Pay-Cloak: A Biometric Back Cover for Smartphone with Tokenization Principle for Cashless Payment

By Alak Majumder, Joyeeta Goswami, Shirsha Ghosh, Rishu Shrivastawa, Saraju P. Mohanty, and Bidyut K. Bhattacharyya

Continuous progress in technologies and quality of life, has made a strong impression on the development on payment techniques. After the evolution of NFC technology, contactless payment has recently got a huge attention because of its short range conducive nature. Again, as mobile computing took a great leap due to enormous development of smartphone platform, companies like Google, Samsung & Apple has embedded NFC in smartphone to provide 'On the Go' payment eliminating the need of payment cards. But due to interoperability and high cost, the technologies are not available to the common people. So, there is a hunt for a technology, which will provide the best features of the contactless payment with reliable security and low cost. This article presents a prototype of hardware module called "Pay-Cloak" which could be used as back cover of NFC enabled smartphone. The module communicates with an Android Application installed in the smartphone via Bluetooth after verifying through a capacitive fingerprint Sensor. The Application serves as both 'Merchant POS payments using Quick Response (QR) Code' and 'P2P payment using NFC'. The security of the transaction is also enhanced using Tokenization technique. The App also serves the ID virtualization purpose.

I. Electronic Payments: A User Centered Perspective

ONE of the oldest relationship that exists from the evolution of the earth is between the Payer and Payee. The concept of exchanging goods came into picture with the need basic commodities in daily life. Soon it turned to the concept of payment that provides high priced goods such as precious metals, gems etc. With the steady development of technologies and human needs, the payment methods changed enormously. With the progress of the society and technology, people changed the means of payment, in particular with the emergence of smart cities [1]. From business point of view, payment systems can be classified on various types of e-commerce as depicted in **Fig. 1**. Business-to-Business (B2B) model of e-commerce offers a form of organization where the companies depends on suppliers and distribution of product to respond more effectively to the continuous changing market and consumer demand to achieve an efficient operation. This allows the possibility to work more closely with the manufacturer, which provides a freedom of customization and much more control on business activities. Business-to-Customers (B2C) model offers customers to have an influence on manufacturing and customization of products. It provides consumer convenient shopping methods of products, electronic banking, information and services and personal finance management. Customer-to-Customer (C2C) e-commerce does not belong to B2C model and mainly deals with the matters like personal auctions payments and debt settlement [3].

Again, on the basis of form of money representation and modes of money transfer existing payment systems may be classified into two groups: Electronic Cash mechanism and Account Based system as displayed in **Fig. 2** [3]. Electronic cash is something like a mirrored image of conventional cash. When users exchange electronic tokens that represent value just as banknotes and coins, it determine a nominal value of conventional cash money. The fundamental of account based system is that exchange or transfer of money between accounts are basically maintained by payment service provider. Users can authorize charges against their Electronic Payment System (EPS) accounts as they may go with usual bank accounts, though process of authorization may be different for various systems. Debit Card, Credit and content based EPS are under this category. In the past issue, we discussed a new system called "Swing-Pay" as a method of contactless payment using biometric authentication [2]. The current article presents "Pay-Cloak", a system that additionally uses tokenization principle and Bluetooth and can be used as a back cover of NFC Enabled Smartphone. Due to tremendous development in smartphone industry along with the Mobile Computing, presently smartphones are capable to work like a portable computer. So researchers are developing smartphone based system to handle payment related needs. In the Swing-Pay article, we introduced a method and a device which can handle all types of payment related needs independently. But those who carry a NFC enabled smartphone, can make the transaction using their smartphone only. They do not need to carry a separate device with them. The smartphone can process payments alone, using Pay-Cloak, the system becomes more secure. Pay-Cloak uses fingerprint authentication and Tokenization scheme to make the

transaction process more secure. “Swing-Pay” and “Pay-Cloak” both have the same functioning and process. The key difference is that *“Swing-pay” is a novel separate module that can handle all payment and identity needs, whereas Pay-Cloak can be attached with existing NFC enabled smartphones* to process the transactions and identity virtualization.

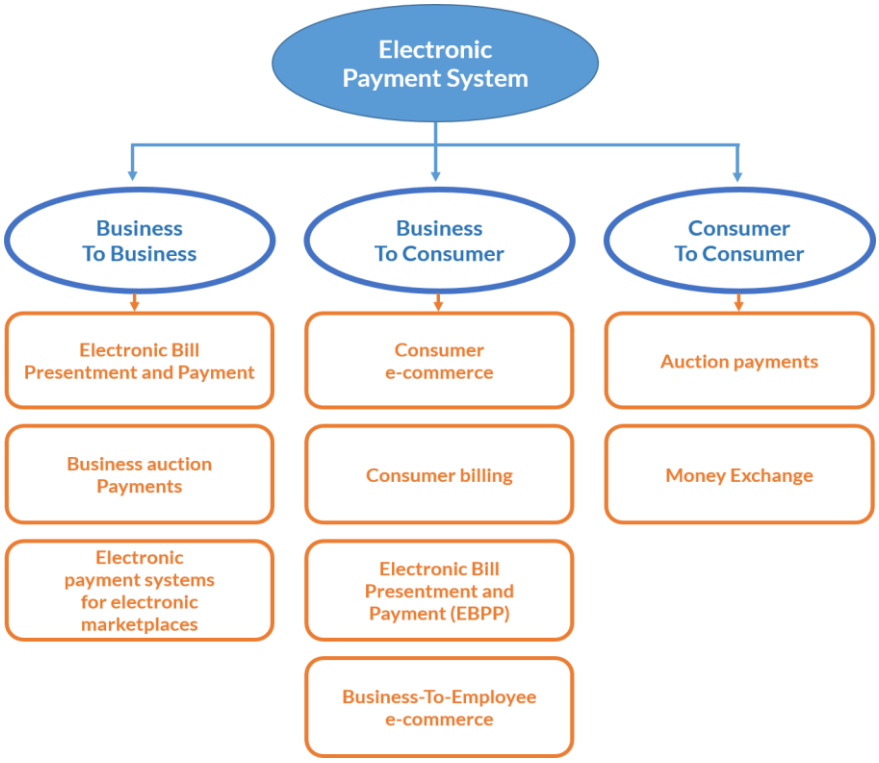


Fig. 1: Electronic Payments for Different e-Commerce [3].

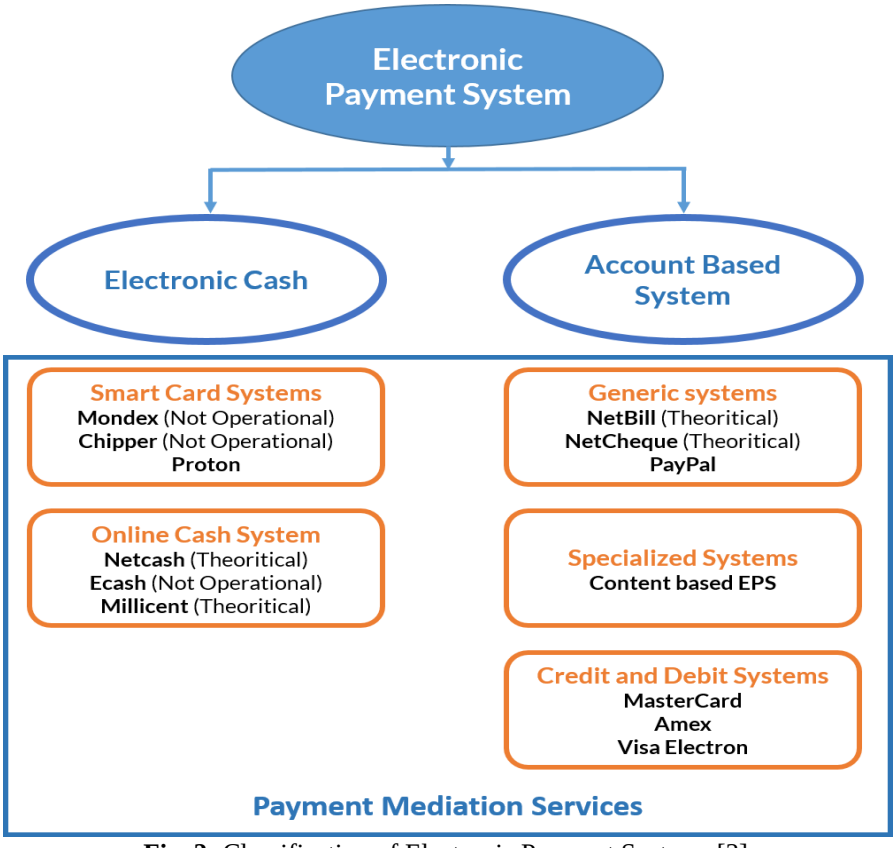


Fig. 2: Classification of Electronic Payment Systems [3].

In the year 1983, when C. Walton patented his revolutionary RFID technique [4] for short range communication, a new form of payment, which is known as Contactless Payment, came in to existence. The first contactless payment was implemented in 1995 in Seoul Bus transport followed by Speed-pass in 1997 to pay fuel charges in US gas stations [5]. In 2003 ISO/IEC approved NFC technology, which is considered as a successor of RFID [6]. Since then, it has attained a huge popularity in contactless payment technologies. NFC has two different modules: tag and reader. The reader acts as the active part, whereas the tags may be active or passive. If the tags are active, they always powered by an external power source and if they are passive then gets energy from the reader tag within the range [7]. So, the antenna coil inside the reader produces a magnetic field around it which always exhibits an EMF. When this reader comes close to any NFC passive tag or if any passive tag enters within the magnetic field of reader antenna, the tag get energized by the RF waves propagating from the reader antenna. After verification of the tag present in the range, the reader couples with the tag and originates a small amount of AC current. The tag converts this AC current into DC to send a RF signal back to the reader and in this manner the data transmission is established between the NFC tag and reader. This data transmission is standardized in ISO/IEC 18092 which is compatible with smart card standard ISO 14443 [7]. It has a significant advantage over RFID, due to its Peer-to-Peer communication feature, by which two active devices can communicate between each other. Due to its property of communicating within very small range, NFC reduces the risk of Eavesdropping and Man in Middle attack, which makes it ideal for payment related applications [8]. Unlike RFID, NFC provides better security, using a module embedded called the Secure Element. In 2007, Barclay Card first implemented NFC based credit cards in UK [9]. As NFC technology is currently embedded in Smartphone, the users can use their phone for money transaction, instead of using a traditional payment cards.

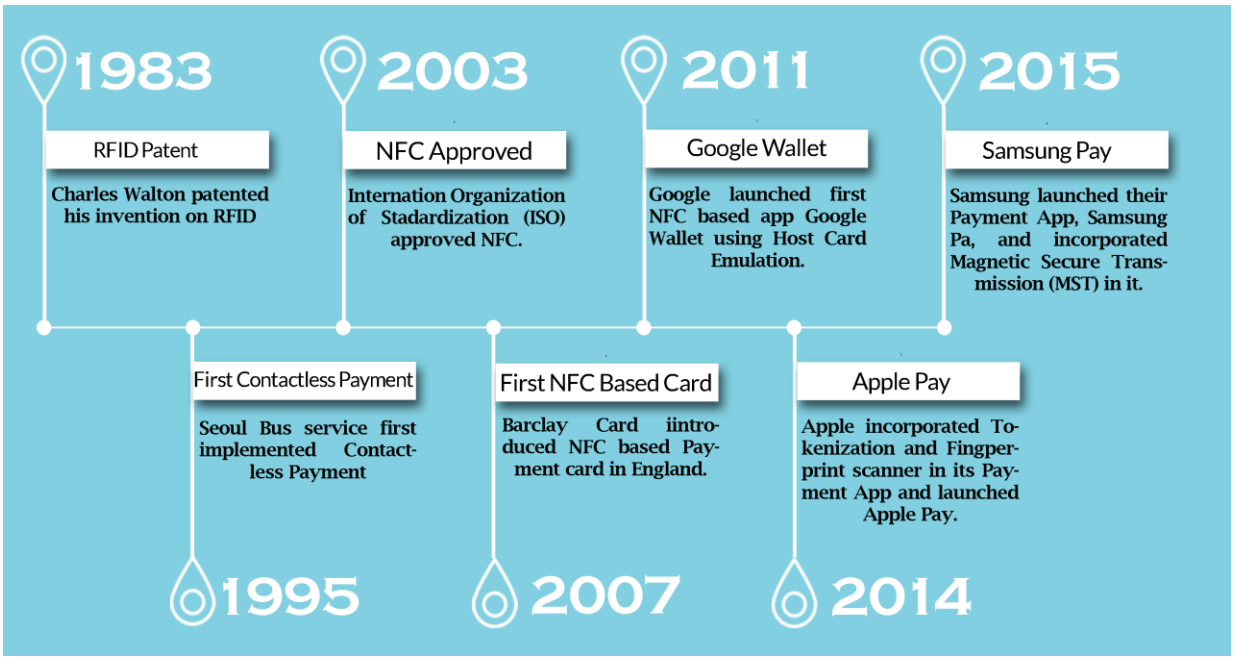


Fig. 3: Chronology of Mobile Application Based Payment System Development: From RFID to Samsung Pay.

Due to a huge development in Mobile Operating systems and Mobile Computing, there is a constant trend to use smartphone based apps and facilities. This trend is also seen payment industry with the development of several mobile wallets and mobile banking features. It is found in [10] that, 50% people is handling phones but only 37% possess a bank account. In 2011, Google introduced NFC antenna on their Nexus-S smartphone [11]. NFC allows the communication between two active devices using Peer-to-Peer mode. Google launched their first Mobile Wallet Application, known as the Google Wallet [12]. It uses the Host Card Emulation feature of NFC and no transmit credit card information in a Contactless Point-of-Sale (POS) terminal. Soon after that, companies like PayPal came up with their mobile payment wallets [13]. Recently in 2014, Apple has brought a mobile payment feature known as Apple Pay [14]. This wallet does not only uses fingerprint authentication but also uses Tokenization to secure sensitive data like credit card information etc. Samsung also followed the same path and launched Samsung pay in 2015, which also uses a technology known as Magnetic Secure Transmission [15]. The timeline of mobile app based payment system development is depicted in **Fig. 3**.

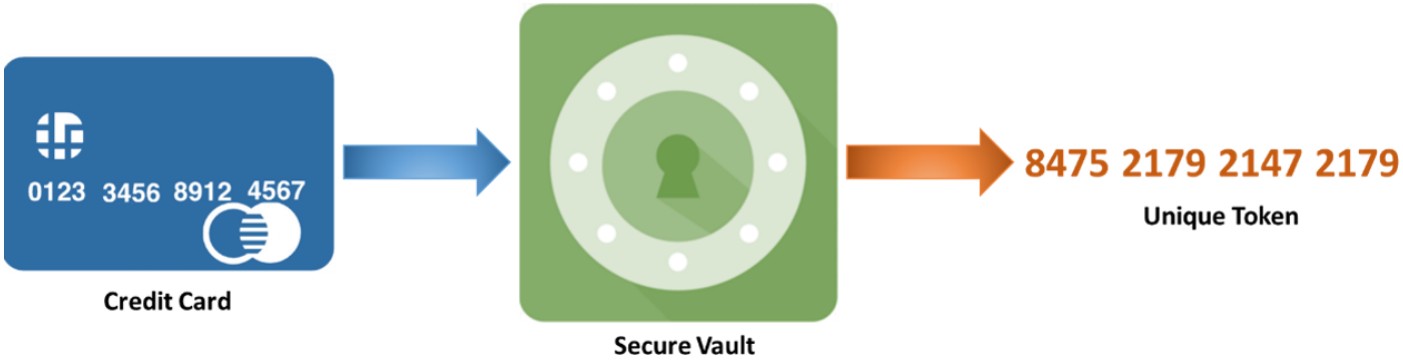


Fig. 4: Tokenization Concept.

Tokenization is a system in which information like credit card number, CVV, expiry date etc. are replaced with a unique token which are randomly generated. These tokens are formatted with proper cryptography concepts to ensure data security. The card information are provided to a highly secure server, mostly known as "Vault" as shown in **Fig. 4**. The Vault then saves the card information to generate a unique token and returns it to the merchant payment environment for further process. The Token is then used as a dependable substitute of credit card information [16].

Tokenization is important because it majorly cuts down the merchant's risk for data breach because the system gets rid of sensitive card information from a merchant's environment [17]. Another payment technique has evolved using the QR Codes, where anyone with a smartphone can actually scans the QR code in the retailer outlets and pays instantly with the mobile [18]. PayPal is now incorporating the QR code feature and made purchases much easier on the internet [19]. Starbucks are also accepting QR code based payments, where the merchant scans the QR code generated by the buyer's mobile app [20]. Zapper is another payment company focused on the restaurant business. In their method, the buyers scans the merchant QR code in the Zapper wallet app and pays instantly [21]. In this paper, we have developed a prototype which could be considered as the back canvas of a smartphone incorporating fingerprint scanner. The hardware prototype is connected to the android application installed in the smartphone via Bluetooth. The purpose of our proposed model is in three folds. The application can be used as POS terminal at Merchant incorporating QR code and Peer-to-peer money using NFC. It can also be used to serve as Identity card virtualization of Voter ID card, Passport and driving license etc.

The organization of the paper is as follows: Section II deals with the related work on app based payment system. Section III describes the proposed methodology for its application as payment and ID virtualization. The prototype development is presented in section IV. Section V highlights the future possible application of the proposed model. And, section VI concludes the work.

II. Survey of The State-of-the-art

In the recent years, with the adaption of POS payments, Contactless payments, and Cloud based payments, the growth of digital money transfer is increasing exponentially. The digital payments are becoming more secure with the invention of technologies like biometric security, 3D secure algorithm, Tokenization etc. In all cases, the customers opted for a solution that is secure and convenient. Big IT industry are continuously trying to be a market leader in the digital payment domain, by embedding more features in their flagship smartphones. People are also slowly adapting them [22]. Around 20% of the users that uses iPhone, have tried Apple Pay in their daily life [23]. Though some of the countries are still far behind, they are gradually adapting digital payment means as services like, Mobile Wallets, Electronic Fund transfer etc [24].

In the year 2011, the concept of QR code based payment system has been proposed. In this system the information hidden in any unique code such as QR code can be retrieved. This model was provided for mobile devices, so that the consumers can make payment with their smartphone by scanning the QR code. The image of the QR code is captured on the mobile device and processed to gather the product information (price, merchant, description). The user then selects the product and purchase, after which the product and payment information is transmitted from the device to a payment provider which process the payment to the proper recipient [25]. J. Lee et al. devised a system by which the POS based payment can be processed using QR code [26]. In this work, the buyer scans the QR code generated by the merchant and it forwards the digital signature and the transaction information to the payment gateway. The process is secured by SSL/TLS technology. Upon successful completion of the process, the Payment Gateway acknowledges the merchant [27].

In 2014, a Tokenization based payment system schemes was proposed. In this module, a token has been used in

application layer in place of using the card holder's actual payment account information (card holder's name, card account number etc.). Here, critical information about the user's account is captured and stored in a tokenization prior and a useless string, called the token, has been generated against the stored information. This token is just a pointer of the actual information from which it is impossible to gather any information about the actual account [27]. In the US Patent [28], the inventors have come up with credit card tokenization schemes. The credit card numbers are stored in a central database and a unique Token is generated against that. According to Payment Card Industry Data Security Standard (PCI-DSS), the generated token should be of same length of the Card number and should have some similarity with the actual card number. The token is also allotted some amount of time, between which the transaction have to be completed. In 2016, an Indian Patent [29] is filed on a digital card serving payment and identity needs. The invention further deals with an electronic process of NFC based communication and biometric security eliminating the need of high cost NFC based smartphone. Using the inbuilt Magnetic Strip, the card can also work as a traditional ATM card. But the advantage of this card is, as the card cannot be turned on without scanning the finger of the user, it provides more security than the traditional ATM cards.

Fig. 5: Different Researches in App Based Payment Systems.

Seamless launched a QR code based mobile payment called SEQR. This system defines some quick response codes through which one can directly pay for their purchases using their mobile phones. This means, when a customer scans a QR code at the cash register, an authorization is given to the retailer to draw the amount from their bank or payment account, for which the customers do not need to pay the fees charged by the financial institutions. But, in case of the retailers using the SEQR, the cash registers having cashier integration as well as a unique code with the Seamless ER 360° platform, allows them to directly send the total amount of the transaction to the customer's handset for authorization, and the authorized sum will automatically be withdrawn directly from the customer's account [30]. In [31], they proposed a mobile wallet based on QR code and also increased the security of the system using Public Key and Private Key technique. A peer-to-peer based application is presented in

[32], which defines the usage of NFC and Bluetooth technologies for money transaction between mobile devices. In [33], another application of secure peer-to-peer based NFC micro-payment system is devised for Android mobile phones. It defines mobile-to-POS micro-payment services with the required hardware. Also, a cloud computing based NFC payment management system is available in which the payment process trough NFC can be controlled by using cloud computing.

Another most widely used wireless technology is the Bluetooth technology. A peer-to-peer m-payment system, known as P2P-Paid was proposed to define a wireless payment system for mobile users over the Bluetooth communications and allows related secured transactions with the server [34]. Another payment system incorporating a NFC and Bluetooth bridge was described in [35], where Bluetooth enabled mobile devices communicates with NFC enabled consumer services. This system consists of NFC-Bluetooth Bridge and software driver program. The NFC-Bluetooth Bridge is the electronic device having two air interfaces: Bluetooth air interface establishes a wireless connectivity with Bluetooth devices and the NFC air interface establishes the wireless connectivity with NFC devices. The driver is a little software program that drives the communication between NFC devices and the Bluetooth. A taxonomy based representation on different researches is shown in **Fig. 5**.

Based on these above contactless technologies the industries have turned the way of payment through only the mobile phones using various mobile android applications. Some of the latest popular apps are:

A. Google Wallet

This is a payment app launched by Google, first in the year 2011 in US. It works in the peer-to-peer mode of NFC. This allows the user to pay online by storing debit and credit cards, to use in store gifts cards and can be used with a desktop also. This app can be used through Gmail or Google wallet physical card also. To use this app, the user needs to open an a/c in Google wallet by linking their debit or credit cards with their mobile numbers. The physical Google Wallet card can be used as a normal payment cards in ATM or in POS terminals. This app does not have any accession charge. From the point of security Google makes this app secure by storing the data of the user on a secure server. Also when the user use this app they need a 4 digit PIN to access their Google Wallet. At present in the year 2015 Google has launched ‘Android Pay’ based on this Google Wallet [12].

B. Apple Pay

As the name suggests, it is the mobile payment system of Apple Inc., using NFC technology and is launched in the year 2014 with the iPhone 6 mobile [36]. It defines that all the Apple devices which have the NFC enabling capability such as: iPad Air 2, iPad Pro, iPad Mini 3, Apple watch, iPhone 6, 6 Plus etc. can be used for payment purposes. To use this app it is not necessary to have any Apple Pay- specific contactless payment terminals, rather it can be used with any contactless terminals. In this app, the service secures the payment information of customer by creating dynamic security codes for each transaction. With the POS payment, the user have toauthenticate their fingerprint on the Apple devices. Apple disclosed that in the first three days of launching this Apple Pay app, more than 1 million credit cards have been registered, which shows the intention of people around the glove looking forward to cashless payment.

C. PayPal

It’s a worldwide payment system launched by PayPal Holdings Inc. in the year 1999. It is the electronic money transfer method replacing cheques and money orders. In 2015, PayPal launched “PayPal.Me” payment platform using peer-to-peer mode which permits the customer to send a unique link for requesting funds via several messaging methods [37]. For security purposes, PayPal uses security key system to access the account by the user. This is like our traditional OTP system, which means when the user tries to login by giving Login ID and password then a 6 digit code is provided to user in their mobile phones and the user needs to enter that code into the login screen.

D. Samsung Pay

It is the online payment enabling the mobile payments using Samsung devices (Galaxy Note 5, Galaxy S6 Edge plus, Galaxy S6 Edge and Galaxy S6). It is first launched in South Korea and US in the year 2015. This app can be used by Samsung’s NFC enabled mobiles and POS terminals also using the patented Magnetic Secure Transmission (MST) technology [38]. In matters of security it is as same as Google Wallet and Apple Pay.

Apart from these large payment apps, several more apps are there which is used by people such as Loop-pay (now owned by Samsung), Tilt, Square cash, Venmo, Dwolla, Tab, Level Up, Block-chain etc. [39].**Fig. 6** displays a bar chart showing the user acceptance rate of major payment apps in the world.

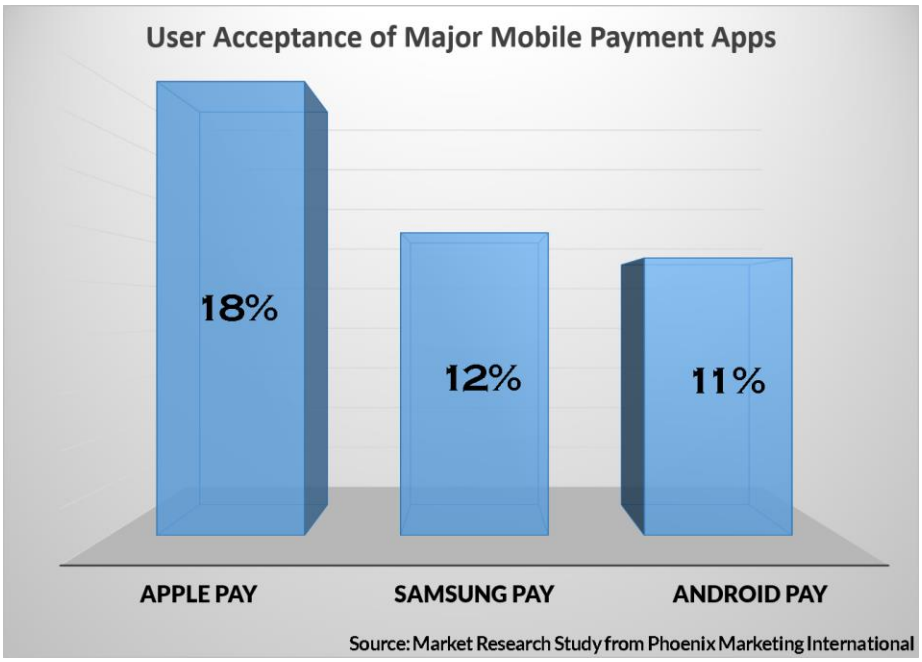


Fig. 6: User Percentage using the Present Mobile Payment Apps.

III. A Specific Methodology: Mobile Application

In present days, the security of a system is critical question in every field as hacking is a big concern. As the payment technologies are being converted to internet based service, hacking has also become a major threat to crack a system. So, while developing a payment technology it is very much required to concentrate on the security. **Fig.7** describes the proposed system of Pay-Cloak. In the proposed methodology, we have tried to increase the security with the use of biometric trait of the user. This architecture mainly has two parts: App development for NFC enabled Smartphone and an external hardware part, which will be basically realized as a back cover of the phone. Here, in the proposed method an android application installed in the smartphone communicates with the external hardware through Bluetooth and also connected with a cloud server through GPRS. The system also incorporates the Tokenization technique to eliminate the need of sending sensitive information over the network. The functioning of the proposed mobile Application can be divided into three parts: QR Code Based Merchant Payment, Peer To Peer money transaction and ID virtualization.

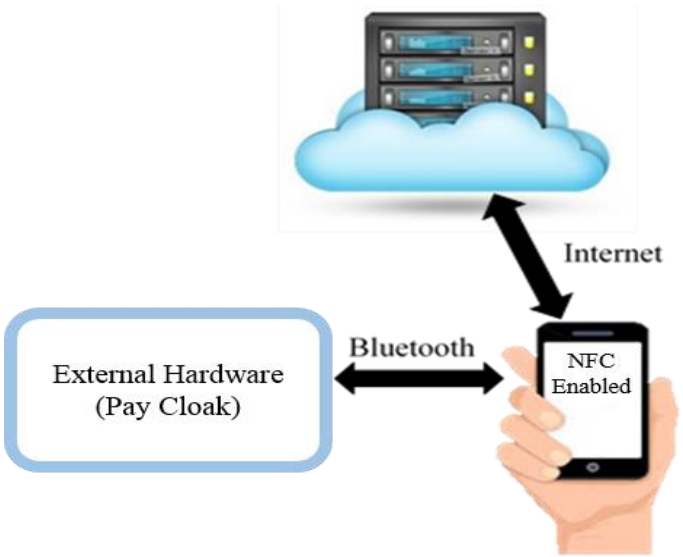
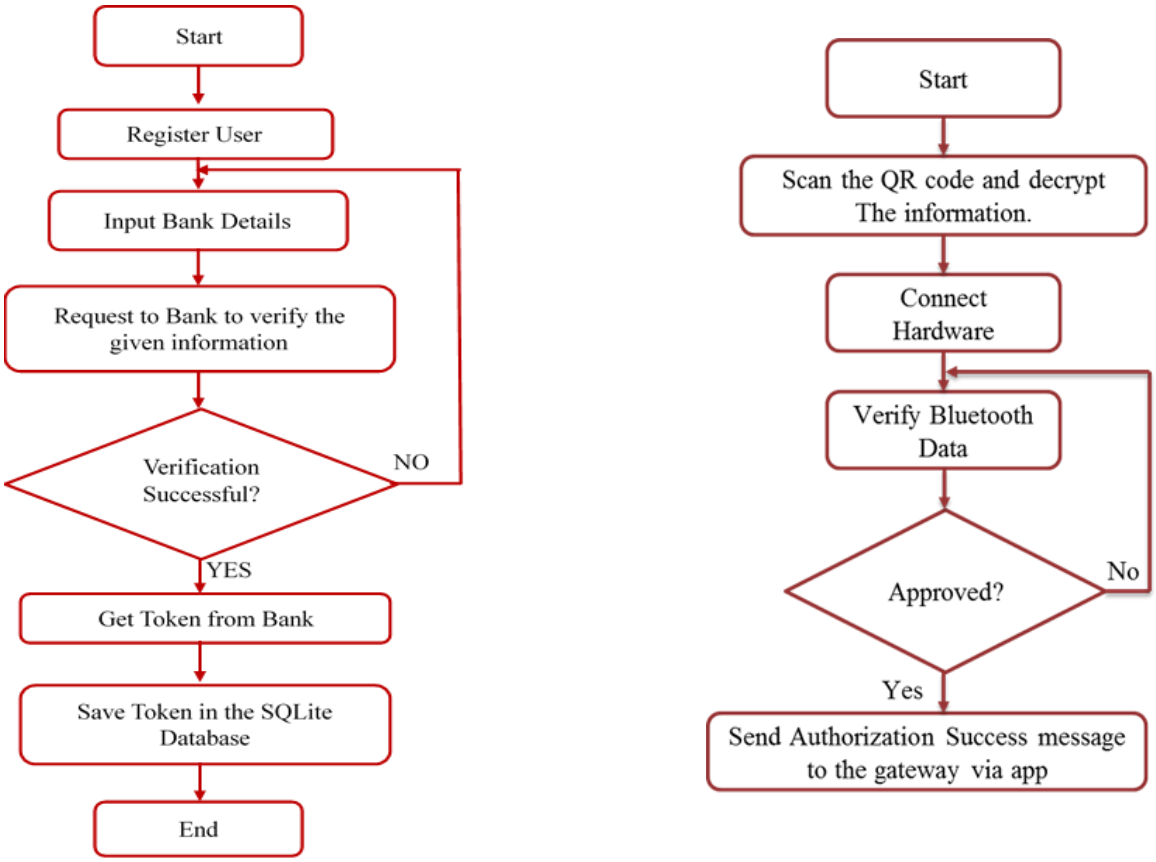


Fig. 7: Block Level Representation of the Proposed System.

1) QR Code Based Merchant Payment

For this type of transaction, we have incorporated the flexibility of QR code based system. For the system to work properly there should be a proper trust agreement between the Merchant, Cloud Server and the Bank of Both Merchant and the Buyer. The merchant registers on the cloud payment processer by providing his bank account details and other necessary information. The cloud server will then provide him a unique payment ID known as Merchant Payment ID (MPI). When any person buys the back cover and registers himself in the cloud using the application installed in his smartphone, he will be asked for his bank account details. The cloud server then requests the given bank server for authenticating the user. The bank sends an OTP in the registered mobile number of the customer. The customer has to provide the OTP in the application. Upon successful verification, the bank generates a unique TOKEN against the bank account information and saves it in the bank database. The generated TOKEN is then sent to the cloud server, which then sends it to the mobile app. The mobile app saves the TOKEN in the local SQLite database of the android mobile. The TOKEN will not be saved elsewhere. Even the user, himself, may not know the TOKEN. In this way we have decreased the possibility of data breach. The TOKEN is saved in the Highly Secure PCI-DSS complaint bank server and in the Local Android Database. In the rest of the process, only this TOKEN works as a reliable alternative of the Bank account information of the user. Due to Android's inbuilt security, it is impossible to access the SQLite database of one application by another, unless the user is given the permission to access it. After the end of the verification process the customer is provided with a unique Customer Payment ID (CPI). **Fig.8a** is the Flowchart of the registration.



(a) **(b)**

Fig. 8: Flowchart for a) First time Registration b) QR Code based Payment.

At the time of transaction, at first the merchant creates the QR code, which contains the Transaction ID, unique MPI of the merchant and the Payable amount. Customer then scans the QR code on the mobile App and gets the information regarding the transaction. After that the app forces the customer to connect the external hardware using Bluetooth for fingerprint verification. Then the customer authenticates him using the fingerprint scanner. If the verification is successful, then an approved message is sent to the mobile app from the external hardware. If the verification is failed then a failure message is sent to the mobile app over Bluetooth. Upon receiving the message from the external hardware, the application decides whether to proceed for payment or not. If the verification is failed, then the customer will be provided the chance to authenticate himself again for 3 times, after which the transaction is aborted. If the verification is successful, then the application moves to the next step. In this step the mobile app concatenates the Payee CPI and the TOKEN with the Merchant MPI along with the other information like transaction amount etc. and forwards them to the cloud server using HTTP GET method. The cloud server then gets the information

regarding the MPI and CPI. From the CPI, the cloud server gets the bank account information of both the merchant and the customer. Then the cloud server requests the Customer Bank to transfer the requested amount to the merchant bank. The bank server then verifies the TOKEN and if the TOKEN is matched, then the requested amount is transferred to the merchant account. After successful completion of the transaction, the Bank server replaces the previous TOKEN with a new randomly generated TOKEN and send it back to the cloud server. The cloud server then send it to the Mobile App. So after each successful transaction, the TOKEN is replaced. **Fig.8b** displays the flowchart for QR code based payment.

2) Peer-to-Peer Money Transaction

Another function of the system is the Peer-to-Peer money transfer system, which makes the system much more unique than the other competitor available in the market. **Fig.9** describes the flow of the process. When the user chooses Peer-to-Peer transfer, the app starts the session with the unique CPI of the particular user which was also saved in the SQLite database. The user is asked to enter the amount needed to be transferred. After entering the amount, the user has to authenticate himself using the fingerprint sensor. If the authentication is successful, an approved message will be sent to the mobile app from the external hardware using Bluetooth. If the verification is successful, the app constructs an NDEF encoded text which has 3 parts: the CPI of the Payee, the transaction amount and the TOKEN. The payee then transfers the text to the payer device using NFC beam. After the successful reception of payee CPI, transaction amount and the TOKEN, the receiver sends a HTTP GET request to the cloud server which consists payee CPI, transaction amount and the TOKEN. Then, the cloud server sends request to the payee bank with all the parameters. If the TOKEN is matched, the bank processes the transaction and transfers the money from the payee account to the payer account. After the transaction is over, the TOKEN is replaced the newly generated TOKEN from the bank and is sent to the Payee mobile app.

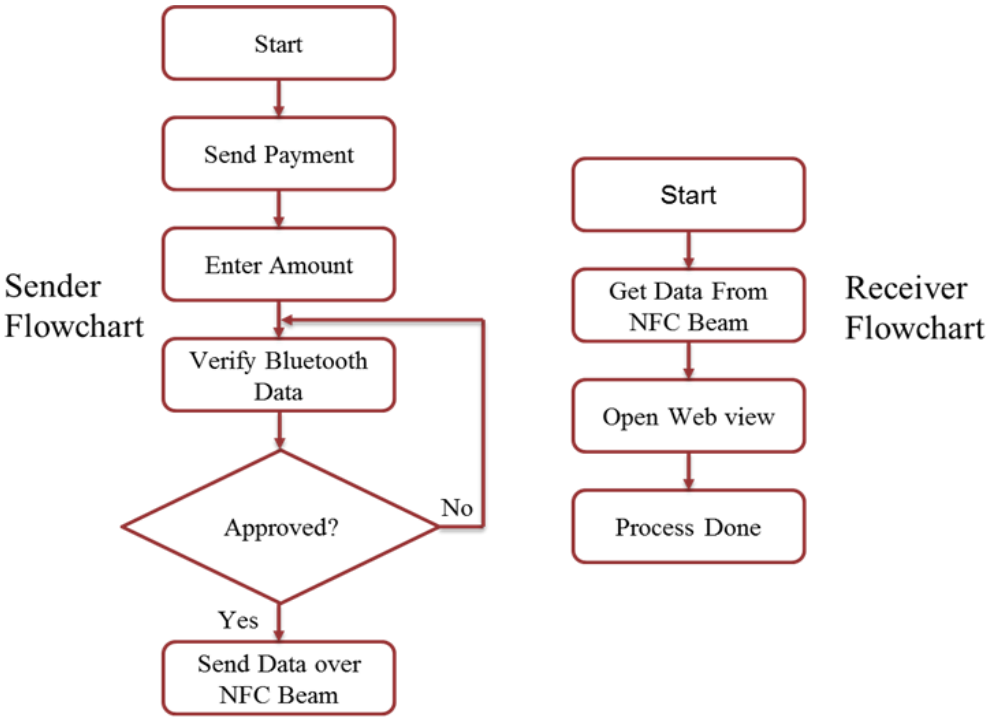


Fig. 9: Flowchart of Peer-to-Peer Payment.

So, using this system prevents the sensitive data of the customers to be used for any transaction, instead the transaction is done using a onetime unique TOKEN. We also tried to make the system more secure by using the Physical Address (MAC ID) of the mobile. Using the MAC ID we have verified that the incoming TOKEN should come from the device on which the TOKEN is generated. If the MAC ID of both the devices do not match, the transaction is aborted and the user is notified about the possible misuse of his property.

3) ID Virtualization

Figure 10 describes the flow diagram on how our proposed module works as virtual identity card. For ID Virtualization, the user has to choose ID virtualization after the login process. Then, he will be again asked for finger print verification. After successful fingerprint verification, an NDEF encoded text will be generated, which will contain the unique CPI of the user that is stored before, along with a customized web service call. This NDEF text will then be transferred to the reader terminal. After

getting the NDEF text, the reader terminal sends the request to the cloud server. The server then sends back the required information according to the request. And finally, the information or the required ID will be displayed in the reader terminal. Here, in the prototyping, we have used another NFC enabled smartphone as the reader terminal.

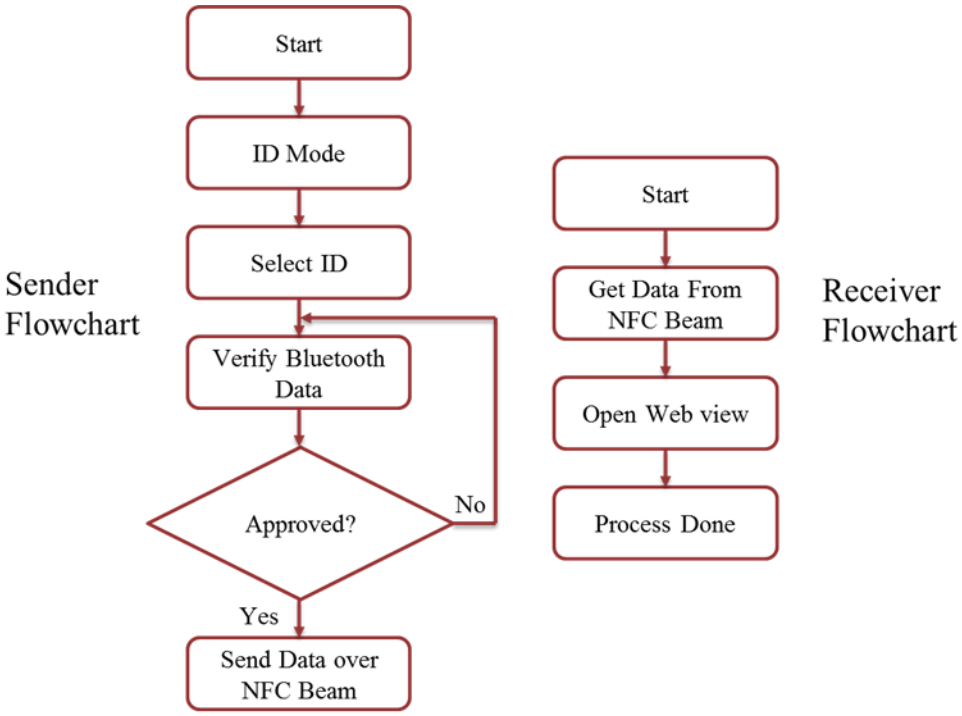


Fig. 10: Flowchart for ID Virtualization.

IV. PAY-CLOAK: HARDWARE PROTOTYPE

The hardware module consists of 3 integral parts: Host microcontroller, Fingerprint Sensor and Bluetooth module. The host microcontroller is an Arduino DUE based on ARM Cortex M3, which has a 32-bit processor, 512 KB Flash Memory and 96 KB SRAM [40]. The Bluetooth module, we have used, is a Seeedstudio Bluetooth shield. Both of these modules are based on open source hardware. The documentation and the design files are readily available in the respective website. For the fingerprint module we have used FPC-AM3 from Fingerprints Corporation, Sweden as our Hardware Secure Element. It is also used by some leading smartphone manufacturers for their smartphones. With its high image capturing capability, it can capture 256 greyscale value in a single pixel. This module can store a large no. of fingerprint templates. Both the Bluetooth and FPC-AM3 communicates with the Host Controller using Serial UART protocol as shown in **Fig. 11**. We have used the Hardware serial ports of the Arduino DUE because it provides more stability than the emulated Software Serial.

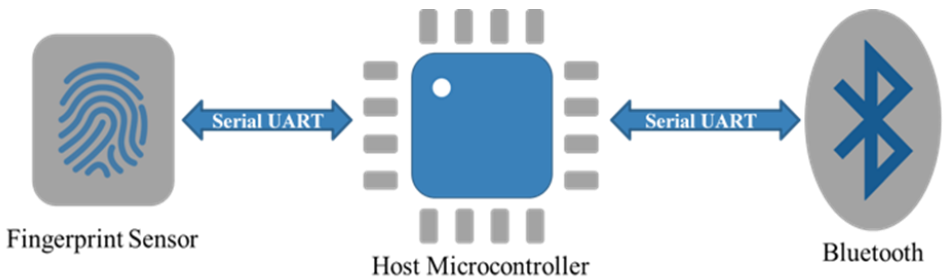


Fig. 11: Block Diagram of the External Hardware.

When the user will buy the device for the first time, the fingerprint data will be stored in the FPC-AM3 fingerprint sensor. It has an inbuilt flash memory that can save up to 990 fingerprint templates. FPC-AM3 is also used as the hardware secure element for the prototype as it verifies the biometric trait of the user. The FPC-AM3 gets command from the Arduino and replies with the result using Serial UART. Upon verification, the host microcontroller sends the command to the Bluetooth, which then forwards the message to the Mobile Application. Integration of all the components is done using some open source tools. The FPC-AM3 module has 1.27-mm pitch female headers, so it was very difficult to connect the pins as the pins are very dense. In this regard, we have incorporated one PCB board that will convert 1.27 mm pitch to standard 2.54 mm pitch header. The Bluetooth was built in a readymade shield, which has just been put on the top of our Arduino DUE board. Then the FPC-AM3 was connected to Arduino Board using standard Male to Female connectors. **Fig. 12** shows all the components of the total hardware prototype of the system.

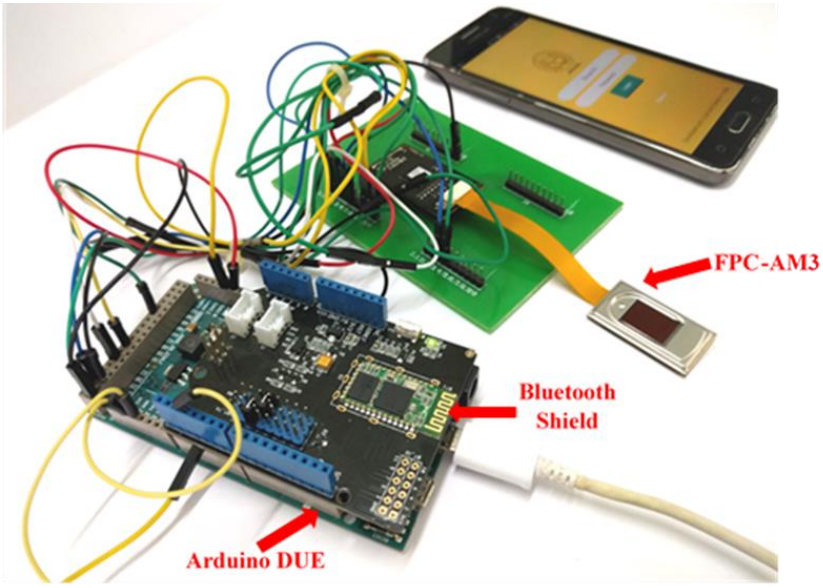


Fig. 12: Total Prototype of the System.

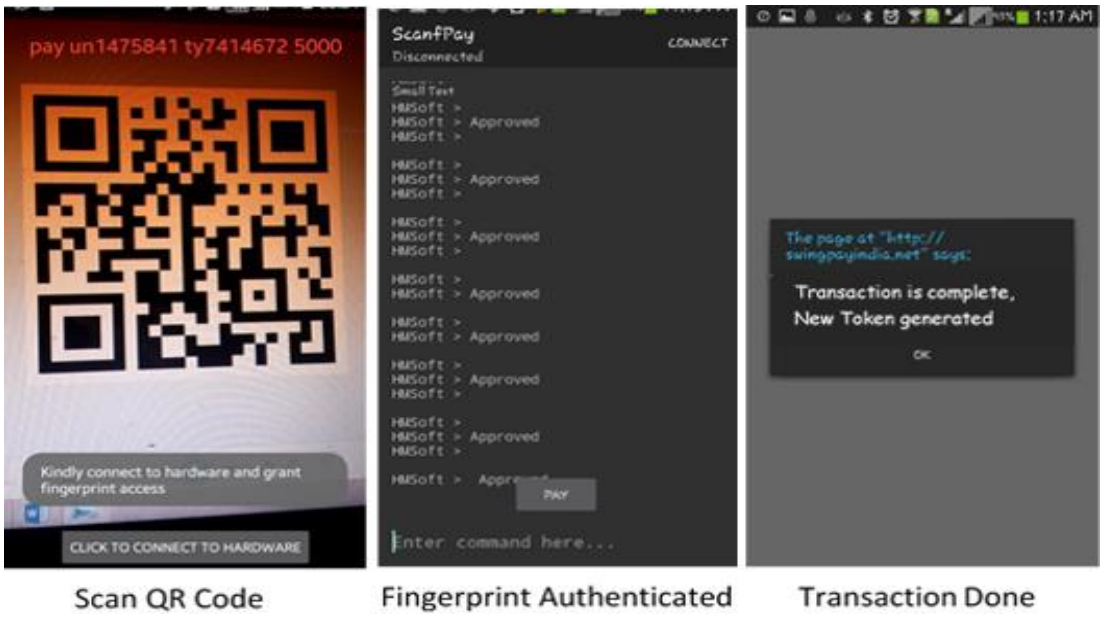
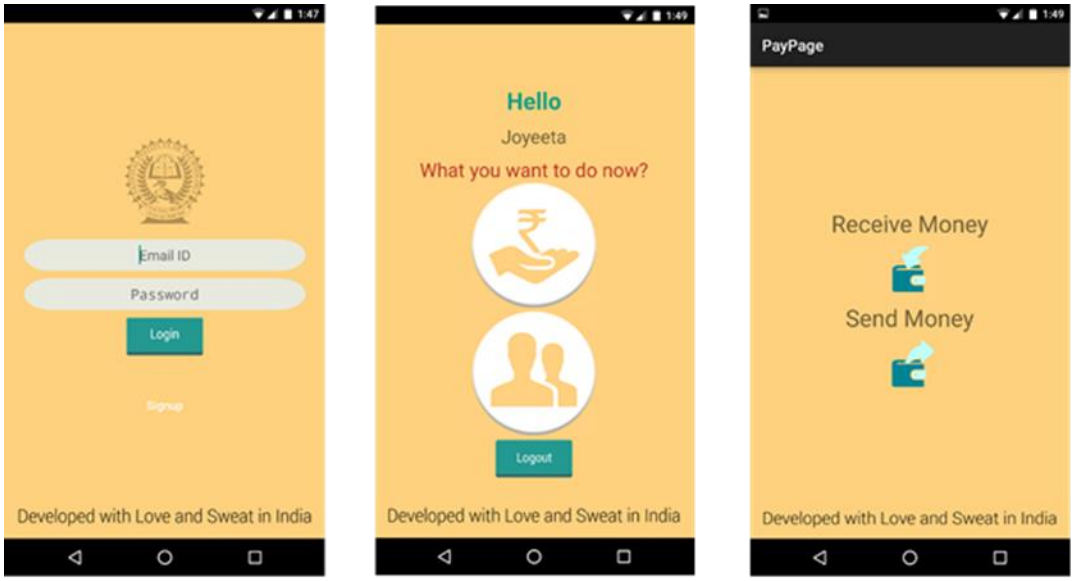


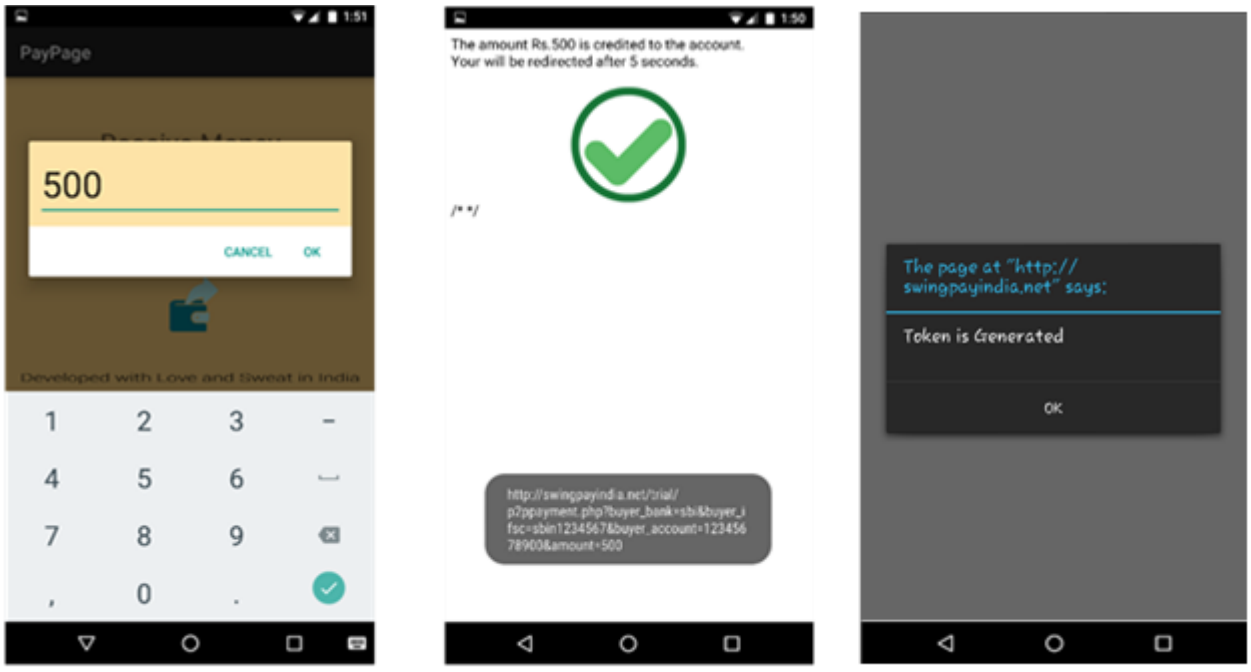
Fig. 13: Merchant Payment based on QR Code.

In **Fig. 13**, we have shown the screenshots of the application working as a merchnat based POS terminal payment module. The user first scans the QR code generated by the merchant. After that he authenticates himself using the fingerprint. If the authentication is successful, the payment will be done and the new Token will be generated. The Peer-to-Peer payment mode is shown in **Fig. 14** and **Fig. 15**. The user first choose the payment mode, enters the amount and authenticates the fingerprint. The activity that authenticates the fingerprint is same as that the activity used in QR code payment mode. If the authentication is successful, the app asks the user to tap to the payee's phone. After the payer taps his phone to payee's phone, a message is sent to the payee's phone using NFC Beam and the transaction is done. A new token will be generated for the payee for the next transaction.



Login Page | Choose between Payment and ID | Choose between Send or Receive

Fig. 14: Peer to Peer money and ID Virtualization.



Enter Amount | Transaction Done | New Token Generated

Fig. 15: Peer to Peer money transfer.

V. Conclusions

In this article, we presented a system incorporating a NFC enabled smartphone, which could be realized as an external smartphone cover consisting of a fingerprint sensor and a Bluetooth. The fingerprint sensor authenticates the user and sends appropriate data to the smartphone app. The application can perform both physical Point of Sale transaction and ecommerce transaction using QR codes. The process is very intuitive because the user does not have to put any information like card number, expiry date etc. like traditional systems. In the Peer-to-Peer transaction, the app takes the advantage of Android's NFC beam feature to communicate with another smartphone. All the information is sent to another mobile using NDEF encoding. Also we have used the fingerprint sensor as our hardware secure element, which verifies the biometric trait of the user. We have also integrated the Tokenization technique and QR code scanning feature in the application. The app securely stores the Token in the local database which can only be used if the Biometric data is matched. All the process runs in the background without the need of entering bank / card information manually. As the Token only stored in the Bank server and customer's mobile device, the chance of data breach is less compared to other existing solutions. The App can also be used to virtualize the identity information, eliminating the need of carrying all the ID cards like driving license, passport, voter ID card etc. The ID information is displayed on a reader device with NFC antenna.

Using the cover with the Application installed, everyone with an NFC enabled smartphone will be able to do the POS payments and Peer-to-Peer payments. We are constantly working on the project to increase the usability of the system like to use it for public transport ticketing system, gift card sharing, access control etc. We are also trying to incorporate NFC antenna in the hardware prototype of smartphone back cover, so that anyone with a smartphone or tab without NFC, can use the system.

Though the system is working for payment related needs, we are trying to incorporate more features in the app to make it more useful for the customer. The app may be used for ticketing purposes in public transport like Bus or Train. Using a small device which have a NFC reader, GSM modem and embedded printer, ticket can be purchased 'on the go'. The App can also be used in merchant terminal eliminating the need of a typical Point of Sale terminal. Though we are currently generating the QR code in a PC terminal, in near future, the merchant will be able to generate a QR code on the app itself. The App can be also used in access control like the way any lock or door is opened using the Biometric feature etc., which could be used as room key in a hotel making the check-in and check-out procedure easy without waiting in a queue. As the information of owner is stored in the module in terms of fingerprint or else, this module can also be used for electronic voting machine, if voting terminal provides NFC read terminal.

Acknowledgement

Some of the co-authors are thankful to the Ministry of Electronics and Information Technology (MEITY), Government of India, for providing the financial assistance under Special Manpower Development Program – Chip to System Design (SMDP-C2SD) to carry out the work.

About the Authors

Alak Majumder (majumder.alak@gmail.com) is an Assistant Professor in the Department of ECE at National Institute of Technology, Arunachal Pradesh, India. He has filed 1 US Provisional Patent and 1 Indian Patent. There are many papers, in international journals & conferences, credit to his name. His current research interests include Analog and Digital VLSI and High Speed Signaling. He is a Member of IEEE, IAENG and IACSIT.

Joyeeta Goswami (joyeetatit@gmail.com) received her master degree in Mobile Communication and Computing from National Institute of Technology Arunachal Pradesh, India, in 2016. She has filed one Indian Patent in February 2016. Her current research interests are Wireless Networks, Internet of Things, Security development in Near Field Communication and Light Fidelity (Li-Fi).

Shirsha Ghosh (shirshatit@gmail.com)received hisMasters degree in Mobile Communication and Computing from National Institute of Technology Arunachal Pradesh, India, in 2016. He has an Indian patent filed to his credit. His research areas include Embedded System, Near Field Communication, Wireless Networks, Real Time Operating Systems, and Internet of Things.

Rishu Shrivastawa(rishu.0793@gmail.com)received the B-Tech degree in Electronics & Communication engineering from the National Institute of Technology, Arunachal Pradesh, in 2016.He has published an IEEE conference paper and also applied for 1 Indian Patent. He is currently working as Software Developer at Shiksha Infotech at Electronic City, Bangalore, India. His research interest includes Low Power Embedded Systems and biometrics.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a Professor at the Department of Computer Science and Engineering, University of North Texas. He is an inventor of 4 US patents. He is an author of 200 peer-reviewed journal and conference publications and 3 books. He is currently the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine. He currently serves on the editorial board of 5 peer-reviewed international journals including IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems and ACM Journal on Emerging Technologies in Computing Systems. Prof. Mohanty has been the Chair of Technical Committee on Very Large Scale Integration (TCVLSI), IEEE Computer Society (IEEE-CS) to oversee a dozen of IEEE conferences. He serves on the steering, organizing, and program committees of several international conferences. More about him can be available from: http://www.smohanty.org.

Bidyut K. Bhattacharyya, (bkbhatta1@yahoo.com) is a Professor Electronics and Communication Engineering department at NIT Agartala. He has published 54 Papers, about 27 US Patents and filed 9 Indian Patents. In the year 2000, he was awarded the *Fellow IEEE* Grade for his contributions to the electronics packaging. He is also the recipient of Intel Achievement Award (IAA) given by the founders of Intel Corporation Dr. Andy Grove and Dr. Gordon Moore.

REFERENCES

[1] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", IEEE Consumer Electronics Magazine, Volume 6, Issue 3, July 2016, pp. 60--70.

[2] S. Ghosh, J. Goswami, A. Majumder, A. Kumar, S. P. Mohanty, and B. K. Bhattacharyya, "Swing-Pay: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment", IEEE Consumer Electronics Magazine, Volume 7, Issue 1, Jan 2017, pp. in press.

[3] D. Abrazhevich, "Electronic Payment Systems: A User-Centered Perspective and Interaction Design", Ph.D. Thesis, Eindhoven University of Technology, The Netherlands.

[4] C. A. Walton, "Portable radio frequency emitting identifier" US Patent 4 3842 88, Dec.30, 1980.

[5] Smart Card Alliance, "Contactless Payment and the Retail Pint of Sale: Applications, Technologies and Transaction Models", Smart Card Alliance. Princeton Junction, NJ, Mar. 2003.

[6] Radio Electronics, "NFC Near Field Communication Tutorial," [Online]. Available: http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-tutorial.php.

[7] S. Ghosh, J. Goswami, A. Kumar, A. Majumder, "Issues in NFC as a form of contactless communication: A comprehensive survey", in Proc. ICSTM, 2015, pp. 245-252

[8] E. Haselsteiner, & K. Breitfuß, (2006, July). Security in near field communication (NFC). Presented at Workshop on RFID security, [Online]. Available: http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf, 2006.

[9] NFC Times. Barclay Card. [Online]. Available: http://nfctimes.com/company/barclaycard.

[10] C. P. Beshouri and J. Gravråk, "Capturing the promise of mobile banking in emerging markets," McKinsey & Comp., New York City, NY, Apr. 2010.

[11] S. Clark. "Google unveils first Android NFC phone — but Nexus S is limited to tag reading only for now", [Online]. Available: http://www.nfcworld.com/2010/12/07/35385/google-unveils-first-android-nfc-phone-but-nexus-s-is-limited-to-tag-reading-only-for-now/. Dec. 2010.

[12] Google, "Google Wallet". [Online]. Available: https://www.google.com/wallet/faq

[13] C. Mercer. "History of PayPal: the history of the biggest online payment system in the world," [Online]. Available: http://www.techworld.com/picture-gallery/e-commerce/history-of-paypal-1998-now-3630386/#4. Nov. 2015.

[14] G. Paul, and J. Irvine. (2016). "IEDs on the Road to Fingerprint Authentication: Biometrics have vulnerabilities that PINs and passwords don't." IEEE Consumer Electronics Magazine 5(2), pp. 79-86.

[15] Antonio Villas-Boas, "Samsung has a key technological advantage that makes it much better to pay with your phone" Online, Available: http://www.techinsider.io/how-magnetic-secure-transmission-works-on-samsung-pay-2015-9, Sep. 2015.

[16] T. Horton, R. McMillon. "A Primer on Payment Security Technologies: Encryption and Tokenization". Online. Available: https://www.firstdata.com/downloads/.../primer-on-payment-security-technologies.pdf, 2011.

[17] First Data, "Avoiding a Data Breach: An Introduction to Encryption and Tokenization", First Data Corp. Atlanta, GA. 2013.

[18] P. M. Banerjee, C. Wigginton, "Smart device, Smart pay: Taking mobile payments from coffee shops to retail stores". Deloitte University Press. [Online]. Available: http://dupress.com/articles/mpayments-mobile-pos-system-in-retail/. June. 2015.

[19] Business card QR Codes. "QR Payments." [Online]. Available: http://www.businesscardsqrcode.com/qr-payments.html.

[20] BeQRious. "Pay For Coffee with Phone in Starbucks". [Online]. Available: http://beqrioustracker.com/pay-for-coffee-with-phone-in-starbucks/

[21] Zapper FAQ. [Online], Available: https://www.zapper.com/services.php.
[22] O. Kharif. “Apple Pay Seeks Growth in Asia, Europe after Slow U.S. Adoption”, Bloomberg Technology. [Online]. Available: http://www.bloomberg.com/news/articles/2015-12-24/apple-pay-seeks-growth-in-asia-europe-after-slow-u-s-adoption. Dec. 2015.
[23] R. Boden, “Trustev reports on US adoption rates for Apple Pay versus Android Pay and Samsung Pay”. [Online]. Available: http://www.nfcworld.com/2015/11/06/339308/trustev-reports-on-us-adoption-rates-for-apple-pay-versus-android-pay-and-samsung-pay/. Nov. 2015.
[24] C. Merritt. Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments, Federal Reserve Bank of Atlanta, Atlanta, GA. [Online]. Available: https://www.frbatlanta.org/-/media/Documents/rprf/rprf_resources/wp0810.pdf, 2010.
[25] A.D. Parikh, “Payment Using Unique Product Identifier Code,” U.S. Patent 2011/0137742A1, Jun. 9, 2011.
[26] J. Lee, C. H. Cho, & M. S. Jun. “Secure quick response-payment (QR-Pay) system using mobile device”. In Proc. ICACT. 2011, pp. 1424-1427.
[27] K.M. McGuire, R. Taggart, J.A. Chapman, “Tokenized Payment Processing Schemes”, U.S. Patent 8,763,142 B2, Jun.24, 2014.
[28] D. Gaspar, “Credit card tokenization techniques”, U.S. Patent 9,092,777 B1, Jul 28, 2015.
[29] A. Majumder, B.K. Bhattacharyya, S. Ghosh, J. Goswami, “A Digital Card serving Identity and Payment Purpose”, filed Indian Patent at IPO Kolkata, Application No. 201631004666, 10th February 2016.
[30] R. Boden, “Seamless adds HCE to Seqr mobile wallet” [Online]. Available: http://www.nfcworld.com/2015/10/23/338922/seamless-adds-hce-to-seqr-mobile-wallet/. October 2015.
[31] T. Ma, H. Zhang, J. Qian, X. Hu, & Y. Tian. “The Design and Implementation of an Innovative Mobile Payment System Based on QR bar Code”. In Proc. ICNISC. 2015. pp. 435-440.
[32] D.M. Monteiro, J.J.P.C. Rodrigues, J. Lloret, “A Secure NFC Application for Credit Transfer among Mobile Phones”. In Proc. CITS, 2012, pp. 1- 5.
[33] L. Mainetti, L. Patrono, & R. Vergallo. “IDA-Pay: an innovative micro-payment system based on NFC technology for Android mobile devices,” In Proc SoftCOM, 2012, pp. 1- 6.
[34] J.Gao, J.C.K. Patel, S. Shim, “A Wireless Payment System”, In Proc. ICESS , 2005. pp. 8-pp.
[35] C.Y. Leong, K.C. Ong, K. K. Tan, O. P. Gan, “Near Field Communication and Bluetooth Bridge System for Mobile Commerce”, in Proc. ICII, 2006.
[36] MacRumours, “Apple Pay Overview,”. [Online]. Available: http://www.macrumors.com/roundup/apple-pay/
[37] Sarah Perez; “PayPal Launches PayPal.Me, A Simpler Way To Request Money Using Your Own Personalized URL”; [Online]. Available: http://techcrunch.com/2015/09/01/paypal-launches-paypal-me-a-simpler-way-to-request-money-using-your-own-personalized-url/
[38] George Wallner, "System and method for a baseband nearfield magnetic stripe data transmitter." U.S. Patent 8,628,012, January 14, 2014.
[39] http://www.practicalecommerce.com/articles/87765-11-Innovative-Mobile-Payment-Apps
[40] Arduino Due Documentation, [Online]. Available: https://www.arduino.cc/en/Main/ArduinoBoardDue.