Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Secure Mobile Payments in M-Commerce

Lavanya G
Computer Engineering, Dept of CS & E, P.E.S College of Engineering, Mandya,
Karnataka, India

Abstract— Mobile phones have increasingly become tools that consumers use for banking, payments, budgeting, and shopping. The security requirement for m-payment is increasing day by day due to rapid growth over mobile phones m- payment is characterized as any payment exchange including the buy of goods or benefits that are finished with a wireless device. M-payments encourage m-trade were clients make online purchases from their cell phones remotely whenever. This paper reviews the survey on security issues during design implementation, and attaining secure m-payment system (MPS) having a glance over vulnerabilities, threats, etc. The earlier literature on mobile payments, break down the different variables that affect MPS is studied and proposed bearings for future direction in this as yet developing the field. Contemporary Exploration best secures consumer point of view of Mobil payments and specialized security and trust. The effects of social and cultural components on mobile payments and, also, the comparison between the conventional and current payment systems are entirely un-investigated issues. The majority of the components sketched out by the framework have been tended to by exploratory and early stage studies.

Keywords— Future research, Literature review, Mobile phone, m-Commerce, m-Payment.

I. INTRODUCTION

The m-payment is become popular due to its broad applications, which can be used to tablets, smartphones, mPOS devices adoption by merchants, more growth app-based payments. The m-payment with secure payment and privacy towards the customer data is the big challenge. As the senior director Vanish Pandey in "strategy and product marketing", San Jose, California, states that "mobile and mobile based devices are becoming the latest mode for access to banking also for commerce". The mobile is emerging with enlarged opportunity for financial and business institutions to provide uninterrupted service to its customers. The growth of m-payment has lent strict rules and regulations to secure transactions [1].

A payment system that whose function is to provide secure financial transactions for its organization or another organization by using the mobile network is known as, m-payment system or in short (MPS). Commonly m-payment (m-p) gives the better quality of opportunity for merchants, financial institutions and also for the customers/users. The 'm-p' allows accessing the user/customer information by merchant and selects the specified group of the customer through different programs. Since last ten years the m-payment has gained more popularity due to increased mobile internet speed, wide spread application of many portable device and rapid growth towards mobile cellular service (MCS), (as per Group forecast of Garner) which has 96% users in 2013 while internet user rate was 40% [2]. The m-payment has got 450 millions of end users and expected that transaction of US$721 billion all over the world [3]. The generalized m-payment is executed with the mobile wallets, credit cards, debit cards, etc. m-payment is used in daily life is classified as two types, for purchases, and bill payments. The purchase through m-payment is carried out by cash, credit cards, cheques or debit cards while bill payments are the account based system, which is used to transfer money, payment of internet banking, acceptance of electronic invoice (EI), etc.

This paper aims to review the past m-payment research work and discuss the future research hints to overcome the existing issues in m-payment. The literature survey guides about significant uses of m-payment. The literature review also discusses about the existing frameworks and their reviews. Authors Castelnovo and Ferrari Webster and Watson [4] have suggested that best literature is required to be structured with the concept and also with theory. The presented framework gives the better guiding structure, where the data is accumulated efficiently and explains the previous outcomes. The framework aims to interpret factors of m-payment in market services, on the basis of literature survey the framework clarifies that the review is complete, and the research gap needs to be overlooked. The framework also explains the existing knowledge body by which m-payment market services are overviewed, states the various research findings and perspective of the framework.

The rest of the paper is organized as follows: In Section II, presents the background of this paper. Section III provides significant related work done by other authors. In Section IV gives research methodology conducted in this paper. Section V introduces security issues in mobile payments. Finally, Section VI gives the conclusion and future research direction respectively.

II. BACKGROUND

Mobile devices are the most common means in communication around the whole world. According to the latest statistics of Central Intelligence Agency (CIA), Mobile communication has become the important system in the entire

world. There are more than 7 billion mobile subscribers in 2015 and expected about 60% of growth in 2020.This section comprises the mobile payment methods (MPM), Security consideration, security for mobile devices, user authentication over mobile network and is briefly explained below.

A. Mobile Payment methods:

There are five different modes for MPS transactions, and these are listed in following table.1.

Table. 1. Shows the MPS transaction modes [5].

MPOS	NFC	Bluetooth	QR codes	Apps based on cloud
This kind of payment is carried out by swiping or by inserting the card into smartphone or tablet card reader which allows payment over the wireless network.	In this the smartphones enabled with the NFC will communicate through the contactless RFID transmitter link with POS device. The payment can be done with the card stored in a mobile wallet.	The payment mode is done by using smartphones Bluetooth and other device transmitters.	Like NFC, payment through QR code done by storing payment in the cloud and this can be executed in any smartphone.	This type of MPS is done by using some apps which provide communication between the merchant and buyer without using any QR codes. Ex: PayPal

- **Threats:**

Mobile devices face the same security risks as PCs and laptops, including malicious apps, viruses and other types of malware. They also have the risk of malicious code such as phishing links being inserted into QR codes, according to Kaspersky Lab. In addition, retailers' Wi-Fi networks are vulnerable to intrusion, which poses a security risk for their mPOS devices and customers' smartphones.

B. Security Considerations:

This has three different categories, such as:

- Password or PIN are known
- Cards or tokens are there with user.
- User is of biometrics.

The password and Personal Identification Number (PIN) are the common authentication methods, has problems when passwords sharing with another person [6].

III. REVIEW OF LITERATURE

This section discusses the research work done by the mobile payment and its user security. The authentication for mobile payment is done by confirming the user authentication using mobile channel or web channel. These mobile payments will have many security issues because it needs financial information and personal information for the transaction. To secure the issues related to the mobile payment may authentication techniques can be used. Previously the mobile authentication can be copied to other mobiles. The modern mobile authentication can be solved by trusted third party (TTP) which helps in protect the mobile payment vulnerability.

Kim et al. [7] have given the study of the consumer perception of e-payment and its security concerns. The authors have worked on the security problems of e-payment as per customer viewpoint. The study presented a model that gives security trust for the customers during e-payment.

Dai [8] has introduced an integrated payment system for the mobile phone over 3G network. The author has combined the mobile phone, IC Chip and mobile internet for network transaction. The model has enhanced the customer trust for mobile payment, also gives the customer awareness.

Ganesan et al. [9] have presented secure E-commerce channel by using the digital envelope approach. The researchers have combined the both symmetric AES and Asymmetric HECC algorithms using the digital envelope in JAVA. These algorithms are tested for varies file size. To know the data integrity, MD5 hash algorithm is adapted. For key generation purpose, they have designed and implemented HECEIG algorithm.

Chang [10] has illustrated a secure, operational model for the mobile payment. The presented model has its access control on the basis of an architecture based on its service. In this, the user can have the authorization from two-dimensional (2D) barcode as the certificate for payment provided by the remote server. The generated certificate will have access limit only one time and also the system has the advantage of disabling and remotely lock the mobile payment service.

Yang [11] has presented a protocol for security enhanced Euro-pay MasterCard Visa (EMV) for mobile payment. The authors have worked on the issues of EMV contactless payment where the unauthorized user can use the access credit card. The new EMV protocol will helpful to solve these issues. For user and merchants, the protocol has given the transparent EMV standard. The protocol advances the offline transaction where he user can apply for the offline certificate in advance.

Jamgekar e al. [12] have presented "File Encryption and Decryption Using Secure RSA" a modified version of RSA algorithm (RSAA) to have file transmission securely. RSAA is a kind of asymmetric key cryptography/Public Key Cryptography (PKC). There are two keys are created in RSA, in that one key is employed for encryption, and other is

considered that authenticated receiver can decrypt the message, not by another key. Each communication member needs the only pair of a key for communication with many numbers of communication member. If someone got the key pair, then he/she can have communication with anyone. The commonly known public key for cryptography algorithm is RSA and is the first advancement in PKC.

Shierz et al. [13] have given a study for awareness and advantages of mobile payment for the customers. A model is developed and tested for the factors for customer convince to use the mobile payment. The study outcomes with individual mobility, compatibility effects for marketing strategies for mobile payment.

Tiwari et al. [14] have given the security protocol in the mobile device for wireless payment. The protocol provides multifactor security by which is secure and highly useful. The protocol based on the approach where transaction code and SMS identification is used to provide high security in compared with the traditional approach. This is also known as the two-way authentication protocol.

Saha et al. [15] have presented an analysis of the application of ISO 9564 PIN in mobile payment systems. The authors worked on the ISO specification for closed-loop authentication for payment.

Ho et al. [16] have reviewed the comparison of secure m-commerce mechanisms. (Kerberized or KiloByte SSL) And Wireless Transport Layer Security (WTLs) are the secure transaction mechanism for m-commerce. The review of the authors concludes that the WTLs security level in the mobile device is inadequate in nature. Recently, the number of WAP user is decreased. Hence, KSSL is can be used to redeem the drawbacks in WLTS and how the secure mobile transaction is achieved in future.

Rahma et al. [17] have presented "Hybrid Model for Securing E-Commerce Transaction" of suggesting cipher method; which modify the Diffie-Hellman (D-H) key exchange by using truncated polynomial in discrete logarithm problem (DLP) to increases the complexity of this method over unsecured channel, which again combines the hashing algorithm of MD5, the symmetric key algorithm of AES and the asymmetric key algorithm of Modification of Diffie-Hellman (MDH).

Noh et al. [18] have given a mobile payment and also mobile commerce system by using location based near-field communication. The system allows the users to make business, payment and transaction related to the service over the mobile device.

Isaac et al. [19] have discussed the secure payment system for mobiles. The author has considered the design of mobile payment and its security issues. Also illustrated the many emerging technologies and their expected challenges and also the secure design of m-payment.

Tan et al. [20] have illustrated the mobile cloud computing for payment method by using Technology Acceptance Model (TAM). The study outcomes with theoretical contribution and also gave a useful information for bank, merchants, users, etc.

Suryatrisongko et al. [21] have provided a novel scheme by considering fast, the secure response of payment for cooperative enterprises with minimal infrastructure. The scheme is modified with the QR- Pay mode, by avoiding the connection with the network as the few countries are facing a problem with internet connection. This presents QR encrypted content for improve the security and also two-factor authentication. This gives the reliable model, where the no internet is required only the snap of QR code is needed.

Murdoch et al. [22] have discussed the security protocols in which payment systems fails. The authors have discussed the advantages of EMV protocol over card payment. Many systems are analyzed such as mobile banking applications.

Elbaz et al. [23] have presented "Using Public Key Cryptography in Mobile Phones" of the importance of the privacy of the EMR and the patients' rights. In addition, cryptography algorithms and security requirements have been discussed, and the paper has also discussed different architecture, designs, and systems that have been reported in the literature. In a nutshell, most of these systems are poor in terms of achieving the security requirements, while, on the other side, most of the systems have not discussed the patients' rights and how the system can detect the persons who broadcast these records.

Yadav et al. [24] have given Android-based mobile payment by three-factor authentication. The method is useful in payment, money transfer using Android phones. The system makes the pairing of the android phone with a server and paying client. The authentication for the payment in this system includes the password, USIM card authentication and also facial recognition.

Venkatesh et al. [25] have discussed the evaluation of m-payment and its service providers. The author has investigated the advantages of m-payment and its issues related to security. The study outcomes with methodologies and service providers of m-payment in India.

Girija et al. [26] have presented the study over m-payment business model on the basis of third party m-payment service provider. The model will support the larger mobile service.

Carton et al. [27] have illustrated the framework for the m-payment. The framework gives the theoretical and practical contribution of the mobile technology in the payment industry.

Gaur et al. [28] have presented a view of the role of banks in m-payment and advantages of m-payment. The analysis is useful in strategic assets identification.

Gupta et al. [29] have illustrated the performance evaluation study over AES algorithm for many applications of Elliptic Curve Cryptosystem (ECC).

IV. RESEARCH METHOD

The extensive related wok over m-payment is carried out to have the better direction for present and future generation. The review first phase needs to have knowledge about the scope and required materials. The m-payment is the similar topic as like mobile and electronic business; the related articles are published in different journals. Even, m-payment is

emerging research area; many research articles were published in conferences. The study has both journal papers and conference article in this review. The proceedings of the conference are more informative for the present research work and identification of search gap for future work. The future conference papers are expected with more future based publications.

The literature survey is started with some latest IEEE, conference papers, and academic journals. The databases searched as, IEEE Explore, EBSCO Business Source Premier, Science Direct, ACM Digital Library, Pro Quest Direct, M-lit online bibliographical database, AIS e-Library for the literature of mobile business and google scholar for academic/conference papers. The citation for the particular paper is reviewed in backward order. The search over the internet was as 'm-payments', 'mobile payment', and also 'wireless payments'. To have the better quality conference paper searched in IS, e-commerce, and mobile business fields. Considered only recent papers on m-payment.

The Fig.4 flashes the research conducted in every factor of proposed framework. No past research is indicated as black boxes, and the papers number less than 20 is shown as the grey area. The most research more than 20 papers are shown in white areas. M-Payment Technology (MPT) and the consumer perspective are studied most in a research area. The cultural and structural factors are impacting over m-payment. Also conventional payment services in m-payments are found and uncharted them in black areas with past research. The factors in a gray area are: exploratory, previous phase are conducted, still there is more need of helpful and in-depth research projects are required.

Further, used methodology is analyzed; then each research is classified as: conceptual and empirical. Again the empirical is divided into: quantitative, design research and qualitative research. Almost technical papers were proposed the conceptual construct, in that few describes only the technology. Thus, the conceptual study is divided into descriptions and constructions. In this the technical factor is classified by 'empirical' and further construction is evaluated.

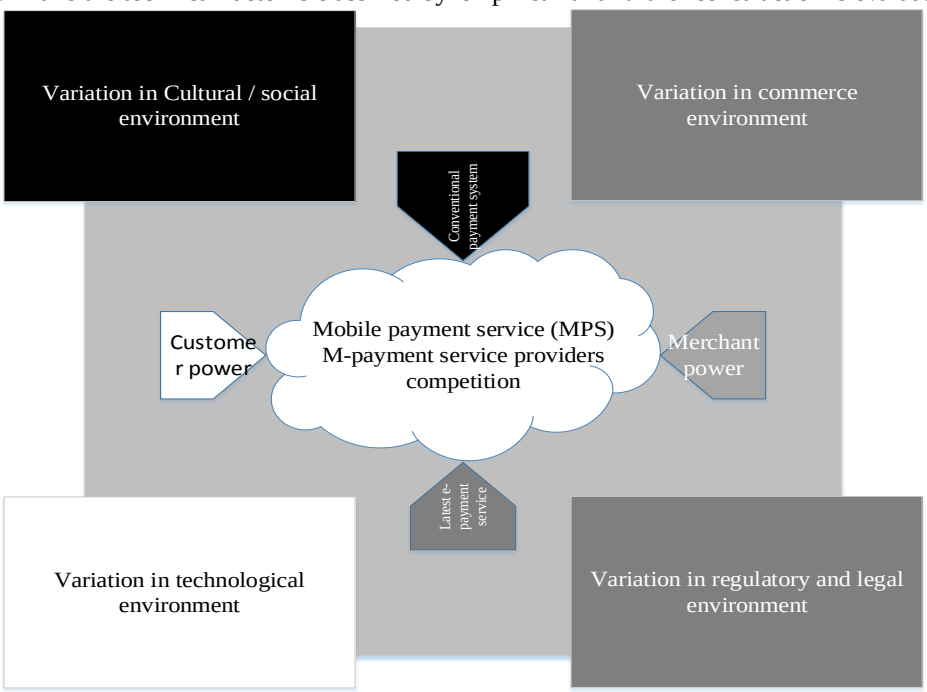

Fig. 4. Shows the Research on various factors of the framework.

V. SECURITY ISSUES

Security is the biggest issue in m-commerce, which needs secure financial transactions during commercial information exchanges. MPS transmits bank account/privacy details of the user, hence secure transactions towards m-commerce is necessary. The security level should have technical and perceived at the high level [31].

There are many e-commerce methods and procedures which are listed in the following Table-2.

Table.2. Shows The Vulnerabilities, Risks, Threats And Protection Solutions In M-Payment Systems [32]- [33]

Vulnerability	Risk	Threat	Protection Solution
Over-the-air transmission between a telephone and purpose of offer.	Identity fraud, data revelation, replay assaults	Interference of movement.	Trusted stage module, secure conventions and encryption.
POS gadgets introduced at vendor premises.	Theft of administration, replay, message adjustment.	Masquerade assaults, messing around with POS	POS seller reviewing, message authenticators, considered approval and bookkeeping.
Faintness of encryption method on SIM cards.	Mischievous transactions supported out on user's behalf, theft of deposited expense credentials.	Tampering of SIM card.	SMS firewall on telephone, condition of workmanship cryptography with adequately long keys, PIN for SIM card.

Accidental establishment by clients of malicious programming on cellular telephones.	Robbery of validation parameters, exchange repudiation.	Downloaded application capture of verification information.	Verification of user PIN and request.
Mobile Internet and abilities of geolocation.	User Data insecurity.	Mobile Malware, low data security by merchants.	User geolocation features to maintain privacy.
Mutual authentication with weak GSM protocol.	modify, spoof signalling, Eavesdrop, delete, replay, and reorder.	Middle attack of Impersonation.	Mutual entity authentication.
Mobile phone replacement and changing.	Lack of technology adoption.	setup complexity and Configuration.	Simple user security parameters , interface, by TTP.

VI. CONCLUSION AND FUTURE WORK

The paper gives the extensive existing m-payment reviews and also provides the outline for future research work in different research areas. In future, the MPS will receive lots of attention from many industries and academics. The statistics reported in this paper states that there will be massive growth in m-payment transactions and users, causing huge security issue parallel. The various new technologies have brought many challenges and many more opportunities for implementation and design of secure m-payment system in current and future generation. The paper has reviewed the existing research works and has organized with the set of factors. The paper suggests researchers think about better technology development for the secure and efficient user and merchant cooperation. Also, suggested that every m-payment models for the business purpose should have advancement from limited solutions to standardized solutions. For the future point of view, the researchers should work in the presented frameworks and then have deep analysis on every service.

REFERENCES

[1] Robin Arnfield, Tom Harper, Kathy Doyle, Will Hernandez, Christopher Hall and Tiffany Smith, "Mobile Payments Security 101", Published by Networld Media Group @ 2015, Networld Media Group, 2015.

[2] P. Wang et al., "Key ICT Indicators for Developed and Developing Countries and the World (Total and Penetration Rates)," World Telecommunication/ICT Indicators Database, 17th ed., Int'l Telecommunication Union, 2013; www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls.

[3] P. Wang et al., "Trends and Prospects for Mobile Payment Industry in China 2012-2015—Creating Innovative Models, Boosting Mobile Financial Services," Financial Services Industry Center of Excellence, Deloitte China, 2012; www.deloitte.com/assets/DcomChina/Local%20Assets/Documents/Industries/Financial%20services/cn_gfsi_TrendsProspectsChinaMobilePaymentIndustry_041212.pdf., Retrived on 27th January, 2016

[4] W. Castelnovo, E. Ferrari, "Electronic Journal Information System Evaluation", Special ECIME, Vol.15, Issue.1, pp. 1-148, 2012

[5] Becher, Michael, et al. "Mobile security catching up? revealing the nuts and bolts of the security of mobile devices." Security and Privacy (SP), 2011 IEEE Symposium on. IEEE, 2011.

[6] Green, Mr Jeremy Swinfen. Cyber Security: An Introduction for Non-Technical Managers. Ashgate Publishing, Ltd., 2015.

[7] Kim, Changsu, et al. "An empirical study of customers' perceptions of security and trust in e-payment systems." Electronic Commerce Research and Applications 9, page no. 84-95, 2010.

[8] Dai, Weihui, et al. "An Integrated Mobile Phone Payment System Based on 3G Network." Journal of Networks 6.9, page. 1329, 2011.

[9] Ganesan, Ramachandran, Mohan Gobi, and KanniappanVivekanandan. "A Novel Digital Envelope Approach for A Secure E-Commerce Channel." IJ Network Security 11, no. 3, pp.121-127, 2010.

[10] Chang, Tao-Ku. "A Secure Operational Model for Mobile Payments." The Scientific World Journal 2014, 2014.

[11] Yang, Ming-Hour. "Security Enhanced EMV-Based Mobile Payment Protocol." The Scientific World Journal 2014, 2014.

[12] Jamgekar, Rajan S., and GeetaShantanu Joshi. "File Encryption and Decryption Using Secure RSA." International Journal of Emerging Science and Engineering (IJESE) 1, no. 4 , pp. 11-14,2013.

[13] Schierz, Paul Gerhardt, Oliver Schilke, and Bernd W. Wirtz. "Understanding consumer acceptance of mobile payment services: An empirical analysis."Electronic Commerce Research and Applications 9, page no. 209-216, 2010.

[14] Tiwari, Ayu, et al. "A multi-factor security protocol for wireless payment-secure web authentication using mobile devices." arXiv preprint arXiv:1111.3010, 2011.

[15] Saha, Amal, and Sugata Sanyal. "Analysis of Applicability of ISO 9564 PIN based Authentication to Closed-Loop Mobile Payment Systems." arXiv preprint arXiv: 1411.2939, 2014.

[16] Ho, Hann-Jang, and RongJou Yang. "A comparison of secure mechanisms for mobile commerce." In Proceedings of the 7th WSEAS International Conference on Mathematics & Computers in Business & Economics, pp. 24-28. World Scientific and Engineering Academy and Society (WSEAS), 2006.

[17] Rahma, Abdul Monem S., Rabah N. Farhan, and Hussam J. Mohammad. "HYBRID MODEL FOR SECURING E-COMMERCE TRANSACTION." International Journal of Advances in Engineering & Technology 1, no. 5, 2011.

[18] Noh, Sun-Kuk, Seong-Ro Lee, and DongYou Choi. "Proposed M-Payment System Using Near-Field Communication and Based on WSN-Enabled Location-Based Services for M-Commerce." International Journal of Distributed Sensor Networks 2014.

[19] Isaac, Jesús Téllez, and Sherali Zeadally. "Secure Mobile Payment Systems." IT Professional 16.3, page no. 36-43, 2014.

[20] Tan, Garry Wei-Han, et al. "NFC mobile credit card: The next frontier of mobile payment" Telematics and Informatics 31, page no. 292-307, 2014.

[21] Suryotrisongko, Hatma, and Bambang Setiawan. "A Novel Mobile Payment Scheme based on Secure Quick Response Payment with Minimal Infrastructure for Cooperative Enterprise in Developing Countries." Procedia-Social and Behavioral Sciences 65, page no. 906-912, 2012.

[22] Murdoch, Steven J., and Ross Anderson. "Security Protocols and Evidence: Where Many Payment Systems Fail."

[23] Elbaz, Limor. "Using public key cryptography in mobile phones." Discretix Technologies Ltd. White Paper (2002).

[24] Yadav, Saurabh, et al. "Android-Based Mobile Payment System Using 3 Factor Authentication."

[25] VENKATESH, DRJ, and MR D. SATHISH KUMAR. "EVALUATION OF MOBILE PAYMENT SYSTEM AND Its SERVICE PROVIDERS."Evaluation 2.4, 2012.

[26] Girija.M, Aswini Nachiyar.M, Srilakshmi Prasana c v, "STUDY OF MOBILE PAYMENT BUSINESS MODEL BASED ON THIRD-PARTY MOBILE PAYMENT SERVICE PROVIDER", International Journal of Computer Science and Engineering Communications- IJCSE.

[27] Carton, Fergal, et al. "Framework for mobile payments integration", The Electronic Journal Information Systems Evaluation 15.1, page No. 13-24, 2012.

[28] Gaur, Aakanksha, and Jan Ondrus. "The Role of Banks in the Mobile Payment Ecosystem: A Strategic Asset Perspective", 2012.

[29] Gupta, Kamlesh, and Sanjay Silakari. "ECC over RSA for Asymmetric Encryption: A review." International Journal of Computer Science Issues 8, no. 3, pp. 370-375, 2012.

[30] S. Kadhiwal and M.A.U.S. Zulfiquar, "Analysis of Mobile Payment Security Measures and Different Standards," Computer Fraud & Security, vol. 2007, no.6, pp. 12–16, 2007.

[31] S. Duangphasuk, M.Warasart, and S. Kungpisdan,"Design and Accountability Analysis of a Secure SMSBased Mobile Payment Protocol," Proc. 8th Int'l Conf.Electrical Engineering/Electronics, Computer, Telecommunicationsand Information Technology (ECTI-CON 11), pp. 442–445, 2011.

[32] Mobile Payments: Risk, Security and Assurance Issues, whitepaper, ISACA, Nov. 2011; www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf.

