Swing-Pay: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment

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

Advancement in payment technologies have an important impact on the quality of life. The emerging payment technologies create both opportunities and challenges for future. Being a quick and convenient process, contactless payment gained its momentum, especially in merchants, where throughput is the main important parameter. However, it poses risk to issuers as no robust verification method of customer is available. Thus giving rise to quests to evolve and sustain a well-organized, efficient, reliable and secure unified payment system, which may contribute to the smooth functioning of the market by eliminating scratch in business. This article presents an approach and module by which one card can communicate with the other using Near Field Communication (NFC) technology to transfer money from payer's bank to payee's bank by digital means. This approach eliminates the need of physical cash and also serves all types of payment and identity needs. Embodiments of this approach furnish a medium for cashless card-to-card transaction. The module, which is called *Swing-Pay,* communicates with its concerned bank via GSM. The security of this module is intensified using biometric authentication. The article also presents an app on Android platform, which works as a scanner of the proposed module to read the identity details of concerned person, the owner of the card. We have also presented the prototype of a digital card. This card can also be used as virtual identity card (ID), accumulating the information of all ID cards including electronic Passport, Voter ID, and Driving License.

I. Electronic Payments: An Historic Perspective

THOUGH the digital payment process was operational from 1960s, with the advancement of technology and e-commerce evolution, digital cashless payments have become a mainstream in the recent past [1]. Due to the relentless effort of research community, several electronic payment models such as JW model and N.Asokan model are devised. JW model is the traditional payment system, where both the sellers and buyers need some sort of involvement in a particular transaction to be taken place [2]. In 1998, the N.Asokan Model was introduced, which also incorporates the transaction to be processed between the bank and any one of the buyer or seller, in case both of them are not involved in any transaction (Refer **Fig. 1**) [3]. The "3e model" which is based on the N.Asokan Model was introduced but included in credit card, electronic cash and electronic cheque payment models [2]. It is observed that credit card is the most widely used electronic payment mechanism [4]. With the need of transferring the money between two peers in no time, the concept of electronic fund transfer through internet came into picture. Many possible solutions like Wire Transfer and ATM networks have been developed to support the need (Refer **Fig. 2**).

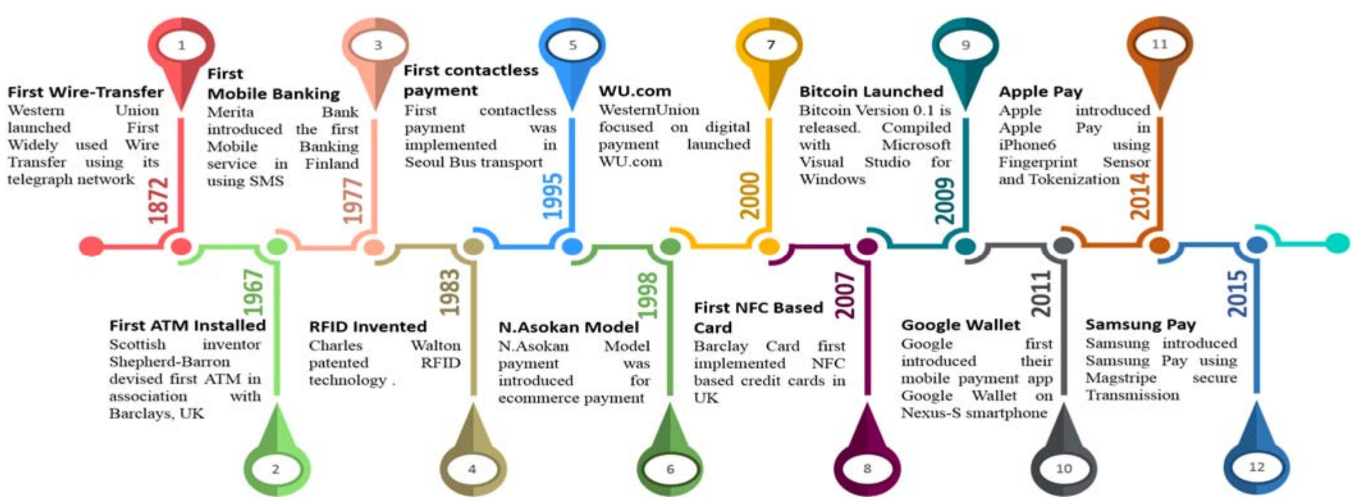

Fig. 1: Chronology of digital payment system development: from JW model to Samsung Pay.

With the passage of time many popular and fast frameworks are available to fulfill the need of international money transfers. At the same time the crypto currencies like Bitcoin and Litecoin, one can transfer money to any other in this world in the blink of an eye. But as there is no central organization to monitor the bitcoin transactions and the identity of the wallet holder. Scammers may also use Bitcoins for illegal activities on the internet. In the past few years, with the introduction of smartphone and desktop, operating systems like Android, iOS, become popular. The peer-to-peer (P2P) money transfers have taken a next stage of development with the concept of Mobile Wallets and Mobile Banking. These allow the usage of a lot of features like bill payment, money transfers and withdrawals, ticket booking, mobile recharges as well as P2P money transfers [5]. In 1977, Merita Bank introduced the first Mobile Banking service in Finland using SMS [6]. This gives a huge opportunity to the masses to access the Banking facilities. It is observed that where 50 percent people use mobiles but only 37 percent have the access to the formal banking [7]. The need and advantages of mobile banking has been studied [8]. Many smartphone apps are available from finance companies by which one can pay anyone in the world anytime. But with increasing usage they became easy prey to hackers who often succeeded in carrying out fraudulent transactions. An ultrathin, stretchable stick is available which can be used for payment when connected with smartphone [9].

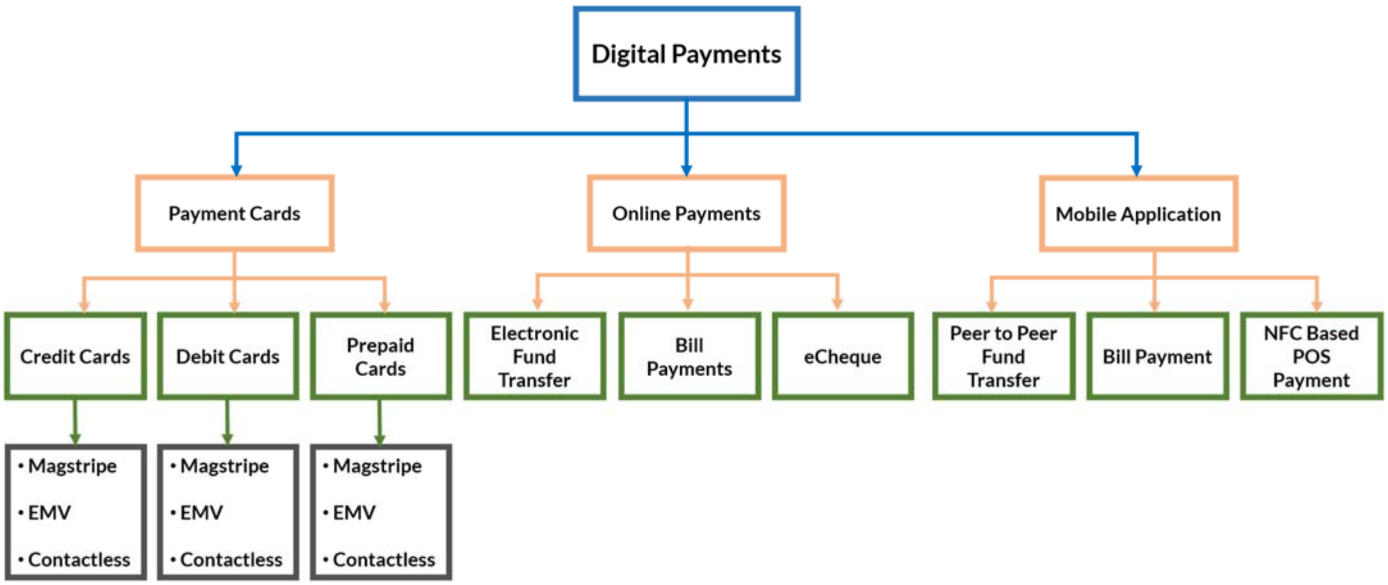

Fig. 2: Different digital payment systems.

With the invention of RFID technology in 1983 by Charles Walton, a new form payment method was developed which is known as Contactless payment (refer **Fig. 3**) [10]. In 1995 First contactless payment was implemented in Seoul Bus transport [11]. Followed by Speedpass in 1997 to pay fuel charges in US gas stations. In 2007, Barclay Card first implemented NFC based credit cards in UK [11]. NFC is the successor of RFID which uses 13.56 MHz frequency to communicate within less than 10cm range. NFC has 3 modes of communication namely, Reader-Writer mode, Peer to Peer mode and Card Emulation mode. In Reader-Writer mode, the preloaded data is either read from the embedded chip on the tag or written in the embedded chip on the tag [12]. In Peer-to-Peer mode two NFC enabled devices communicates between each other to either share a small data or to create a pairing [13]. In Card Emulation Mode, the active device is emulated as a Smart Card based on different standards [14].

Fig. 3: Block diagram of NFC based payment mode.

Soon many leading companies started to incorporate contactless features in their Smartphones. Google first introduced their mobile payment app Google Wallet in 2011 [15]. This App stores the credit card and bank information in the cloud. Then it use it using a passcode and pay in the Point of Sale (POS) terminals which supports the contactless payment. Google also provided a Google Wallet Card, which is linked with the Google wallet and can be used virtually anywhere. To make the transactions more secure, several schemes are developed using the industry standard Protocol such as Tokenization and Point-to-Point encryption (P2PE). In Tokenization scheme, the actual credit or debit card information are replaced by one time tokens. The token can only be identified and decrypted by the Tokenization Server. In Point-to-Point encryption, all the data are encrypted till the data is processed and decrypted only when they arrive at the secure environment of the P2PE [16].

In October 2014, Apple Pay was introduced [16]. These devices have NFC antennas built into them for communication with the POS terminal. Though, Apple pay uses the inbuilt fingerprint scanner to authenticate the user, it does not use Tokenization scheme to secure the credit or debit card information (refer **Fig. 4**). Yet another system, the magnetic secure transmission (MST), gives the users the freedom to use the device on the POS terminal, where only traditional credit or debit cards are supported instead of NFC [17, 18]. Android Pay was introduced in October 2015. It is estimated that 65% of the total transaction in their retails shops will be made by mobile payments by the year 2025 [19].

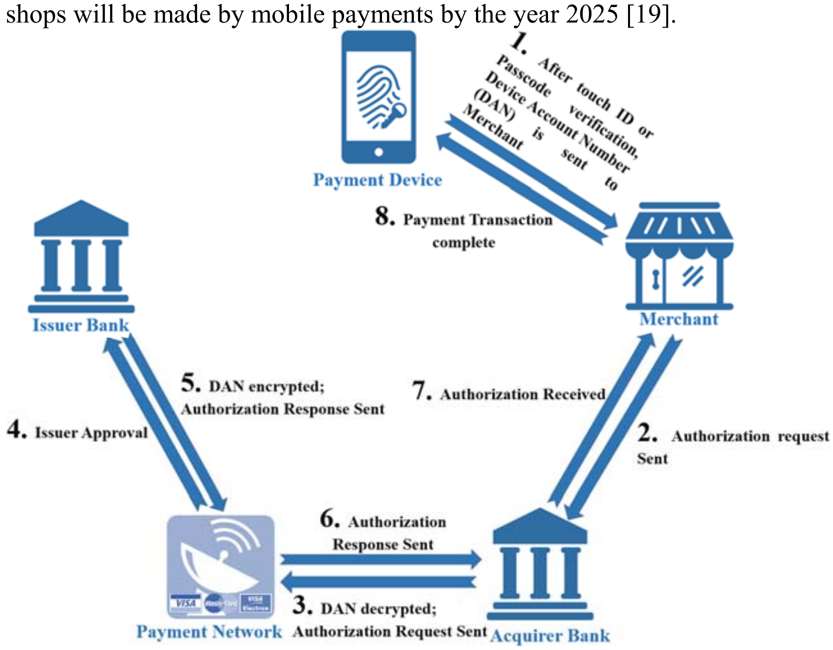

Fig. 4: Illustration of the Apple Pay system.

Though there is a huge advancement in payment technology, the acceptance of them in customers are not satisfactory. There are many factors which are responsible for the successful adaption of mobile wallets in the market. A survey shows that 62% people are concerned about the security of the systems. In 2015, another survey on Consumer Digital Payments finds that that among all the existing systems 16% people prefers digital payment, where as a whopping 67% people still prefers cash. It is also seen that debit card has an acceptance of 59% and 50% people are relying on credit card. It is also pointed out that there is no as huge excitement for the technologies in the common people because only 5-6% more are agreed to use the digital payments method by 2020 [20**]. The acceptance of different payment mediums is presented in **Fig. 5**.

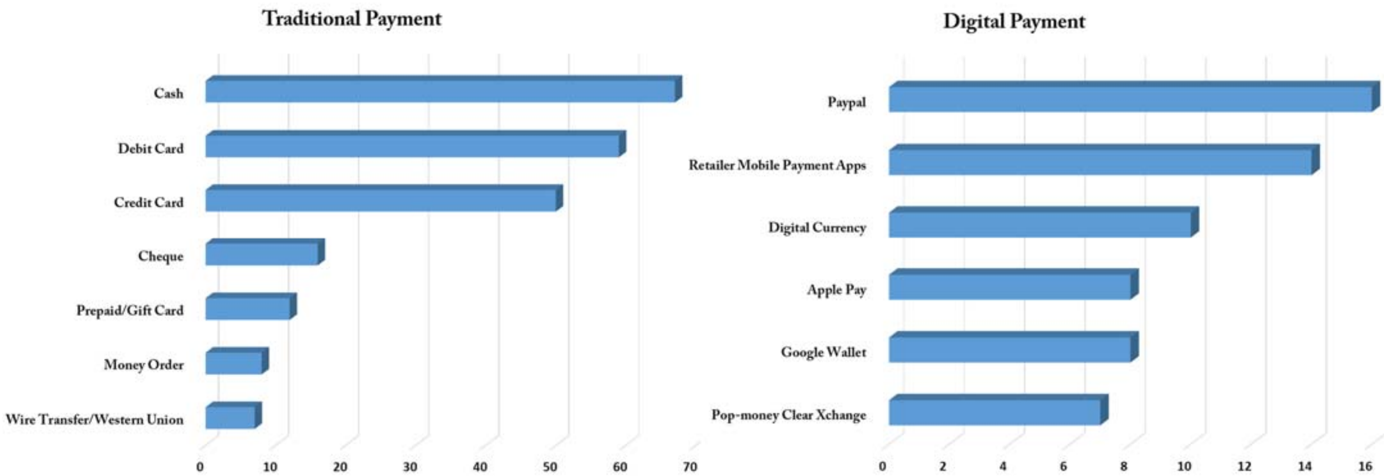

Fig. 5: Acceptance of current payment system.

One of the many reasons of such less acceptance is security concern asked by 45% of the total user. And the most important barrier is that consumers don't like to switch technologies to use mobile payments and 97% people refused to buy a new device to support mobile payments [21]. A survey finds that among several payment technologies, debit card tops with a majority of 43% preference and credit card is claimed as second choice with 35% acceptance [22]. As people are still preferring debit or credit cards, many companies have digitized the payment cards and incorporated several cards in a single one. Stratos, Coin & Plastic card can load up to 3 cards, 8 cards and 20 cards, respectively, while SWYP can store a whopping 25 cards [23]. The payment compatibility and cost of these cards are summarized in **Table 1**. The likelihood to use mobile payment apps are also found very less on a consumer perspective study in 2016; only 5% people are willing to use mobile payment app. The detailed scenario is shown in **Fig. 6** [24]. The main issue with the above methods is that, they all rely on a high budget smartphone which are expensive. But in the countries where very few people can afford that due to the economic conditions, penetrating that consumer class is still challenging. It is estimated that 73% people use mobile in India and it is becoming the second largest market for smartphone. Due to large innovations, total 40% of smartphone users in India have a mobile wallet [25]. It was also found that, 74% people intended to use Mobile Wallets in emerging markets, where the number goes down to only 46% in the developed market [25]. From the above discussions it is evident that while designing a unified payment system, *the top considerations should be security, robustness, ease of use and low cost*. The novel digital card module "Swing-Pay" presented in this article addresses these deficiencies of the existing digital payment system.

TABLE 1:
Payment Versatility and cost of Digital Payment Cards

Card Name	Magstripe	EMV	NFC	Price
STRATOS	✓	✗	✗	$95 Yearly
COIN 2.0	✓	✗	✓	$99 Upfront
SWYP	✓	✓	✗	$99 Upfront
PLASTC	✓	✓	✓	$180 for 18 Months

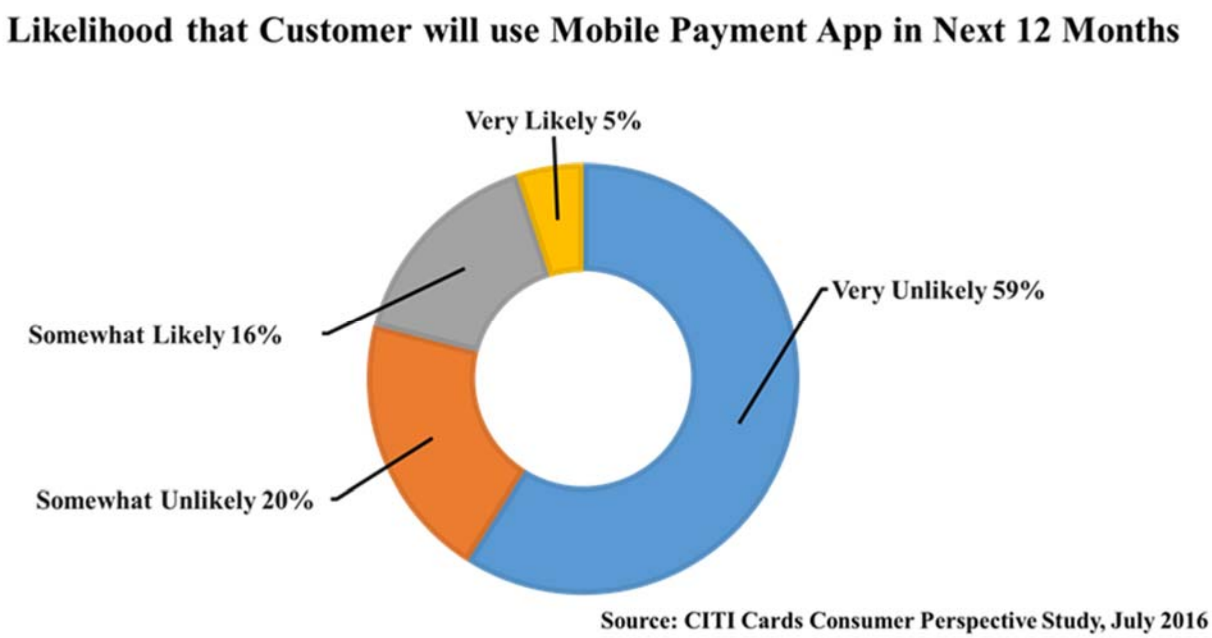

Fig. 6: Percentage of user interested in mobile payment App in next 12 months.

II. Electronic Payments: State-of-The-Art Research

There are many possible solutions available for the digital payment system (refer **Fig. 7**). However, they either rely on a smartphone or serve Point of Sale (POS) payments only. So, we require a unified payment system that will serve all types of payment like POS and P2P and it must be quite secure and economical compared to the other solutions. The system should also be portable so that the users can carry the device with them to pay to anyone any time, possibly anywhere. The device (i.e. Swing-Pay) may allow people to tender exact payment so that they need not to worry about the scarcity of small denominations.

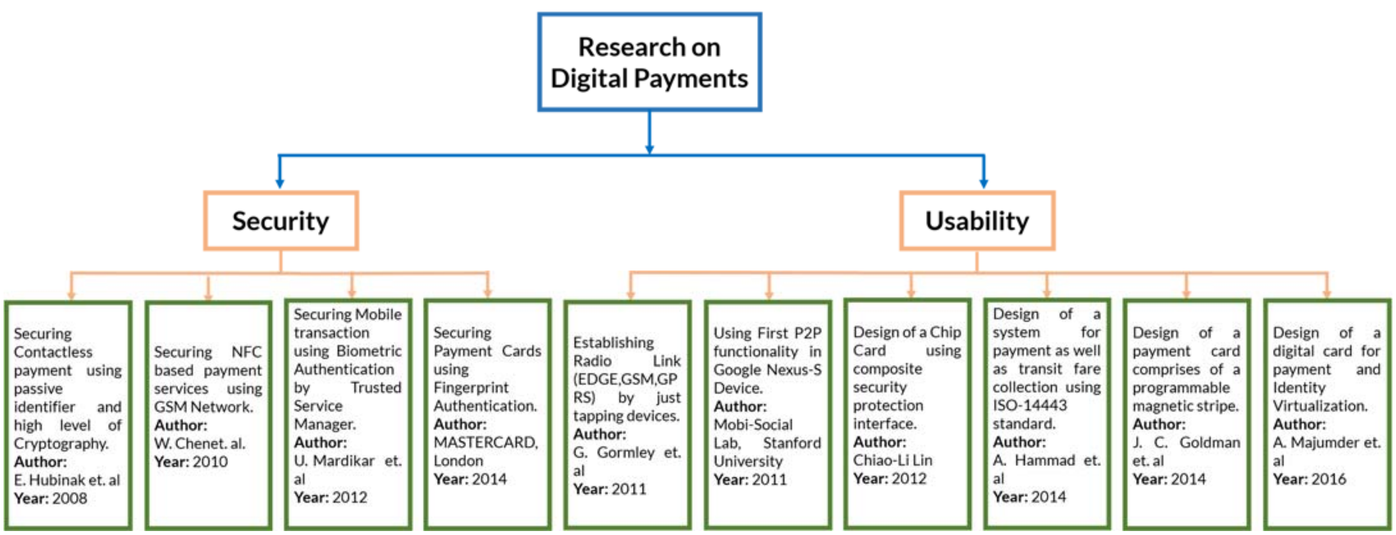

Fig. 7: Different researches in digital payment systems.

A method to secure the contactless payment using high level of cryptography with a passive identifier is available [26]. Again, a way to initiate the establishment of Radio link using EDGE, GPRS or GSM is proposed just by tapping two devices [27]. Though, tapping is very intuitive procedure for starting the data communication, it may lead to a problem if many devices are tapped unintentionally. The inventors have also proposed a way to gather a group data using NFC. Enhanced versions of

NFC, when it was launched by Google on Nexus-S device in 2011, are also explored. Mobi-Social Lab of Stanford developed an app that uses P2P functionality of Nexus-S [28]. NFC Forum standardized a protocol to communicate between two active NFC devices using P2P functionality, known as simple NDEF (NFC Data Exchange Format) exchange protocol (SNEP). In this protocol, the SNEP client sends a request to the SNEP server, which contains a request header and an information field [29]. The server handles the request and sends a response back to the client. Google made it open source so that the developers can use that and develop P2P apps. The SNEP protocol has been improved to introduce OPEN-NPP protocol [30]. NPP or NDEF Push Protocol is built with the Google protocol to push NDEF messages, known as Logical Link Control Protocol (LLCP). NDEF supports several different NFC record types like Text Record, URI Record, Signature Record and Smart Poster Record [31]. Ben Dodson et.al designed a gaming app which uses NFC for loading different applications with the gaming session continues to run over another channel [32]. David Monteiro et.al uses NFC P2P mode, to establish communication between two mobiles using Bluetooth. After establishing the communication, the credit is transferred to one SIM to another [33]. This system is innovative and targets the credit transfer only between two SIM cards. It's not a general money transfer systems. The Host Card Emulation Mode of ISO 14443A smartcard standard is also implemented on Arduino based microcontroller and communicated with the Android Smartphone [34].

To make mobile payment more secure, researchers also explored the use of current GSM network to authenticate NFC based mobile payments [35]. A system has been devices in which the financial transactions are done in any POS and are validated using a Trusted Service Manager (TSM) [36]. The inventors are using smartphones with inbuilt fingerprint scanners to use the Biometric Trait of the user in place of PIN or Chip authentication in traditional Credit Cards. The Biometric data are stored in the second Secure Element (SE) of the device. At the time of any transaction, the SE verifies the Biometric trait and generates transaction data when the verification is successful. This invention serves the POS transactions only and the user must have a smartphone with fingerprint scanner. The design of a chip card with security protection interface and a method to control the same is available [37]. The card comprises of four main components: a carrier, at least one induction coil that is used for reception and transmission, at least one chip, and one security interface. The method of controlling the card includes three steps such as issuance of the chip card by the chip card, triggering the security interface and execution of a contactless transaction. In The design of a system for facilitating the payment as well as transit fare collection using ISO 14443 standard for contactless communication is discussed in literature [38]. This invention also needs a mobile to function. So a standalone device is needed which can do all the payment needs without mobile phone. A multipurpose digital card has been devised, which can emulate different credit or debit cards using the Dynamic magnetic stripe emulator [39]. This card also has an NFC radio, which can be used in contactless terminals. To use the default card, the user will have to give a passcode using the buttons. In 2014, the first payment card with inbuilt fingerprint scanner and NFC is presented [40]. In 2016, a new NFC based digital card is invented which serves both payment and identity needs [41]. This feature is very favorable for the user, but only limited to EMV and contactless terminals. So it cannot be used for Person-to-Person transactions.

III. THE PROPOSED MODULE

In this Section a device module Swing-Pay has been proposed, which is envisioned to meet nearly all forms of payments. Swing-Pay module comprises of the following components (refer **Fig. 8**): 1) Microcontroller, 2) NFC Module, 3) Fingerprint scanner, 4) E-Ink display, 5) GSM module, 6) Capacitive Buttons, and 7) Power Supply Module. An Arduino Due board has been used as it has a 32 bit Atmel SAM3X8E ARM Cortex-M3 CPU, 4 Hardware Serial Ports, Extended SPI support and 512KB SRAM [42]. Out of all the NFC modules available in market, an Elecrow NFC shield is picked as it supports ISO14443 Type A and Type B protocols as well as Peer-to-Peer communication [43]. For the fingerprint sensor, Capacitive fingerprint Sensor (FPC-AM3) has been deployed from Fingerprints Cards, Sweden [44]. This module has two parts: FPC1011F3 Area Sensor and the FPC2020 processor. FPC1011F3 is a CMOS fingerprint Sensor, which takes image with 256 gray scale values every single pixel. FPC562020 is a power efficient ASIC which communicates with FPC1011F3 using Serial Peripheral Interface (SPI) bus. It also stores fingerprint data on external flash memory for later verification.

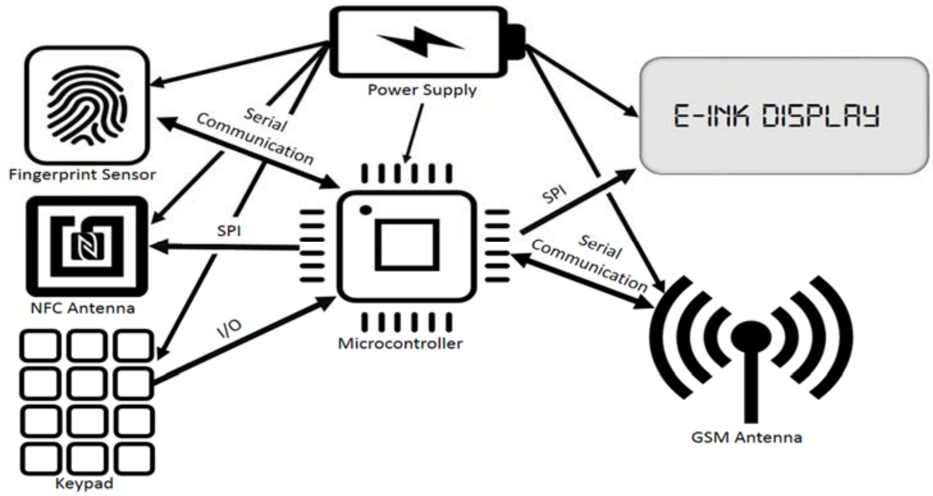

Fig. 8: Block level representation of the proposed novel digital card module, called Swing-Pay.

To reduce the energy consumption of the Swing-Pay module, E-Ink display from pervasive displays has been used. This 2.7” display has 264 x 176 resolution with 117dpi [45]. E-Ink displays are bi-stable, which means it can retain the data on the screen even after the power supply is off. It takes power only to change the state. The E-Ink display has millions of very thin microcapsules suspended in a fluid. The microcapsules contain black particle and white particle, who are negatively and positively charged respectively. When a negative electric field is applied black particles go to the top and when a positive electric field is applied white particles visit the top [46]. There was no library available to support Arduino Due platform. Adafruit has a library, which will only compile for AVR based Arduino boards, Rapberry-pi and MSP430. Also 2.7” displays can only display static images on AVR based Arduino Boards, as because printing of dynamic images and texts requires higher SRAM capacity. The library has been modified by adding some required arguments, so that it can compile on Arduino Due target which is based on SAM3X8E.

For the GSM modem Adafruit Fona has been used due to its small size and higher capabilities. This module uses SIM800 cellular module and can perform all types of cellular functions [47]. A Sticker-type 3dBi GSM Quad-Band Antenna is also used with uFL connections and 3.7Volt, 500 mAh Lithium Ion battery with the GSM module. As specific case, a TTP229 Capacitive Touch Sensor module is used as capacitive buttons. The capacitive buttons works on the basis of the principle of fringing capacitance. When the human body (i.e. finger) approaches the sensor, the fringing electric fields are dissipated from the capacitive plate towards the ground as the human body is grounded. The capacitance increases as the hand approaches the sensor in a nonlinear way due to fringing effects [48]. The TTP229 senses the touch on 16 different buttons and communicates with the host microcontroller with I2C interface.

IV. PEER-TO-PEER MONEY TRANSFER USING SWING-PAY

In the protocol of Swing-Pay, money from payer’s bank account is transferred to payee’s bank account. The Swing-Pay has 3 role players in the system: 1) the hardware module, 2) Cloud Server, and 3) the Bank. The hardware module communicates the cloud server, which then communicates with the bank server to make the transaction happen. When the user buys the module for the first time, he will have to register for a customized account in the cloud server. He will be given a unique ID from the cloud server at the time of registration. All the information of the user such as Bank name, Account number and Routing number etc. will be stored in the registered account of the user in an encrypted format. At the time of registration, the ownership information given by the customer is also validated by using One Time Password (OTP) system. To communicate with the cloud server, SMS can be used instead of GPRS which also minimizes the power consumption of the system. To communicate between two modules, the P2P functionality of NFC can be used. An Arduino targeted library, which uses the NDEF allows the P2P communication between NFC module and Android Mobile using SNEP and LLCP protocol. For the prototyped Swing-Pay, the library is tweaked so that two Arduino modules can communicate between each other. The communication flow of the Swing-Pay is illustrated in **Fig. 9**.

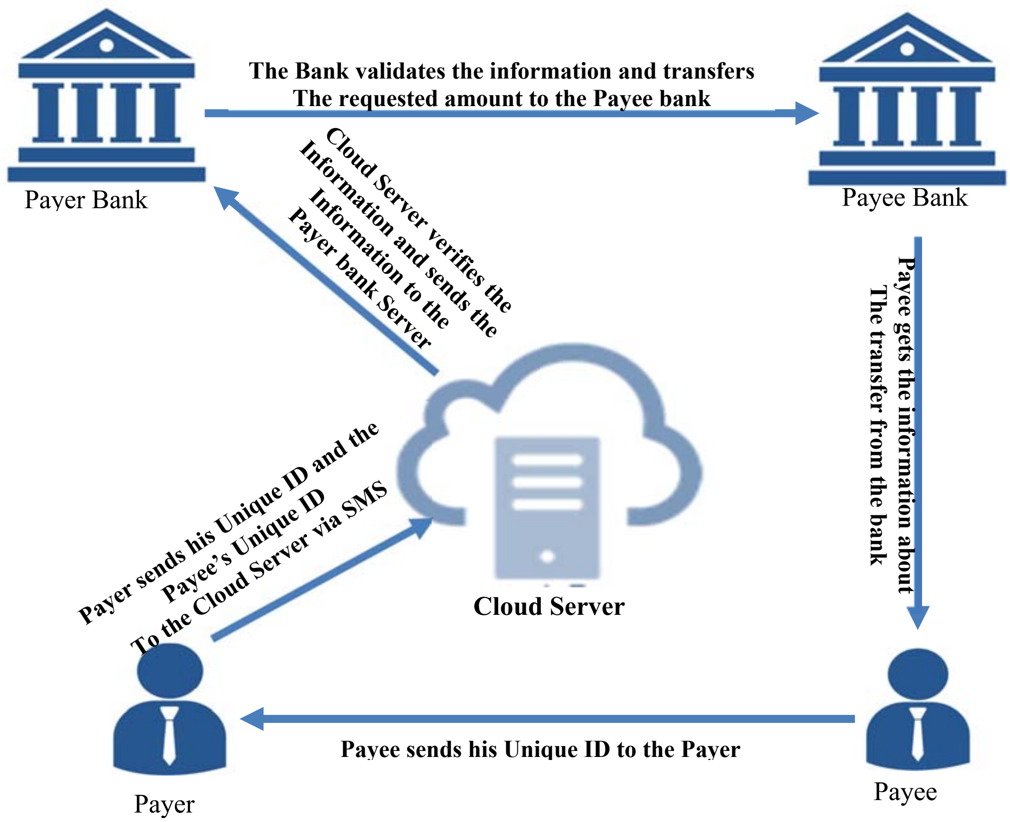

Fig. 9: Communication flow for Peer-to-Peer Money transfer in Swing-Pay.

In the Swing-Pay framework, at first, the Payee activates his card using his finger print. If the fingerprint is authenticated, then the card is activated. After that the payer selects the Pay Money mode and the payee selects Receive Money mode from the module. Then the payee authenticates himself using the fingerprint sensor, and taps his card with the payer's card. If the authentication is successful, the unique ID of the Payee is transferred to the payer module by NFC P2P mode. Otherwise, the transaction will be blocked. When the payer gets the Payee unique ID, he then sets the amount to be sent using the capacitive keyboard. After selecting the amount, the payer has to authenticate himself again using the fingerprint. If the authentication is not successful, after a number of trials the transaction will be cancelled. If the payer successfully authenticates himself, then a SMS will be sent from the hardware module via GSM. The SMS contains 3 forms of information as follows: 1) Payer ID, 2) Payee ID and 3) the transaction amount. If the SMS is sent successfully, then a "Transaction Successful" message is displayed on the screen. Now there are dedicated server as SMS Gateway which are used in industry to handle the SMS commands and call web services as per the commands. They are highly efficient servers with higher throughput. For low-cost prototyping, an Android device can be used as a SMS Gateway. An Android Application that can read SMS and put the data to a Web service using GET method of Hypertext Transfer Protocol (HTTP) has been developed. The main functions of the application are the following: 1) To read the SMSs received on the mobile, 2) To separate the SMS in three part: Payee ID, Payer ID & transaction amount and 3) To put the data in a web service using HTTP GET request. **Fig. 10** highlights the steps between the payer and payee.

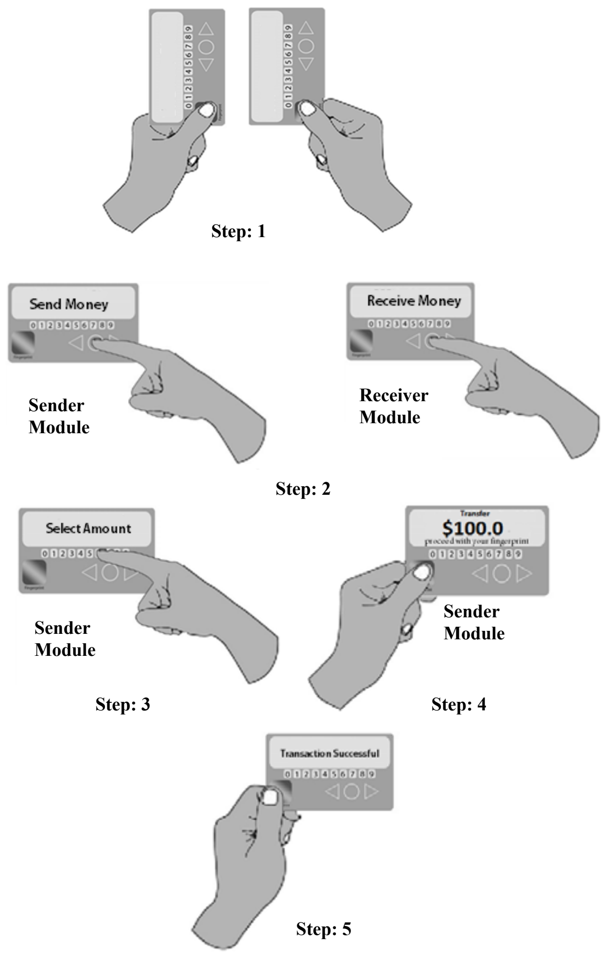

Fig. 10: Steps for Peer-to-Peer Money Transfer in Swing-Pay.

Upon receiving the data, the cloud server uses them to proceed with the transaction. The cloud server has the bank name and account number of both the Payer and the Payee. But the Cloud Server doesn't have the authority to access the Bank Server due to security reasons. The Cloud server sends the Payer Account Number, Payee Account details and the transaction amount to Payer's Bank Server using the bank's Application Programming Interface (API). Then the Payer's Bank transfers the money to the Payee account. Here, we are assuming that the Cloud server and the Bank has proper trust agreement between them. Without the proper Security and trust agreement, the bank will never allow any third party to request any service to the Bank Server. When the transaction is done, the Payee gets a confirmation SMS from the Cloud Server. The detailed steps of Payer Module and Payee Module have been presented in **Algorithm 1** and **Algorithm 2**. **Fig. 11** shows the flowchart of operation for Payer & Payee module.

Algorithm 1: Payer Module

Step 1: start
Step 2: get unique ID from the payee using NFC P2P
Step 3: enter the amount using the Capacitive Buttons
Step 4: authenticate using the fingerprint sensor
Step 5: if authentication is successful then
send transaction SMS to the SMS gateway
else if authentication is unsuccessful then
transaction declined
end if
Step 6: stop

Algorithm 2: Payee Module

Step 1: start
Step 2: select receive money option.
Step 3: authenticate using the fingerprint sensor
Step 4: if authentication is successful then
send the unique ID via NFC P2P.
else if authentication is unsuccessful then
transaction declined
end if
Step 5: stop

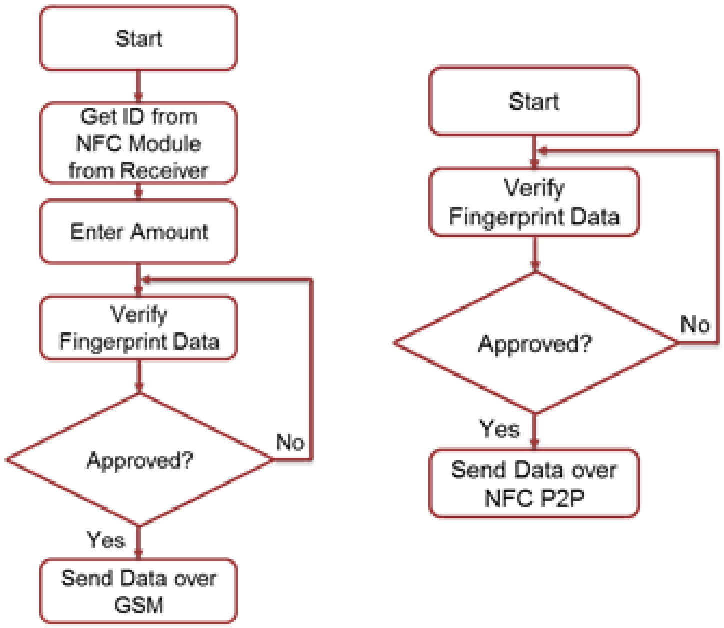

Fig. 11: Flow Chart of Algorithm 1 (Left) and Algorithm 2 (Right).

V. USE OF SWING-PAY FOR OTHER SERVICES: AN IDENTITY CARD EXAMPLE

In this Section the extension of Swing-Pay for use as virtual ID card is discussed. In a typical scenario, one can carry multiple cards including Voter ID card and Driving license. However, as all these always have to be physically carried, there is a chance to lose them. If any of these is lost, it requires a lot of time and official work to re-issue them. A solution as incorporated in Swing-Pay is the virtualization of the ID cards. At the time of registration, the scanned images of all the ID cards are stored in the cloud server against the unique ID given to the user. The images are also stored in the module in X-Bitmap or XBM format. The module sends a web service call via NFC P2P or NFC Beam, which contains the unique ID of the user and specific parameters to access any particular ID information.

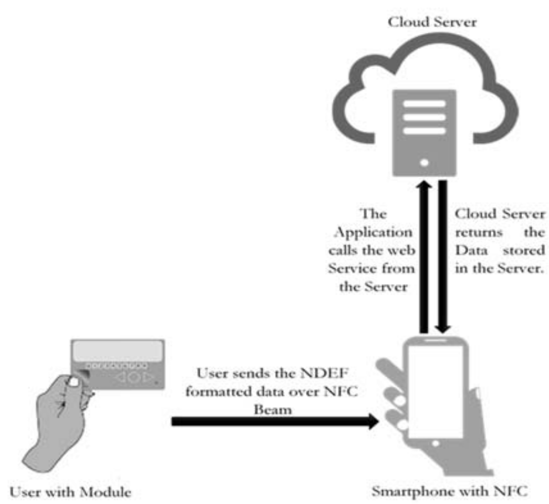

Fig. 12: Communication between the module, smartphone (As reader) and the Server.

To display the images from the server, a reader (or scanner) is required with NFC antenna. The reader may be a PC or a dedicated hardware. In our case we are using Android mobile with NFC to work as the reader. An App has been developed which has two contents in it: NFC Adapter and a Web View. The NFC adapter handles the message came from the module via NFC Beam and triggers the launch of the Application using Android's built in intent system. After launching the application, the Web View calls the web service to display the ID information. So, when the user need to present his ID card to any authority, he/she just selects the ID card he/she want to present from the proposed hardware module. After authentication using the fingerprint sensor, he taps the module on the reader device. Then the module automatically sends the information to the reader. The reader handles the message, calls the web service and displays the information. **Fig. 12** describes the process of how the data are fetched from the server and displayed in the Mobile App.

VI. Prototyping of a Swing-Pay

The whole system which reflects that it is working in P2P mode is shown in **Fig. 13**. For the main microcontroller board, we have chosen Arduino Due. The board is based on SAM3X8E from Atmel, which is based on ARM Cortex M3 architecture. It has 4 hardware serial ports, which are very useful as there are multiple modules that communicate with the host controller with Serial communication. Hardware serial is also reliable than the emulated software serial. Also the board works on 3.3Volt logic level. As most of the parts of our module works on the same logic level, an external logic level converter was not needed. For NFC peer to peer communication, Elecrow NFC shield has been used, which is based on PN532 NFC IC from Philips Semiconductor. PN532 is an integrated module for 13.56MHz band Contactless Communication with 80C51 microcontroller functionalities. It has ISO14443B, ISO 14443A / MIFARE® and FeliCa™ based Reader/Writer Mode (PN532/C1 Datasheet). It supports P2P mode to communicate with Android using LLCP. PN532 also has several communication protocol to interface it with host controller: Serial UART, I2C and SPI. For the proposed prototyping SPI is used to communicate with Arduino. The GSM module is Adafruit FONA, which is 850/900/1800/1900MHz Quad band Antenna. It can receive SMS messages and GPRS data. The module also has a circuit to recharge the connected battery from USB. A 500 mAh Lipoly Battery and a 3dBi sticker type GSM antenna via uFL connector are used. The FONA module is interfaced with Host controller over serial UART.

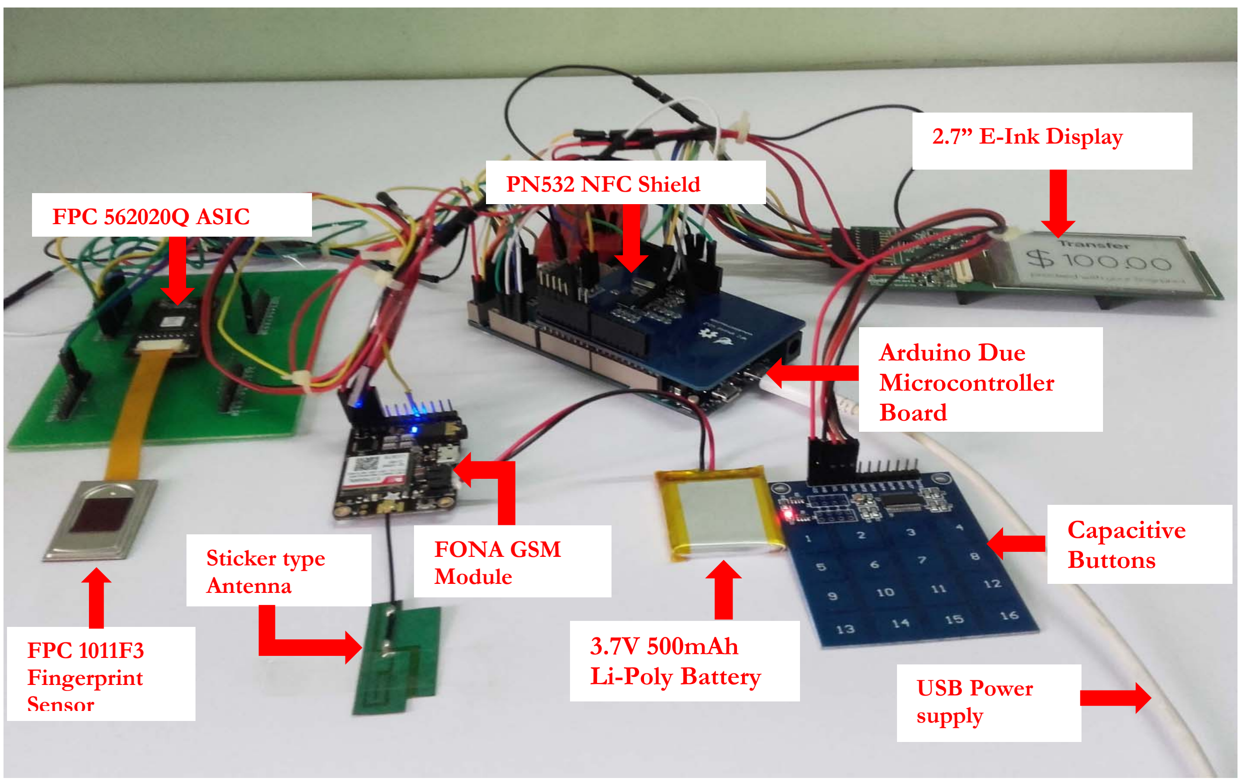

Fig. 13: Complete prototype with different components.

In the specific Swing-Pay prototyping, the fingerprint sensor FPC-AM3 has got 2 parts: FPC1011F3 Area Sensor and the FPC2020 ASIC processor. FPC1011F3 can scan virtually any fingerprint irrespective of dry or wet. It communicates with microcontroller using high speed SPI. FPC2020, which supports FPC1011F3, communicates with host controller via Serial UART or SPI. For the prototype, the Serial UART protocol is used as because unlike SPI, it does not requires polling request to read the sensor data. As the FPC2020Q has 1.27mm pitch male header, we have used a PCB, where it converts the 1.27mm pitch to 2.54mm pitch. Then, Arduino Board is directly interfaced using standard female jumper wires.

Fig. 14: The module working in Identity mode.

A 2.7” E-Ink display from RePaper has been used in the prototype Swing-Pay. It is an active matrix TFT with 264×176 resolution and communicates with Arduino over SPI protocol. It requires very little power to refresh the screen as it is Bi-stable. The E-ink display comes with an interfacing board which has 8Mb serial flash memory and a dedicated temperature sensor. We have connected the board with the In-circuit Serial Programming (ICSP) pins of the host controller using the female connectors. The Capacitive Buttons uses TTP229 IC to communicate with the host controller. TTP229 is interfaced with the host controller using the I2C protocol. It is also possible to interface 8 pins directly from the TTP229 board. The whole module is given power supply from the Arduino Board using a Breadboard. The Arduino board is powered from a PC. The proposed module is also successfully tested as identity virtualization using the developed android app as the possible reader (or scanner) of the card module. **Fig. 14** displays that, the module is working well in ID card mode too.

VII. CONCLUSIONS

A novel cashless module Swing-Pay has been presented for point-to-point transactions to eliminate all the constraints available in the state-of-the-art payment and some recently developed all-in-one payment card like Plastic and Stratos. A complete prototype of a digital card that can be utilized for any type of payment and identity needs has been discussed. Capacitive Fingerprint sensor is employed to increase the security of the card. The libraries available for the E-Ink Display are successfully ported for Arduino-Due target and the e-paper display runs successfully on it. The 16 channel capacitive button module, TTP229, is also interfaced along with the FONA GSM module. Upon successful fingerprint authentication, the module sends an SMS via GSM to cloud with the full details of Payer, Payees and transaction amount in a particular format. To receive the SMS and to pass the data to the cloud sever for the transaction to happen, we have also developed an Android application. In ID virtualization mode, another application is developed again to receive the web service call and display the data received from the server. An appropriate Web API has been made to receive the data from the application and make the transaction. All the data are stored in a server using proper encryption algorithms like SHA and MD5. NFC based P2P transaction and Identity virtualization are successfully tested on our module.

Though the prototype is working properly, further development is needed to make it a commercial product. The magnetic stripe and EMV chip should be included in the module so as to be used everywhere like any traditional payment cards. It is also planned to include a highly efficient paper battery as an external power source of the card to avoid all the constraints in portability. The proposed digital card may have a numerous applications in near future. The possible future applications could be: P2P money transfer, Identity Card virtualization, Point-of-sale payments, conventional debit or credit card and access control. It may also be used as virtual gift card used in shopping mall, ticketing system, Library Management and transit access etc. **Fig. 15** shows a few present and future application of the proposed module.

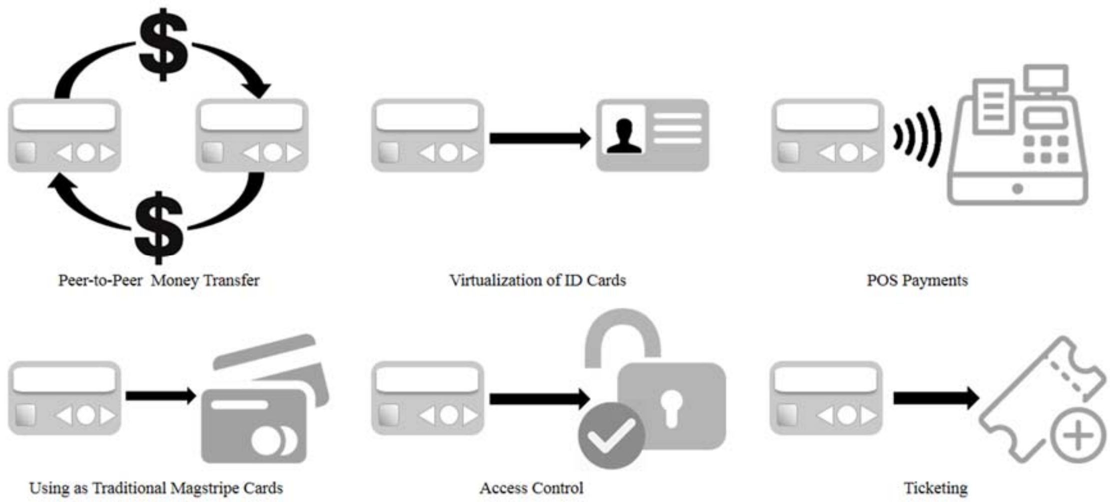

Fig. 15: Applications perspectives of the proposed Swing-Pay card.

ACKNOWLEDGEMENT

A selected co-authors are thankful to the Department of Electronics and Information Technology (DEITY), 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

Shirsha Ghosh (shirshatit@gmail.com) received his Masters 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, Internet of Things.

Joyeeta Goswami (joyeetatit@gmail.com) received her masters 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 NFC and Li-Fi.

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.

Abhishek Kumar **(**ak9990566501@gmail.com) received his bachelors degree in Electronics & Communication Engineering from the National Institute of Technology, Arunachal Pradesh, in 2016. He has received Gold Medal for best Hardware project within the institute. He is a co-founder of Bluesole Technologies Pvt. Ltd New Delhi, India and working as Chief Operating Officer in the same organization. His interest includes in IoT based Real Life Applications and System Design.

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 IAA award given by the founders of Intel Corporation Dr. Andy Grove and Dr. Gordon Moore.

REFERENCES

[1] M. Baddeley. (2004). Using e-cash in the new economy: An economic analysis of micro-payment systems. *Journal of Electronic Commerce Research,* 5(4), pp. 239-253. Available: http://web.csulb.edu/journals/jecr/issues/20044/Paper3.pdf

[2] B. Meng, and Q. Xiong. "Research on electronic payment model," in *Proc*. *The 8th International Conference on Computer Supported Cooperative Work in Design*, 2004, pp. 597 - 602.

[3] N. Asokan, "Fairness in Electronic Commerce", Ph.D. dissertation, Dept. Computer Science, University of Waterloo, Ontario, Canada, 1998

[4] S. Singh, "Emergence of payment systems in the age of electronic commerce: The state of art." in *Proc. AH-ICI* 2009, pp. 1-18.

[5] C Merritt, "Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments" Federal Reserve Bank of Atlanta. Aug. 2010.

[6] COMPASS PLUS Corp., Nottingham, UK. *White Paper Mobile Banking: One Size Doesn't Fit All*. [Online]. Available: http://www.compassplus.com/collateral/whitepapers/336

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

[8] B. Gates and M. Gates, "Mobile Banking Will Help the Poor Transform Their Lives," [Online]. Available: https://www.gatesnotes.com/2015-Annual-Letter?page=3&lang=en.

[9] R. Boden, "Wearable smart stamp to support NFC payments," [Online]. Available: http://www.nfcworld.com/2016/04/18/344048/wearable-smart-stamp-support-nfc-payments/, 2016.

[10] Charles A. Walton, "Portable radio frequency emitting identifier" U.S. Patent 4 3842 88, Dec.30, 1980.

[11] BARCLAYCARD Corp., Northampton, UK, "Hands off: a short history of contactless technology," [Online]. Available: http://www.home.barclaycard/news/contactless-timeline.html, Dec. 2014.

[12] T. Yorozu, M. Hirano, K. Oka, and Y. Tagawa. (1987). Electron spectroscopy studies on magneto-optical media and plastic substrate interface. *IEEE Translation Journal on Magnetics* in Japan 8(2): 740-741.

[13] 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

[14] NFC FORUM. [Online]. Available: http://nfc-forum.org/what-is-nfc/what-itdoes/.

[15] M. Hamblen, "A short history of NFC," [Online]. Available: http://www.computerworld.com/article/2493888/mobile-payments/a-short-history-of-nfc.html, Dec. 2012.

[16] R. Arnfield, "Mobile Wallets 101", [Online] Available: https://lists.w3.org/Archives/Public/public-webpayments-ig/2015Oct/att-0026/cardlinx_guide_final.pdf, 2015.

[17] G. Wallner, "System and method for a baseband nearfield magentic stripe data transmitter" U.S. Patent 8 628 012, Feb.17, 2014.

[18] L. Savvides, "Samsung Pay: What you need to know (FAQ)", [Online]. Available: http://www.cnet.com/news/samsung-pay-what-you-need-to-know-faq/

[19] R. Boden, "Mobile payments will overtake cards and cash by 2025, says UK retailer", [Online]. Available:http://www.nfcworld.com/2016/04/19/344092/mobile-payments-will-overtake-cards-cash-2025-says-uk-retailer, 2016.

[20] ACCENTURE. "North America Consumer Digital Payments Survey When it comes to payments today, the customer rules". [Online]. Available: https://www.accenture.com/t20151021T165757__w__/us-en/_acnmedia/Accenture/next-gen/na-payment-survey/pdfs/Accenture-Digital-Payments-Survey-North-America-Accenture-Executive-Summary.pdf, 2015.

[21] ACCENTURE, "Mobile Payments Survey Insights: DRIVING VALUE AND ADOPTION CONSUMERS WANT MORE!",[Online]. Available :https://www.accenture.com/in-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_5/Accenture-Mobile-Payment-Infographic.pdf

[22] TSYS. "Consumer Payments Study", [Online], Available: http://tsys.com/Assets/TSYS/downloads/rs_2014-consumer-payments-study.pdf. 2014.

[23] Kevin Cash, "Stratos, Coin, Plastc, Swyp: Sizing Up Multi-Account Cards", [Online]. Available: https://www.nerdwallet.com/blog/credit-cards/stratos-coin-plastc-swyp-sizing-multiaccount-cards/. 2015.

[24] CITI Bank. "CITI Cards Consumer Perspective Study". July 2016

[25] PAYMENTS CARDS AND MOBILE, "Asia pacific Study of digital Payment Adoption", [Online] Available: http://www.paymentscardsandmobile.com/asia-pacific-study-of-digital-payment-adoption/

[26] E. Hubinak, M. Florek and M. Masaryk, "Systems and Methods for Contactless Payment Authorization" U.S. Patent 8 275 364, Dec.30, 2008.
[27] G. Gormley, W. Wang, R. Buck, V. Goulart, J. Gough, B. Brindle, P. Carney and P S. T. Chow, "Data exchange initiated by tapping devices" U.S. Patent 8 565 676, Jun.24,2011.
[28] S. Clark, "Stanford researchers develop first Android NFC P2P apps", [Online]. Available: http://www.nfcworld.com/2011/01/31/35785/stanford-researchers-develop-first-android-nfc-p2p-apps/, 2011.
[29] *Simple NDEF Exchange Protocol Technical Specification,* NFC Forum™ SNEP 1.0, 2011.
[30] A. Lotito, D. Mazzocchi. "OPEN- NPP: An Open Source Library to Enable P2P over NFC", in *Proc. of 4th International Workshop on Near Field Communication*, 2012, pp. 57-62.
[31] S. Burkard, "Near Field Communication in Smartphones," [Online]. Available: https://www.snet.tu-berlin.de/fileadmin/fg220/courses/WS1112/snet-project/nfc-in-smartphones_burkard.pdf.
[32] B. Dodson, H. Bojinov, M. S. Lam, "Touch and Run with Near Field Communication (NFC)", Computer Science Department, Stanford Univ., Stanford, CA.
[33] D.M. Monteiro, J.J.P.C. Rodrigues, J. Lloret, "A Secure NFC Application for Credit Transfer Among Mobile Phones", in *Proc. of CITS*, 2012, pp. 1- 5.
[34] R.S. Basyari, R. Saefulloh, S.M. Nasution, and B. Dirgantara. "Implementation of host card emulation mode over Android smartphone as alternative ISO 14443A for Arduino NFC shield" *in Proc. of ICCEREC*, 2015, pp. 160-165.
[35] W. Chen, G. P. Hancke, K. E. Mayes, Y.Lien, and J. H. Chiu., "NFC mobile transactions and authentication based on GSM network,". *in Porc. of Second International Workshop on Near Field Communication*, 2010 (pp. 83-89).
[36] U. Mardikar and E. Duprat, "Biometric Authentication of Mobile Financial Transactions by Trusted Service Managers", U.S. Patent 0 173 434, Mar.12, 2012.
[37] Chiao-Li Lin, "Composite chip card with a security protection interface and a method for controlling the same", U.S. Patent 8 167 201, May.1,2012.
[38] A. Hammad and P. Dixon, "Mobile payment device" U.S. Patent 8 827 156, Sep.9, 2014.
[39] J. C. Goldman, D. A. Auten, C. P. Leon, "Electronic Card with a Programmable Magnetic Stripe" U.S. Patent 8 910 879, Dec.16, 2014.
[40] MASTERCARD, London, UK, "MasterCard and Zwipe Announce the Launch of the World's First Biometric Contactless Payment Card with Integrated Fingerprint Sensor", [Online.] Available: http://newsroom.mastercard.com/press-releases/mastercard-zwipe-announce-launch-worlds-first-biometric-contactless-payment-card-integrated-fingerprint-sensor/, Oct. 17, 2014.
[41] A. Majumder, B.K. Bhattacharyya, S. Ghosh, J. Goswami, "A Digital Card serving Identity and Payment Purpose", filed as Indian Patent at IPO Kolkata, Application No. 201631004666, 10th February 2016.
[42] ARDUINO LLC, "Arduino Due Documentation" [Online]. Available: https://www.arduino.cc/en/Main/ArduinoBoardDue
[43] ELECROW, "NFC Sheild" [Online]. Available: http://www.elecrow.com/wiki/index.php?title=NFC_Shield.
[44] FINGERPRINTS CARDS, Göteborg, Sweden, "FPC-AM3 Product Sheet," [Online] Available: http://www.fingerprints.com/wp-content/uploads/2013/07/FPC-AM3-product-sheet1.pdf.
[45] ADAFRUIT INDUSTRIES, New York, NY, "Repaper 2.7" Graphic E-Ink Development Board" [Online]. Available: https://www.adafruit.com/product/1346.
[46] E Ink Corp, Billerica, MA, "Ink Technology". [Online]. Available: http://www.eink.com/technology.html.
[47] ADAFRUIT INDUSTRIES, New York, NY, "FONA" [Online] Available: https://www.adafruit.com/product/2542
[48] TEXAS INSTRUMENTS, Dallas, TX, "FDC1004: Basics of Capacitive Sensing and Applications", [Online]. Available: www.ti.com/lit/an/snoa927/snoa927.pdf, 2014.