Identity Authentication Security Management in Mobile Payment Systems

Feng Wang

Ge Bao Shan

Yong Chen

Xianrong Zheng
Old Dominion University, x1zheng@odu.edu

Hong Wang

See next page for additional authors

Original Publication Citation

Feng, W., Ge Bao, S., Yong, C., Xianrong, Z., Hong, W., Sun, M., & Li, H. Identity management in mobile payment systems. Journal of Global Information Management, 28 (1), 189-203. https://doi.org/10.4018/JGIM.2020010110

Authors
Feng Wang, Ge Bao Shan, Yong Chen, Xianrong Zheng, Hong Wang, Sun Mingwei, and Li Haihua

Journal of Global Information Management
Volume 28 • Issue 1 • January-March 2020

Identity Authentication Security Management in Mobile Payment Systems

Feng Wang, School of Management, Jilin University, Changchun, China

Ge Bao Shan, School of Management, Jilin University, Changchun, China

Yong Chen, School of Business, Texas A&M International University, Laredo, USA

Xianrong Zheng, Department of Information Technology and Decision Sciences, Old Dominion University, Norfolk, USA
https://orcid.org/0000-0003-2695-9642

Hong Wang, College of Business and Economics, North Carolina A&T State University, Greensboro, USA

Sun Mingwei, Public Education and Teaching Department, Changchun Automobile Industry Institute, Changchun, China

Li Haihua, School of Management Science and Information Engineering, Jilin University of Finance and Economics, Changchun, China

ABSTRACT

Mobile payment is a new payment method offering users mobility, reachability, compatibility, and convenience. But mobile payment involves great uncertainty and risk given its electronic and wireless nature. Therefore, biometric authentication has been adopted widely in mobile payment in recent years. However, although technology requirements for secure mobile payment have been met, standards and consistent requirements of user authentication in mobile payment are not available. The flow management of user authentication in mobile payment is still at its early stage. Accordingly, this paper proposes an anonymous authentication and management flow for mobile payment to support secure transaction to prevent the disclosure of users' information and to reduce identity theft. The proposed management flow integrates transaction key generation, encryption and decryption, and matching to process users' personal information and biometric characteristics based on mobile equipment authentication carrier.

KEYWORDS

Anonymous Authentication, Authentication, Flow Management, Mobile Payment, Security

1. INTRODUCTION

The advent of electronic commerce, the growth of the Internet, and the development of wireless technologies promoted various payment methods in the past two decades (Assarzadeh and Aberoumand, 2018; Hassani, Huang, and Silva, 2018; Khan, Olanrewaju, Baba, Langoo, and Assad, 2017; Oliverio 2018; Viriyasitavat and Hoonsopon, 2018; Whitmore et al 2015). Particularly, the astonishing growth of mobile network and mobile devices make mobile payment globally applicable (De Vriendt, Lainé, Lerouge, and Xu, 2002; Paunov and Vickery, 2006). Wireless technologies, such as Near Field Communication (NFC), Bluetooth, Quick Response (QR) Code, and Radio Frequency Identification (RFID), enable consumers to process payment over mobile networks with their mobile devices for both online purchases and offline micropayments (Khan, Olanrewaju, Baba, Langoo, and Assad, 2017). Mobile payment is changing the payment market (Hedman and Henningsson, 2015)

DOI: 10.4018/JGIM.2020010110

and becomes an alternative to using cash, check, credit cards, or debit cards at a retail point of sale (Chen, 2008). In emerging economies where penetration of formal banking system is low, mobile payment has been well accepted (Khan, Olanrewaju, Baba, Langoo, and Assad, 2017). According to Statista (2018), worldwide transaction value with mobile payment amounts to $391.435 billion in 2018. Transaction value via mobile payment is expected to grow 35.7% annually from 2018 to 2022. The total amount of transaction value via mobile payment will be $1,328.244 billion in 2022.

Mobile payment provides users mobility, reachability, compatibility, and convenience (Kim, Mirusmonov, & Lee, 2010). It frees consumers from temporal and spatial limitations and enables them to make payment at anytime from anywhere (Yan and Yang, 2015; Zhou, 2015). However, mobile payment involves great uncertainty and risk due to its electronic and wireless nature (Leong, Ewing, & Pitt, 2003). Mobile networks are vulnerable to hacker attack and mobile devices may be infected by viruses or be lost (Zhou, 2015). For example, when mobile payment users connect their mobile devices with unsafe Wi-Fi, the authentication of their information might be intercepted (Chen & Chen, 2012; Li & Liu, 2014; Zhou, 2014). When mobile devices are lost or stolen, the stored sensitive information may fall into the wrong hands (Xi, Ahmad, Han, & Hu, 2011). Thus, security is a major concern among mobile payment users (Chen, 2018; Dahlberg, Guo, & Ondrus, 2015).

User authentication aims to confirm or deny a person's claimed identity. Cryptography is a conventional method of authenticating users and protecting communication messages in electronic payment systems (Xi, Ahmad, Han, & Hu, 2011). Traditional authentication methodologies are based on what the user knows (e.g., secret phrase, password, Personal Identification Numbers (PINs), and userIDs) or on what the user has (e.g., token, electronic card, passport, badges or smartcards). However, passwords, PIN, and key can be guessed out. In mobile payment, Subscriber Identity Module (SIM) cards are embedded in users' mobile devices, which are easy to be lost or stolen. Therefore, traditional authentication methodologies security countermeasures do not meet the requirements of mobile payment (Conti, Militello, Sorbello, & Vitabile, 2009). As a result, biometric techniques are applied in mobile payment for user authentication. For example, Apple Pay and Google's Android Pay use fingerprint recognition to certify consumer identity and conduct payments in 2013(Cheng, Hsu, & Lo, 2017). Alipay began to use fingerprint recognition functions to guarantee security of user information in 2015 (Guo & Bouwman, 2016). Although technology requirements for secure mobile payment have been met, standards and consistent requirements are not available. The flow management of user authentication in mobile payment is still at its early stage. Accordingly, this paper proposes an anonymous authentication and management flow for mobile payment to support secure transaction, to prevent the disclosure of users' information, and to reduce identity theft.

2. BACKGROUND

2.1. Mobile Payment

Mobile payment refers to payments for goods, services and invoices using a mobile device via wireless and other communication technologies (Dahlberg, Guo, & Ondrus, 2015). Mobile devices include smart phones, wireless handsets, personal digital assistants, radio frequency devices, or near field communication-based devices (Chen & Nath, 2008). The advance of mobile network technologies and mobile devices provides different formats of mobile payment. Wang, Hahn, and Sutrave (2016) classify mobile payment into mobile payment at the POS (e.g. Apple Pay and Google Wallet), mobile payment as the POS (e.g. Square Register), mobile payment platform (e.g. PayPal, Alipay, and WeChat payment), independent mobile payment system (e.g. mobile apps from Amazon and Starbucks), and direct carrier billing (e.g. Boku).

Mobile payment provides convenient payment features for daily purchases, including restaurant bills, bus and train tickets, movie tickets, as well as utility bills, and tuition fees (GeekPark, 2014). It reduces transaction fees and increases convenience (Hoofnagle, Urban, & Li, 2012). Fast data connections, broad areas of network coverage, and cheaper data plans make mobile payment widely adopted by consumers across the world (Chen, 2018).

2.2. Security in Mobile Payment

Data security refers to confidentiality, authentication, integrity, and non-repudiation (Merz, 2002; Li and Xu 2017). It involves methodology, technology, and practices which guarantee that data is secured from alteration or unintentional change, and unauthorized access, and that approved clients can get access to data promptly (Khan, Olanrewaju, Baba, Langoo, & Assad, 2017).

In the context of mobile payment, confidentiality means that transaction information of payments can only be viewed by authorized users (Chen, 2006; Khan, Olanrewaju, Baba, Langoo, & Assad, 2017; Merz, 2002). Data exchanged during a mobile payment transaction can only be read and understood by intended users (Suh & Han, 2003). Thus, transaction information of payments is encrypted to guarantee confidentiality (Merz, 2002).

Authentication means that data exchanged during a payment transaction is restricted to legitimate users only (Chen, 2006; Chen & He, 2013). It guarantees that the transaction information originates from the presumed transaction partner (Merz, 2002). Authentication includes user authentication and transaction data origin authentication. Authentication is a visible procedure that is directly related to payment security, and thus influences consumers' perceptions of security and trust (Chen & He, 2013; Kousaridas, Parissis, & Apostolopoulos, 2008; Tsiakis & Sthephanides, 2005). PINs, passcodes, screen locks, and fingerprints are usually required to guarantee authentication. Recently, many biological detection payment methods have been developed to ensure security certification in mobile payment transactions (Cheng, Hsu, & Lo, 2017).

Integrity means that data exchanged during a payment transaction remains intact and cannot be altered (Chen, 2006; Chen & He, 2013; Merz, 2002). It refers to the validity, accuracy and completeness of data (Hahn & Kodó, 2017), and measures the security of consumers' payment information during and after a payment process (Romdhane, 2005). Digital signatures are required to guarantee integrity (Merz, 2002).

Non-repudiation means that the participants of a payment transaction cannot deny their participation in the transaction (Suh & Han, 2003). In other words, no one should be able to claim that the transaction on his/her behalf was made without their knowledge (Merz, 2002). Digital signatures can guarantee non-repudiation and prevent either a consumer or a mobile payment service provider from denying a transmitted message (Merz, 2002).

2.3. Authentication in Mobile Payment

Cryptography is applied in mobile payment aiming for guaranteeing that only the user who possesses the correct cryptographic key can access the encrypted content (Xi, Ahmad, Han, & Hu, 2011). Cryptographic algorithms can be coarsely grouped into symmetric algorithm and asymmetric algorithm. Advanced Encryption Standard (AES), which adopts symmetric algorithm, was released by the U.S. Federal Bureau of Standards in 1997. CAST256, MARS, and Rivest Cipher (RC) 6 all follow AES. The symmetric algorithm is fast and suitable for encrypting long message (Xi, Ahmad, Han, & Hu, 2011). But exchanging cryptographic keys between a sender and a receiver is risky. In contrast, asymmetric algorithm does not need to exchange cryptographic keys between a sender and a receiver. Rivest-Shamir-Adleman (RSA), the most widely applied asymmetric algorithm, was proposed by Rivest, Shamir, & Adleman (1978). Miller (1985) and Koblitz (1987) propose an asymmetric cryptographic scheme called Elliptic Curve Cryptography (ECC), which has a smaller key size but offers the same security strength as RSA. Although ECC provides higher level of authentication than AES, it makes the signature computations very expensive and is applied in short message encryption/decryption only (Martinez-Pelaez, Rico-Novella, & Satizaba, 2010; Xi, Ahmad, Han, & Hu, 2011). Therefore, ECC is preferable for mobile devices that have small memories and low computational powers (Ahmad, Hu, & Han, 2009).

Compared with traditional electronic payment systems, mobile payment requires higher level of authentication. Meanwhile, user authentication in mobile payment cannot be too simple or too complex, because easy authentication is not able to guarantee that transaction is restricted to legitimate users only, whereas complex authentication systems may sacrifice the convenience of mobile payment (Al-Qayedi, Adi, Zahro, & Mabrouk, 2004; Chen, 2006). At present, many authentication mechanisms have been adopted to ensure mobile payment security, including user name/password, PINs, and token (Wang, Hahn, & Sutrave, 2016). These authentications are based on either knowledge that users know, such as passwords and PINs, or token that users have, such as SIM cards (Xi, Ahmad, Han, & Hu, 2011).

2.3.1. Password Authentication

Password authentication is the basic scheme of information assurance and security at the lowest cost (Hu, Sueng, Liao, & Ho, 2012). Single Sign-On (SSO) and One Time Password (OTP) are the main modes of password authentication. They conduct identifications via user ID and password. SSO is widely adopted by enterprises because users just need to log on once for accessing application systems on a network. Common SSO commercial modes include Access Master developed by Evidian, Etrust developed by Computer Associates, Tivoli Global Sign-On developed by IBM, Secure Login developed by Novell, and V-GO Single Sign-On developed by Passlogix (Wang, Ge, Zhang, Chen, Xin, & Li, 2013).

Scholars have studied password authentication from diverse perspectives. For example, In 1980s, an identity authentication solution based on a password list for access of remote users was presented (Akowuah, Yuan, Xu, & Wang, 2013). Purdy (1974) proposes to use a one-way function $Y=f(x)$ transformation for acquiring the corresponding relation between a password and an explicit text. Lamport (1981) presents a long-distance user authentication scheme based on a code (or password) table. Chang and Wu (1991) present a long-distance password authentication scheme based on the smart card of double-factor identity authentication. Ferraiolo and Kuhn (1992) propose the RBAC model, which authenticates users based on their name ID and passwords. Benenson, Dewald, and Freiling (2009) identify the security problem of users' authentication protocol in the sensor network and propose a multi-party authentication mechanism. Das, Saxena, and Gulati (2004) present a password authentication scheme based on dynamic ID. Nyang and Lee (2009) improve Das' double-authentication protocol. Liao, Lee, and Hwang (2005) improve Das' scheme and propose the double-way authentication. Aydos, Yanik, and Koc (2001) present ASK, a wireless authentication protocol, based on ECC. Liang and Wang (2005) propose a wireless authentication protocol using ECC for digital signature. Compared with traditional big-number operation password system, the performance of ECC is better in mobile identity authentication protocols (Akowuah, Yuan, Xu, & Wang, 2013; Chen & Chen, 2012; Shi, 2007; Xie & Liu, 2013; Yang, Lu, & Cao, 2011; Yang, Lu, & Cao, 2012).

The main disadvantage of password authentication mode is that it brings users a lot of difficulties. In addition, password-only mode of authentication does not fit for mobile payment because passwords are easy to forget, lose, or leak. In addition, it is extremely hard to identify who provides passwords (Han, Hu, Yu, Feng, Zhou, 2006; Hu & Han, 2009; Han, Hu, Yu, & Wang, 2007). However, although the security level of password-based long-distance identity authentication is low, password authentication is the most convenient, rapidest, and simplest identity authentication mode.

2.3.2. Biometric Authentication

As a secure and effective method for individual authentication, biometric authentication verifies users' unique and personal biometric features (Conti, Militello, Sorbello, & Vitabile, 2009). To improve security and privacy protection, intrinsic, specific, and exclusive biological features of human body, such as fingerprint, face, iris, sound, and vein, are adopted in mobile payment for user authentication (Cheng, Hsu, & Lo, 2017). Biometric authentication is effective because everyone has biometric features, which are unique from person to person and remain stable throughout one's lifetime (Xi, Ahmad, Han, & Hu, 2011). Biometric authentication provides higher level protection than conventional knowledge-based and token-based authentication methods (Maltoni, Maio, Jain, & Prabhakar, 2009). Biometric authentication consists of three steps, namely biometric signature acquisition, digital biometric signature extraction, and matching between the acquired biological signature and the stored correspondent one (Conti, Militello, Sorbello, & Vitabile, 2009).

If a person's physiological or behavioral features meet 7 requirements, these features can be used as biological features for authentication. Since 1990s, biometric identity theory and applications, especially the research on fingerprint and facial expression identification, have attracted much attention (Shen, Wang, Xu, Ma, Chaudhry, & He, 2016; Yang, Lu, & Cao, 2012; Yen, 2011). Face authentication becomes the focus of artificial intelligence and modal identification. Many algorithms are developed for promoting face authentication. Some applications for face authentication have been developed. So far face authentication is based on two main technologies. One is the picture-based 2D face authentication. The other is 3D face authentication that is based on 3D geometric information. Mature applications of face authentication were adopted by Beijing Olympic Games in 2008 and Shanghai World Expo in 2010 for detecting terrorists and preventing destructive or criminal activities.

However, unlike conventional knowledge-based and token-based authentication methods in which IDs, passwords, and certificates can be replaced, biometric data will be permanently compromised if it is stolen (Conti, Militello, Sorbello, & Vitabile, 2009).

2.3.3. Multi-factor Authentication

Multi-factor authentication includes double factor authentication and triple-factor authentication. Based on single-factor authentication (e.g. Secure Electronic Transaction), double-factor authentication uses an additional authentication token to generate dynamic passwords. For example, bio-cryptography combines the advantages of conventional cryptography and biometric security. Most triple-factor authentications integrate password, smart card, and biological features together (Wang, Ge, Zhang, Chen, Xin, & Li, 2013). Scholars have developed multi-factor authentication methods ready for mobile payment. For instance, Lee, Li, and Hwang (2002) present a fingerprint-based combined smart card to achieve triple-factor authentication based on long-distance users. Bhargav-Spantzel, Squicciarini, Modi, Young, Bertino, and Elliott (2007) propose a multi-factor long-distance authentication scheme that can conceal users' identity. Li and Hwang (2010) present a triple-factor authentication scheme based on the random function and one-way Hash function. At present, anonymous identity authentication becomes the trend for improving security in mobile payment.

3. PAYMENT FLOW MANAGEMENT IN ANONYMOUS BIOMETRIC AUTHENTICATION

In this section, three key components in biometric authentication will be discussed, namely users' personal information, biometric characteristics, and mobile devices. Authentication in mobile payment relies on these components. Only after these components are verified, can entrusted credit be provided and fund transactions be completed. Biometric authentication usually collects users' fingerprint, face, or iris.

A biometric identification system for mobile payment should be able to scan and map the biometric characteristics for users, register them on a database, and create a template that can be checked against all further scans to verify the user's identity (Conti, Militello, Sorbello, & Vitabile, 2009). Take fingerprint authentication as an example. First, users' fingerprint is preprocessed. Then users' fingerprint minutiae are extracted. Finally, fingerprint templates matching is conducted to find the correspondence between a processed fingerprint image and one or more stored templates.

3.1. Anonymous Biometric Authentication for Mobile Payment

According to Chen, Chen, Shih, and Wei (2011), anonymous authentication has requirements. First, authenticating servers cannot find anything about a user with a credential that is encrypted and transferred with or without the identity. Second, authenticating servers can decrypt a credential with a secret key or private key that is generated for verifying organizations only.

The three components required by anonymous biometric authentication are users' personal information (ID number, name, age, gender, title, and photo), biometric characteristics (fingerprint, face, or iris), and mobile equipment authentication carrier (short message service (SMS) card).

The following are the three conditions required by anonymous biometric authentication.

1. Hardware requirements. Users' mobile devices should have a video camera or a fingerprint CPU to collect their fingerprint, face, or iris. Users' mobile devices should have enough memory and space for processing collected biometric characteristics.
2. Biometric authentication system. Users' mobile devices and the mobile payment system should be embedded with biometric authentication system. Users' mobile devices should be able to initiate the collected biometric characteristics and to perform the preparation for real-time identity comparison. In addition, users' mobile devices should be able to generate the key for mobile payment and to send it to the mobile payment system. The mobile payment system should be able to compare users' biometric characteristics template, to decipher the transaction, and to complete the anonymous authentication.
3. Network. 2G/3G/4G/5G wireless networks or Wi-Fi network is needed to support the communication between users' mobile devices and mobile payment system. Biometric authentication relies on fast and reliable network connection.

With the development of technologies for mobile devices, many cell phones have built in camera now. This feature makes the collection of face much easier. In contrast, only some high-end cell phones have fingerprint collector. Accordingly, it is more convenient to collect face than fingerprint. Compared with fingerprint authentication, face authentication is easier to perform for mobile payment. As the development of mobile technologies, biometric authentication is expected to be adopted wider in mobile payment (Carton, Hedman, Damsgaard, Tan, & McCarthy, 2012).

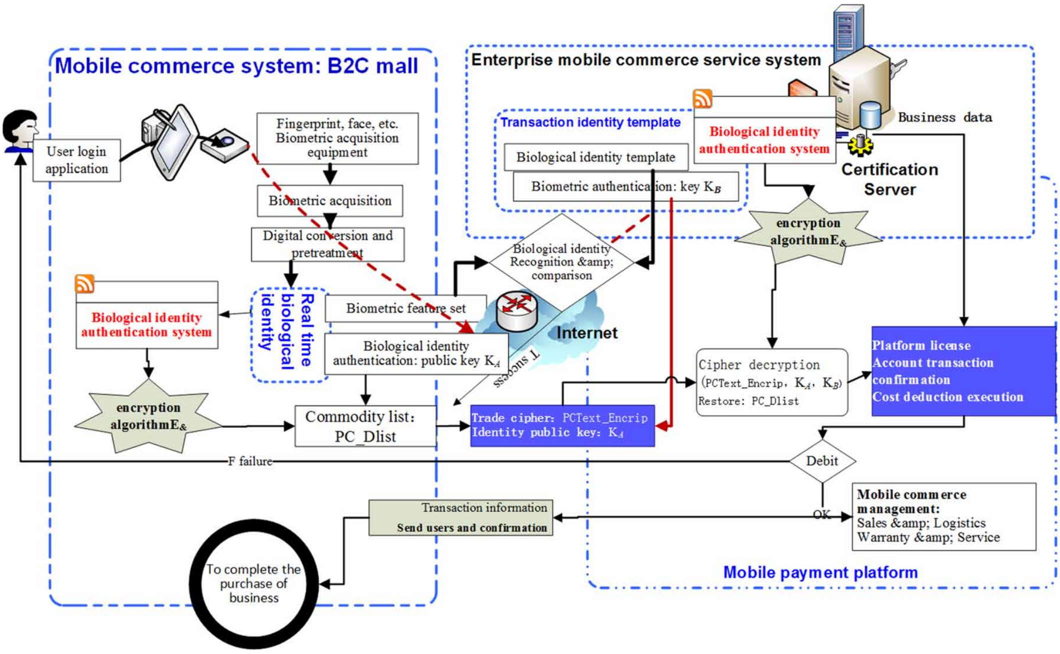
3.2. Anonymous Biometric Authentication and Mobile Payment Management Flow

Anonymous biometric authentication in mobile payment aims to protect users' identity and to achieve confidential communication and secure transaction. In practice, anonymous biometric authentication can effectively prevent users' information disclosure in interactions and protect users' privacy in mobile payment. However, standards and consistent requirements are missing in authentication of mobile payment. Although technology requirements for secure mobile payment have been met, flow management in mobile payment is still at its early stage. A wide-accepted flow management is not available for mobile payment. As shown in Figure 1, each component in flow management of mobile payment works individually. Accordingly, loopholes exist in existing flow management of mobile payment.

Take fingerprint authentication in mobile payment for an example. If users' signature is accepted, users' fingerprint is preprocessed on users' mobile devices and then transmitted from users' mobile devices to an authentication server. Next, minutiae in users' fingerprint are extracted on the server. At last, fingerprint templates matching is conducted on the server to find whether there is correspondence between a processed fingerprint image and one or more stored templates. A matching algorithm is required to perform the matching. If matching is found, the authentication is successful, and users can move to the next stage of transaction in mobile payment.

Face information includes eye model, nose and mouth vector triangle features, and expression features. In face authentication, a local field information assembly model O is generated for each person. Model O is a topographical structure model, where O=[(x,y),θ_A,θ_B,θ_C,f_i] (A, B, C are different feature points). In addition, face features of individuals are collected for generating the identity template standard structural assembly O'=[(x', y'), θ_A',θ_B', θ_C', f_i'] when users initiate face authentication. If detail points in users' face feature are same, the directional field and frequency field of O, A, B, C are same as well: Ψo(x,y)=Ψ'o' (x, y). Otherwise, displacement and rotation between a processed

Figure 1. Anonymous authentication and management flow in mobile payment


Mobile commerce system: B2C mall
User login application
Fingerprint, face, etc. Biometric acquisition equipment
Biometric acquisition
Digital conversion and pretreatment
Real time biological identity
Biological identity authentication system
encryption algorithmE$_&$
Biometric feature set
Biological identity authentication: public key K_A
Commodity list: PC_Dlist
F failure
Transaction information
Send users and confirmation
To complete the purchase of business
Enterprise mobile commerce service system
Transaction identity template
Biological identity template
Biometric authentication: key K_B
Biological identity authentication system
Business data
Certification Server
encryption algorithmE$_&$
Biological identity Recognition &amp; comparison
Internet
1 success
Trade cipher: PCText_Encrip
Identity public key: K_A
Cipher decryption
(PCText_Encrip, K_A, K_B)
Restore: PC_Dlist
Platform license
Account transaction confirmation
Cost deduction execution
Debit
OK
Mobile commerce management:
Sales &amp; Logistics
Warranty &amp; Service
Mobile payment platform

face image and one stored template can be found. All nodes in users' face need to be calculated for finding whether the deviation of certain statistical points of the standard nodes in *O* is more than *O*' (see Figure 2).

3.3. Anonymous Authentication Payment Transaction Application and Management

Anonymous payment needs mobile payment users to initiate the transaction request, including the category and quantity of purchased items, total amount of expenses, as well as the list of purchased items. Transactions of mobile payment occur on mobile payment users' devices and mobile payment platforms by following the steps below.

1. First, users' face feature is collected and preprocessed by their mobile devices. The radiofrequency camera in users' mobile devices collects users' face. Some parameters, such as system identification threshold and identification refuse rate *FAR*, are initialized.
2. Users' mobile devices send real-time request to the mobile payment platform asking for double-way authentication. After the request is received, the mobile payment platform conducts search in stored templates based on received characteristics and then discloses the face template it found. Next, a comparison between collected face data and the disclosed template is conducted by the mobile payment platform. At the end, the result of the comparison is returned from the mobile payment platform to users' mobile devices. If there is no matching, the mobile payment process stops.
3. If there is a matching in the comparison, the mobile payment platform establishes the transaction record and creates the product list *PC_Dlist* in this payment. Then the mobile payment platform follows its security encryption protocol standard to establish a public key K_A and a private key K_B. The encryption protocol management involves two categories of protocols, namely symmetrical protocols and asymmetrical protocols. Among these two protocols, asymmetrical one provides

Figure 2. Flow of getting the mobile payment key from biometric identity modeling

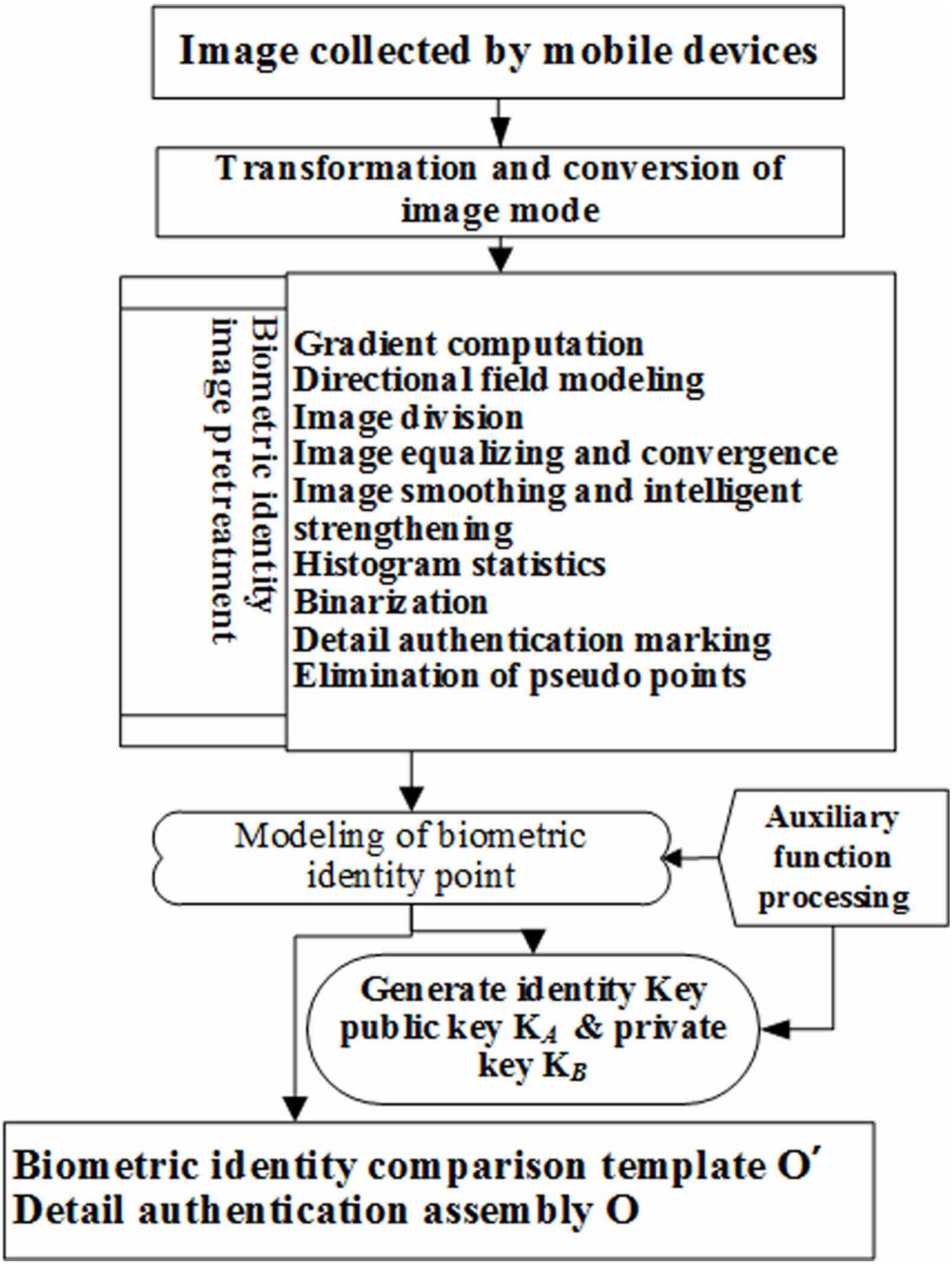


Image collected by mobile devices
Transformation and conversion of image mode
Biometric identity image pretreatment
Gradient computation
Directional field modeling
Image division
Image equalizing and convergence
Image smoothing and intelligent strengthening
Histogram statistics
Binarization
Detail authentication marking
Elimination of pseudo points
Modeling of biometric identity point
Auxiliary function processing
Generate identity Key public key K_A & private key K_B
Biometric identity comparison template O′
Detail authentication assembly O

higher security, because it is based on the elliptical hyperbola. The mobile payment platform keeps the public key K_A and then receives *PPText _Encrip* from users' mobile devices.

4. After getting *PPText _Encrip*, the mobile payment platform uses the private key K_B and the public key K_A to decipher it. Then the mobile payment platform gets the *PCDlis*t transaction

record to acquire the total amount in the transaction. At this stage, if mobile payment users do not cancel their transaction, the mobile payment platform will continue the process by establishing the automatic expense settlement based on users' authorization commitment and generating the settlement disposal result. Next, the mobile payment platform saves the transaction record *PC_Dlist*, keeps the transaction time, authorizes the information from users' mobile devices, and processes the record *PC_Dlist* and anonymous mobile transactions. At the end, the mobile payment platform closes the transaction line and ends the linking to users' mobile devices. If users make mobile payment for their online shopping, the shopping site will arrange shipping for users after it receives the confirmation of payment.

4. SUMMARY OF USER AUTHENTICATION IN MOBILE PAYMENT

The advent of electronic commerce, the growth of the Internet, and the development of wireless technologies promoted various payment methods in the past two decades (Bi et al 2018; Huang et al 2018; Lu 2018; Xu, He and Li 2014; Xu, Xu and Li 2018). Wireless technologies, such as Near Field Communication (NFC), Bluetooth, Quick Response (QR) Code, and Radio Frequency Identification (RFID), enable consumers to process payment over mobile networks with their mobile devices for both online purchases and offline micropayments (Cheng et al 2018; Jia et al 2018; Jiang et al 2014; Li et al 2013, 2015, 2018; Mao et al 2016; Wang et al 2014; Xu and Viriyasitavat 2014; Yang and Xu 2018; Zhai et al 2016). Mobile payment involves great uncertainty and risk given its electronic and wireless nature. Therefore, mobile payment needs to integrate identity authentication and privacy protection for strengthening access control. Compared with password authentication, biometric authentication can provide safer authentication. Particularly, anonymous biometric authentication can effectively prevent users' information disclosure in interactions. Biometric authentication has be adopted in mobile payment in recent years. For example, Apple, Alipay and Wechat Payment adopted fingerprint authentication in mobile payment in 2013. Later, Alipay and Wechat Payment apply face authentication in mobile payment. Biometric authentication is expected to be adopted more widely in mobile payment (Du, Wang, Du, Xu, Chaudhry, Bi, Guo, Huang, & Li, 2017; Kim, Mirusmonov, & Lee, 2010).

Although the main mobile payment platforms have adopted biometric authentication and technology requirements for secure mobile payment have been met, standards and consistent requirements are not available. The flow management of user authentication in mobile payment is still at its early stage. Accordingly, this paper proposes an anonymous authentication and management flow for mobile payment to support secure transaction, to prevent the disclosure of users' information, and to reduce identity theft.

The proposed management flow integrates public key and private key generation, encryption and decryption of the transaction, tracing management, and matching to process users' personal information and biometric characteristics based on mobile equipment authentication carrier. The management flow supports safe business transactions and payment settlement in mobile payment by reducing internal identity alteration and decryption risks. Anonymous authentication of biometric identity will be adopted more widely in mobile payment. Future studies should validate the management flow proposed by this paper and integrate pseudo face, fingerprint, and dynamic identity authentication to improve user authentication in mobile payment (Chen 2017; Lu and Xu 2018; Xu 2017; Xu et al 2009).

ACKNOWLEDGMENT

This research was partially supported by the National Science Foundation of China (NSFC) under Grant No. 71232011 and 71372077 and 985 Project of Jilin University under project 2017ZZ042.

REFERENCES

Ahmad, T., Hu, J., & Han, S. (2009, October). An efficient mobile voting system security scheme based on elliptic curve cryptography. In *Network and System Security, 2009. NSS'09. Third International Conference on* (pp. 474-479). IEEE. doi:10.1109/NSS.2009.57

Akowuah, F., Yuan, X., Xu, J., & Wang, H. (2013). A survey of security standards applicable to health information systems. *International Journal of Information Security and Privacy*, *7*(4), 22–36. doi:10.4018/ijisp.2013100103

Al-Qayedi, A., Adi, W., Zahro, A., & Mabrouk, A. (2004, March). Combined web/mobile authentication for secure web access control. In *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE* (Vol. 2, pp. 677-681). IEEE.

Assarzadeh, A., & Aberoumand, S. (2018). FinTech in Western Asia: Case of Iran. *Journal of Industrial Integration and Management*, *3*(3), 1850006. doi:10.1142/S2424862218500069

Aydos, M., Yanik, T., & Koc, C. K. (2001). High-speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor. *IEE Proceedings. Communications*, *148*(5), 273–279. doi:10.1049/ip-com:20010511

Benenson, Z., Dewald, A., & Freiling, F. C. (2009). Presence, Intervention, Insertion: Unifying Attack and Failure Models in Wireless Sensor Networks (Vol. 356). Technical report, University of Mannheim.

Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security*, *15*(5), 529–560. doi:10.3233/JCS-2007-15503

Bi, Z., Liu, Y., Krider, J., Buckland, J., Whiteman, A., Beachy, D., & Smith, J. (2018). Real-time force monitoring of smart grippers for Internet of Things (IoT) applications. *Journal of Industrial Information Integration*, *11*, 19–28. doi:10.1016/j.jii.2018.02.004

Carton, F., Hedman, J., Damsgaard, J., Tan, K. T., & McCarthy, J. (2012). Framework for mobile payments integration. *Electronic Journal of Information Systems Evaluation*, *15*(1), 14–25.

Chang, C. C., & Wu, T. C. (1991). Remote password authentication with smart cards. *IEE Proceedings. Computers and Digital Techniques*, *138*(3), 165–168.

Chen, H. (2017). Applications of Cyber-Physical System: A Literature Review. *Journal of Industrial Integration and Management*, *2*(3). doi:10.1142/S2424862217500129

Chen, L., & Nath, R. (2008). A socio-technical perspective of mobile work. *Information Knowledge Systems Management, 7*(1-2), 41-60.

Chen, L. D. (2006). A theoretical model of consumer acceptance of m-payment. *AMCIS 2006 Proceedings*, 247.

Chen, L. D. (2008). A model of consumer acceptance of mobile payment. *International Journal of Mobile Communications*, *6*(1), 32–52. doi:10.1504/IJMC.2008.015997

Chen, T. H., Chen, Y. C., Shih, W. K., & Wei, H. W. (2011). An efficient anonymous authentication protocol for mobile pay-TV. *Journal of Network and Computer Applications*, *34*(4), 1131–1137. doi:10.1016/j.jnca.2010.11.005

Chen, Y. (2018). *Security Risk Tolerance in Mobile Payment: A Trade-off Framework*. Academic Press.

Chen, Y., & Chen, J. (2012). Study on the business model of mobile payment industry. *Enterprise Economy, 8*, 99-104.

Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. *The International Review of Research in Open and Distributed Learning*, *14*(5). doi:10.19173/irrodl.v14i5.1632

Cheng, J., Chen, W., Tao, F., & Lin, C. (2018). Industrial IoT in 5G environment towards smart manufacturing. *Journal of Industrial Information Integration*, *10*, 10–19. doi:10.1016/j.jii.2018.04.001

Cheng, Y. W., Hsu, S. Y., & Lo, C. P. (2017). Innovation and imitation: Competition between the US and China on third-party payment technology. *Journal of Chinese Economic and Foreign Trade Studies*, *10*(3), 252–258. doi:10.1108/JCEFTS-05-2017-0012

Conti, V., Militello, C., Sorbello, F., & Vitabile, S. (2009). A multimodal technique for an embedded fingerprint recognizer in mobile payment systems. *Mobile Information Systems*, *5*(2), 105–124. doi:10.1155/2009/284124

Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications*, *14*(5), 265–284. doi:10.1016/j.elerap.2015.07.006

Das, M. L., Saxena, A., & Gulati, V. P. (2004). A dynamic ID-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics*, *50*(2), 629–631. doi:10.1109/TCE.2004.1309441

De Vriendt, J., Lainé, P., Lerouge, C., & Xu, X. (2002). Mobile network evolution: A revolution on the move. *IEEE Communications Magazine*, *40*(4), 104–111. doi:10.1109/35.995858

Du, X., Wang, H., Du, Y., Xu, L. D., Chaudhry, S., Bi, Z., & Li, J. et al. (2017). An industrial information integration approach to in-orbit spacecraft. *Enterprise Information Systems*, *11*(1), 86–104. doi:10.1080/1751 7575.2016.1173728

Ferraiolo, D., & Kuhn, R. (1992). Role-Based Access Control. *15th NIST-NCSC National Computer Security Conference*, 554-563.

GeekPark. (2014). Pay for the New Future-Six Major Change You Can't Miss. *Business Next*. Retrieved October 25th, 2018 from www.bnext.com.tw/article/33511/BN-ARTICLE-33511

Guo, J., & Bouwman, H. (2016). An ecosystem view on third party mobile payment providers: A case study of Alipay wallet. *Info*, *18*(5), 56–78. doi:10.1108/info-01-2016-0003

Hahn, I., & Kodó, K. (2017). Acceptance of Online and Mobile Payment: A Cross-Country Analysis of Germany, Hungary, and Sweden. Academic Press.

Han, F., Hu, J., Yu, X., Feng, Y., & Zhou, J. (2006, January). A novel hybrid crypto-biometric authentication scheme for ATM based banking applications. In *International Conference on Biometrics* (pp. 675-681). Springer.

Han, F., Hu, J., Yu, X., & Wang, Y. (2007). Fingerprint images encryption via multi-scroll chaotic attractors. *Applied Mathematics and Computation*, *185*(2), 931–939. doi:10.1016/j.amc.2006.07.030

Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. *Journal of Management Analytics*, *5*(4), 256–275. doi:10.1080/23270012.2018.1528900

Hedman, J., & Henningsson, S. (2015). The new normal: Market cooperation in the mobile payments ecosystem. *Electronic Commerce Research and Applications*, *14*(5), 305–318. doi:10.1016/j.elerap.2015.03.005

Hoofnagle, C. J., Urban, J. M., & Li, S. (2012). *Mobile payments: Consumer benefits & new privacy concerns*. Retrieved September 16th, 2018 from https://www.ftc.gov/es/system/files/documents/public_comments/2013/12/00007-89102.pdf

Hu, J., & Han, F. (2009). A pixel-based scrambling scheme for digital medical images protection. *Journal of Network and Computer Applications*, *32*(4), 788–794. doi:10.1016/j.jnca.2009.02.009

Hu, J. Y., Sueng, C. C., Liao, W. H., & Ho, C. C. (2012, January). Android-based mobile payment service protected by 3-factor authentication and virtual private ad hoc networking. In *Computing, Communications and Applications Conference (ComComAp), 2012* (pp. 111-116). IEEE.

Huang, B., Huan, Y., Xu, L., Zheng, L., & Zou, Z. (2018). Automated trading systems statistical and machine learning methods and hardware implementation: A survey. *Enterprise Information Systems*. doi:10.1080/1751 7575.2018.1493145

Jia, H., Sheng, Y., Han, W., & Wang, S. (2018). Data access control in data exchanging supporting big data arena. *Journal of Management Analytics*, *5*(3), 155–169. doi:10.1080/23270012.2018.1490212

Jiang, L., Xu, L., Cai, H., Jiang, Z., Bu, F., & Xu, B. (2014). An IoT Oriented Data Storage Framework in Cloud Computing Platform. *IEEE Transactions on Industrial Informatics*, *10*(2), 1443–1451. doi:10.1109/TII.2014.2306384

Khan, B. U. I., Olanrewaju, R. F., Baba, A. M., Langoo, A. A., & Assad, S. (2017). A Compendious Study of Online Payment Systems: Past Developments, Present Impact, and Future Considerations. *International Journal of Advanced Computer Science and Applications*, *8*(5), 256–271.

Kim, C., Mirusmonov, M., & Lee, I. (2010). An empirical examination of factors influencing the intention to use mobile payment. *Computers in Human Behavior*, *26*(3), 310–322. doi:10.1016/j.chb.2009.10.013

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, *48*(177), 203–209. doi:10.1090/S0025-5718-1987-0866109-5

Kousaridas, A., Parissis, G., & Apostolopoulos, T. (2008). An open financial services architecture based on the use of intelligent mobile devices. *Electronic Commerce Research and Applications*, *7*(2), 232–246. doi:10.1016/j.elerap.2007.04.003

Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, *24*(11), 770–772. doi:10.1145/358790.358797

Lee, C. C., Li, L. H., & Hwang, M. S. (2002). A remote user authentication scheme using hash functions. *Operating Systems Review*, *36*(4), 23–29. doi:10.1145/583800.583803

Leong, E. K., Ewing, M. T., & Pitt, L. F. (2003). Australian marketing managers' perceptions of the internet: A quasi-longitudinal perspective. *European Journal of Marketing*, *37*(3/4), 554–571. doi:10.1108/03090560310459087

Li, C. T., & Hwang, M. S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, *33*(1), 1–5. doi:10.1016/j.jnca.2009.08.001

Li, H., & Liu, Y. (2014). Understanding post-adoption behaviors of e-service users in the context of online travel services. *Information & Management*, *8*(8), 1043–1052. doi:10.1016/j.im.2014.07.004

Li, S., & Xu, L. (2017). *Securing the Internet of Things*. Syngress Press, Elsevier.

Li, S., Xu, L., & Wang, C. (2013). Compressed Sensing Signal and Data Acquisition in Wireless Sensor Networks and Internet of Things. *IEEE Transactions on Industrial Informatics*, *9*(4), 2177–2186. doi:10.1109/TII.2012.2189222

Li, S., Xu, L., & Zhao, S. (2015). The Internet of Things: A Survey. *Information Systems Frontiers*, *17*(2), 243–259. doi:10.1007/s10796-014-9492-7

Li, S., Xu, L., & Zhao, S. (2018). 5G Internet of Things: A Survey. *Journal of Industrial Information Integration*, *10*, 1–9. doi:10.1016/j.jii.2018.01.005

Liang, W., & Wang, W. (2005). On performance analysis of challenge/response based authentication in wireless networks. *Computer Networks*, *48*(2), 267–288. doi:10.1016/j.comnet.2004.10.016

Liao, I. E., Lee, C. C., & Hwang, M. S. (2005, August). Security enhancement for a dynamic ID-based remote user authentication scheme. In *Next Generation Web Services Practices, 2005. NWeSP 2005. International Conference on*. IEEE.

Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. *Journal of Management Analytics*, *5*(4), 231–255. doi:10.1080/23270012.2018.1516523

Lu, Y., & Xu, L. (2018). Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet of Things Journal*. DOI: 10.1109/JIOT.2018.2869847

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media. doi:10.1007/978-1-84882-254-2

Mao, J., Zhou, Q., Sarmiento, M., Chen, J., Wang, P., Jonsson, F., & Zou, Z. et al. (2016). A Hybrid Reader Transceiver Design for Industrial Internet of Things. *Journal of Industrial Information Integration*, *2*, 19–29. doi:10.1016/j.jii.2016.05.001

Martinez-Pelaez, R., Rico-Novella, F. J., & Satizaba, C. (2010). Study of mobile payment protocols and its performance evaluation on mobile devices. *International Journal of Information Technology and Management*, *9*(3), 337–356. doi:10.1504/IJITM.2010.030948

Merz, M. (2002). E-Commerce und E-Business: Marktmodelle,Anwendungen und Technologien (2nd ed.). Dpunkt Verlag.

Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417-426). Springer.

Nyang, D., & Lee, M. K. (2009). Improvement of Das's Two-Factor Authentication Protocol in Wireless Sensor Networks. *IACR Cryptology ePrint Archive, 2009*, 631.

Oliverio, J. (2018). A Survey of Social Media, Big Data, Data Mining, and Analytics. *Journal of Industrial Integration and Management*, *3*(3), 1850003. doi:10.1142/S2424862218500033

Paunov, C., & Vickery, G. (2006). *Online Payment systems for E-Commerce. Organization for Economic Co-operation and development*. OECD.

Purdy, G. B. (1974). A high security log-in procedure. *Communications of the ACM*, *17*(8), 442–445. doi:10.1145/361082.361089

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. doi:10.1145/359340.359342

Romdhane, C. (2005). Security implications of electronic commerce: A survey of consumers and businesses. *Internet Research: Electronic Networking Applications and Policy*, *9*(5), 372–382.

Shen, L., Wang, H., Xu, L., Ma, X., Chaudhry, S., & He, W. (2016). Identity management based on PCA and SVM. *Information Systems Frontiers*, *18*(4), 711–716. doi:10.1007/s10796-015-9551-8

Shi, H. (2007). *Factors of influence on consumer intention to use mobile payment services*. Zhejiang University Press.

Statista. (2018). *Mobile POS payments.* Retrieved September 20th, 2018 from https://www.statista.com/outlook/331/100/mobile-pos-payments/worldwide#market-revenue

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, *7*(3), 135–161. doi:10.1080/10864415.2003.11044270

Tsiakis, T., & Sthephanides, G. (2005). The concept of security and trust in electronic payments. *Computers & Security*, *24*(1), 10–15. doi:10.1016/j.cose.2004.11.001

Viriyasitavat, W., Hoonsopon, D. (2018) Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*. 10.1016/j.jii.2018.07.004

Wang, F., Ge, B., Zhang, L., Chen, Y., Xin, Y., & Li, X. (2013). A system framework of security management in enterprise systems. *Systems Research and Behavioral Science*, *30*(3), 287–299. doi:10.1002/sres.2184

Wang, L., Xu, L., Bi, Z., & Xu, Y. (2014). Data Cleaning for RFID and WSN Integration. *IEEE Transactions on Industrial Informatics*, *10*(1), 408–418. doi:10.1109/TII.2013.2250510

Wang, Y., Hahn, C., & Sutrave, K. (2016). Mobile payment security, threats, and challenges. In *Mobile and Secure Services (MobiSecServ), 2016 Second International Conference on* (pp. 1-5). IEEE. doi:10.1109/MOBISECSERV.2016.7440226

Whitmore, A., Agarwal, A., & Xu, L. (2015). The Internet of Things-A Survey of Topics and Trends. *Information Systems Frontiers*, *17*(2), 261–274. doi:10.1007/s10796-014-9489-2

Xi, K., Ahmad, T., Han, F., & Hu, J. (2011). A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. *Security and Communication Networks*, *4*(5), 487–499. doi:10.1002/sec.225

Xie, P., & Liu, H. (2013). ICT, mobile payment and electronic currency. *Financial Research, 10*, 1-14.

Xu, B. (2017). Guest Editorial. *Journal of Industrial Integration and Management*, *2*(3), 1702002. doi:10.1142/S242486221702002X

Xu, L., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*, *10*(4), 2233–2248. doi:10.1109/TII.2014.2300753

Xu, L., Liu, H., Wang, S., & Wang, K. (2009). Modeling and Analysis Techniques for Cross-Organizational Workflow Systems. *Systems Research and Behavioral Science*, *26*(3), 367–389. doi:10.1002/sres.978

Xu, L., & Viriyasitavat, W. (2014). A Novel Architecture for Requirement-oriented Participation Decision in Service Workflows. *IEEE Transactions on Industrial Informatics*, *10*(2), 1478–1485. doi:10.1109/TII.2014.2301378

Xu, L., Xu, E., & Li, L. (2018). Industry 4.0: State of the Art and Future Trends. *International Journal of Production Research*, *56*(8), 2941–2962. doi:10.1080/00207543.2018.1444806

Yan, H., & Yang, Z. (2015). Examining mobile payment user adoption from the perspective of trust. International Journal of u-and e-Service. *Science and Technology*, *8*(1), 117–130.

Yang, P., & Xu, L. (2018). The Internet of Things (IoT): Informatics Methods for IoT-enabled Health Care. *Journal of Biomedical Informatics*. 10.1016/j.jbi.2018.10.006

Yang, S., Lu, Y., & Cao, Y. (2011). Study on the adoption of cross channel consumer mobile payment. *Research Management*, *10*, 79–88.

Yang, S., Lu, Y., & Cao, Y. (2012). Model of initial adoption of mobile payment service and its empirical study. *Management Journal*, *9*, 1365–1372.

Yen, Y. S. (2011). The Impact of Perceived Value on Continued usage Intention in Social Networking Sites. *2nd International Conference on Networking and Information Technology, IPCSIT*, 217-223.

Zhai, C., Zou, Z., Chen, Q., Xu, L., Zheng, L., & Tenhunen, H. (2016). Delay-aware and reliability-aware contention-free MF-TDMA protocol for automated RFID monitoring in industrial IoT. *Journal of Industrial Information Integration*, *3*, 8–19. doi:10.1016/j.jii.2016.06.002

Zhou, T. (2014). An empirical examination of initial trust in mobile payment. *Wireless Personal Communications*, *77*(2), 1519–1531. doi:10.1007/s11277-013-1596-8

Zhou, T. (2015). An empirical examination of users' switch from online payment to mobile payment. *International Journal of Technology and Human Interaction*, *11*(1), 55–66. doi:10.4018/ijthi.2015010104

Feng Wang's research interests include Big Data, investment management; strategic management and rapid growth of enterprises; corporate governance and institutional management; international management and international entrepreneurship.

Yong Chen is an assistant professor of Management Information Systems at Texas A&M International University, Laredo, USA. Professor Chen earned his Ph.D.in information technology from Old Dominion University, USA. His research interests include information systems, information security, mobile payment, and social media. Professor Chen has published over 30 refereed papers in journals including Internet Research, Information Technology and Management, Systems Research and Behavioral Science, and Journal of Computer Information Systems.

Xianrong (Shawn) Zheng is an Assistant Professor of Information Technology and Decision Sciences Department, Old Dominion University, Norfolk, Virginia, United States. He received his Ph.D. degree in Computer Science from Queen's University, Canada. His research areas are Computing and Informatics, which involve Computer Science and Information Systems. His research interests are Data Science (Cloud Computing and Big Data), Artificial Intelligence (Machine Learning and Deep Learning), Electronic Commerce (Recommender Systems and Online Reviews), and FinTech (Blockchain and Bitcoin). He is a member of the ACM, the IEEE, and the AIS. Also, he is a Technical Program Committee Member of the IEEE International Conference on Internet of Things (IEEE ICIOT 2018-2019). Contact him please by email x1zheng@odu.edu.

Hong Wang received his Ph.D. in Management Information Systems/Decision Sciences from The Ohio State University. He is currently a Full Professor of MIS at North Carolina A&T State University in the USA. His research interests include Decision Sciences, Information Systems, Enterprise Systems, System Security and Information Assurance, Business Intelligence, Artificial Intelligence, Networking, and Business Process Reengineering. He has published numerous articles in academic journals such as Expert Systems with Applications, Expert Systems, Enterprise Information Systems, Systems Research and Behavioral Science, Electronic Government, International Journal of Management and Enterprise Development, Computers and Industrial Engineering, International Journal of Production Research, Computers and Operations Research, Information Technology and Management, Information Systems Frontiers, International Journal of Information Security and Privacy, Journal of Industrial Integration and Management, among others. He has also secured grants from the US National Science Foundation (NSF) and other sources totaled over $3.6 million. He is an active referee for several journals and conferences.

Sun Mingwei specializes in English culture and teaching including Intelligent manufacturing, Big Data, industrial information management, Industry 4.0, and e-commerce in IT field of computer science.

Li Haihua was born in Jilin Province, China, in 1975. She received the B.S. degree from Changchun University of Technology of China, in 1997 and the M.S. degree from Changchun University of Technology, in 2000, both in Computer science and technology. She received the Ph.D. degree from Changchun Institute of Optics, Fine Mechanics and Physics (CIOMP), Chinese Academy of Sciences (CAS), in 2003.