of the currently selected card. E-Paper displays are permanent that needs no power to retain the image on a screen. This helps the card to run on a small battery for several months. The user can add a new card, erase a particular one or even delete all using a smartphone app. The card is enabled with Bluetooth radio to communicate with the smartphone.

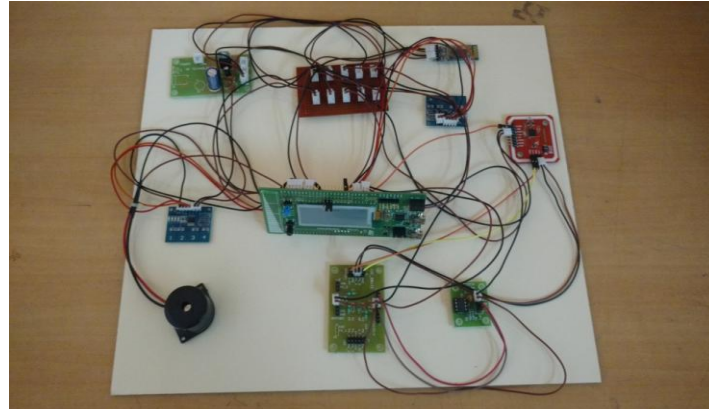


Figure 3. Card Unit



Figure 4. NFC Reader/Writer Unit

The transaction part demo can be carried out using an NFC enabled Android smartphone or using a separately designed NFC reader-writer device as shown in Figure 3 & Figure 4. This device consists of an NFC controller to communicate with the card and a graphics display to show the results.

4. CONCLUSION

In future, this design is implemented by product type card. The proposed system is of two main parts, namely, a map unit, and NFC reader/writer unit. The entire payment process carried over NFC, which is a secure and universal contactless payment technology. A powerful NFC transponder chip is embedded on the card to support this. This chip also acts as the permanent memory area to store the card details. An E-Paper display embedded on the card will show the details of the currently selected card. E-Paper displays are permanent that needs no power to retain the image on screen. This helps the card to run on a small battery for several months.

REFERENCES

- [1] ABI Research, et al., *Near Field Communications (NFC). Simplifying and Expanding. Contactless Commerce, Connectivity, and Content*, 2006.
- [2] J.Park, et al. *Security technologies and applications for convergence environments,* Security and Communication Networks, 2012.
- [3] D. Kastanis, et al. *An efficient authentication scheme for contactless smartcards using elliptic curve cryptography,* Communication, Network, and Information Security, 2006.
- [4] Global Platform, et al. *The Global Platform Proposition for NFC Mobile: Secure Element Management and Messaging*, April 2009.

-
- [5] I. Askoxylakis, et al. *Integration of a secure mobile payment system in a GSM/UMTS SIM smart card*, System, 2007.
- [6] Ferina Ferdianti, Yusuf Triyuswoyo, Dewi Agushinta R. Utilization of Near Field Communication Technology for Loyalty Management, *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, Vol 11, No 3, September 2013, PP. 617-624.
- [7] Swati Verma, Birendra Kumar Sharma, New Proxy Blind Multi Signature based on Integer-Factorization and Discrete-Logarithm Problems, *Bulletin of Electrical Engineering and Informatics (BEEI)*, Vol 1, No 3, September 2012, pp. 185-190.
- [8] Kazeem B. Adedeji, Akinlolu A. Ponnle. Improved Image Encryption for Real-Time Application over Wireless Communication Networks using Hybrid Cryptography Technique, *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, Vol 4, No 4, December 2016, pp. 307-318.
- [9] K.Prabakaran, M.Prabu. Secure and Efficient Data Contribution Using Extended Identity-Based Encryption in Cloud Computing, *International Journal of MC Square Scientific Research (IJMSR)*, Vol 9, No. 1, 2017, pp. 189-194.