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).