Increasing security measures in ATM Transactions using NFC

Trisha Saha[a], MR. K. Senthil Kumar[b]

[a] Department of Computer Science, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India
[b] Associate Professor, Department of Computer Science, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Automated Teller Machine (ATM) is a helpful method to gather the financial necessities of the clients. Notwithstanding, the utilization of charge bank card or different kinds of bank cards during bank ATM exchanges has a few issues like inclined to bank ATM skimming, attractive segments of card getting harmed, assembling and carrying cost of ATM cards, longer an ideal opportunity to validate clients and so forth The target of this examination is to think about smart mobile phone in Near-Field Communication (NFC) Card Emulation approach as an option in contrast to ATM bank cards. In NFC the space between the particular gadgets should be little (regularly under 4 cm) which makes NFC perfect for building expenses and different exchanges including delicate/private information. In the proposed framework, to validate at the ATM booth, the client needs to swipe his/her advanced mobile phone before the NFC per user. An ATM card isn't needed for verification and the framework will in any case have a more grounded protection contrasted with the framework where the ATM card was utilized. Security examination and danger demonstrating appeared in this paper features the security strength of the framework during verification.

Keywords: Secure Authentication, ATM, One Time Password, Near Field Communication, Security Attacks.

I. Introduction

The blend of the world's most famous cell phone, the mobile phone, with the novel remote innovation NFC (Near Field Communication makes a conceivable assortment of business openings. Installment, tagging, access control, content dispersion, shrewd publicizing, shared information/cash move – the potential is boundless. NFC builds up a protected, interoperable working climate for outsider NFC-empowered applications. To accomplish this, the venture assists with characterizing open business and specialized systems for NFC-empowered administrations on cell phones.

A few developments and explorers depend on totally novel thoughts, meaning to broaden the limits of human information. In different cases, existing models, ideas, or advancements are consolidated or utilized in a novel system bringing about new turns of events and developments.

Installment, tagging, access control, and recognizable proof, content conveyance, medical care data the executives, brilliant publicizing, shared information/cash move – the potential is boundless. Cell phones have become the essential foundation of ubiquitous computing. There are currently more than 2 billion mobile phone clients worldwide and a large number of these clients convey these gadgets with or near them. As these gadgets fill in prominence, advances that empower more common collaborations between clients, gadgets, and their surroundings have prodded a rich and lively exploration of the local area. Almost certainly, as opposed to conveying enlarged ordinary articles as proposed by clients will rather convey a solitary gadget that has similar uses as the present regular items.

For instance, rather than a labeled vehicle key, a mobile phone could be approved to open and begin a vehicle. Near field communication (NFC) is an innovation developed from short reach radio frequency identification (RFID). Like RFID, NFC works through attractive field enlistment and is intended for straightforward and safe exchange of information between viable gadgets. Viable reach is restricted to 20 centimeters and information move rates top at 424 kbits/s making it a decent innovation for check/contact co-operations. A portion of the examination work put forward various kinds of monetary apps dependent on NFC. One of the utilizations of NFC innovation is in contactless installment activity. A NFC buy exchange between an NFC cell phone (or an NFC bank card) and an NFC retail location way is performed immediately and inside a little scope of statement (around 10 CM) with no actual contact.

II. Literature Review:

Near Field Communication (NFC) as a type of innovation has seen numerous enhancements lately because of the expanding accessibility of NFC empowered gadgets. It is utilized for little reach communication and dependent on the current guidelines of the Radio frequency identification (RFID) framework. Straightforward and secure bidirectional communication between NFC empowered gadgets is made conceivable by this innovation. In this survey term paper, NFC innovation is advanced concerning its execution, working modes, its application as

labels just as installments, and its guidelines and conventions. NFC app in the field of installments is clarified with the assistance of NFC gadget design. Essential NFC gathering engineering and dangers concerning this innovation are likewise examined. Remote Technology is quickly supplanting the wired innovation. An increase of 128% in the shipment of telephones outfitted with remote innovation rose from 120M to 275 M out of 2013. As per Information Handling Service (IHS), from 2013 through the finish of 2018 shipments could rise 325%. End clients currently expect that a solitary gadget can be utilized to get to an assortment of supplies, for example, contact, amusement, and business. This has gotten gigantic upgrades in the field of contactless innovation; NFC being one of them. NFC has numerous app as well as contactless installments typically alluded to as NFC Transfer Payments. NFC transfer Payments are being acknowledged by retailers in created/non-industrial nations giving a choice, which may demonstrate help to individuals [1]. NFC gives intends to quick proximity contactless ID and correspondence for mobile telephones and exclusive devices the identical. NFC is another technology yet its miles growing brief as its miles being normalized. The foremost NFC administrations have commonly been fundamental programs but with the development of NFC tech and its app zones, there is a dire need to shift from autonomous app to administrator driven assistance formation and conveyance model. In this article we current another NFC access procedure for system ambitious administrations. It is intended to permit network-based help formation and conveyance for administrators and lightweight app for end clients. We additionally show and assess our execution of the planned NFC access procedure. Late years have seen an extension in the utilization of Radio Frequency Identification (RFID) in modern areas assisting with smoothing out strategic cycles specifically. NFC is a side project of RFID with an expectation to take contactless communication for ordinary use. NFC is a radio frequency interface expected for collaborations among labels and electronic gadgets in closeness. Notwithstanding its basic role of utilization, for example, contactless identification, NFC additionally empowers installment and tagging applications and information trade. The most unmistakable objective gadget to go about as an NFC peruser is by all accounts a cell phone, albeit presently NFC is likewise spread out different sorts of electronic apparatuses and utilizations, for example, programmed matching and arrangement of PC and others. NFC is a radio message innovation working in the open 13.56 MHz freq band with 106-424 kbps information move speeds. The inactive labels are fueled by the methods for inductive pairing in the perusing cycle in the interest of the starting peruser gadget. The communication space is directed by the range of the peruser radio wire and it is by and by in the scope of a few CM. Regular NFC service is an independent apps on cell phones. These apps typically read Radio RFID labels and are identified with everyday life issues, for example, medical care services. When contacting a tag with a per-user, the NFC gadget peruses the information put away on the tag and starts the proper activity after the client's affirmation. Typically the information is shipped off a foundation framework for additional preparation. NFC app can, for instance, open a Web page, call a most loved number, or send an SMS. Little things, for example, Web connections can likewise be shared by contacting another NFC gadget. NFC services can likewise be utilized to peruse business cards in sequence and save this information to cell phone contact data set. NFC-based services are quickly extending in various territories, albeit business services are yet rare. Practically all until now and proposed NFC services are intensely terminus ward. These terminus-driven NFC services are huge applications that crowd a great deal of terminus resources and posture exacting prerequisites to running climate. Regularly these applications are made with portable Java (J2ME) which may cause gradualness and unwavering quality issues. One significant issue for terminal-driven NFC services is the service conveyance measure. Application should be downloaded and introduced on each telephone before the service can be utilized unexpectedly. This can be a repetitive cycle and it may even dismiss expected clients from the administrator's perspective. This is the reason another organization-driven service model is required for NFC applications [2]. NFC is an arising remote short-range communication innovation development that depends on existing principles of the Radio Frequency Identi cation (RFID) framework. In this paper, we give an outline of NFC innovation and examine its variation around the world. We at that point center around the latest things and utilization of NFC innovation in India. Both existing NFC applications and some possible future circumstances are dissected in this association. Besides, security concerns, troubles, and present clashes are likewise talked about. After the improvement of RFID advancement, detecting applications using RFID before long dominated. Sensors were given the adaptability to discuss remotely, with low or zero effect on force utilization. Notwithstanding, when the information created by these sensors needed to be handled, a PC was required, which implied that a connection was fundamental between a PC and the sensor. Generally, a particular RFID per-user would be utilized to assemble information from the detecting component, after which the per-user would be genuinely or remotely associated with a PC. These strategies are anyway getting dynamically obsolete and quicker; a more flexible system is required in various applications [3]. As NFC is familiarizing, its protection vulnus and security techniques had been broadly addressed. These paper units up an NFC protection model based on the OSI model. Security chance and countermeasure of every layer of the safety version are defined as the base of the previous works. Valuation methods are planned to assess the safety model, then the consequences show an excessive safety stage. And the NFC safety model can be perfected usually with the improvement of the NFC technology [4]. The communication needs of cell phones and their portable clients have developed as a result of the multiplication of

such communication and shopper gadgets. To make the foundation of these associations less difficult, the Near Field Communication (NFC) innovation was made; in any case, concerning confirmation, the difficulty to tackle difference of security and convenience restricts the prospects - and this additionally remains valid for cell phones. The applications introduced in this paper serve the consistently more grounded market need to proliferate the - most buyer - hardware gadgets and the substance services dependent on them for shoppers and suppliers also. The utilization cases introduced here are consequences of the MOBILISE project [5].

III. NFC Security:

1. Threats

NFC banking applications provide high-level security in contactless cash transactions. NFC programs together with contactless coins charge demand a high degree of protection. In NFC possible problems are explained below.

2. Eavesdropping

Eavesdropping is called a sniffing or snooping attack. In this attack, if the user can try to access the bank in a secured network, hackers can hack the data from an unsecured network in sending or receiving the data. Here bank user can lose their passwords and their cash transactions also.

3. Data Corruption and Manipulation

Data corruption means in the IT field read and writing process it not properly happened this one called as data corruption. In NFC reading and writing are happened by the system with encrypted format and its correctness also high. And data manipulations are adjusted the data incorrect manner in data reading time.

4. Man- in- the Middle attack

Man in the middle attack is a type of eavesdropping attack. In a time of transactions like sending or receiving data in middle, any hackers trying to access the bank user data in middle is called Man in middle. These kinds of attacks are happening on normal bank transactions.

5. NFC Worm

NFC trojan horse assault is determined in NFC-enabled telephones. In this, the PushRegistry can be abused to intercept all URI NDEF messages. It is carried out by the usage of the standardized NFC Java API. Push Registry allows the programs to sign up themselves for coping with a few particular information like snapshots

IV. Proposed System:

A database and a bank server are included in the project's proposed system architecture. The user taps their NFC-based ATM card on the ATM system, the system decrypts the details, and the user enters their PIN generated on their phone using the PIN generation android app.

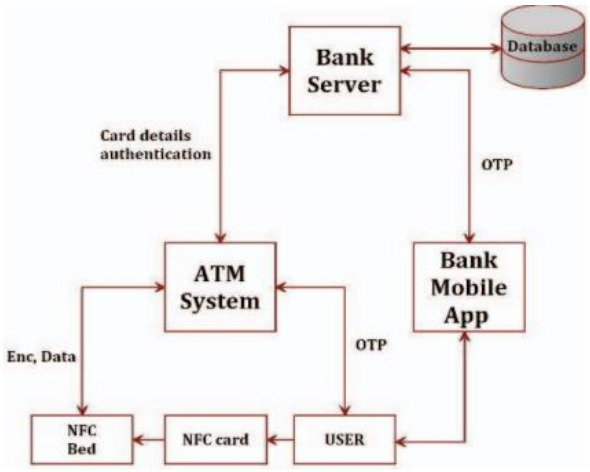


Fig 1 : System Architecture

The data is sent from the ATM to the bank server for authentication, where it is linked to the data stored in the database. The customer is logging in and can proceed with a transaction if the data is found to be authentic.

NFC is a popular technology (Near field communication). For example, this whole scheme would only function if the registered user's phone is within range. This prevents someone other than the authorized customer from completing an ATM transaction.

The system's main goal is to include safe ATM card use, including protection against skimming devices, shoulder surfing, and fake keyboards, as well as cost-effectiveness through the use of novel and increasingly popular hardware, while still proving to be user friendly. It gives us a blueprint for reducing the number of cybercriminals in ATM transactions.

V. Methodology

1. NFC Writing

NFC expands the capabilities of RFID devices by allowing two-way communication between endpoints, whereas previous systems such as contactless smart cards only permitted one-way communication. It can replace previous one-way applications because unpowered NFC "tags" can be read by NFC devices.

2. NFC Reading

When a customer taps their card into an ATM, the xor data is translated to original data before reading NDEF data from an NFC tag with the English language convention and sending the original data to the server. Data is dumped into the tag, but before it is dumped into the card, an Intent Filter is declared to notify the device that it is allowed to operate with NFC. When NFC is detected, Android can call a process. Make a method for constructing an NDEF message. Create an NDEF (NFC Data Exchange Format) message composing method.

3. MVC architecture

Model View Controller, or MVC as it is more commonly known, is a software design pattern for creating web applications.

Model - The lowest level of the pattern which is responsible for maintaining data.

View - This is responsible for displaying all or a portion of the data to the user.

Controller - Software Code that controls the interactions between the Model and View.

MVC is popular because it distinguishes between the application logic and the user interface layer, allowing for separation of concerns. The Controller receives all application requests before collaborating with the Model to prepare any additional information that the View needs. The View then uses the data prepared by the Controller to create a final presentable answer.

VI. Implementation And Results

WEB APPLICATION

Home Page of Web Application

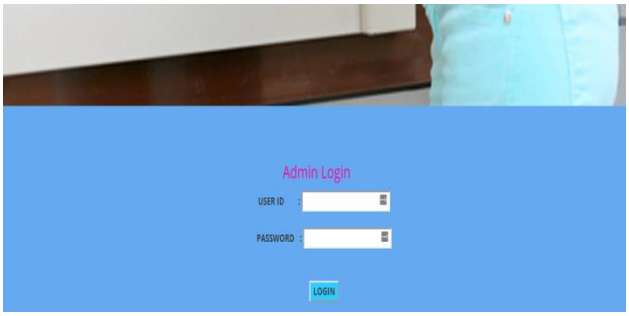
This page serves as a portal to two related sections of our proposed web system.

1. Admin Login section

2. User Login section

1. Admin Login section

Admin page of the web application. Admin can log in using his/her login credentials.

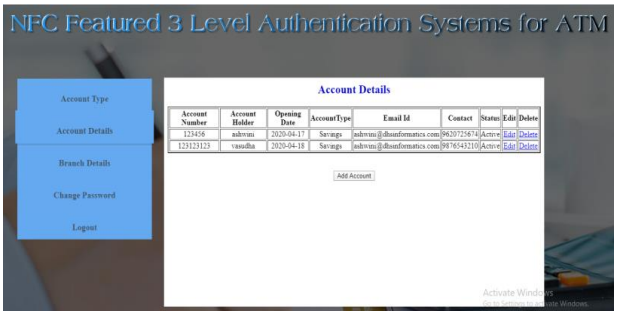


Admin Home Page

This section is for bank workers with admin access who are responsible for establishing new accounts for customers.

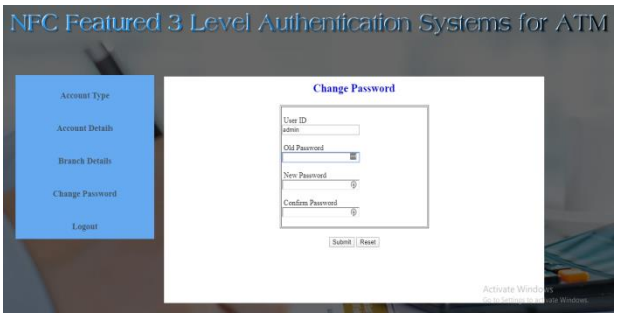
Account details

This section is to register the user details by admin and while registering it sends user information to the user's mail id (account number and password).



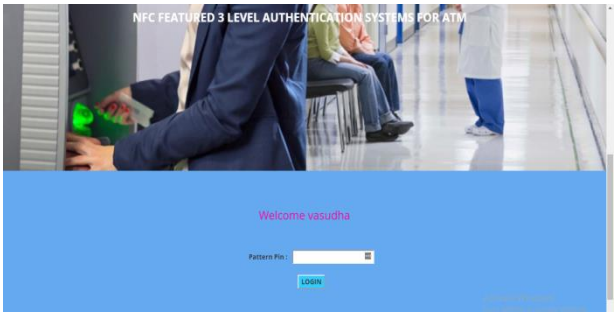
Admin Change Password

Admin can change his/her password.



2. User Login section

The user will be taken to the user login page after tapping his or her NFC card on the ATM. The user must first enter the Dash Matrix Pin to gain access. The user will then perform transactions, check their balance, and see their mini statement.

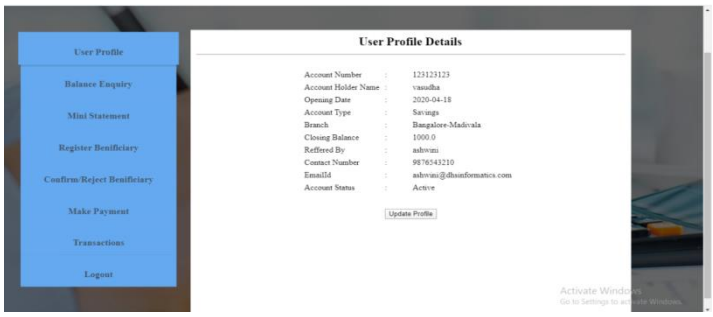


User Home Page:

Once a user enters the proper Dash matrix pin he/she can be redirected to the home page.

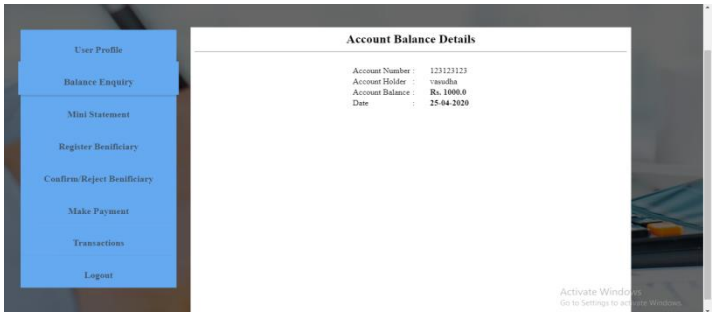
User Profile:

User can see their profile.



Balance Enquiry:

In this section, the user can check his/her balance.

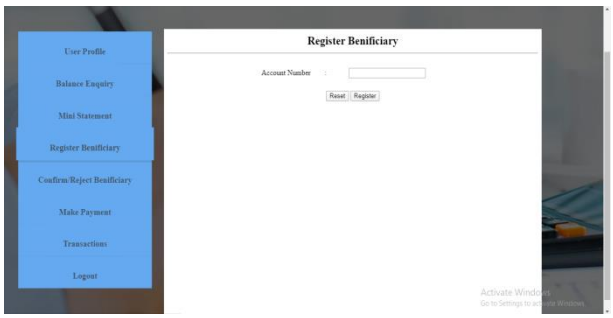


Mini Statement Details:

Users can see the details about balance and statement Date.

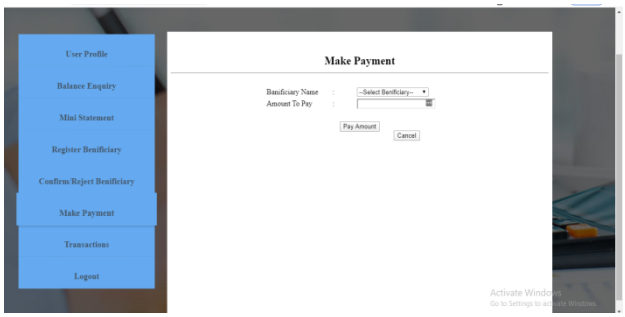
Register Beneficiary

The function of introducing a beneficiary is achieved by submitting a verification mail that includes an authentication URN number.



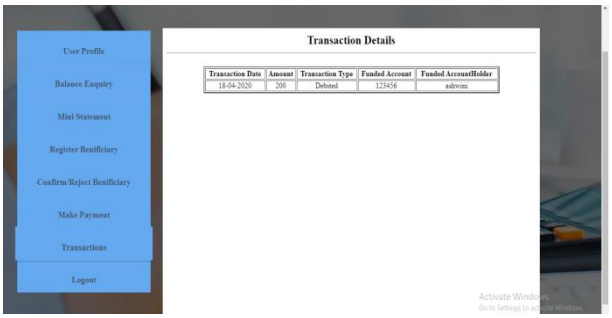
Make Payment

In this section, the user can perform a transaction.



Transaction Details:

In this section, the user can see the transaction history.

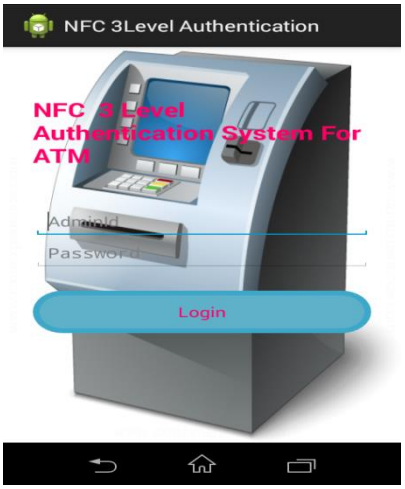


Android Application

Admin:

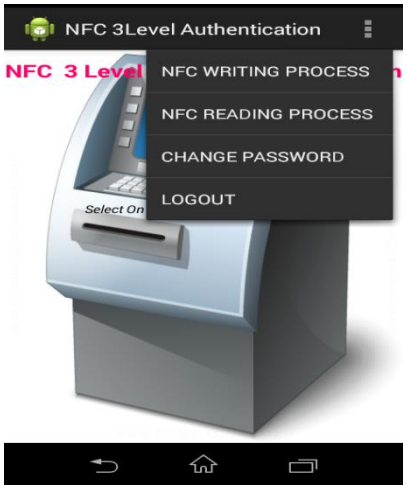
Admin login:

The administrator account is verified by a layer of admin login provided by the admin application.



Admin Home Page

Once the admin enters a proper username and password admin can be redirected to the home page.



Write Account Details:

It enables the banking authority to read and write NFC cards for on-the-go use by customers. Before being written to the card, the information is encrypted. In the prototype, the data is encrypted using the XOR operation.

ATM

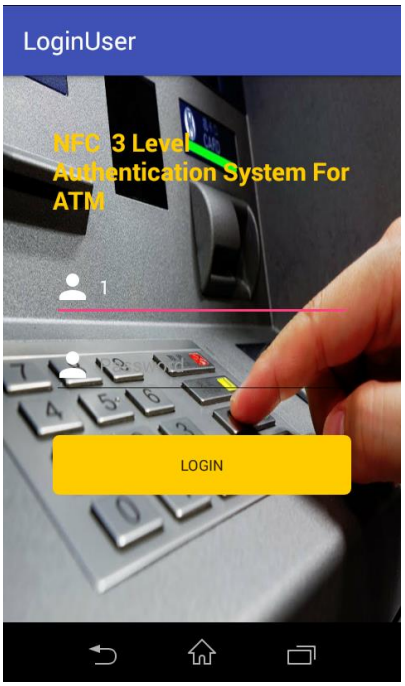
The ATM program serves as a connection between the bank and its clients. Users should use an ATM to make transactions further flexible and available on the go. Since the smartphone has an inbuilt NFC card reader, the prototype uses an android application.

Verification

The user is then instructed to tap his or her NFC card. A prompt message is created after the NFC card has been successfully read. The web application immediately greets the customer after the NFC card swipe is verified.

User:

All of the bank's customers have access to the user application. It is the user's responsibility to create a dynamic dot matrix pin during every bank transaction. To enter the pattern generation page, the user must first have login credentials such as username and password, after which he can create a specific pin pattern using the dot matrix algorithm.



Draw Pattern:

Each dot is denoted by a number in the dot matrix algorithm, and a randomly connected pattern produces a unique pin each time the user needs to make a transaction.

VII. Conclusion And Future Work:

The three major issues concerning ATM security are:

1. Data Theft using scanners
2. Fake Keypads
3. Shoulder surfing.

The risk estimates were very high before the beginning of the project. The main aim of this project was to use risk estimates pre and post-mitigation to reduce those risk factors before and after implementation. All of the key factors relating to ATM larceny have been greatly minimized with the aid of the proposed prototype. This new proposal is put forward to diminish the concept of PIN as a password for the process in an ATM system. As long as password attacks such as peeping attacks, brute-force attacks, retrieving passwords from systems, and skimmers exist in the future, this new technique can be used to prevent them. It is easy to open a website using NFC without wasting time browsing. Via the use of three-tier authentication schemes. We're putting together a safe framework.

References

[1] Young-Gon Kim and Moon-Seog Jun, "A design of User Authentication system using QR code identifying method", 6th International Conference on Computer Science and Convergence, Information Technology, IEEE Transactions, pp. 31-35, Nov-Dec 2011.

[2] Blake Ross, C. Jakson, N. Miyake, D. Boneh, and J.C. Mitchell, “Stronger password authentication using browser extensions,” in SSYM’05: Proc. 14th Conf. USENIX Security Symp., Berkeley, CA, pp. 2-2, USENIX Association,2005.

[3] Zhengming Li, Lijie Xue and Fei Tan, “Face detection in complex background based on skin color features and improved AdaBoost Algorithm” Progress in Informatics and Computing (PIC), 2010 IEEE International Conference, Vol . 2 , pp. 723-727, Dec. 2010.

[4] Chris Karlof, U. Shankar, J. D. Tygar and D. Wagner, “Dynamic pharming attacks and locked sameorigin policies for web browsers” in CCS’07:proc. 14th ACM Conf. Computer Communications Security, New York, 2007, pp. 58-71, ACM.

[5] Min Wu, S. Garfinkel and R. Miller, “Secure Web authentication with mobile phones” in DIMACS Workshop usable Privacy Security Software, Citeseer, 2004. N.

[6] Provos, D. Mcnamee, P. Mavrommatis, K. Wang and N. Modadugu, “ The ghost in the browser: Analysis of Web based Malware” Proc. 1st Conf. Workshop Hot Topics in Understanding Botnets, Berkeley, CA, 2007.

[7] Alimi, V. and Pasquet, M. (2009), 'Post-Distribution Provisioning and Personalization of a Payment Application on a UICC-Based Secure Element,' Proceedings of the International Conference on Availability, Reliability and Security, ISBN: 978-0-7695-3564-7, 16-19 March 2009, Fukuoka, Japan, 701-705.