Swing-Pay: One Card Meets All User Payment and Identity Needs

A digital card module that uses NFC and biometric authentication for peer-to-peer payment and identity.

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

©ISTOCKPHOTO/ASKOLD ROMANOV

Advancement in payment technologies has an important impact on one's quality of life. Emerging payment technologies create both opportunities and challenges for the future. Being a quick and convenient process, contactless payment gained momentum, especially with merchants, with throughput being the main parameter. However, it poses risks to issuers, as no robust customer verification method is available. Thus, efforts have been underway 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 obstacles in business.

This article presents an approach and module by which one card can communicate with another using near-field communication (NFC) technology to digitally transfer money from the payer's bank to the payee's bank. This approach eliminates the need for physical cash and also serves all types of payment and identity needs. Embodiments of this approach furnish a medium for cashless card-to-card transactions. The module, which is called Swing-Pay, communicates with a bank via global systems for mobile communication (GSM). The security of this module is intensified using biometric authentication.

We also present an app on the Android platform, which works as a scanner of the proposed module to read the identity details of the card owner. A prototype of a digital card is also detailed. This card can also be used as a virtual identity (ID) card, accumulating the information of all ID cards, including an electronic passport, voter ID, and driver's license.

ELECTRONIC PAYMENTS: A HISTORIC PERSPECTIVE

Although the digital payment process has been operational since the 1960s, with the advancement of technology and

Digital Object Identifier 10.1109/MCE.2016.2614522
Date of publication: 14 December 2016

2162-2248/17©2017IEEE

e-commerce evolution, digital cashless payments have become mainstream [1]. Due to the relentless effort of the research community, several electronic payment models, such as the JW model and the N. Asokan model, have been devised. The JW model is the traditional payment system, where both sellers and buyers need some sort of involvement in a particular transaction to take 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 are not involved in any transaction (Figure 1) [3]. The "3e model," which is based on the N. Asokan model, included credit card, electronic cash, and electronic check payment models [2]; however, the credit card is the most widely used electronic payment mechanism [4]. With the goal of instantly transferring money between two peers, the concept of electronic fund transfer through the Internet developed. Many possible solutions, like wire transfer and ATM networks, have been developed to support this goal (Figure 2).

Many popular and fast frameworks are available to fulfill international money transfers. Using crypto currencies like Bitcoin and Litecoin, one can transfer money to anyone in the world in the blink of an eye. But there is no central organization to monitor 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, operating systems such as Android and iOS have become popular. Peer-to-peer (P2P) money transfers have moved to the next stage of development with the concept of mobile wallets and mobile banking, which offer features including bill payment, money transfers and withdrawals, ticket booking, mobile recharges, and P2P money transfers [5].

In 1977, Merita Bank introduced the first mobile banking service in Finland using a short message service (SMS) [6], which allowed people fast and easy access to their banking facilities; it has been observed that 50% people use mobile phones, but only 37% have

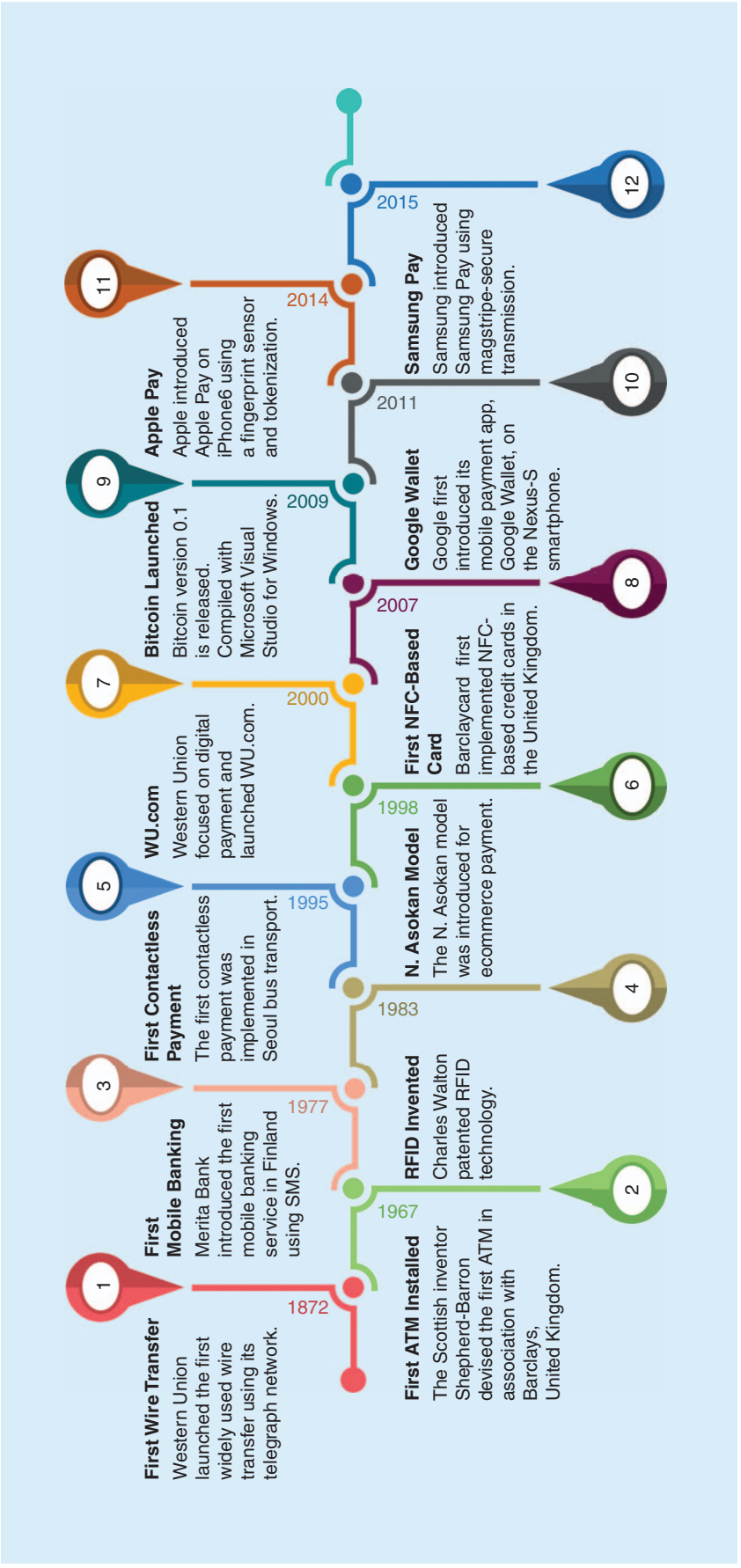

FIGURE 1. The chronology of digital payment system development, from the JW model to Samsung Pay.

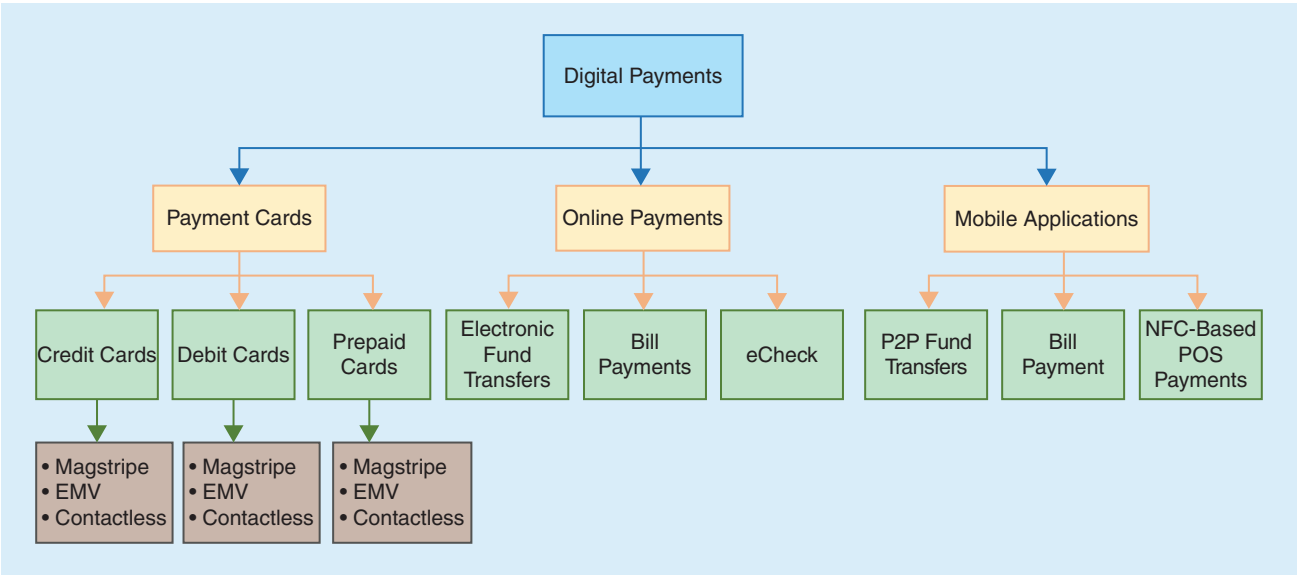

FIGURE 2. An overview of the different digital payment systems.

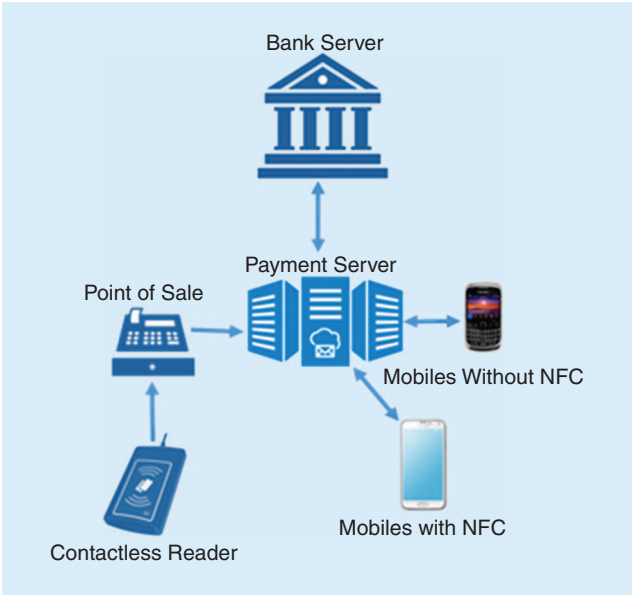

FIGURE 3. A block diagram of the NFC-based payment mode.

mobile banking access [7]. The need for and advantages of mobile banking have been studied [8]. Many smartphone apps are available from finance companies with which one can pay anyone in the world at any time. But with increasing usage, they became easy prey for hackers, who often succeeded in carrying out fraudulent transactions. Additionally, an ultrathin, stretchable stamp is available that can be worn on the skin and used for payment when connected with a smartphone [9].

ALONG COMES NFC AND RFID

With the invention of radio-frequency identification (RFID) technology in 1983 by Charles Walton, a new method was developed, known as contactless payment (Figure 3) [10]. In 1995, the first contactless payment was implemented by Seoul bus transport [11], followed by Speedpass in 1997 to pay fuel charges at U.S. gas stations. In 2007, Barclaycard first implemented NFC-based credit cards in the United Kingdom [11]. NFC is the successor of RFID, which uses 13.56-MHz frequency to communicate within an extremely short range (closer than 10 cm). NFC has three modes of communication: reader-writer, P2P, and card emulation. 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 P2P mode, two NFC-enabled devices communicate between each other to either share a small amount of 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].

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 uses a pass code at the point of sale (POS) terminal, which supports the contactless payment. Google also provided a Google Wallet card, which is linked with Google Wallet and can be used virtually anywhere. To make the transactions more secure, several schemes have been developed using industry-standard protocols, such as tokenization and point-to-point encryption. In the tokenization scheme, the actual credit or debit card information is replaced by one-time use tokens. The token can only be identified and decrypted by the tokenization server. In point-to-point encryption, all the data are encrypted until they are processed and decrypted only when they arrive at the secure environment of the point-to-point encryption [16].

In October 2014, Apple Pay was introduced [16]. Apple Pay devices have NFC antennas built into them for communication with the POS terminal. Although Apple Pay uses the built-in fingerprint scanner to authenticate the user, it does not use the tokenization scheme to secure the credit or debit card information (Figure 4). Yet another system, the magnetic secure transmission, 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 transactions in retail shops will be made by mobile payments by the year 2025 [19].

BY THE NUMBERS

Although there have been huge advancements in payment technology, their acceptance by customers is unsatisfactory. There are many factors 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 found that, among existing systems, 16% of people prefer digital payment, whereas a whopping 67% of people are still partial to cash; debit cards have an acceptance rate of 59%, and 50% of people rely on credit cards. There also does not seem to be much excitement for contactless payment technologies; only 5–6% of those surveyed feel they would use a digital payment method by 2020 [20]. The acceptance rates of different payment mediums are presented in Figure 5.

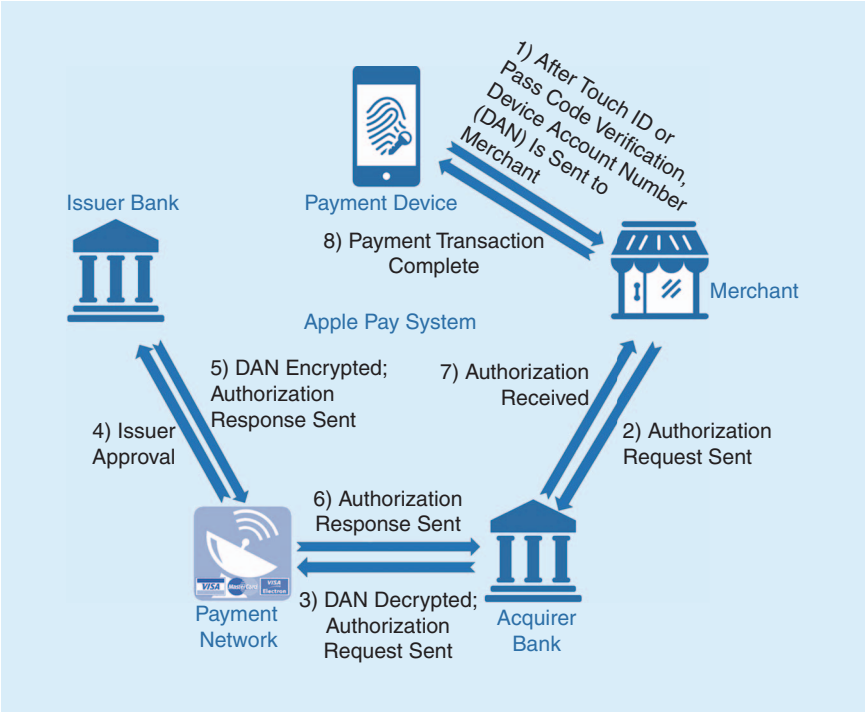

FIGURE 4. An illustration of the Apple Pay system.

A survey found that, among several payment technologies, the debit card is the most popular, preferred by 43% of those surveyed, while credit cards are the second choice, preferred by 35% of respondents [22]. As people are more comfortable using debit or credit cards, many companies have digitized the payment cards and incorporated several cards in a single product. Stratos, Coin, and Plastic cards can load up to three cards, eight 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.

One of the many reasons for this resistance is security, which was mentioned by 45% of those surveyed. However, the most important barrier seems to be that consumers don't like to switch technologies; 97% of people refused to buy a new device to support mobile payments [21]. The likelihood that people would use mobile payment apps was also found to be low on a consumer perspective study conducted in 2016; only 5% people stated that they would be willing to use a mobile payment app. The detailed scenario is shown in Figure 6 [24].

The main issue with mobile payment methods seems to be that they all rely on high-budget smartphones, which are expensive. In countries where very few people can afford them, it is challenging to gain support for mobile banking. It is estimated that 73% of people use mobile phones in India, and it is becoming the second largest market for smartphones. Due to significant innovations in the technology, 40% of smartphone users in India have a mobile wallet [25]. It was also found that 74% of people intended to use

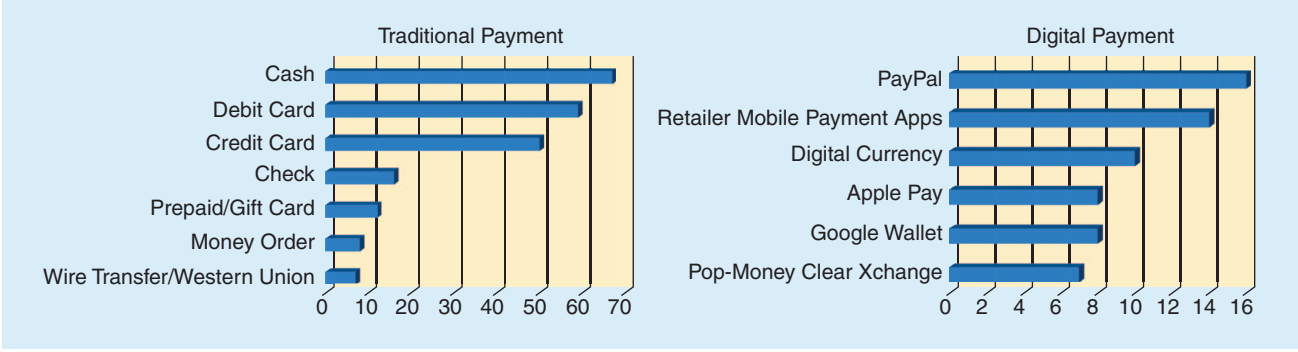

FIGURE 5. The acceptance rates of current payment systems.

Table 1. Payment versatility and the cost of digital payment cards.

Card Name	Magstripe	EMV	NFC	Price
STRATOS	✔	✖	✖	US$95 yearly
COIN 2.0	✔	✖	✔	US$99 up front
SWYP	✔	✔	✖	US$99 up front
PLASTC	✔	✔	✔	US$180 for 18 months

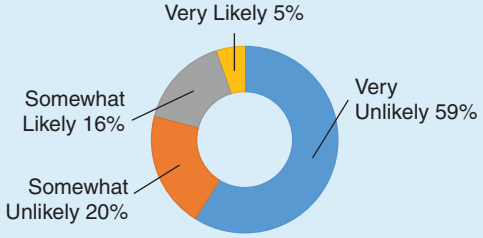

FIGURE 6. The percentage of users interested in using a mobile payment app within the next 12 months [24].

mobile wallets in emerging markets, while that number drops to only 46% in the developed market [25].

From the prior discussion, 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.

ELECTRONIC PAYMENTS: STATE-OF-THE-ART RESEARCH

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

A method to secure contactless payment using high-level cryptography with a passive identifier is available [26]. Again, a way to initiate the establishment of a radio link using enhanced data rates for GSM evolution, a general packet radio service (GPRS), or GSM is proposed just by tapping two devices [27]. Although tapping is a very intuitive procedure for

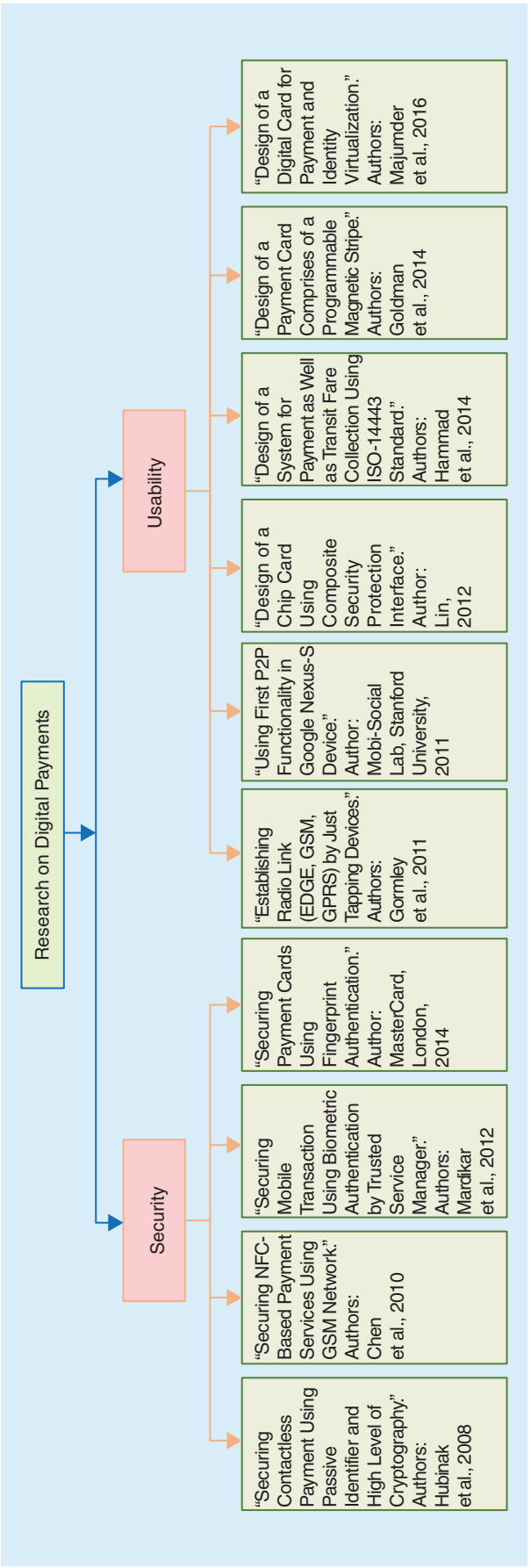

FIGURE 7. A summary of research into digital payment systems.

starting the communication of data, it may lead to a problem if devices are tapped unintentionally.

The inventors have also proposed a way to gather group data using NFC. Enhanced versions of NFC, when it was launched by Google on the Nexus-S device in 2011, were also explored. Mobi-Social Lab of Stanford developed an app that uses the P2P functionality of the Nexus-S [28]. NFC Forum standardized a protocol to communicate between two active NFC devices using P2P functionality, known as simple NFC data exchange format (NDEF) 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 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].

Dodson et al. designed a gaming app that uses NFC for loading different applications while the gaming session continues to run over another channel [32]. Monteiro et al. uses the NFC P2P mode to establish communication between two mobile phones using Bluetooth. After establishing communication, the credit is transferred from one subscriber identification module (SIM) to another [33]. This system is innovative and targets credit transfer only between two SIM cards. It's not a general money transfer system. The Host Card Emulation Mode of the International Organization for Standardization (ISO) 14443A smartcard standard is also implemented on Arduino-based microcontrollers and communicated with the Android smartphone [34].

To make mobile payment more secure, researchers also explored the use of the current GSM network to authenticate NFC-based mobile payments [35]. A system has been devised in which financial transactions are conducted at any POS and validated using a trusted service manager [36]. The inventors are focusing on smartphones with built-in fingerprint scanners to employ the biometric trait of the user in place of a personal identification number 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 the 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 a fingerprint scanner.

The design of a chip card with a security protection interface and a method to control the same is available [37]. The card comprises 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 including issuance of the chip card by the chip card, triggering the security interface, and execution of a contactless transaction.

> In 1995, the first contactless payment was implemented by Seoul bus transport, followed by Speedpass in 1997 to pay fuel charges at U.S. gas stations.

The design of a system for facilitating payment as well as transit fare collection using ISO 14443 standards for contactless communication is discussed in the literature [38]. This product also needs a separate smartphone device to function. So a standalone device is required that can handle all these payment needs without a mobile phone. A multipurpose digital card has been devised that 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, a person would have to give a pass code using the buttons. In 2014, MasterCard and Zwipe announced their first payment card with a built-in fingerprint scanner and NFC [40]. This feature is very favorable for the user but is limited to Europay, MasterCard, Visa (EMV), and contactless terminals; therefore, it cannot be used for person-to-person transactions. In 2016, a new NFC-based digital card was created that serves both payment and identity needs [41].

THE PROPOSED MODULE

In this section, a device module, Swing-Pay, is proposed that is envisioned to meet nearly all forms of payments. The

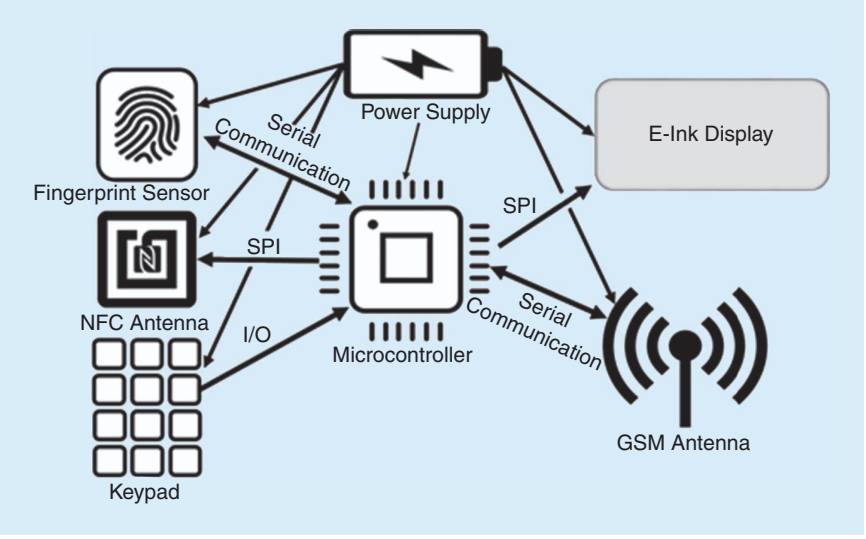

FIGURE 8. A block diagram of the proposed novel digital card module, Swing-Pay.

To make mobile payment more secure, researchers also explored the use of the current GSM network to authenticate NFC-based mobile payments.

Swing-Pay module comprises the following components (Figure 8): 1) microcontroller, 2) NFC module, 3) fingerprint sensor, 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 central-processing unit, four hardware serial ports, extended serial peripheral interface (SPI) support, and 512-kB static random-access memory (SRAM) [42]. Out of all the NFC modules available on the market, an Elecrow NFC shield was chosen because it supports ISO14443 Type A and Type B protocols as well as P2P communication [43]. For the fingerprint sensor, a capacitive fingerprint sensor (FPC-AM3) was chosen from Fingerprint Cards, Sweden [44]. This module has two parts: an FPC1011F3 area sensor and the FPC2020 processor. FPC1011F3 is a complementary metal–oxide–semiconductor fingerprint sensor, which takes an image with 256 grayscale values per pixel. FPC562020 is a power-efficient ASIC that communicates with FPC1011F3 using an SPI bus. It also stores fingerprint data on external flash memory for later verification.

To reduce the energy consumption of the Swing-Pay module, an e-Ink display from Pervasive Displays has been used. This 2.7-in display has 264 × 176 resolution with 117 dpi [45]. E-Ink displays are bistable, which means that they 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 particles and white particles, which 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 move to the top [46]. There was no library available to support the Arduino Due platform. Adafruit has a library, which will only compile for AVR-based Arduino boards, Rapberry-Pi and MSP430. Also, 2.7-in displays can only display static images on AVR-based Arduino boards because printing dynamic images and texts requires higher SRAM capacity. The library has been modified by adding some required arguments so that it can compile on the Arduino Due target, which is based on SAM3X8E.

For the GSM modem, Adafruit FONA was chosen due to its small size and higher capabilities. This module uses a SIM800 cellular module and can perform all types of cellular functions [47]. A sticker-type 3-dBi GSM quad-band antenna is also used with uFL connections and a 3.7-V, 500-mAh lithium-ion battery with the GSM module. A specific case, a TTP229 capacitive touch sensor module, is used for the capacitive buttons. The capacitive buttons work on 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 toward 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 the I2C interface.

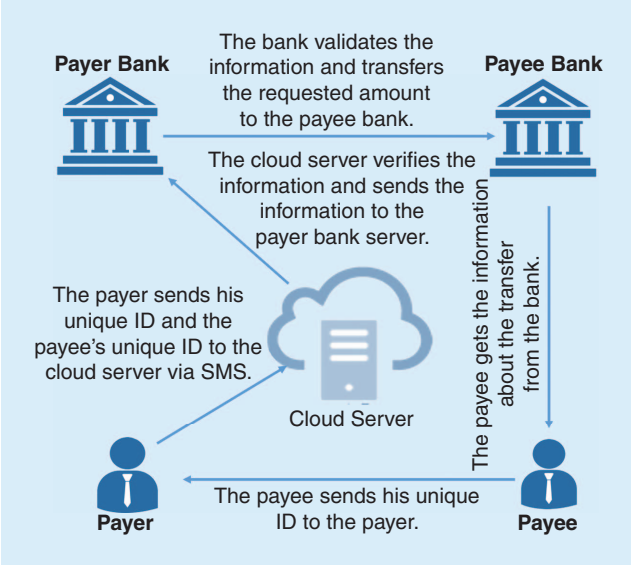

FIGURE 9. The communication flow for a P2P money transfer in Swing-Pay.

P2P MONEY TRANSFER USING SWING-PAY

In the protocol of Swing-Pay, money from the payer's bank account is transferred to the payee's bank account. The Swing-Pay has three role players in the system: 1) the hardware module, 2) the cloud server, and 3) the bank. The hardware module communicates with 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 and will be given a unique ID from the server at this time. All of the user's information, such as the bank name, account number, and routing number, will be stored in a registered account in an encrypted format. At the time of registration, the ownership information given by the customer is also validated using a one-time password. 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 the NFC module and Android Mobile using SNEP and LLCP protocols. For the prototyped Swing-Pay, the library is tweaked so that two Arduino modules can communicate with each other. The communication flow of Swing-Pay is illustrated in Figure 9.

In the Swing-Pay framework, the payee activates his card using his fingerprint. If the fingerprint is authenticated, then the card is activated. After that, the payer selects the Pay Money mode and the payee selects the 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 would be blocked. When the payer gets the payee's 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 an SMS will be sent from the hardware module via GSM.

The SMS contains three forms of information: 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. There are dedicated servers as SMS gateways that 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 an SMS gateway. An Android application that can read SMS and put the data to a web service using the 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 parts: payee ID, payer ID, and transaction amount; and 3) to put the data in a web service using an HTTP GET request. Figure 10 highlights the steps between the payer and payee.

Upon receiving the data, the cloud server uses it 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. The cloud server sends the payer's account number, the payee's account details, and the transaction amount to the payer's bank server using the bank's application programming interface (API). Then the payer's bank transfers the money to the payee's account. Here, we are assuming that the cloud server and the bank have a proper trust agreement between them. Without the proper security and trust agreement, the bank will never allow any third party to request service to the bank server. When the transaction is complete, the payee gets a confirmation SMS from the cloud server. The detailed steps of the Payer Module and Payee Module have been presented in Algorithm 1 and Algorithm 2. Figure 11 shows the flowchart of operation for both of these modules.

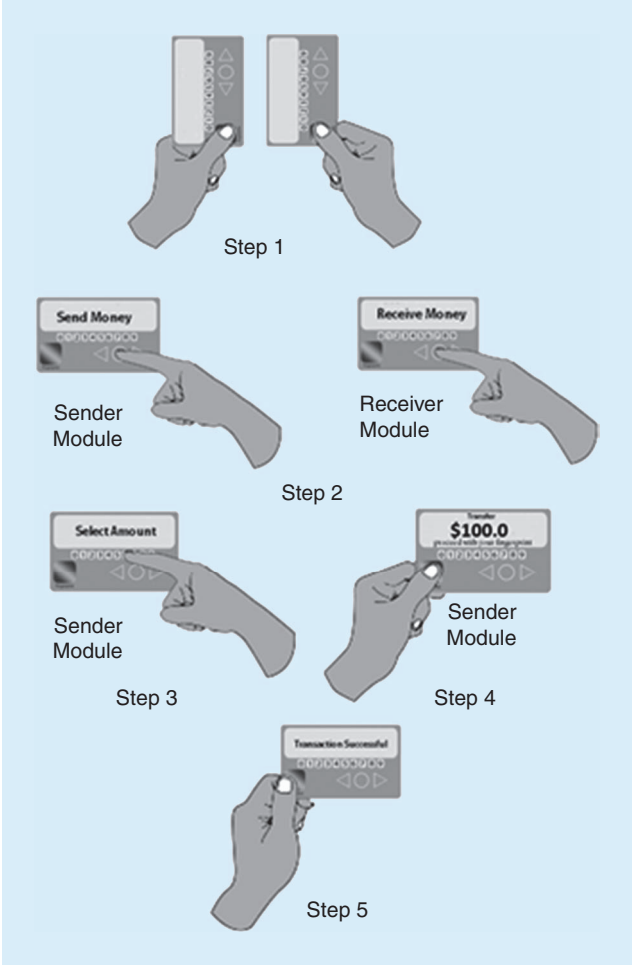

FIGURE 10. The steps for a P2P money transfer in Swing-Pay.

USE OF SWING-PAY FOR OTHER SERVICES

Typically, people carry multiple identification cards, including a voter ID card and a driver's license. However, as all of these

Algorithm 1: The 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: The 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

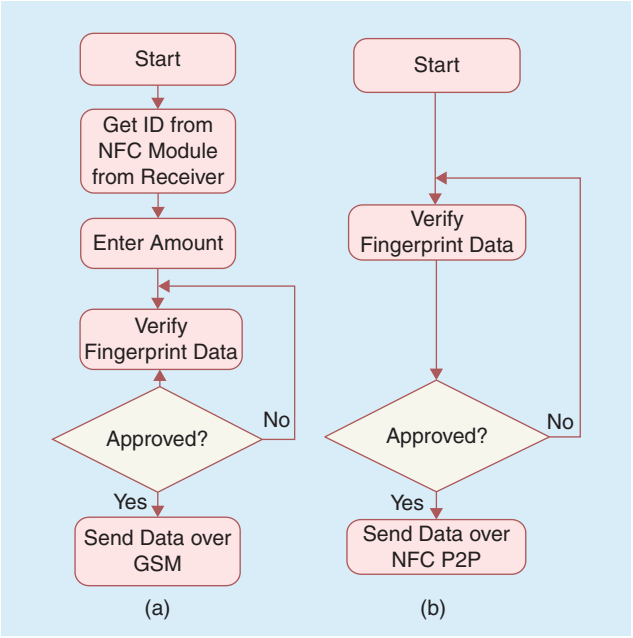

FIGURE 11. The flowcharts for (a) Algorithm 1 and (b) Algorithm 2.

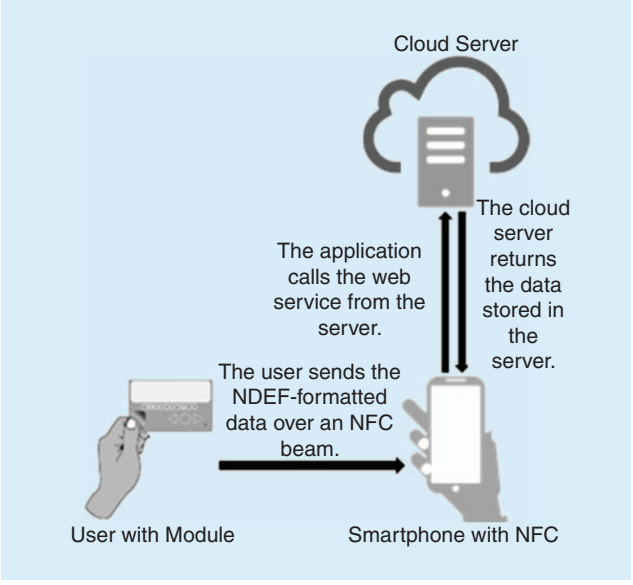

FIGURE 12. The communication between the module, the smartphone (as a reader), and the server.

options have to be physically carried, there is always the risk that they may be lost, and replacing them requires a lot of time and effort. A solution to this problem is the virtualization of the ID cards; this solution is incorporated in Swing-Pay. At the time of registration, the scanned images of all 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 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.

To display the images from the server, a reader (or scanner) is required with an NFC antenna. The reader may be a PC or other dedicated hardware. In our case, we are using Android mobile with NFC to work as the reader. An app has been developed that has two components in it: an NFC adapter and a web view. The NFC adapter handles the message 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 needs to present his ID card to any authority, he just selects the ID card he wants 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. Figure 12 describes the process of how the data are fetched from the server and displayed in the mobile app.

PROTOTYPING SWING-PAY

The whole system that reflects that Swing-Pay is working in P2P mode is shown in Figure 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 four 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 more reliable than the emulated software serial. Also, the board works on a 3.3-V logic level. As most of the parts of our module work on the same logic level, an external logic level converter was not needed. For NFC P2P communication, an Elecrow NFC shield has been used, which is based on PN532 NFC IC from Philips Semiconductor. PN532 is an integrated module for the 13.56-MHz band contactless communication with 80C51 microcontroller functionalities. It has ISO14443B, ISO 14443A/MIFARE, and FeliCa-based reader/writer mode (PN532/C1 data sheet). It supports P2P mode to communicate with Android using LLCP. PN532 also has several communication protocol to interface it with host controller: Serial universal asynchronous receiver/transmitter (UART), I2C, and SPI.

For the proposed prototyping, SPI is used to communicate with Arduino. The GSM module is Adafruit FONA, which is an 850/900/1800/1900-MHz quad-band antenna. It can receive SMS messages and GPRS data. The module also has a circuit to recharge the connected battery from a USB. A 500-mAh lithium-polymer battery and a 3-dBi sticker-type GSM antenna via a uFL connector were used. The FONA module is interfaced with a host controller over serial UART.

In the Swing-Pay prototype, the fingerprint sensor FPC-AM3 has two parts: the FPC1011F3 area sensor and the FPC2020 ASIC processor. FPC1011F3 can scan virtually any fingerprint, whether dry or wet. It communicates with the microcontroller using high-speed SPI. FPC2020, which supports FPC1011F3, communicates with the host controller via serial UART or SPI. For the prototype, the serial UART protocol is used because unlike SPI, it does not require polling requests to read the sensor data. As the FPC2020Q has a 1.27-mm pitch male header, we have used a PCB, where it converts the

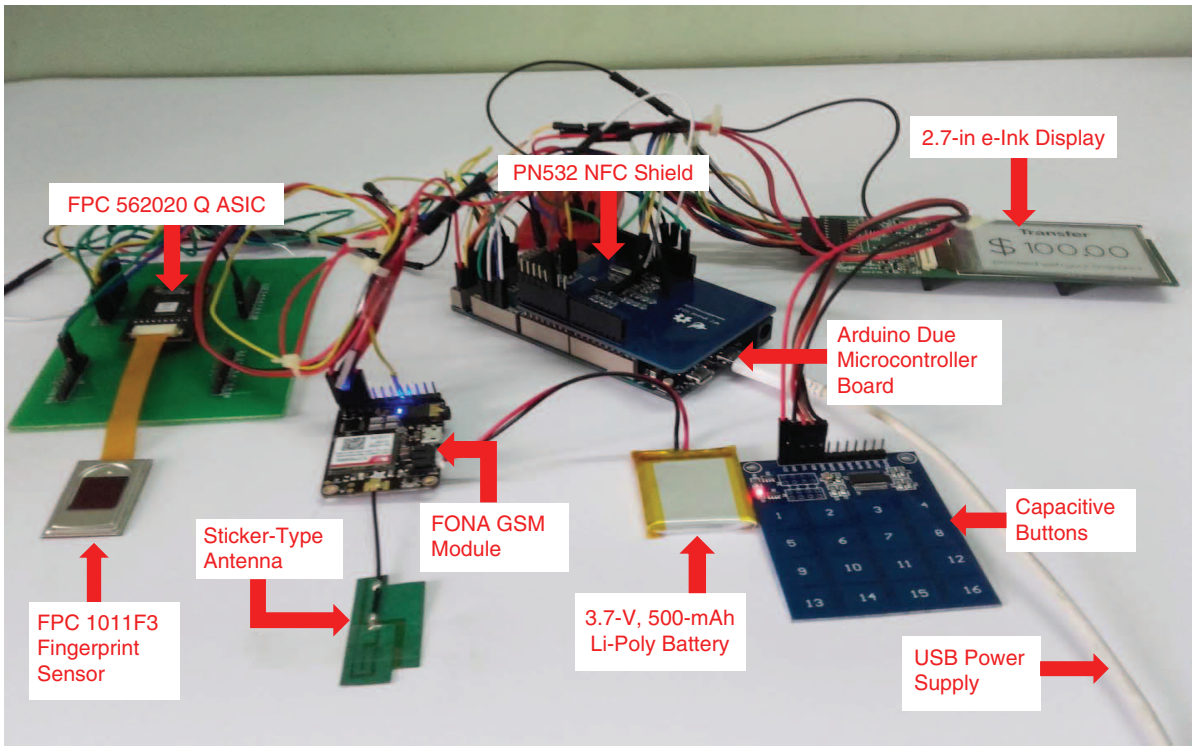

FIGURE 13. A complete prototype with different components.

FIGURE 14. The module working in Identity mode.

1.27-mm pitch to a 2.54-mm pitch. Then the Arduino board is directly interfaced using standard female jumper wires.

A 2.7-in 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 bistable. The e-Ink display comes with an interfacing board that has 8 Mb of serial flash memory and a dedicated temperature sensor. We have connected the board with the in-circuit serial programming pins of the host controller using the female connectors. The capacitive buttons use 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 eight pins directly from the TTP229 board. The whole module is provided power by the Arduino board using a breadboard. The Arduino board is powered from a PC. The proposed module also successfully tested as identity virtualization using the developed Android app as the possible reader (or scanner) of the card module. Figure 14 displays that the module works well in ID card mode as well.

CONCLUSION

A novel cashless module, Swing-Pay, has been presented for point-to-point transactions to eliminate all the constraints seen in state-of-the-art payment methods and some recently developed all-in-one payment cards like Plastic and Stratos. A complete prototype of a digital card that can be utilized for any type of payment and identity need has been discussed. A capacitive fingerprint sensor is employed to increase the security of the card. The libraries

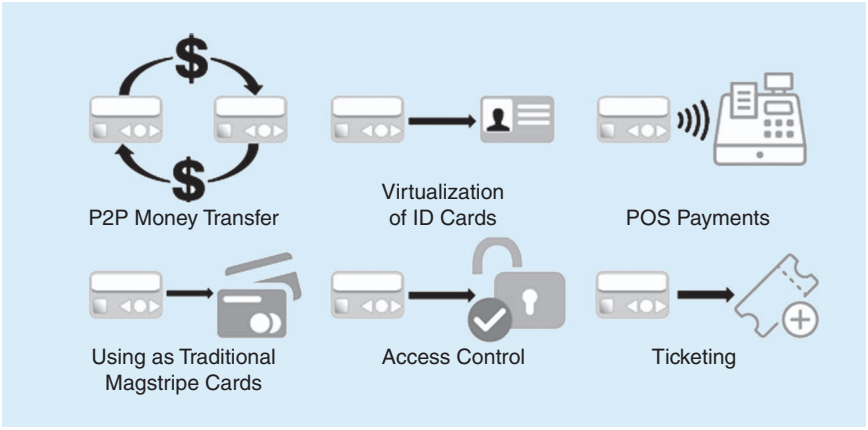

FIGURE 15. The applications perspectives of the proposed Swing-Pay card.

available for the e-Ink display are successfully ported for the 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 the cloud with the full details of the payer, the payee, and the 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 such as SHA and MD5. NFC-based P2P transaction and identity virtualization were also successfully tested on our module.

Although 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 they can be used everywhere like traditional payment cards. It is also planned to include a highly efficient paper battery as an external power source to avoid all portability constraints. The proposed digital card may have numerous applications in the near future, including P2P money transfer, identity card virtualization, POS payments, and conventional debit or credit card information and access control. It may also be used for related purposes, such as a virtual gift card, ticketing system, library card, and transit access card. Figure 15 shows a few present and future applications of the proposed module.

ACKNOWLEDGMENTS

We are thankful to the Department of Electronics and Information Technology, Government of India, for providing financial assistance to some of the coauthors under the Special Manpower Development Program—Chip to System Design to carry out this work.

ABOUT THE AUTHORS

Shirsha Ghosh (shirshatit@gmail.com) earned his M.Tech. degree in mobile communication and computing from the National Institute of Technology in Arunachal Pradesh, India, in 2016. His research areas include embedded systems, near-field communication, wireless networks, real-time operating systems, and the Internet of Things.

Joyeeta Goswami (joyeetatit@gmail.com) earned her M.Tech. degree in mobile communication and computing from the National Institute of Technology in Arunachal Pradesh, India, in 2016. Her current research interests are wireless networks, the Internet of Things, and security development in near-field communication and light fidelity.

Alak Majumder (majumder.alak@gmail.com) is an assistant professor in the Department of Electronics and Communication Engineering at the National Institute of Technology in Arunachal Pradesh, India. His current research interests include analog and digital very-large-scale integration and high-speed signaling. He is a Member of the IEEE, International Association of Engineers, and International Association of Computer Science and Information Technology.

Abhishek Kumar (ak9990566501@gmail.com) earned his B.S. degree in electronics and communication engineering from the National Institute of Technology in Arunachal Pradesh, India, in 2016. He is a cofounder and chief operating officer of Bluesole Technologies Pvt. Ltd in New Delhi, India. His interests include real-life applications of the Internet of Things and system design.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a professor in the Department of Computer Science and Engineering at the University of North Texas, Denton. He is currently the editor-in-chief of *IEEE Consumer Electronics Magazine* and serves on the editorial board of five 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*. He is a Senior Member of the IEEE.

Bidyut K. Bhattacharyya (bkbhatta1@yahoo.com) is a professor of electronics and communication engineering at the National Institute of Technology in Agartala, India. In 2000, he became an IEEE Fellow for his contributions to electronics packaging. He is also the recipient of the Intel Achievement Award given by the founders of Intel Corporation, Andy Grove and Gordon Moore.

REFERENCES

[1] M. Baddeley. (2004). Using e-cash in the new economy: An economic analysis of micro-payment systems. *J. Electron. Commerce Res.*, vol. 5, no. 4, pp. 239–253. [Online]. Available: http://web.csulb.edu/journals/jecr/issues/20044/Paper3.pdf

[2] B. Meng and Q. Xiong, "Research on electronic payment model," in *Proc. 8th Int. Conf. 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. Asian Himalayas Int. Conf. Internet*, 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, GA, White Paper, 2010.
[6] Compass Plus, "Mobile banking: One size doesn't fit all," Compass Plus Corp., Nottingham, United Kingdom, White Paper. [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, NY, Apr. 2010.
[8] B. Gates and M. Gates. (2015). 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. (2016). Wearable smart stamp to support NFC payments. [Online]. Available: http://www.nfcworld.com/2016/04/18/344048/wearable-smart-stamp-support-nfc-payments
[10] C. A. Walton, "Portable radio frequency emitting identifier," U.S. Patent 4 3842 88, Dec. 30, 1980.
[11] Barclaycard Corp. (2014). Hands off: a short history of contactless technology. [Online]. Available: https://www.home.barclaycard/insights/contactless/contactless-timeline.html
[12] T. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," *IEEE Transl. J. Magn. Jpn.,* vol. 2, no. 8, pp. 740–741, Aug. 1987.
[13] S. Ghosh, J. Goswami, A. Kumar, A. Majumder, "Issues in NFC as a form of contactless communication: A comprehensive survey," in *Proc. Int. Conf. Smart Technologies and Management for Computing, Communication, Controls, Energy, and Materials (ICSTM)*, 2015, pp. 245–252.
[14] NFC Forum. [Online]. Available: http://nfc-forum.org/what-is-nfc/what-itdoes
[15] M. Hamblen. (2012). A short history of NFC. [Online]. Available: http://www.computerworld.com/article/2493888/mobile-payments/a-short-history-of-nfc.html
[16] R. Arnfield. (2015). Mobile wallets 101. [Online]. Available: https://lists.w3.org/Archives/Public/public-webpayments-ig/2015Oct/att-0026/cardlinx_guide_final.pdf
[17] G. Wallner, "System and method for a baseband nearfield magnetic 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. (2016). Mobile payments will overtake cards and cash by 2025, says U.K. retailer. [Online]. Available: http://www.nfcworld.com/2016/04/19/344092/mobile-payments-will-overtake-cards-cash-2025-says-uk-retailer
[20] Accenture. (2015). 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
[21] Accenture. (2013). 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. (2014). Consumer payments study. [Online]. Available: http://tsys.com/Assets/TSYS/downloads/rs_2014-consumer-payments-study.pdf
[23] K. Cash. (2015). 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
[24] Citi Bank. (2016, July 28). Survey: Consumers adopting mobile payments, but at a slow pace. *Networld Media Group*. [Online]. Available: http://www.mobilepaymentstoday.com/news/survey-consumers-adopting-mobile-payments-but-at-a-slow-pace/
[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. (2011). 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
[29] *Simple NDEF Exchange Protocol Technical Specification*, NFC Forum SNEP 1.0, 2011.
[30] A. Lotito and D. Mazzocchi, "OPEN-NPP: An open source library to enable P2P over NFC," in *Proc. 4th Int. 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, and M. S. Lam, "Touch and run with near field communication (NFC)," Computer Science Department, Stanford University, Stanford, CA.
[33] D. M. Monteiro, J. J. P. C. Rodrigues, and J. Lloret, "A secure NFC application for credit transfer among mobile phones," in *Proc. Int. Conf. Computer, Information, and Telecommunication Systems (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. Int. Conf. Control, Electronics, Renewable Energy, and Communications (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 *Proc. Second Int. Workshop 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] C. 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, and C. P. Leon, "Electronic card with a programmable magnetic stripe," U.S. Patent 8 910 879, Dec. 16, 2014.
[40] MasterCard. (2014). 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
[41] A. Majumder, B. K. Bhattacharyya, S. Ghosh, and J. Goswami, "A digital card serving identity and payment purpose," Indian Patent 201631004666, Feb. 10, 2016.
[42] Arduino LLC. Arduino due documentation. [Online]. Available: https://www.arduino.cc/en/Main/ArduinoBoardDue
[43] Elecrow. NFC shield. [Online]. Available: http://www.elecrow.com/wiki/index.php?title=NFC_Shield
[44] Fingerprints Cards. FPC-AM3 product sheet. [Online]. Available: http://www.fingerprints.com/wp-content/uploads/2013/07/FPC-AM3-product-sheet1.pdf
[45] Adafruit Industries. Repaper 2.7 Graphic e-Ink development board. [Online]. Available: https://www.adafruit.com/product/1346
[46] E Ink Corp. Ink technology. [Online]. Available: http://www.eink.com/technology.html
[47] Adafruit Industries. FONA. [Online] Available: https://www.adafruit.com/product/2542
[48] Texas Instruments. (2014). FDC1004: Basics of Capacitive Sensing and Applications. [Online]. Available: www.ti.com/lit/an/snoa927/snoa927.pdf