Received August 27, 2020, accepted September 15, 2020, date of publication September 21, 2020, date of current version October 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3025429

A Novel Mobile Wallet Model for Elderly Using Fingerprint as Authentication Factor

SARWAT IQBAL[1], MUHAMMAD IRFAN[2], KAMRAN AHSAN[1], M. A. HUSSAIN[1], MUHAMMAD AWAIS[3], (Member, IEEE), MUHAMMAD SHIRAZ[1], (Member, IEEE), MOHAMMED HAMDI[4], (Member, IEEE), AND ABDULLAH ALGHAMDI[4]

[1]Department of Computer Science, Federal Urdu University of Arts, Science and Technology, Karachi 75300, Pakistan
[2]Electrical Engineering Department, College of Engineering, Najran University, Najran 61441, Saudi Arabia
[3]School of Computing and Communications, Lancaster University, Lancaster LA1 4YW, U.K.
[4]College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia

Corresponding author: Muhammad Shiraz (muh_shiraz@yahoo.com)

ABSTRACT Due to the availability of fingerprint verification technology on mobile devices, fingerprint based human identification has become the most widely used biometric technology in everyday life. The elderly find digital payment applications difficult to operate and unsecure. This work has exploited fingerprint verification availability on mobile devices to provide a user friendly and secure digital wallet payment facility to elderlies who are unable to avail this facility due to the complex infrastructure of traditional authentication mechanisms. A novel digital payment mechanism is presented which uses Bluetooth technology of mobile devices for billing at the point of sale and fingerprint verification for user authentication. A proof of the concept study is presented to validate the proposed model using state of the art usability questionnaires and attributes with the target group. The result indicates that the proposed methodology provides satisfaction and ease of use to the user.

INDEX TERMS Biometric verification, design for usability, elderly support, fingerprint verification, digital payment support for elderly, user centered design.

I. INTRODUCTION

Digital wallet or mobile wallet applications are used to pay shopping bills using a mobile device such as a mobile phone. Digital wallet applications store payment card(s) on the client side and being compatible with most of the e-commerce applications offers numerous benefits to customers such as anytime, anywhere immediacy payment facility. They are more secure than any other card technology and are equivalent to the physical wallet [1]. In digital wallet applications, a user can replace his physical cards with virtual cards, storing them on his mobile devices such as mobile phones, tablets, and smartwatches; hence a tangible card is replaced by an intangible virtual card. By digital wallet application user can get rid of keeping physical cards in his pocket or textile wallet, fumble them and selecting appropriate card while paying bills at POS, hence can avail a quicker, safer and easy to use way of paying the bill using virtual cards saved in the mobile device.

The associate editor coordinating the review of this manuscript and approving it for publication was Kashif Munir.

Digital payment at the point of sale (POS) uses a checkout counter machine for payment purposes. Traditionally two technologies are being used for POS payments, near field communication (NFC) method and payment through a mobile device. Elderly users especially feel it difficult to pay their bills at POS using physical cards as swapping and inserting the card properly at POS machine is not an easy task for them. Diverse design limitations such as dual nature of machine (chip and magnetic card acceptance capability in a single machine), the different placing of reader slot, correct orientation of card or swapping properly, keeping the card in the machine for a specified time interval and entering the PIN make the process of presenting physical card properly to a POS machine challenge. The following are the contributions of the study:

1) The proposed study highpoints the issues and challenges in different digital wallet and payment systems in detail. An extensive search has been carried out in order to highlight the issues and challenges.
2) After presenting the issues and challenges proposed study presents a novel digital wallet payment system

that uses Bluetooth technology and fingerprint scanner, available on mobile devices for payment at the point of sale (POS).
3) A usability study has been presented to evaluate the proposed payment mechanism. The results of the study are presented using statistical tools.

The proposed methodology is novel as existing studies lack to focus on the special needs of the elderly population at the time of paying bills at POS. The proposed work particularly focuses on user-centered design (UCD) in order to create a digital wallet payment application for the elderly. In UCD the user's need, goal, and success are given prime importance. UCD should fit the mental model of the user and the requirement of the task to be performed with that application. The UCD approach increases the applicability and acceptance of mobile applications. If the user perspective is tacit then the system may be modeled which fulfills the special needs of the targeted user community [2].

The rest of the paper is organized as follows. In section 2 literature review of the digital wallet applications and their challenges are presented. Section 3 discusses the proposed payment mechanism. In section 4 the design of the proposed mechanism, mobile application based on proposed mechanism, evaluation approach in detail, usability study and its results have been discussed. Discussion about the study is presented in section 4. Finally, section 5 presents the conclusion.

II. LITERATURE REVIEW

Biometric information to authenticate a user has been used in different payment systems at POS [3] [4]. Traditionally a specialized hardware device is used at POS which authenticate the user in addition with a shopping card (credit/Debit card).

Fingerprint based authentication mechanism has been used mostly in biometric technology. Fingerprint based authentication of the user has more superiority than other biometric methods due to its availability, reliability and high accuracy. At POS fingerprint based authentication method is easier to develop as compared to other biometric methods. A fingerprint based POS payment has been proposed by [5] which uses a specialized algorithm to detect and remove false minutia. In traditional POS, the method of swipe payment card is used that may require entering a PIN to the electronic machine available at POS. The use of this authentication provides a single factor authentication which is considered a less secure method. Since fingerprint biometric authentication is considered the most secure and also a legitimate proof of evidence throughout the world, it has been used widely in different payment systems. A biometric fingerprint payment system using mobile devices have been introduced by [6]. In this system, the POS terminals have electronic equipment in which biometric reader is installed which takes the fingerprint information of the users and then authenticates them by sending the biometric information to a remote server. The remote server matches the information with the previously stores users' information. Furthermore, the system supports a mobile device with a fingerprint scanning capability to send information directly to the remote servers for authentication. The scheme presented by [7] uses a fingerprint to generate a token to replace the physical card. In this scheme fingerprint data is collected from the user, encoding is done by adding some other parameters and then the transaction is done. To verify a transaction a fingerprint based mechanism at POS is proposed by [8]. The hardware installed at POS receives and sends fingerprint data to the payment card organization in order to authenticate the user. The same method is used if the user wants to purchase his home PC by using specialized hardware connected with PC. A secure online shopping mechanism which uses a credit card and biometric information of buyer is presented in [9]. This mechanism uses a special storage device provided to the user from card issuer. The buyer is required to use a storage device to generate an encrypted electronic internet shopping card (EISC) image. The storage device will use the buyer fingerprint to authenticate him and generate a unique, one-time EISC image. The EIS image is used to complete the payment process. A mechanism to make a transaction using a wireless communication device is presented by [10]. The method is made secure by generating a personal identification entry (PIE) by fingerprint data using the sensor of users' mobile device.

Digital wallet applications eliminate the need of taking the physical card out of the pocket or textile wallet, selecting an appropriate card and presenting it to the reader machine properly. Digital wallet applications do all of these tasks electronically by the selection of appropriate choice form application menus. Navigation through menus available in digital wallet applications poses some usability issues for the users, especially for elderly users. Since digital wallet application fetches the tangible card to intangible virtual card stored electronically on mobile devices, the need for creating them usable augmented considerably.

A. USABILITY HELP IN CREATING MOBILE APPLICATIONS

Usability attributes may be used by software designers to improve their strategy and present software so that user can communicates with applications with maximum ease. Authors in [11] presented a usability guide that helps in creating an application for children with Down syndrome. An improved self-assessment system, exploiting usability parameters, for chronic disease is presented by [12]. Free-handmicrogesture usability is evaluated by a usability study [13]. The study revealed that small changes in gesture may improve user accuracy and task completion time.

Issues faced by User while Accepting Digital Wallet Applications:

As mobile payment is done using electronic devices, different issues hinder its acceptance. The user is considered as the main actor for which the whole payment mechanism is constructed. Some issues highlighted by literature are discussed below.

1) SECURITY, PRIVACY AND USABILITY ISSUES

Digital wallet applications are required to be highly secure and usable. No mechanism will attract users towards digital wallet despite its sophistication as the successful implementation of the digital wallet system depends on how the security and privacy dimensions are perceived by the user as well as a merchant [14]. The mechanism should be secure and the user should be able to perform easily the necessary actions quickly and correctly [15].

Besides usability and security, the most critical factor of digital payment application is to authenticate the user who is using that mobile device to pay the bill through the web from his home location or at the point of sale (POS) terminal. Traditionally stronger user authentication, one-factor, two-factor, and multi-factor authentication mechanisms were used as swords against this. Although these authentication mechanisms strengthen the authentication but to follow an authentication mechanism successfully may be difficult for a user due to its complexity [16]. One time password (OTP) is also an authentication method in which instead of the traditional password the payment authority sends the password for completion of each transaction.

The most common method of user authentication requires the user to enter a PIN (Personal Identification Number) or OTP (one-time password) [17], which is only successful when user keys in the accurate PIN or OTP within a short interval of time. If the user fails to enter, the transaction may be aborted.

Different types of encryption are done when data is sent from one stakeholder to another and secure coding practices are followed while developing applications for payment so that applications cannot be tapped [18].

Biometric authentication simplifies the authentication mechanism and may be adopted instead of the authentication mechanisms mentioned before. Highly secure digital payments can be made by using biometric-enabled mobile devices instead of using traditional password verification methods [19]. Fingerprint verification, a very common authentication mechanism, can be done through many commercially available mobile devices. These devices access fingerprint by using embedded hardware or through a home screen button.

Security architectures are employed to guard passcode and fingerprint data in fingerprint verification methods [20]. The fingerprint verification chip encrypts the fingerprint data and shields it with a secure key. Apart from digital payment, plastic cards such as credit card and debit cards are also used in electronic payment methods. Factors such as security, ease of use and user authentication are considered explicit problems in electronic payment. Payment through plastic cards is very much vulnerable and fraudulent attacks may hinder its acceptance [16]. Lack of trust, awareness and less availability in rural areas are some other factors that impede the acceptability of digital wallet applications [14]. The issues such as accountability and privacy policy were found highly challenging in the design process of mobile payment protocols [21]. As mobile payments are mostly done by using a wireless network, the need to safeguard the process through security attacks becomes crucial. Different cryptography techniques are used in mobile payment solutions. The methods which use public key cryptography, such as the mechanism by [22], do not offer a secure solution. The secure payment solution is provided by using different layers of security such as the use of TCP/IP channel over the internet and WAP channel over the cellular network. Apart from these methods, the use of short-range communication technologies such as Bluetooth, NFC, Infrared and RFID make mobile payment more secure. Security measure at the application level is required to guard a mobile payment solution from unauthorized access, in this case maintaining a secure electronic transaction (SET) is mandatory as highlighted by [23]. The physical limitations of mobile devices pose challenges of usability. The most common mobile devices' screen size is from 2.5 inches to 7 inches. Displaying a list of items with their information on these small screen sizes creates problems for designers. To input data, a small area of the screen is reserved for on-screen keyboard display which requires special consideration to be focused by the designer. Furthermore, mobile devices are used in different contexts. These varying contexts and user mobility is challenging for the designer.

Text value entry on mobile devices having only numeric keypad is a tedious and error-prone process. Apart from the keyboard for data entry mobile devices also present voice recognition facilities to quickly enter data but the voice recognition performance degrades in a noisy environment. Table 1 shows the comparisons of different issues discussed by different authors.

2) MONETARY AND HEDONIC ISSUES

Different monetary factors involved in digital payment solutions affect its acceptance rate. The users may feel overspending fear while adopting to pay form smart devices. The trust factors of providing their card information to payment parties may increase the fear of losing money. Maintaining credit for wallet application compromises the interest amount which may be awarded to users if they put their money in a fixed deposit account. Affordability of supported devices, such as smartphone, may pose a financial burden on user pocket. Spillover effect in channel choice has a negative effect on accepting of digital wallet applications. Although payment cost involved for a successful transaction is very low but the cost of using internet connection through payment device, charges of possessing debit/credit card, the tax applied on an online transaction by authorities and switching cost together make the digital payment applications less attractive to users. Furthermore hedonic and emotional issues such as enjoyments and gamification make the acceptance of digital payment difficult for users. Monetary and hedonic issues, reported by different authors are summarized in table 2.

TABLE 1. Security, privacy and usability issues faced by users.

Reference	Security	Trust	Personal Privacy Risks	Usefulness or Perceived Usefulness	Influence of Experience	Complexity of Application	Non-Tech-Savvy or Uneducated Background
[24]	✓	✓		✓			
[25]	✓						
[26]	✓			✓			✓
[27]	✓						✓
[28]	✓						
[29]	✓						
[30]	✓						
[31]	✓	✓	✓	✓	✓		
[32]		✓	✓	✓			✓
[33]	✓	✓					
[34]	✓	✓		✓	✓	✓	
[35]	✓	✓					
[36]	✓	✓	✓				
[37]	✓	✓	✓				✓
[38]		✓	✓	✓			
[39]		✓	✓	✓			
[40]		✓					
[41]			✓	✓			✓
[42]			✓				
[43]				✓			
[44]				✓			
[45]				✓			
[46]				✓			
[47]				✓			
[48]				✓			
[49]	✓	✓	✓	✓			✓
[50]		✓		✓			
[51]				✓			
[52]				✓			
[53]			✓			✓	
[54]		✓					✓
[55]		✓		✓		✓	

TABLE 2. Monetary and hedonic issues faced by users.

Reference	Financial Risk	Hedonic Issues	Involved Transaction Cost or Switching Cost	Smart Phone Affordability	Spillover Effect in a channel choice context
[24]	✓	✓			✓
[25]	✓				
[26]			✓	✓	
[27]			✓		
[31]		✓			
[33]	✓				
[34]		✓	✓		
[39]	✓				
[40]			✓		
[41]		✓			
[42]	✓	✓			
[48]			✓	✓	
[53]			✓		
[54]			✓		

B. ISSUES FACED BY MERCHANTS WHILE ACCEPTING DIGITAL WALLET APPLICATIONS

Merchant is considered as one of the important stakeholder involved in the digital wallet ecosystem. Different barriers have been reported on merchant side. Merchants need to install necessary hardware as well as software for payment process which may involve heavy investment. In some cases merchant are hesitant using new technology(ies) equipment at their side. Furthermore payment solutions by different providers have still not attained the required critical mass. The growth and efficiency of mobile payment solutions need to be reached on appropriate level so that merchants' willingness to accept payment solution can be increased. Table 3 illustrates a comparison of issues, faced by merchants, reported in literature by different authors.

III. MATERIALS AND METHODS

The proposed mechanism enables an elderly to pay his shopping bills at POS with maximum ease. Fingerprint verification method through mobile devices has been exploited by

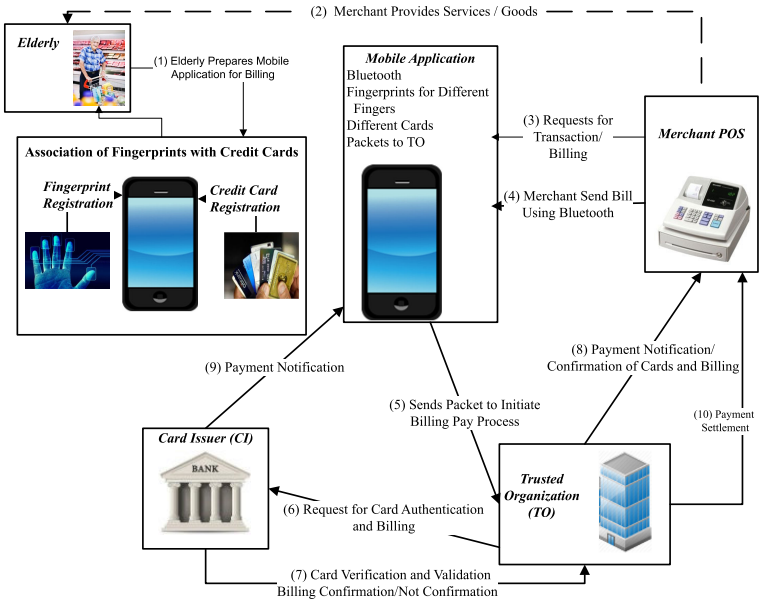


FIGURE 1. Proposed digital wallet model .

TABLE 3. Issues faced by merchant.

Reference	Limited Merchants	Devices Dependency	Payment Devices Dependency	Merchant Willingness	Huge Investment	Support Technology	Lack of Critical Mass
[26]	✓			✓			
[29]	✓			✓	✓	✓	
[32]							✓
[40]	✓						
[48]		✓	✓				
[53]							✓

which the elderly may effortlessly pay his shopping bills. Elderly may enjoy digital wallet payment facility by using his fingerprints only with different merchants' POS. Elderly may select different cards by just placing his finger on the fingerprint scanner of the mobile device. Elderly may associate his cards to any of his fingers and use this association at the time of billing. Figure 1 shows the overall working model of the proposed mechanism.

For this work, it was assumed that buyer had a smartphone with Bluetooth and fingerprint verification technology. The buyer and merchant should register with the trusted organization (TO; the payment gateway) before any transaction takes place. The trusted organization was the third party which was responsible to authenticate the transaction and authorizes the payment settlement. Buyer, merchant, trusted organization and card issuer would exchange their private keys through some secure mechanism. The overall payment process of the proposed mechanism would be composed of two main phases. These two main phases would be further divided into sub-phases. The two main phases would be:

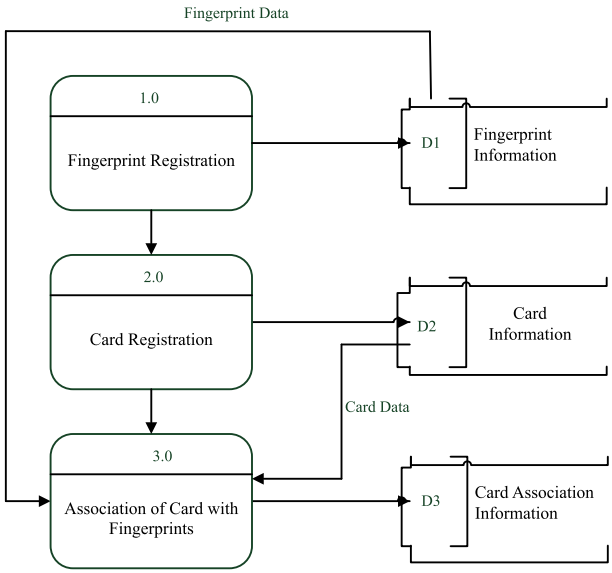


FIGURE 2. Data Flow diagram of Phase-2.

A. MOBILE PHONE APPLICATION PREPARATION

The data flow diagram of this process is represented in figure 2.

The mobile phone application preparation process is divided into three phases.

1) Fingerprint Enrollment Process: In this process, the buyer (user) would be required to enroll his fingers on his mobile device. The buyer could save his fingerprints as allowed by fingerprint enabled mobile devices (for example Samsung Galaxy S7 and LG G5). The buyer could save the maximum fingerprints (the value of n depends on the fingerprints allowed to enroll in the particular mobile device). Fingerprint information would be saved on mobile devices in encrypted form and the mobile application would access this information at the time of billing. Successfully enrolling fingerprint on a mobile device would enable the buyer to pay the bill at POS. The overall flow of this phase is given in figure 3.
2) Card Parking Process: In this process, the buyer would be required to save his credit/debit card information in his mobile application. The buyer would save different cards that were in his possession. The card information could be a card name, card number, security code or card verification value (CVV) code, expiry date and card type. This process will help the user to store all of his card information in digital format only once, after that he can put all of his cards in his preferred secure place so that card safety and loss issue will be removed.
3) Fingerprint Attaching Process: In this process, the buyer would be required to associate/attach his fingers (fingerprints) to his cards. The buyer may attach his five fingers to his five cards (as mobile devices available to date were allowing saving up to five fingerprints). In this way, one finger would act as one of his cards. This process will help the buyer to select a particular card at POS at the time of paying the bill. Attaching each card to one of his fingers will enable a buyer to easily memorize his cards' detail as he will not have to take out any card from his pocket at the time of billing. One time attaching card to his finger will let him free from any physical card security and missing issue.

The overall flow of the car parking and finger print attaching process is given in figure 5.

B. PAYMENT EXECUTION PROCESS

Payment execution process was the process through which request from the mobile application would be sent to trusted organization. The trusted organization would process the payment for the buyer and perform settlement for the merchant. General notations used to describe the proposed payment process in this paper are listed in table 4.

The data flow diagram of the phase-2 of the payment mechanism is presented in figure 3.

Payment execution process is divided into the following seven phases.

1) The first phase was the payment request, which involved the buyer and merchant. In this phase, the buyer would request the billing process with the merchant. The merchant would calculate the total amount of the bill. This calculation of bill would be totally dependent on the merchant internal billing process and would be handled on a merchant site (This process was beyond the scope of this paper and not discussed in detail). The buyer would provide his Bluetooth ID to the merchant for receiving the bill information on his mobile phone. $Buyer \rightarrow Merchant : BTID$
$Merchant \rightarrow POS : BTID$
2) The second phase was bill delivery to the buyer. Once the user has communicated his Bluetooth ID to the POS operator, the payment app will receive a detailed transaction summary created by POS so that the user can view and confirm the details of the current transaction. According to the proposed mechanism, the merchant would provide the six important points of information, namely TID, DT, TT, LOC, Amount, TVT to buyer mobile phone through Bluetooth communication after preparing the billing information. The points of information which merchant would be sent to buyer include transaction ID (TID), date of the transaction (DT), time of the transaction (TT), location of the transaction (LOC; traditionally it would be the store ID of the merchant which would be known to trusted organization prior to transaction), transaction validity period time (TVT; this time can be the start time and date of the information plus a range of minutes till which the transaction was valid) and total amount of bill (Amount). These points of information would act as essential entities during the billing process. Merchant may add some special points in this message. The merchant would generate a data packet, termed as data packet-1 in the proposed mechanism, by using the public key of the buyer.
$POS \rightarrow Buyer :$
$TID, DT, TT, TVT, LOC, Amount_{PuKB}$
3) The third phase was the payment process initiation. In this phase, transaction creation would be done. This phase would involve the buyer and the trusted organization. The buyer mobile application would decrypt *data packet-1* by using its private key. Buyer mobile application would use the information provided by the merchant to initiate the billing process. The buyer would use his mobile application in order to select the card from which he wants to make the payment. This selection of cards would be done by fingerprints of the buyer through the one-touch protocol (touch fingerprint sensor only once). One touch protocol selects the payment card for the transaction. For this selection, each finger of buyer would act as a card for him. The application would show the card selected by the buyer. The buyer would be required to confirm his selection by two touch protocol (putting the same finger twice on the fingerprint sensor with a short delay). Two-touch protocol confirms the card to be used for the transaction.

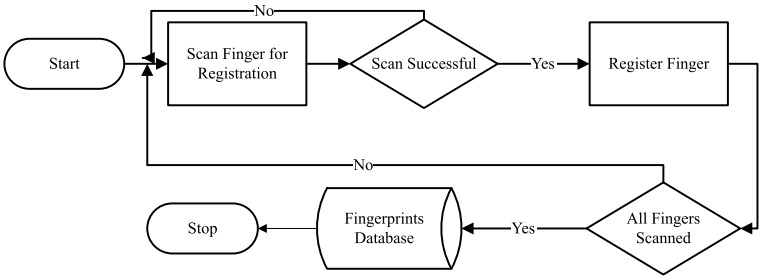


FIGURE 3. Flowchart of finger registration process.

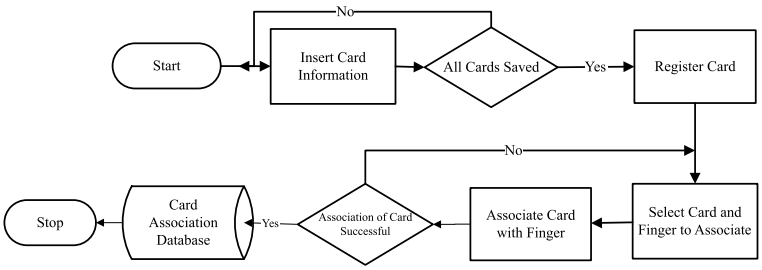


FIGURE 4. Flowchart of card association process.

TABLE 4. Notations used in proposed mechanism.

Symbol	Description	Symbol	Description
CI	Card issuer	CID	Card issuer ID
CCN	Credit card number	TVT	Transaction validity time
CVV	Card verification value	BTID	The Bluetooth ID of buyer
CED	Card expiry date	P_uK_B	Public key of buyer
DT	Date of transaction	P_RK_B	Private Key of buyer
TT	Time of transaction	P_uK_M	Public key of merchant
LOC	Location of transaction	P_RK_M	Private key of merchant
AMT	Amount of transaction (Total Bill)	P_uK_T	Public key of TO
TO	Trusted organization	P_RK_T	Private key of TO
POS	Point of sale (Place of the transaction)	P_uK_C	Public key of card issuer
TVT	Transaction validity time	P_RK_C	Private key of card Issuer
TID	Transaction ID	SR	The status of the transaction whether it is rejected or accepted
{Message Token}	Message token	$\{MessageToken\}_X$	The message token encrypted by X key

Two-touch protocol will only be active when the user has already selected a card and the app screen is showing the selected card image.

4) The fourth phase was payment request form buyer to TO. As soon as the card selection and confirmation was done by the buyer the mobile application would generate a token (message) containing the information received by merchant's POS and his card information like credit card number (CCN), card verification value (CVV), and card expiry date (CED). This information would be sent from buyer mobile phone to TO through an encrypted message. This message was termed as *data packet-2* in the proposed mechanism and would be encrypted through the public key of TO. This message was described as:
$Buyer \rightarrow TO$:
$TID, DT, TT, TVT, LOC, Amount, CCN,$
CVV, CED_{PuKT}

5) The fifth phase was payment authentication. The TO would decrypt the *data packet-2* using its private key and would create a message for card issuer (CI) termed as *data packet-3*. This message would be encrypted using card issuer public key. This message was described as:
$TO \rightarrow CI$:
$TID, DT, TT, TVT, LOC, Amount, CCN,$
CVV, CED_{PuKc}

6) The sixth phase was payment confirmation. Card issuer would use its own private key to decrypt the message and would authenticate the payment. Card issuer would then inform trusted organization about the payment confirmation by creating a message to buyer (*data packet-4*) and trusted organization (*data packet-5*) using buyer's and trusted organization public keys respectively. Trusted organization will inform merchant (*data packet-6*) about the payment confirmation

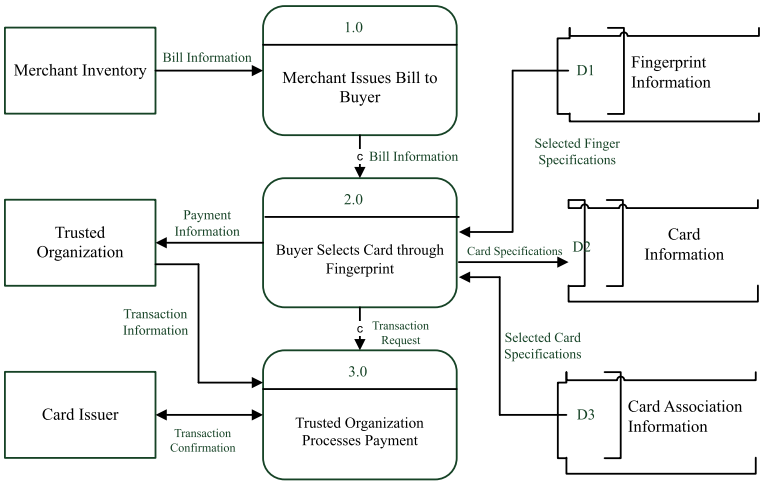


FIGURE 5. Data flow diagram of phase-3.

using merchant's public key. These messages were described as:
$CI \rightarrow Buyer$:
$TID, CCN, DT, TT, LOC, SR, Amount_{PuKB}$
$CI \rightarrow TO$:
$TID, DT, TT, CCN, LOC, SR, Amount_{PuKT}$
$TO \rightarrow POS$
$TID, DT, TT, CCN, LOC, SR, Amount_{PuKM}$

7) The seventh phase was payment settlement and would be done within TO and CI (the detail of this settlement process was beyond the scope of this paper and not discussed). The overall flow of this phase is given in figure 6.

The proposed work intended to focus on elderly ease of use so research group put most of the attention on elderly comfort. A prototype mobile application on Android platform has been developed as proof of the concept study. Marshmallow and Android 6.0 API were used. Samsung Galaxy S7 smartphone was used as a mobile device to test and run the application as it contained a built-in fingerprint sensor. The extremely simplified user interface was designed for the first prototype so that the mechanism can be evaluated positively.

C. PROTOTYPE DESIGN AND DEVELOPMENT

For the proposed model evaluation, the research group configured three servers to be acted as main stakeholders of digital payment, namely, POS server, trusted organization server, and card issuer/financial organization server. Two different mobile applications were developed in order to validate the usability and effectiveness of the proposed mechanism. One mobile application used the traditional authentication process in which the user selects the card and precedes the billing process using two-factor authentication process. The other application used the proposed mechanism in which fingerprint method of card association and selection were second-hand as user authentication to be used at POS. The second application was not the first application in which fingerprints are used for billing but its novelty lies in the fact that it is the first application in which card association and selection are done with fingerprints to carry out authentication.

For the evaluation of the propos mechanism android phones with a fingerprint scanner, either on the front or at the back of the mobile phones were used. All mobile phones were running either Marshmallow or Nougat version of Android. The prime aim of the evaluation study was to assess the usability challenges faced by participants while using the digital wallet application at POS. The other aim was to assess the usability and usefulness of the proposed application.

D. METHODOLOGY

The methodology is explained as follows.

1) INSTRUMENT AND ASSESSMENT METHOD

The research group analyzed the design and examined some of the issues on digital wallet applications. Design and implementation of the application have been performed to evaluate how it satisfies the various usability criteria. It is examined how the proposed application managed to provide a user interaction technique that presents an excellent interface with a secure method.

The research group used a customized questionnaire in order to collect participants' responses to the system. The questionnaire was made through the guidelines of SUS [56] and SUMI. Participant's response against seven selected attributes of system performance and usability were analyzed.

2) USER GROUPS

A two-phase user study has been done in which two user groups were created in order to assess the opinion about the payment system. The first group consisted of 20 elderly (male = 12, female = 8) aged between 67 to 85 years (mean age = 74±6.04) from non-computer science background and second group consisted of 20 experts (male = 15, female = 5)

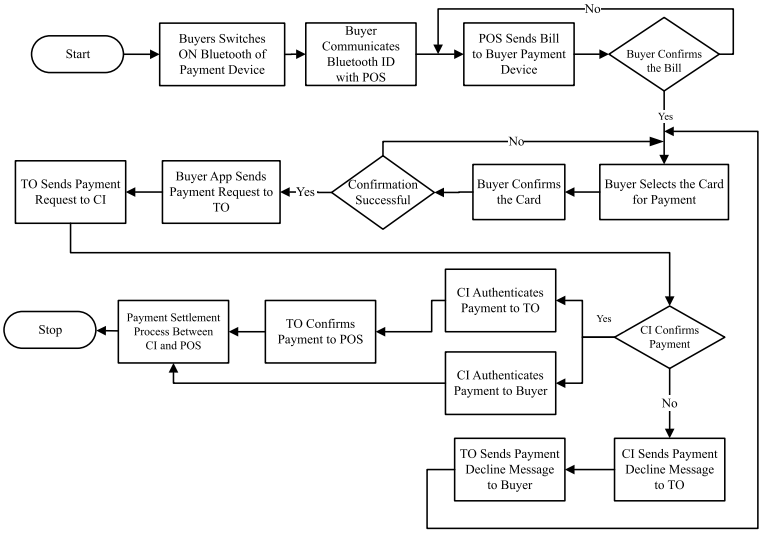


FIGURE 6. Payment execution process.

TABLE 5. General details of user groups.

Elderly Group		Expert Group	
Male	Female	Male	Female
12	8	15	5

aged between 45 to 75 years (mean age = 54 ±8.62) from the field of computer science. Table 5 shows the general details of user groups. The participants of both groups were users of mobile phone and had experience by using different mobile applications. The participants who did not have experience with mobile technology and applications were excluded from the user groups.

In the first group, 11 (55%) participants were fully aware, 5 (25%) participants were partially aware and 4 (20%) of them were not aware with digital payment applications. In the second group, 9 (45%) participants were fully aware, 5 (25%) participants were partially aware and 6 (30%) of them were not aware with digital payment applications. Overall a good number of participants (75%) were aware with a digital payment applications.

All the participants were observed keenly by research group during the sessions in order to note the participants' trouble, anxiety, and confusion in performing different tasks. Special focus was done on observing user mistakes and the observations were documented which helped in improving the user interface. Separate sessions with both participants were conducted due to the limited resources of the research group.

3) ASSESSMENT METHOD

The assessment method consisted of three phases. In the first phase of evaluation, all elderly participants were provided a complete guide about the use of digital wallet payment applications having a traditional authentication mechanism. A little training session has been conducted in which the billing process was explained to all by the coordinators of the research group.

Different payment cards, printed by the research group to mock real credit/debit cards, were distributed to participants. The participants were randomly divided into two equal groups and each participant of the first group was provided 5 cards and each participant of the second group was provided with 6 cards. From these cards, both groups were requested to perform 6 billing processes (for their practice before an actual performance) by using the traditional mobile application.

Both groups of participants were demonstrated the billing process and all other basic functionalities of the mobile application. As the mobile application was designed according to the real needs of the elderly, both groups showed a positive and enthusiastic response towards the mobile application. Elderly usually take more time to comprehend a process so all the necessary tasks in order to complete a billing process using the mobile application were demonstrated in detail and ample time was given to them to comprehend the processes.

The participants were given different cards to make billing processes. All participants were divided randomly into two equal groups and each participant of the first group was given 4 cards and each participant of the second group was given 5 cards. Participants were requested to enroll their fingerprints on mobile devices, attach each finger to one and only one card and then perform 8 complete mock billing processes. All the processes performed by participants were keenly observed by the research group so that future improvement in the mobile application can be done. This is observed that all participants completed their billing processes with very little help from the research group.

After the handling of mobile applications and performing the mock shopping by elderly groups, the customized

questionnaire was given to each elderly and the scores were calculated. Usability attributes *Efficiency, Satisfaction, Memorability, Learnability, Attractiveness, Error tolerance* and *Security* were asked to rate on a 10 point Likert. The same experiment with the expert group was conducted who belonged to the field of computer science and 5 of them have used mobile payment applications in past. Most of the expert group participants were experienced in mobile phone application design and developing process. A four-hour session was conducted with the expert group in which details of the proposed mechanism, details of relevant facts and mobile application were demonstrated.

The proposed mobile application was made available to be installed and payment cards were handed over in order to be saved on expert participants' mobile devices. Fifty percent of the expert participants were provided 6 different cards and the other fifty percent were provided 7 different cards. All of the expert participants were requested to perform 8 billing processes. After completing the mock shopping tests of mobile applications by expert groups, the customized questionnaire was given to each elderly and the scores were asked against usability attributes *Efficiency, Satisfaction, Memorability, Learnability, Attractiveness, Error tolerance* and *Security* were asked to rate on a 10 point Likert Scale. Furthermore, the usability factors efficiency, learnability, memorability, error, and satisfaction, as suggested by Nielsen (1993)[52] were also evaluated. Their general feedback and comments were also recorded and analyzed for future improvements of the proposed mechanism and mobile application design. This is revealed that the proposed mechanism outperformed in speed and cognitive load under ordinary conditions.

IV. RESULTS AND DISCUSSION

The results and discussion are as follows.

A. DATA ANALYSIS

Data analysis aimed to compare the proposed model with the traditional two-factor authentication model for smartphone applications. This research study used several statistical measures to get statistical results from respondents. The research group carefully selected 7 usability attributes from the work of [56]. These seven attributes were *Efficiency, Satisfaction, Memorability, Learnability, Attractiveness, Error tolerance* and *Security*. The sample contained 40 participants. In this study first, the descriptive analysis of data obtained against using mobile applications of the traditional and proposed mechanism is presented followed by comparative analysis. The reliability and validity of data are also presented followed by association analysis to ensure that the participants evaluated both models independently.

1) DESCRIPTIVE ANALYSIS OF DATA

For descriptive analysis, both user groups responded against usability attributes against the traditional model and proposed model. The mean and standard deviation of the elderly participants' response was calculated against seven aspects of usability.

Figure 7 shows the mean ratings of the elderly participants' responses against seven selected aspects of usability. This is observed that elderly rated all attributes of fingerprint model higher than the traditional model. Learnability was the only attribute that is rated as equal to the traditional model.

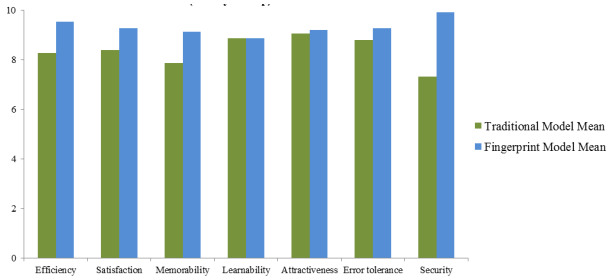


FIGURE 7. Traditional model mean and fingerprint model mean (elderly group).

Figure 8 shows the standard deviation as rated by elderly participants. This is observed that against most of the attributes (efficiency, satisfaction, memorability and security) in fingerprint model the ratings are closed but in the traditional model, the participants' ratings are very much dispersed. Hence this is concluded that fingerprint model is more consistent than the traditional model.

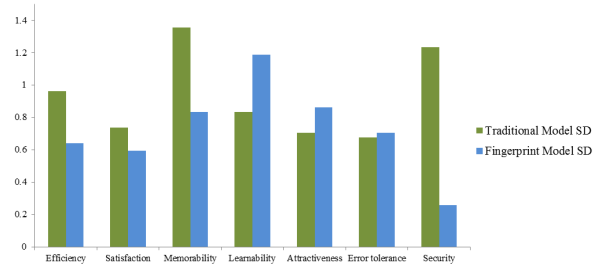


FIGURE 8. Traditional model SD and fingerprint model SD (elderly group).

Figure 9 shows the mean ratings of the expert participants' responses as per seven selected aspects of usability. This is observed that expert rated all attributes except learnability of fingerprint model higher than the traditional model. Learnability was the only attribute that is rated as less than the traditional model.

Figure 10 shows the standard deviation as rated by expert participants. This is observed that against most of the attributes (efficiency, satisfaction, memorability, error tolerance and security) in fingerprint model, the ratings are closed but in the traditional model, the participants' ratings are very much dispersed. Hence this is concluded that fingerprint model is more consistent than the traditional model.

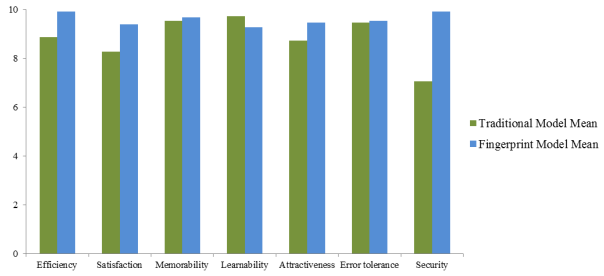


FIGURE 9. Traditional model mean and fingerprint model mean (expert group).

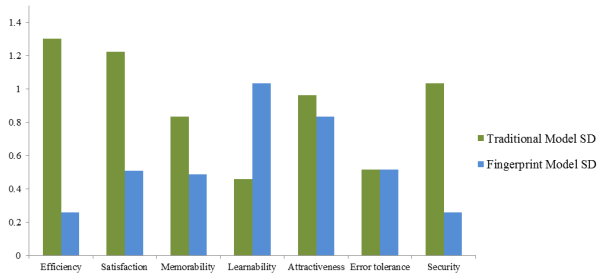


FIGURE 10. Traditional model SD and fingerprint model SD (expert group).

2) COMPARATIVE ANALYSIS OF DATA

The research group used a Likert scale for user response, having a rating from 1 to 10, against each attribute of usability with the same weight to each attribute of both models for an overall evaluation. The mean score for learnability is found the same in both the traditional model and proposed a model. In other attributes, the proposed model has higher mean values. This reveals that the elderly participants believed the proposed fingerprint model more usable in targeted attributes as compared to the traditional model. The results are supported by the standard deviation of the two models. The standard deviation against efficiency, satisfaction, memorability, and security is higher while standard deviation against learnability, attractiveness and error tolerance is lower. This means that elderly participants feel fingerprint model more consistent in terms of learnability, attractiveness and error tolerance and traditional model more consistent in terms of efficiency, satisfaction, memorability, and security. Comparisons of elderly participants' ratings against selected attributes of usability have been depicted in figures 11a to 11g. The elderly participant ratings against fingerprint model efficiency and traditional model efficiency are depicted in figure 11. 12 expert participants of the study rated the fingerprint model higher inefficiency, 3 of them rated fingerprint model equal inefficiency and no participant rated fingerprint model lower inefficiency.

The elderly participant ratings against fingerprint model satisfaction and traditional model satisfaction are depicted in figure 12. 8 elderly participants of the study rated the fingerprint model higher in satisfaction, none of them rated

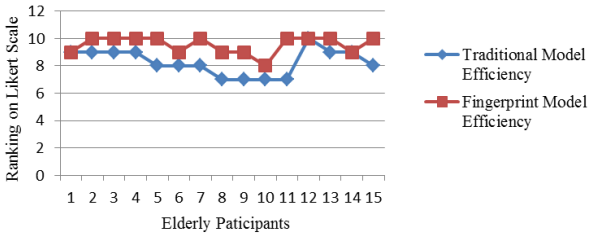


FIGURE 11. Traditional model efficiency Vs fingerprint model efficiency.

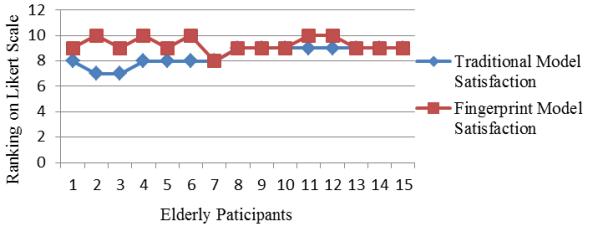


FIGURE 12. Traditional model satisfaction Vs fingerprint model satisfaction.

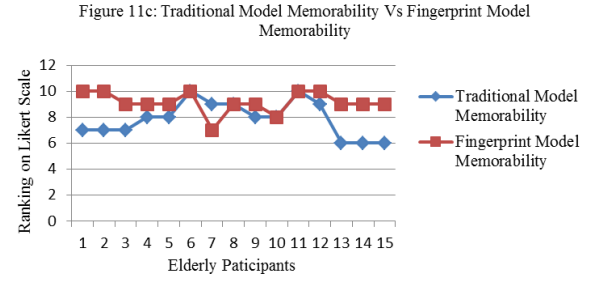


FIGURE 13. Traditional model memorability Vs fingerprint model memorability.

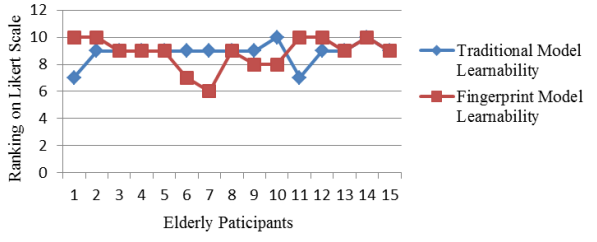


FIGURE 14. Traditional model learnability Vs fingerprint model learnability.

fingerprint model equal in satisfaction and 7 participant rated fingerprint model lower in satisfaction. The elderly participant ratings against fingerprint model memorability and traditional model memorability are depicted in figure 13. 10 elderly participants of the study rated the fingerprint model higher, 4 of them rated fingerprint model equal in and only 1 participant rated fingerprint model lower in memorability. The elderly participant ratings against fingerprint model learnability and traditional model learnability are depicted in figure 14. 4 elderly participants of the study rated the

fingerprint model higher in learnability, 7 of them rated fingerprint model equal in learnability and 4 participants rated fingerprint model lower in learnability. The elderly participant ratings against fingerprint model attractiveness and traditional model attractiveness are depicted in figure 15. 7 elderly participants of the study rated the fingerprint model higher in attractiveness, 4 of them rated fingerprint model equal in attractiveness and 4 participants rated fingerprint model lower in attractiveness. The elderly participant ratings against fingerprint model in error tolerance and traditional model in error tolerance are depicted in figure 16. 6 elderly participants of the study rated the fingerprint model higher in error tolerance, 8 of them rated fingerprint model equal in error tolerance and only 1 participant rated fingerprint model lower in error tolerance. The elderly participant ratings against fingerprint model security and traditional model security are depicted in figure 17. 14 elderly participants of the study rated the fingerprint model higher in security, 1 of them rated fingerprint model equal in security and none of them rated fingerprint model lower in security. Comparisons of expert participants' ratings against each selected attribute of usability have been depicted in figures 18 to 24.

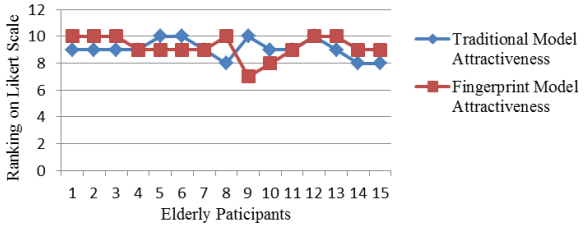


FIGURE 15. Traditional model attractiveness Vs fingerprint model attractiveness.

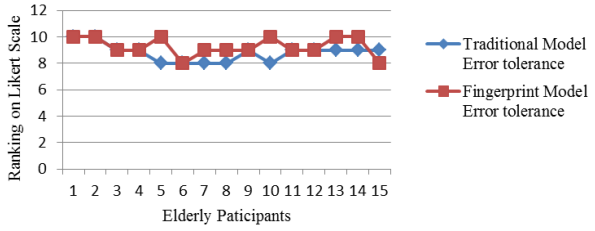


FIGURE 16. Traditional model error Tolerance Vs fingerprint model error tolerance.

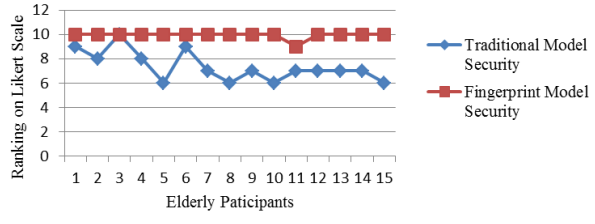


FIGURE 17. Traditional model security Vs fingerprint model security.

The expert participant ratings against fingerprint model efficiency and traditional model efficiency are depicted in figure 18. 9 expert participants of the study rated the fingerprint model higher in efficiency, 6 of them rated fingerprint model equal in efficiency and no participant rated fingerprint model lower in efficiency. The expert participant ratings against fingerprint model satisfaction and traditional model satisfaction are depicted in figure 19. 9 expert participants of the study rated the fingerprint model higher in satisfaction, 6 of them rated fingerprint model equal in satisfaction and no participant rated fingerprint model lower in satisfaction.

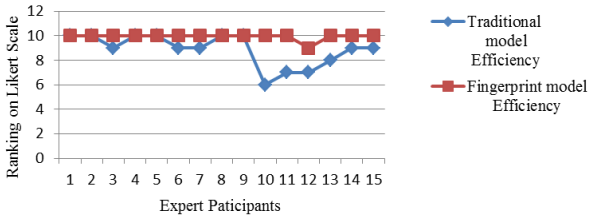


FIGURE 18. Traditional model efficiency Vs fingerprint model efficiency.

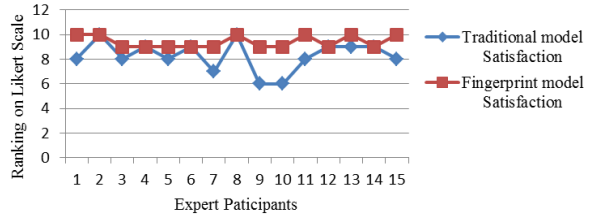


FIGURE 19. Traditional model satisfaction Vs fingerprint model satisfaction.

The expert participant ratings against fingerprint model memorability and traditional model memorability are depicted in figure 20. 2 expert participants of the study rated the finegrprint model higher in memorability, 9 of them rated fingerprint model equal in memorability and 3 participants rated fingerprint model lower in memorability.

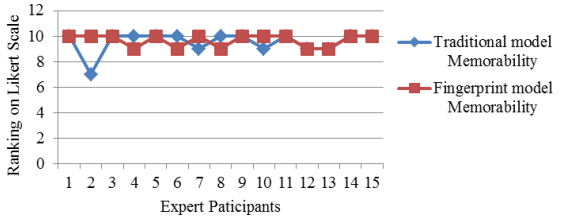


FIGURE 20. Traditional model memorability Vs fingerprint model memorability.

The expert participant ratings against fingerprint model learnability and traditional model learnability are depicted in figure 21. 1 expert participant of the study rated the finegrprint model higher in learnability, 9 of them rated fingerprint

model equal in learnability and 5 participants rated fingerprint model lower in learnability.

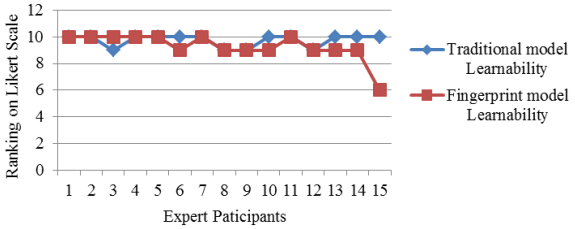


FIGURE 21. Traditional model learnability Vs fingerprint model learnability.

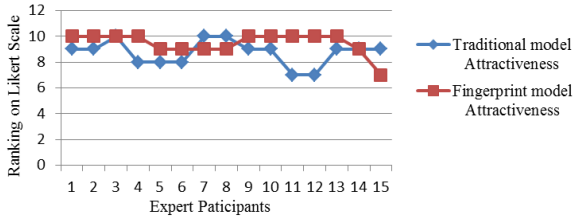


FIGURE 22. Traditional model attractiveness Vs fingerprint model attractiveness.

The expert participant ratings against fingerprint model attractiveness and traditional model attractiveness are depicted in figure 22. 10 expert participants of the study rated the finegrprint model higher in attractiveness, 2 of them rated fingerprint model equal in attractiveness and 3 participants rated fingerprint model lower in attractiveness. The expert participant ratings against fingerprint model error tolerance and traditional model error tolerance are depicted in figure 23. 5 expert participants of the study rated the finegrprint model higher in error tolerance, 4 of them rated fingerprint model equal in error tolerance and 6 participants rated fingerprint model lower in error tolerance. The expert participant ratings against fingerprint model security and traditional model security are depicted in figure 24. All 10 expert participants of the study rated the fingerprint model higher in security, no of them rated lower or equal.

3) RELIABILITY AND VALIDITY OF DATA

For this study, the traditional payment model was paired with the proposed fingerprint model together so a paired T-test was used to evaluate the differences between the mean of the traditional model and mean of proposed fingerprint model. An F-test has been used to compare the responses and variance difference against both models. The hypotheses for the test were H1, H2, H3, H4, H5, H6 and H7 for each usability attribute. These hypotheses are shown in table 6.

The results of reliability and validity analysis are shown in table 7.

Test statistics and confidence interval values are given in table 7. From table 7 this is observed that both models performance was significantly different. According to

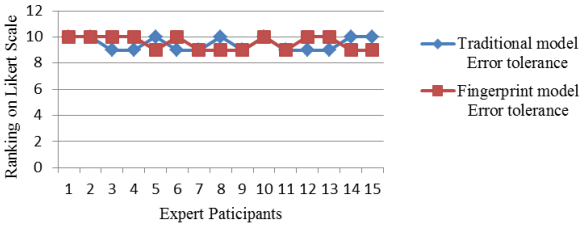


FIGURE 23. Traditional model error tolerance Vs fingerprint model error tolerance.

Figure 12g: Traditional Model Security Vs Fingerprint Model Security

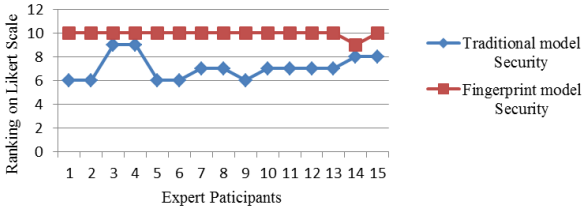


FIGURE 24. Traditional model security Vs fingerprint model security.

the elderly participants rating traditional model performed better on usability aspects *learnability, attractiveness* and *error tolerance* and if elderly participants rate on usability aspects *efficiency, satisfaction, memorability,* and *security* fingerprint model leaded to improvement. The t statistics values here indicated that the fingerprint model performed better than traditional model on usability aspects *efficiency, satisfaction memorability,* and *security*.

From F-Test this is revealed that consistency situation of traditional model is different in terms of *security* and *memorability*. Fingerprint model had lower variance on usability aspects *security* and *memorability*. The consistency of both models is same in terms of *efficiency, satisfaction, learnability, attractiveness* and *error tolerance*. In F-test, the null hypotheses were that both models have the same consistency against the alternate hypotheses that fingerprint model has low consistency. Research group applied left tailed test with alpha value 0.05. The null hypotheses were accepted in usability aspects *security* and *memorability*. The alternate hypotheses were accepted in usability aspects *efficiency, satisfaction, learnability, attractiveness* and *error tolerance*.

From table 8 this is observed that both models performance was significantly different. According to the expert participants rating fingerprint model performed better on usability aspects *efficiency, satisfaction and security* and if expert participants rate on usability aspects *memorability, learnability, attractiveness and error tolerance* traditional model leaded to improvement. The t statistics values here indicated that the fingerprint model performed better than traditional model on usability aspects *efficiency, satisfaction and security.*

From F-Test this is revealed that consistency situation of fingerprint model is different in terms of *efficiency, satisfaction, memorability, learnability and security*. The fingerprint

TABLE 6. Hypotheses from H1 to H7.

Usability Attributes	Hypothesis Statement to be Tested
Efficiency	H1: Fingerprint Model has the same efficiency as a traditional model.
Satisfaction	H2: Fingerprint Model has the same satisfaction as a traditional model.
Memorability	H3: Fingerprint Model has the same memorability as a traditional model.
Learnability	H4: Fingerprint Model has the same learnability as the traditional model.
Attractiveness	H5: Fingerprint Model the same attractiveness as a traditional model.
Error tolerance	H6: Fingerprint Model performs the same error tolerance as a traditional model.
Security	H7: Fingerprint Model has the same security as the traditional model.

TABLE 7. Results of T-Test and paired F-Test with elderly participants.

Elderly Participants				
Hypotheses	Paired T-Test		Paired F-Test	
	Test Statistics	Sig Value	Test Statistics	F critical
Efficiency	5.551	0.000071	0.443	0.402
Satisfaction	3.389	0.004	0.649	0.402
Memorability	3.199	0.006	0.378	0.402
Learnability	0.000	1.0000	0.493	0.402
Attractiveness	0.414	0.685	0.667	0.402
Error tolerance	0.292	0.774	0.923	0.402
Security	8.107	0.000001	0.0438	0.402

TABLE 8. Results of T-Test and paired F-Test with expert participants.

Expert Participants				
Hypotheses	Paired T-Test		Paired F-Test	
	Test Statistics	Sig Value	Test Statistics	F critical
Efficiency	3.378	0.005	0.039	0.402
Satisfaction	3.900	0.002	0.172	0.402
Memorability	0.521	0.610	0.342	0.402
Learnability	-1.606	0.131	0.196	0.402
Attractiveness	2.048	0.060	0.752	0.402
Error tolerance	0.323	0.751	1.000	0.402
Security	9.865	0.000	0.0625	0.402

model had lower variance on usability aspects *efficiency, satisfaction, memorability, learnability and security*. In F-test, the null hypotheses were that both models have the same consistency against the alternate hypotheses that fingerprint model has lower consistency. Research group applied left tailed test with alpha value 0.05. The alternate hypotheses were accepted in usability aspects *efficiency, satisfaction, memorability, learnability and security*. The null hypotheses were accepted in usability aspects *attractiveness and error tolerance*.

4) ASSOCIATION ANALYSIS

For this study research group evaluated both model one after the other. It was very necessary to evaluate the association level between these two models. The results of the association level described whether users have evaluated both models independently or not. Research group performed a test of seven hypotheses (H1 through H7) for each usability parameters. The strength and direction of the linear relationship between two categorical variables may be observed through the Pearson correlation coefficient. Pearson correlation coefficient may generate a result from -1 to $+1$. A high positive correlation is presented by $+1$ and a high negative correlation is represented by -1. If the correlation coefficient is zero then there is no correlation between the two variables. The values between 0 and 1(or -1) represent the degree of relationship. The Spearman correlation is a rank order, nonparametric version of Spearman correlation coefficient. The strength and direction of the association between two categorical ranked variables may be calculated through the Spearman correlation coefficient. The results obtained from running the Pearson correlation coefficient and Spearman correlation coefficient are summarized in table 9. From table 9 it is revealed that in all usability aspects elderly participants' ranked proposed model and traditional model independently. There is no significant relationship between these two models' ranking and elderly participant ranked both models independently. From table 10 it is revealed that in all usability aspects expert participants' ranked proposed model and traditional model independently. There is no significant relationship between these two models' ranking and expert participants ranked both models independently.

B. DISCUSSION

The data was taken during the session from both groups. Different observations were as follows:

TABLE 9. Results of pearson and spearman correlation coefficient with elderly participants.

Elderly Participants				
Hypotheses	**Correlation Coefficient**			
	Pearson Correlation Coefficient		**Spearman Correlation Coefficient**	
	Test Statistics	Sig Value	Test Statistics	Sig Value
Efficiency	0.449	0.093	0.406	0.133
Satisfaction	-0.098	0.728	-0.108	0.703
Memorability	0.080	0.777	0.191	0.495
Learnability	-0.308	0.264	-0.299	0.279
Attractiveness	-0.259	0.351	-0.179	0.522
Error tolerance	0.270	0.330	0.237	0.394
Security	0.075	0.791	0.032	0.909

TABLE 10. Results of pearson and spearman correlation coefficient with elderly participants.

Expert Participants				
Hypotheses	**Correlation Coefficient**			
	Pearson Correlation Coefficient		**Spearman Correlation Coefficient**	
	Test Statistics	Sig Value	Test Statistics	Sig Value
Efficiency	0.397	0.143	0.359	0.189
Satisfaction	0.392	0.149	0.327	0.233
Memorability	-0.059	0.836	-0.059	0.834
Learnability	0.010	0.972	0.195	0.486
Attractiveness	-0.190	0.497	-0.197	0.481
Error tolerance	-0.196	0.483	-0.96	0.483
Security	0.075	0.909	0.032	0.909

1) Fingerprint Enrollment Process: The data was collected when both the groups were performing the process of fingerprint enrollment with a mobile application. It was observed that 85% of the elderly people group and all participants from the expert group performed the task without assistance.
2) Card Parking Process: Card parking involved the process of inserting card information through application user interface. This was observed that elderly group faced little problems while providing data to the mobile application, in contrast to the expert group who performed the process in a very efficient manner. Only one participant needed assistance in this process.
3) Fingerprint Attaching Process: Fingerprint attaching process has made simple easy for the user so this was observed that it was the process in which both groups performed very well and needed no assistance. This was observed that all of the participants completed the process without any assistance.
4) Payment Request Process: For the payment request process it was observed that both groups made little mistakes. The reason for this problem may be the interface screen of the application. Research group tried to make this process more effortless in the next version,
5) Payment Process Initiation: Both groups of the participants made little mistakes in this process. The reason behind their mistakes could be that both groups were using the application for the first time and were not very much familiar with this.

This was observed that there was a difference in performance when the user used fingerprint sensor available at the front or back of the mobile device. This was observed that the participants were performing the task well when fingerprint scanner was available at front of the mobile phone as compared to when it was available at the back of the mobile phone. The participants who performed the test with a mobile phone having a fingerprint sensor at the back found the application difficult to use and hence were stuck in the process of providing fingerprint at the time of payment. This shows that the sensor at back was not suitable for the applications which used fingerprint for authentication.

Participants shared that two-touch protocol satisfied them and they felt that this gave more confidence and self-assurance on security and control.

One of the interesting observations, which was revealed to the research group, that most of the participants preferred primarily their thumb and index finger for the enrollment in a mobile application. Most of the participants used their thumb, index finger and little finger of right hand. Left thumb and left index finger were used if participants needed to use the left hand.

After the evaluation study, a general question was asked to the participant that whether they would prefer to use the digital wallet for their billing at POS. All the participant replied positively in favor of use because the proposed authentication mechanism satisfied them on both criteria of usability and security.

1) KEEPING A LOT OF CARDS

Elderly brain cannot focus on detail of events. Keeping things in order is difficult for them. Elderly would not need to fumble their cards through wallet using the proposed mechanism.

Keeping a few cards in their wallet may create confusion and would be cumbersome. By the proposed mechanism elderly could get rid of keeping cards all the time in the wallet. Elderly may use the mobile application ubiquitously without the need of presenting the physical card at POS.

2) MEMORIZATION

Facing difficulty in memorizing their valuables is a well-known problem of elderly. The proposed work helps elderly through fingerprint verification method. By using fingerprints all his cards were saved on a mobile device so there will be no need to memorize any password. Instead of using one factor, two factors or multi-factor authentication [14], this work exploited the biometric authentication method. Furthermore, elderly may face difficulty to complete a transaction using one-time password (OTP) or personal identification number (PIN) due to its complicated method. Elderly may lose attention during the process. OTP and PIN both are vulnerable to brute force attack and extremely disposed to be misused by an unauthorized user, result in user dissatisfaction. Drawing an authentication pattern on the touch screen is also a widely held method in payment application but it requires memorizing and drawing a correct pattern each time to use the device which is difficult for an elderly user. The proposed mechanism completes a transaction by only three tapping of the same finger on mobile device hence user does not need to memorize PIN, entering an OTP or drawing a pattern on touchscreen.

3) SHOULDER SNOOPING

Since the POS location is always a public place and crowded area with a lot of people present around, the user may not feel secure using and entering his password for the transaction. The proposed mechanism required fingerprint of the user to complete a transaction hence no shoulder snooping was possible. The user can start a complete a transaction without having any fear of his password being stolen.

4) SECURITY ISSUES

Security issue is considered most challenging for the mobile application designer. The unapproved party may have access to confidential information such as user and merchant identity, payment card number, the time, location, amount of the billing and mode of billing. The outflow of this confidential information may negatively affect the buyer as well as a merchant. Both physical security and user security are needed for digital wallet application. Physical security is concerned with the issues such as communication channel, and token exchange between the stakeholders involved in the payment mechanism. User security keeps track of matters such as user actions in order to complete a transaction. The biometric verification method has been employed in the proposed mechanism as it is considered the most trusted authentication methods in theory [55]. The credit card information and fingerprints of the user will be saved using state of the art encryption techniques that confidential information could not be viewed stored and transported. The mobile devices stored fingerprint data as a mathematical representation that cannot be reversed. No algorithm can reverse engineer the fingerprint data. Instead of providing a physical card at POS the buyer used his fingerprint to complete a billing process so even the card number was not exposed to the merchant. The card remained saved and secured with the buyer. The card was free-form physical loss, unintentional damage, or any other kind of harm. Traditionally the merchant is responsible to arrange the billing process by adding some hardware to his system. The new payment system should be easy to integrate with merchant POS. The proposed mechanism did not bother the merchant to keep and install extra hardware for billing. The billing information will be sent to user mobile devices through Bluetooth technology which is mostly available in POS systems. The buyer information was not disclosed to the merchant as payment details were sent through buyer mobile device not form merchant POS. The proposed mechanism ensured that the buyer's detail and billing request were sent in encrypted form. The buyer felt safe while making the billing process.

5) IDENTITY THEFT

The algorithm suggested for billing in the proposed work used fingerprint verification for each transaction. This saved buyer form the identity theft attack, reported, from any unauthorized party. Nobody can make a billing process even in the presence of a buyer mobile device. If the mobile device of the buyer is lost or stolen and used by another person then it will not be able to generate any data packet to TO in the absence of buyer fingerprint data. The TO confirmed the validity of the data packet by using a time stamp form data packet. The data packet from the mobile application was sent to TO after making all necessary security requirements.

6) LESS NETWORK TRAFFIC

Most of the communication for the billing authentication process was done between the merchant's POS and buyer's mobile device and it was buyer mobile device that sent a request for billing to To. Hence no network traffic for TO and the financial organization was generated. The buyer mobile application prepared a data packet to TO after the authentication of the buyer. In this way, only one encrypted message from the buyer mobile device to TO was generated to request for payment form his account.

7) SECURED TRANSACTION

The proposed mechanism made the transaction secure by not keeping any information about the buyer at the merchant application. The merchant requires only the Bluetooth ID of the buyer and the bill will be sent on Bluetooth ID of the buyer. The merchant POS will not be able to use any information from the buyer. No information of the buyer will be accessible by POS even if POS is captured by an unauthorized party.

8) FAST TO USE

The proposed mechanism proved to be fast to use the mechanism as the participants were able to complete a transaction within a very short interval of time as no password, PIN, or OTP was required to complete a transaction. The bill was paid as soon as the participant selected and confirmed the card. The payment is done and a confirmation message is received.

9) IMPOSSIBLE TO REPLICATE

The billing process was impossible to replicate as no user can replicate the transaction without the user's fingerprint. The cards were electronically saved on using mobile devices with fingerprint association so no other party could replicate it.

10) TAMPER PROOF

The proposed mechanism provided a temper proof transaction as no party can change, open or remove the transaction. The token is transmitted from user mobile to TO with the user confirmation hence no tempering is possible. The proposed mechanism required the user to explicitly confirm the details of each transaction made by his mobile device.

11) ERROR CONTROLLING MECHANISM

Error control module of the proposed application handled user mistakes in the billing process and made sure that the user was able to recover from his mistakes. It was made easy to recover from any error done by the user. The application provided a cancel button on appropriate screens so that the user can come out form any error situation. Easily accessible processes helped the user to complete the billing process with maximum ease.

12) CARD SAFETY

As the presented work was specially intended to elderly, the proposed mobile application provided a highly simplified user interface so that anytime the card information as well as fingerprint information may be changed by the elderly. The elderly may alter any association of cards and fingerprints through an easy process supported by pictures. The association of finger and cards can be seen by elderly anytime so he will be able to keep association fresh in his memory. Before any billing process, he may view the association.

13) PAYMENT CONFIRMATION

Buyer received a payment confirmation message with the card number and merchant information when his bill amount was credited from his account. In this way, the buyer was able to endorse any unauthorized activity from his account.

14) COGNITIVE OVERLOAD

As the working memory of elderly becomes weak and learning new skills is a complex task for the them, the payment solution made for the elderly should not put any mental or technical overload to them. The proposed mechanism made the task of authentication easy for them by just providing fingerprint at the time of billing.

15) ACTIVITY LOG

All the user's billing information was saved in the application so that the user was able to analyze his buying profile. This profile was maintained as a user-specific requirement and anytime the user was able to alter the profile.

V. CONCLUSION

We conclude that digital wallet payment solutions could be enhanced if provided with the ease of access. The novelty of the proposed work lies in the technique through which an elderly user's fingerprint is captured and used for the billing at POS. The proposed technique of card selection through fingerprint has not been used so far in digital wallet applications. All elderly payment cards are virtually stored on the digital wallet application with the association of his one fingerprint. Elderly felt secure while paying bills at POS by the proposed mechanism. The result of the prototype evaluation showed that the proposed mechanism was highly secure and satisfied with the target user. The use of fingerprint authentication proved that the billing process cannot be initiated without the involvement of the actual owner of the mobile device. According to elderly ratings fingerprint model performed better on usability aspects efficiency $t(14)=5.551$, $P=0.000071$, satisfaction $t(14)=3.389$, $P=0.004$ and security $t(14)=8107$, $P=0.000001$. According to expert participants fingerprint model performed better on usability aspects efficiency $t(14)=3.378$, $P=0.005$, satisfaction $t(14)=3.900$, $P=0.002$ and security $t(14) =9.866$, $P=0.000$.

ACKNOWLEDGMENT

The authors thank the support from the Deanship of Scientific Research, Najran University, Saudi Arabia.

REFERENCES

[1] M. Taghiloo, M. Ali Agheli, and M. Reza Rezaeinezhad, "Mobile based secure digital wallet for peer to peer payment system," 2010, *arXiv:1011.0279*. [Online]. Available: http://arxiv.org/abs/1011.0279

[2] D. Lanter and R. Essinger, "User-centered design," in *The International Encyclopedia of Geography*. Atlanta, GA, USA: American Cancer Society, 2017, pp. 1–4.

[3] M. Y. Cortes, A. Guerrero, J. V. Zapata, M. L. Villegas, and A. Ruiz, "Study of the usability in applications used by children with down syndrome," in *Proc. 8th Comput. Colombian Conf. (CCC)*, Aug. 2013, pp. 1–6.

[4] D. Tao and C. Or, "A paper prototype usability study of a chronic disease self-management system for older adults," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage.*, Dec. 2012, pp. 1262–1266.

[5] D. Way and J. Paradiso, "A usability user study concerning free-hand microgesture and wrist-worn sensors," in *Proc. 11th Int. Conf. Wearable Implant. Body Sensor Netw.*, Jun. 2014, pp. 138–142.

[6] P. S. Rachna, "Issues and challenges of electronic payment systems," *Int. J. Innov. Res. Develop.*, vol. 2, no. 9, pp. 25–30, 2013.

[7] E. L. Gilje, "Usability challenges for contactless mobile payment at a physical point of sale: Central themes and trade-offs," M.S. thesis, Institute for datateknikkoginformasjonsvitenskap, 2009.

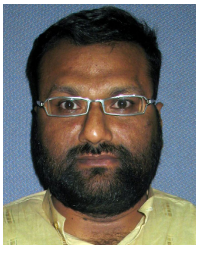
[8] Y. Wang, C. Hahn, and K. Sutrave, "Mobile payment security, threats, and challenges," in *Proc. 2nd Int. Conf. Mobile Secure Services (MobiSecServ)*, Feb. 2016, pp. 1–5.

[9] O. S. Okpara and G. Bekaroo, "Cam-wallet: Fingerprint-based authentication in M-wallets using embedded cameras," in *Proc. IEEE Int. Conf. Environ. Electr. Eng. IEEE Ind. Commercial Power Syst. Eur. (EEEIC/ICPS Eur.)*, Jun. 2017, pp. 1–5.
[10] D. Ray and S. Dutta, "Mobile-the digital wallet & efficiency booster for user-friendly banking system: Prospects & hurdles ahead," *SIT J. Manage.*, vol. 2. no. 2, pp. 230–250, Dec. 2012.
[11] W. Yang, J. Hu, S. Wang, J. Yang, and L. Shu, "Biometrics for securing mobile payments: Benefits, challenges and solutions," in *Proc. 6th Int. Congr. Image Signal Process. (CISP)*, Dec. 2013, pp. 1699–1704.
[12] K. Xi, T. Ahmad, F. Han, and J. Hu, "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment," *Secur. Commun. Netw.*, vol. 4, no. 5, pp. 487–499, May 2011.
[13] M. V. A. Dizaj, R. A. Moghaddam, and S. Momenebellah, "New mobile payment protocol: Mobile pay center protocol 2 (MPCP2) by using new key agreement protocol: VAM," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process.*, Aug. 2011, pp. 12–18.
[14] A. Tiwari, S. Sanyal, A. Abraham, S. J. Knapskog, and S. Sanyal, "A multi-factor security protocol for wireless payment–secure Web authentication using mobile devices," 2011, *arXiv:1111.3010*. [Online]. Available: https://arxiv.org/abs/1111.3010
[15] H. El, H. Houmani, and H. Madroumi, "A secure electronic transaction payment protocol design and implementation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 5, no. 5, pp. 172–180, 2014.
[16] F. Liébana-Cabanillas, F. Muñoz-Leiva, and J. Sánchez-Fernández, "A global approach to the analysis of user behavior in mobile payment systems in the new electronic environment," *Service Bus.*, vol. 12, no. 1, pp. 25–64, Mar. 2018.
[17] R. Batra and N. Kalra, "Are digital wallets the new currency?" *Apeejay J. Manage. Technol.*, vol. 11, no. 1, pp. 1–12, 2016.
[18] A. Brahma and R. Dutta, "Cashless transactions and its impact—A wise move towards digital India," *Int. J. Sci. Res. Comput. Sci., Eng. Inf. Technol.*, vol. 3, no. 3, pp. 14–28, 2018.
[19] J. Nicolaisen, "Digital challenges for the payment system," in *Proc. Financial Ind. Digit. Services Conf.*, 2016, pp. 1–5.
[20] A. Gupta, "Digital payment: A giant step towards cashless India," *Int. J. Acad. Res. Develop.*, vol. 2, no. 6, pp. 410–412, 2017.
[21] R. Singla, "Digital wallet: A handy solution in the wake of demonetisation," *Econ. Times*, vol. 8, no. 1, 2017.
[22] B. A. Urs, "Security issues and solutions in e-payment systems," *Fiat Iustitia*, vol. 11, no. 1, pp. 172–179, 2015.
[23] J. Khalilzadeh, A. B. Ozturk, and A. Bilgihan, "Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry," *Comput. Hum. Behav.*, vol. 70, pp. 460–474, May 2017.
[24] S. Singh and R. Rana, "Study of consumer perception of digital payment mode," *J. Internet Banking Commerce*, vol. 22, no. 3, pp. 1–4, 2017.
[25] B. S. Gupta, "E-Wallet: Challenges for rural market," *PARIDNYA-MIBM Res. J.*, vol. 5, no. 1, pp. 36–46, 2017.
[26] S. Hillman and C. Neustaedter, "Trust and mobile commerce in north america," *Comput. Hum. Behav.*, vol. 70, pp. 10–21, May 2017.
[27] S. Tang, Z. Wu, X. Zhang, G. Wang, X. Ma, H. Zheng, and B. Zhao, "Towards understanding the adoption and social experience of digital wallet systems," in *Proc. 52nd Hawaii Int. Conf. Syst. Sci.*, 2019, pp. 5093–5102.
[28] S. Daskapan, J. V. D. Berg, and A. A. Eldin, "Towards a trustworthy short-range mobile payment system," *Int. J. Inf. Technol. Manage.*, vol. 9, no. 3, p. 317, 2010.
[29] M. M. Rahman and T. Sloan, "Opportunities and challenges of M-commerce adoption in Bangladesh: An empirical study," *J. Internet Banking Commerce*, vol. 20, no. 3, pp. 1–9, 2015.
[30] T. Zhou, "An empirical examination of users' switch from online payment to mobile payment," *Int. J. Technol. Hum. Interact.*, vol. 11, no. 1, pp. 55–66, Jan. 2015.
[31] G. De Kerviler, N. T. Demoulin, and P. Zidda, "Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers?" *J. Retailing Consumer Services*, vol. 31, pp. 334–344, Jul. 2016.
[32] F. Liébana-Cabanillas, J. Sánchez-Fernández, and F. Muñoz-Leiva, "The moderating effect of experience in the adoption of mobile payment tools in virtual social networks: The m-payment acceptance model in virtual social networks (MPAM-VSN)," *Int. J. Inf. Manage.*, vol. 34, no. 2, pp. 151–166, Apr. 2014.
[33] N. Koenig-Lewis, M. Marquet, A. Palmer, and A. L. Zhao, "Enjoyment and social influence: Predicting mobile payment adoption," *Service Industries J.*, vol. 35, no. 10, pp. 537–554, Jul. 2015.
[34] Y. Yang, Y. Liu, H. Li, and B. Yu, "Understanding perceived risks in mobile payment acceptance," *Ind. Manage. Data Syst.*, vol. 115, no. 2, pp. 253–269, Mar. 2015.
[35] J. Lu, J. E. Yao, and C.-S. Yu, "Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology," *J. Strategic Inf. Syst.*, vol. 14, no. 3, pp. 245–268, Sep. 2005.
[36] N. Arvidsson, "Consumer attitudes on mobile payment services–results from a proof of concept test," *Int. J. Bank Marketing*, vol. 32, no. 2, pp. 150–170, Apr. 2014.
[37] T. Zhou, "An empirical examination of Users' switch from online payment to mobile payment," *Int. J. Technol. Hum. Interact.*, vol. 11, no. 1, pp. 55–66, Jan. 2015.
[38] R. Thakur, "Customer adoption of mobile payment services by professionals across two cities in India: An empirical study using modified technology acceptance model," *Bus. Perspect. Res.*, vol. 1, no. 2, pp. 17–30, Jan. 2013.
[39] G. W.-H. Tan, K.-B. Ooi, L.-Y. Leong, and B. Lin, "Predicting the drivers of behavioral intention to use mobile learning: A hybrid SEM-neural networks approach," *Comput. Hum. Behav.*, vol. 36, pp. 198–213, Jul. 2014.
[40] A. Gannamaneni, J. Ondrus, and K. Lyytinen, "A post-failure analysis of mobile payment platforms," in *Proc. 48th Hawaii Int. Conf. Syst. Sci.*, Jan. 2015, pp. 1159–1168.
[41] A. S. Al-Ajam and K. Md Nor, "Challenges of adoption of Internet banking service in yemen," *Int. J. Bank Marketing*, vol. 33, no. 2, pp. 178–194, Apr. 2015.
[42] S. Padashetty and K. S. Kishore, "An empirical study on consumer adoption of mobile payments in Bangalore city—A case study," *Res. World*, vol. 4, no. 1, p. 83, 2013.
[43] E. Tan and J. Leby Lau, "Behavioural intention to adopt mobile banking among the millennial generation," *Young Consumers*, vol. 17, no. 1, pp. 18–31, Apr. 2016.
[44] T. Wadhera, R. Dabas, and P. Malhotra, "Adoption of M-wallet: A way ahead," *Int. J. Eng. Manage. Res.*, vol. 7, no. 4, pp. 1–7, 2017.
[45] N. Mallat, "Exploring consumer adoption of mobile payments—A qualitative study," *J. Strategic Inf. Syst.*, vol. 16, no. 4, pp. 413–432, 2007.
[46] S. Nagaraju, "A research study on select customers perception on digital money and digital payments associate professor," *Gandhi Acad. Tech. Educ.*, vol. 7, no. 7, pp. 55–68, 2018.
[47] N. Cooharojananone, P. Kongnim, A. Mongkolnut, and O. Hitoshi, "Evaluation study of usability factors on mobile payment application on two different service providers in thailand," in *Proc. IEEE/IPSJ 12th Int. Symp. Appl. Internet*, Jul. 2012, 233-238.
[48] J. Brooke, "SUS: A 'quick and dirty'usability," *Usability Eval. Ind.*, vol. 189, no. 194, pp. 4–7, 1996.
[49] J. Kirakowski and M. Corbett, "SUMI: The software usability measurement inventory," *Brit. J. Educ. Technol.*, vol. 24, no. 3, pp. 210–212, Sep. 1993.
[50] H. Melkas, "Effective gerontechnology use in elderly care work: From potholes to innovation opportunities," in *The Silver Market Phenomenon*. Berlin, Germany: Springer, 2011, 435-449.
[51] R. Likert, "A technique for the measurement of attitudes," *Arch. Psychol.*, vol. 140, no. 55, 1932.
[52] J. Nielsen, *Usability Engineering*. San Mateo, CA, USA: Morgan Kaufmann, 1993.
[53] D. Tromp, A. Dufour, S. Lithfous, T. Pebayle, and O. Després, "Episodic memory in normal aging and alzheimer disease: Insights from imaging and behavioral studies," *Ageing Res. Rev.*, vol. 24, pp. 232–262, Nov. 2015.
[54] D. Dennehy and D. Sammon, "Trends in mobile payments research: A literature review," *J. Innov. Manage.*, vol. 3, no. 1, pp. 49–61, Apr. 2015.
[55] M. O. Derawi, B. Yang, and C. Busch, "Fingerprint recognition with embedded cameras on mobile phones," in *Proc. Int. Conf. Secur. Privacy Mobile Inf. Commun. Syst.* Berlin, Germany: Springer, 2011, pp. 136–147.
[56] M. Gordon and S. Sankaranarayanan, "Biometric security mechanism in mobile payments," in *Proc. 7th Int. Conf. Wireless Opt. Commun. Netw. (WOCN)*, 2010, pp. 1–6.

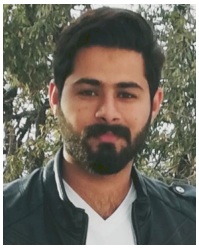
SARWAT IQBAL received the Ph.D. degree from the Federal Urdu University of Arts, Science and Technology. She is working as a Visiting Faculty Member with the Department of Computer Science, Federal Urdu University of Arts, Science and Technology. She has authored more than 18 publications in different national and international journals. Her research interests include disability assistance, elderly assistance, mobile and wireless communication, information systems, knowledge management, and healthcare.

MUHAMMAD IRFAN received the Ph.D. degree in electrical and electronic engineering from the Universiti Teknologi PETRONAS, Malaysia, in 2016. He is currently working as an Assistant Professor with the Electrical Engineering Department, Najran University, Saudi Arabia. He has two years of industry experience and three years of teaching experience. He has authored more than 50 research articles in reputed journals, books, and conference proceedings. His main research interests include automation and process control, condition monitoring, vibration analysis, artificial intelligence, the Internet of Things (IoT), smart cities, and smart healthcare.

KAMRAN AHSAN received the Ph.D. degree from the University of Staffordshire, U.K. After completing his Ph.D. degree with a vast experience of teaching and research projects, he returned to Pakistan with the spirit to serve the country and its people. He is an Avid Researcher and takes highest level of responsibility in ensuring the integrity of the research process. He is currently leading the Department of IT as the Director and as an Assistant Professor with the Department of Computer Science, FUUAST. He holds one patent to his credit while four others are almost finishing the process. He has widely published for his research in the area of disaster and health management through mobile technology which particularly includes his work for the disabled. In the limited span of time, he has earned great respect for his research; he has chaired several international conferences and worked on multiple funded projects. He has served as the Director of Quality Enhancement Cell (QEC) for a fairly long tenure in which he has initiated the entire department and its processes.

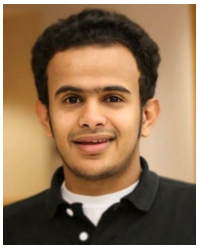


M. A. HUSSAIN is currently a Researcher with the Computer Science Department, Federal Urdu University of Arts, Science and Technology, Karachi, Pakistan. His research interests include disability assistance and elderly person's interaction with computer and smart devices.



MUHAMMAD AWAIS (Member, IEEE) received the B.S. degree in computer science from the University of Sargodha, Sargodha, Pakistan, in 2017, and the M.S. degree in computer science from COMSATS University Islamabad, Islamabad, Pakistan, under the supervision of Dr. Nadeem Javaid. He is currently pursuing the Ph.D. degree in communication systems with the School of Computing and Communications, Lancaster University, Lancaster, U.K., under the supervision of Dr. Haris Pervaiz. He also worked as a Research Associate with the Communications over Sensors Research Group, Department of Computer Science, COMSATS University Islamabad. He is also working as a Teaching Assistant with Lancaster University. He has authored over 20+ papers in technical journals and international conferences. His research interests include smart grid, routing in underwater wireless sensor networks, the Internet of Things-enabled WSNs, blockchain-based Systems, data science-based WSNs, and the Internet of Things enabled underwater sensor networks. He received the Best Paper Award Certificate in an International Conference namely EIDWT 2019. He also serves as a Regular Reviewer for numerous ISI indexed journals.

MUHAMMAD SHIRAZ (Member, IEEE) received the bachelor's degree (Hons.) from the CECOS University of Information Technology and Emerging Sciences, Peshawar, Pakistan, in 2004, the master's degree in computer science from Allama Iqbal Open University, Islamabad, Pakistan, in 2007, and the Ph.D. degree (Hons.) from the University of Malaya, Malaysia, in 2013. From 2013 to 2014, he was a Postdoctoral Fellow with the Centre for Mobile Cloud Computing Research, University of Malaya. He is currently an Assistant Professor with the Department of Computer Science, Federal Urdu University of Arts, Science and Technology Islamabad, Pakistan. His research interests include distributed applications design for ubiquitous networks, distributed systems, lightweight applications, smart client applications and optimization strategies, and mobile cloud computing. He received the Gold Medal from the CECOS University of Information Technology and Emerging Sciences, in 2004.



MOHAMMED HAMDI (Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science from Southern Illinois University, Carbondale, Il, USA, in 2013 and 2018, respectively. He is currently the Vice-Dean for Development and Quality. He is also an Assistant Professor of computer science with the College of Computer Science and Information Systems, Najran University, Saudi Arabia. His main research interests include database systems, database security, query optimization, data mining, big data, networks, and cryptography.

ABDULLAH ALGHAMDI received the B.Sc. degree in information systems from Al-Imam Muhammed Bin Saud University, Saudi Arabia, the M.Sc. degree in networking and systems administration from the Rochester Institute of Technology, Rochester, NY, USA, and the Ph.D. degree in computer and information systems engineering from Tennessee State University, Nashville, TN, USA. He is currently working as an Assistant Professor and the Head of the Information Systems Department, College of Computer Science and Information Systems, Najran University, Najran, Saudi Arabia. He has many publications in international journals and conferences. He is experienced in teaching, administration and research. His current research interests include security, privacy, the IoT, interdisciplinary applications, computer education, and academic leadership. He has been a Reviewer and guest editor of many journals, and he attended several conferences.