International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 04, 2020
ISSN: 1475-7192

Vulnerability, threats, and attacks in E-Payments System: Security Solutions

[1]Dr. Chitra Kiran. N, [2]Mr. Suhas Suresh, [3]Mrs. Suchira Suresh

Abstract—*the current payment system through online applications has to trend at a furious pace. The various and multiple numbers of online transaction methods (i.e., E-payment systems) has been proposed for various security aspects. However, with the increasing of E-payment methods, the various cyber-attacks methods are also increasing at an advanced level. Therefore, in this study have presented a terminology of E-payment system including with various existing methods. Also illustrates security provisions and solutions. The primary objective is to provide the roadmap of E-payment mechanism and its opportunities for future scope.*

Keywords— *E-Payment System, E-Transaction, M-Payment, Security, Secure E-Transaction.*

I. INTRODUCTION

With the rise of modernization in telecommunication and digital era, the majority of the commercial products are available online. The beginning of e-commerce began more than a decade ago; however, in reality, the picture of usage is quite different. Till now, in India, 50% of people, even being aware of Electronic-payment system (i.e., online payment), don't adopt the services. The prime cause of this less frequency of adoption is because of fear of security incorporations rendered by the services. More clearly, with the increasing growth in E-commerce application and using mobile transactions, there are lots of opportunities for cyber-attacks. As a mercantile, you require to guarantee that you provide the best E-payment security and customers no need to worry about their data. However, the research community believes that E-payment has come up from infancy stage and slowly began to enter in the sophisticated area of mobile payment (m-payment) system with the existing tablet PC and Smartphone services available [1]. Mobile payment method is the smart method where users can utilize their mobile devices to pay for products and services. This method includes internet cloud service providers, banking institutions and mobile devices, contains the functionalities of E-payment as well as communication systems. It provides the end users with banking services including money transfer, and online payment [2], [3]. As increasingly use of verities of E-payment methods, also it has become challenge of cybercrime [4] [5]. During the E-payment process, users require to send the payment related information to the 3rd party of mobile payment such as order information, retailer information or payment information. These information concern the users payment security, and it may causes major consequences if the attacker used. The security of 3rd party payment system is also become a most significant factor to the E-payment systems as well as banking institutions [6].

Most of the security protocols applied in E-payment are based upon traditional encryption technique, which utilizes the public key cryptographic algorithms including Elliptic Curve cryptosystem (ECC) and RSA algorithm[7], [8]. These algorithms supports high hardware infrastructures, and are not suitable for smart devices

[1]*Professor & HOD, Alliance University, Bengaluru, suchitsupreeth@gmail.com*

[2] *5th Semester, BBA LLB, KLE Society's Law College, Bengaluru, suhassuresh2009@gmail.com*

[3] *Senior Software Engineer, Robert Bosch Engineering, Business Solutions, India, suchirasuresh14@gmail.com*

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

with limited resources. Additionally, these cryptographic algorithms does not contain the functionality of against quantum attacks. In the study of shoret.al [9] introduced a discrete-quantum algorithm to secure the E-payment against threat, but has short term security public key cryptography algorithm used in m-payment systems is no more secure. Another cryptographic approach i.e. Lattice based cryptosystem doesn't require more computing resources to support the m-payment process and it has the feature of mitigate the quantum attacks.

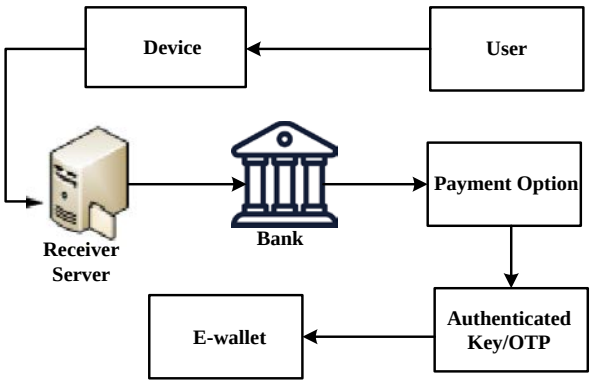

Figure 1: Typical E-Payment process

The typical E-Payment mechanism is represented in above figure-1, which pictorially illustrates how an entire payment process happens with secure and smart way. In order to attain secure E-transaction, the significant method is digital signature scheme, where traditional methods ECC and RSA are utilized as signature algorithms since these algorithms can perform decryption correctly after the encryption with secrete key [10].

The significant purpose of present survey study is to provide a beneficial literature review on various E-payment or online transaction mechanisms and their security concerns. Additionally, shown that, how these payment modes are increasingly become more popular and essential in day to day users financial life. The remaining par t of the comprehensive survey paper isorganizedin multiple folds; viz:- section-II briefly introduces verities ofE-Payment methods. The existing research work on E-Payment mechanisms are discussed in section-III followed by security strategies over the e-Payment process is shown in section-IV. Section-Vdefines the overall conclusion of the survey paper.

II. E-PAYMENT METHODS

Nowadays, millions of users are using verities of E-payment methods for various purpose including; online shopping, Electric bill payment, Travelling Tickets booking, online money transmission, and more purposes [11]. The E-payment is a process which takes very less time, and users don't need to suffer from physical problems; for example, in banks payment queuing system. That's the reason this technology attracting to the customers for easy payment transmission process for daily purposes like shopping, traveling, hotels booking and many more reasons where payment process can perform with one single click pay system. The following figure-2 illustrates the different types of e-payments methods:

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

Figure 2: Uses of e-payment system

Types of E-Payment methods

The most popular traditional payment methods are cash, cheques, debit/credit cards. The advent of internet technologies, the advance payment systems have appeared with new functionalities with users facilities like, e.g., E-Payment or Online/Digital payment systems.

Nowadays, with the growing penetration of the smartphone and the development of E-commerce, the m-payment system is becoming an uncontested mode for paying products. Based on money transaction schemes the e-payment system is categorized as the following types [12];

- Account Based
- Real-time cash payment system
- Pre-paid payment
- Post-paid payment
- Smart card payment system
- Credit card based payment
- Mobile POSand
- Mobile wallets

In an account based payment methods, an individual user is associated with their account maintained by the bank as well as internet payment provider. In this payment system, the 3 kinds of transaction processes are available including; i) real-time payment system (e.g., E-cash and beenz), ii) pre-paid transaction through debit cards, and iii) Post-paid transactions through Credit cards.

The smart card based payment system includes smart or chip card which is embedded with integrated circuits example; ATM cards, credit cards, mobile SIM, and many more. A typical smart card is made-up with a plastic coat, i.e., polycarbonate cover containing memory chip and microprocessor with the operating system for

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

memory control. These smart cards are utilized for e-signature, identification, payment processing, as well as data storage purpose.

A credit card based e-payment system allows the customers to pay for goods and services based on payment policies. The card provider makes the revolving account and grants the credit limits to the user in which a user can utilize their amount for payment to the merchant. These cards allow the users continuing the debit balance, subject to interest being charged. The Visa card and Master Card Company designed a SET secure protocol for secure payment transaction using credit cards [13].

Mobil-POS payment method allows the users to purchase goods and services from retailers through mobile phones [14]. From this method customers can make payments through mobile/smart devices with assistance from the service party (i.e., counter clerk or taxi driver). The two most popular M-POS payment system are; automated POS can be done through ATM or retailer vending machines, and another one is attended POS system, e.g., Ultra's mobile payment system.

Mobile-Wallets: It is an m-payment application can be performed through the mobile phone contains details of the customer (including bank account details and credit card information) that enable the customer to make payments using the mobile phone. However, this method also suffers from various security challenges during the payment process. In this context, a white paper summarized the vulnerabilities, threats, and security challenges over the m-payment systems [15].

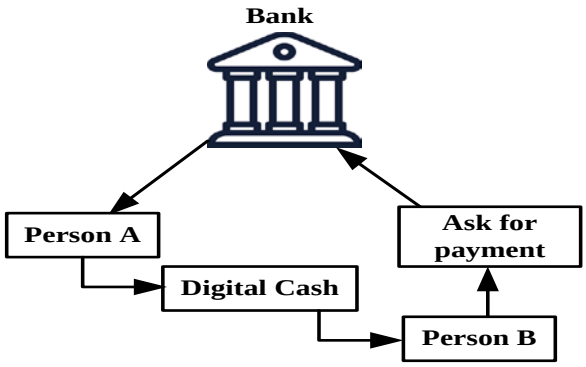

Figure 3: Internet banking system

Inter-Net Banking: - It is another and most popular E-banking method in which both customer and financial institution collaborate through the banking websites (Shown in figure-3). From this method also user can make the payment using various methods including IMPS or NEFT. Nowadays, it is considered as most usable and more secure E-payment system which fulfill the security requirements with user authentication functionality, i.e., Allow the payment with effortless way under user authentication by generating one-time-password on the mobile user device.

III. RELATED WORK

This section discusses various research study on e-Payment transaction methods and security challenges. Also analyzing and evaluating existing methods based on security parameter.

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

From the past decades to till date, there is enormous growth in communication and information technologies, and banking organization follows an electronic mediate multi-channel policy for money transactions [17]. In the year of 1970, the first ATM is launched, later with the development of technologies 1990 online banking services have been launched, e.g., mobile banking service [18]. Mobile banking is an e-payment method performed by mobile terminals with wireless medium [19], [20]. Khalilzadeh et al. [21], has designed an integrated m-payment model that computes the determinants of near field communication-based e-payment scheme in the hotel management. Park et al. [22] introduced an authentication protocol using GSM to secure the user information in the m-payment system. Xu et al. [23] proposed a new m-payment model based on user authentication, which uses the biological characteristics (e.g., face) to ensure the user's authentication. [24]

Cao and Zhu [25], constructed trust based hash-chaining approach for E-money transaction and provided a secure privacy mechanism for ride hailing services.The study considered few significant protocols viz; withdrawal, deposit, payment, refund, high anonymous payment, and etc. . In [26], [27] research study authors investigated an m-payment mechanism to provide a security mechanism in mobile wallet using digital signature algorithms and pseudo-identity scheme. In both study's authors point out the relationship between the real user identity and their pseudonym.

Zahra et al. [28], hasfocusedtrust and security policies for online payment system over Iran country. Authors considered the influencing factors of trust and designed a secure e-payment systemusingpayment information, and accessibility factors. Finally, the authors compared the system performance analysis with existing methods. Karmi et al. [29], investigated similar approach by considering few significant factors, viz; websites, business policies, trust, adoptability, collaboration between the customers, and etc. which influence the e-market world.

At present, various online mode payment methods exist which performed on mobile or small-sizedsmart devices and providemultiple services with limited cost. Nevertheless, customer’s anonymity is a challengingparametersincenewE-payment method provide transaction privacy with limited security. Therefore, from the customers anonymity viewpoint Breaken [30] have proposed a new e-Payment model for blind & visually challenged users. This approach may benificial for the design of newonline-payment scheme. The both studies [31] & [32] havehighlighted the customer’s anonymity issues and securitychallenges over the e-payment system.

At present, more than 60% of users are using online payment transaction methods via mobile or smartphones, and their work becomes more accessible as well as more convenient. The online-transaction through the m-payment method is becoming very common over the rising business world [33]. However, Quick-Response i.e. QR-Code mechanismoffersmultiple features with more data storage capacity, and recognition capability, even datais decrypted by a mobile device [34]. QR code scheme is increasingly utilizing in security sensitive application areas [35] for example, as payment systems.

Suryotrisongko et al. [36] have proposed a novel study on mobile-payment system for the business enterprise. It presented an improved QR-code based payment mechanism by reducing the network overhead. Additionally, it introduced two metrics, i.e., authentication and QR - code scheme to improvise the security level at payment mode. Hence, it is more convenience and reliable with security to transfer money using a mobile phone easily.

Another alternative approach of QR-code is introduced by Dey et al. [37], where the user interface is exploited to seal the data into realistic applications on mobile phones. In [38], Lu et al., adopted a similar QR

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

code mechanism due to its favorable characteristics, especially for the m-payment system. Also proposed a visual cryptographic approach in which shows the security for mobile-payment authentication.

Chitra K et al. [39] worked on digital transaction mechanism by considering the biometric system, and it iscalled as the "swing-pay method". The objective is to consider the user's fingerprints for system authentication. This approach offers arobust secure payment mechanism. In the traditional online payment systems, PayPal and GooglePayis the most commonly applications especially for mobile payment systems. Kang and his team [40] have introduced a privacy-preserving model for smart device payment system to preserve the passenger's mass transit information.

There are multiple number of e-payment methods have been proposed by various researchers in which the primary focus is to maintain the strong security over the online transaction process. However, few traditional e-payment schemesare unable to provide non-repudiation requirement. Therefore, an attacker can easily refuse the transaction and vendorcould not get back their funds. To resolve such issues, Yang [41], have developed an anonymity payment method using mobile device.In the conclusion, authors presented a comparative analysis and showed that proposed e-transaction mechanism which has strong security, and efficientlyapplicable for real-time transaction over the cloud infrastructure.

In [42] Kang and Xu introduced another approach of anonymity e-moneytransaction method to maintain the user's privacy. In this paper authors focused on Chen et al. work and pointed out few limitations of Chen et.al work.Furthermore, authors ensures the characteristics of avoiding retailer frauds. Another research work of Fan et.al [43] presented a similar kind of offline e-cash payment method. Also, the authors presented an E-money renewal policy, by whichauthenticated customer can interchange their expired and unused currencies.

In [44], [45] Chitra and Kumar presented a robust security based micropayment scheme. In [44] both authors given a reliable solution strategy for accomplishing the flexible and strong security E-payment process over the wireless Ad-Hoc networks. This approach doesn't depends upon online transaction process unlike traditional payment methods but this approach is designed for offline transaction process over Ad-Hoc mobile networks using simple approach of public key cryptography. In another paper [45] provided a extended work of previous research which addresses the security implications in micropayment process. Also introduced a significant operation for offline mode payment system by considering multiple users which furnish more flexibility, mobility as well as strong security over micro-payment systems. Basically, this work is inspired by existing work of Jianming [46] and aim was to present a novel approach of offline mode e-payment system to provide strong security over wireless transaction system.

IV. SECURITY MECHANISM IN E-PAYMENT

The strong security is the major concern over current E-payment systems and it is consider as most serious challenge in E-commerce world. As an example; theft and fraud are apparently increasing day-by-day and its is very essential for retailers to provide their customers securitywith secure environment. However, in the past decades it has been seen that most of the retailers have experienced lots of serious problems in payment fraud due to weak security. This section embark the significance of strong security in E-payment systems that to mainly concerning secure transaction.

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

Many research studies and security protocols always advocate to provide significant way in ensuring to protect the retailer stores from security threats.

i. Section of right payment processor: It is a most prior step for accepting E-payment from the user's debit/credit cards. Selection of right payment processing partner should be performed with more protection which could help the user to comply with payment card company security standard. Therefore, it is more essential to have payment partner who has right experience and can understand the payment security measurements.

ii. Authentication system for each transaction:It is very essential for the retailers to predict and analyze about the user buying the product with true cardholder. Different methods can be adopted to prevent this fraud. Implementing the authentication systems in the E-payment process is the significant way to verify and analyze the fraud. During this process, system checks the if the billing address is right or wrong by verifying the cardholder data from the bank.

iii. Encryption mechanism: It is a cryptography mechanism which is too difficult to understand or hacker to decode. The main intension is to ensure strong security and protect the transaction details.

iv. Secure E-Transaction protocol: (SETP)SETP is a embedded payment system by Master-card and VISA which provides safety to the all parties involve in E-transaction process. Especially this protocol is designed to manage the complex functions including; Authentication of cardholders and retailers, maintain confidential payment information, defines security protocols and service providers. A pictorial scenario of SETP is representing in below figure-4.

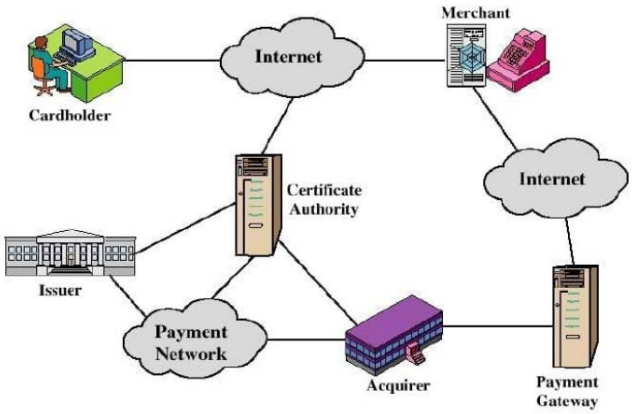

Figure 4: Pictorial representation of SETP.

Another security protocol namely Secure Socket Layer (i.e. SSL is responsible to maintain the integrity of E-transaction process [47]. It is morereliable security protocol and particularly introduced for business payment system with secure payment channels. The both SETP and SSL protocols are invented to improve the security over the E-transaction process.

The E-payment system is a crucial part of current E-commerce world. It is the place where money of both parties is at stake if the strong security is not ensured. Therefore, it is most essential and utmost requirement of

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

both entities to adopt a reliable and robust security protocol which protect and secure the current E-payment system as well as support the future applications also. The table-1 briefly illustrates the various scenarios of vulnerabilities, threats and security solutions.

Table 1: Vulnerabilities, threats and security solutions in E-Payment system

Vulnerabilities	Threats	Security Solutions
E-Transmission between smart device and point of sale	Traffic Interception	Security protocols, encryption algorithm
unintentional installation of spiteful software tools in smartphones	Installed software intercept of authentication data	User Authentication and digital signature, anti-Virus/malware software
Absence of two way authentication	User masquerading	Two-way authentication
Frequently changing /replacing the mobile phone	Configuration and updating setup complexity	The simplified user interface, security factors in TPM created by trusted 3rd party
Mobile phone, Internet accessibility, and environmental capabilities	Malware software installed in mobile phones, inadequate security controls	The cryptography method to support the User privacy vetted authorization & accounting
Lack of digital authentication on the mobile phone	Illegal data distribution	Digital authentication in the smartphone with digital signature mechanism, cryptographic algorithm
Poor performance in GSM encryption for transmission, SMS generated text over the cellular network.	Message alteration, transactions replay, evasion of fraud controls	Robust encryption schemes, SMS text authenticators,
Poor cryptographic protocols	Cryptanalysis and malicious attacks	Strong Security in third-party with cryptography protocols and active encryption keys
Lack in encryption protocol on mobile SIM cards	Tampering or cloning of mobile SIM card	Secure code generation on phone, state-of-art cryptography with OTP for SIM card

V. CONCLUSION

The contribution of the proposed study is to provide a tremendous growth over the E-payment mehtods and understand the terminology of various online payment methods followed by new advance E-payment methods which can be securely beneficial for both customers as well as retailers. Through the literature studies, have examined the performance of existing E-payment methods and identified vulnerabilities, threats, and falsified factors to lead the malicious attacks. The research study on E-payment system provided needful knowledge towards the analysis of various E-money transaction methods with smart way process. From the existing studies

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

have identifies the pros and cons of those methods in terms of their privacy and security concern. The primary intention of this study is to provide vulnerabilities, threats and security protocols in current E-payment system

REFERENCES

1. Heindl, Dr. Eduard. "Online Payment Process." (2008).
2. E. Taylor, "Mobile payment technologies in retail: A review of potential benefits and risks", *Int. J. Retail Distrib. Manage.*, vol. 44, no. 2, pp. 159-177, 2016..
3. S. Ghosh, A. Majumder, J. Goswami, A. Kumar, S. P. Mohanty, B. K. Bhattacharyya, "Swing-Pay: One card meets all user payment and identity needs: A digital card module using NFC and biometric authentication for peer-to-peer payment", *IEEE Consum. Electron. Mag.*, vol. 6, no. 1, pp. 82-93, Jan. 2017
4. Y. Jin et al., "Study on security of mobile payment", *Proc. Int. Conf. Mech. Int. Robot.*, pp. 123-127, Nov. 2017.
5. V. Patel, R. Chellappa, D. Chandra, B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges", *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 49-61, Jul. 2016.
6. Y. Wang, C. Hahn, K. Sutrave, "Mobile payment security threats and challenges", *Proc. 2nd Int. Conf. Mobile Secure Services (MobiSecServ)*, pp. 1-5, Feb. 2016.
7. S.-Y. Chiou, W.-T. Ko, E.-H. Lu, "A secure ECC-based mobile RFID mutual authentication protocol and itsapplication", *Int. J. Netw. Secur.*, vol. 20, no. 2, pp. 396-402, Mar. 2018.
8. J. Tállez, S. Zeadally, "Security in mobile payment systems", *Mobile Payment Systems*, pp. 93-106, Oct. 2017.
9. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Rev.*, vol. 41, no. 2, pp. 303-332, 1999.
10. S. Bai, T. Lepoint, A. Roux-Langlois, A. Sakzad, D. Stehlé, R. Steinfeld, "Improved security proofs in lattice-based cryptography: Using the rényi divergence rather than the statistical distance", *J. Cryptol.*, vol. 31, no. 2, pp. 610-640, Apr. 2018.
11. Huang, Echo, and Fachang Chen. "Electronic Payment Use and Legal Protection." In International Conference on Digital Enterprise and Information Systems, pp. 158-171. Springer, Berlin, Heidelberg, 2011. aaa
12. Raina, Vibha Kaw. "Overview of mobile payment: technologies and security." In Banking, Finance, and Accounting: Concepts, Methodologies, Tools, and Applications, pp. 180-217. IGI Global, 2015.
13. Li & Wang. (n.d.). Secure electronic transaction (SET protocol). Retrieved from http://people.dsv. su.se/~matei/courses/IK2001_SJE/li-wang_SET. pdf
14. Isaac, Jesús Téllez, and Zeadally Sherali. "Secure mobile payment systems." IT Professional 16, no. 3 (2014): 36-43. aaa
15. Mobile Payments: Risk, Security, and Assurance Issues, white paper, ISACA, Nov. 2011; www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf.
16. aa
17. Black NJ, Lockett A, Ennew C, Winklhofer H, McKechnie S (2002) Modelling consumer choice of distribution channels: an illustration from financial services. Int J Bank Mark 20(4):161–173
18. Barnes SJ, Corbitt B (2003) Mobile banking: concept and potential. Int J Mob Commun. 1(3):273–288 Bentler PM (1989) EQS, structural equations, program manual, program version 30. BMDP Statistical Software, Los Angeles
19. J. Kang, "Mobile payment in fintech environment: Trends security challenges and services," *Hum.-Centric Comput. Inf. Sci.*, vol. 8, pp. 32, Oct. 2018.
20. E. Taylor, "Mobile payment technologies in retail: A review of potential benefits and risks," *Int. J. Retail Distrib. Manage.*, vol. 44, no. 2, pp. 159-177, 2016.
21. J. Khalilzadeh, A. B. Ozturk, 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.
22. S. W. Park, I. Y. Lee, "Mutual authentication scheme based on GSM for NFC mobile payment environments", *Adv. Comput. Sci. Ubiquitous Comput.*, vol. 373, pp. 391-395, Dec. 2015.
23. Z. Xu, T. Zhang, Y. Zeng, J. Wan, W. Wu, "A secure mobile payment framework based on face authentication," *Proc. Int. MultiConf. Eng. Comput. Scientists*, vol. 1, pp. 495-501, Mar. 2015.

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

24. Eastlick MA, Lotz SL, Warrington P (2006) An integrated model of privacy concerns, trust, and commitment. J Bus Res 59(8):870–880
25. Cao, Chenglong, and Xiaoling Zhu. "Practical Secure Transaction for Privacy-Preserving Ride-Hailing Services." Security and Communication Networks 2018 (2018).
26. S. Abughazalah, K. Markantonakis, and K. Mayes, “Secure mobile payment on NFC-enabled mobile phones formally analysed using CasperFDR,” in Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom ’14), pp. 422–431, IEEE, Beijing, China, September 2014.
27. Z. Qin, J. Sun, A. Wahaballa, W. Zheng, H. Xiong, and Z. Qin, "A secure and privacy-preservingmobilewalletwith outsourced verification in cloud computing," Computer Standards & Interfaces, vol. 54, pp. 55–60, 2017.
28. Barkhordari, Maryam, Zahra Nourollah, Hoda Mashayekhi, Yoosof Mashayekhi, and Mohammad S. Ahangar. "Factors influencing adoption of e-payment systems: an empirical study on Iranian customers." Information Systems and e-Business Management 15, no. 1 (2017): 89-116.
29. Karimi Anche F, Hozouri S, Mehdizadeh A (2014) An exploration investigation on important factors influencing e-marketing: Evidence from the banking industry. Uncertain Supply Chain Manag 2(1):49–54
30. Braeken, An. "An Improved E-Payment System and Its Extension to a Payment System for Visually Impaired and Blind People with User Anonymity." Wireless Personal Communications 96, no. 1 (2017): 563-581.
31. Yang, J.-H., Chang, Y.-F., & Chen, Y.-H. (2013). An efficient authenticated encryption scheme based on ECC and its application for electronic payment. Information Technology and Control, 42(4), 315–324.
32. Chaudhry, S. A., Farash, M. S., Naqvi, H., & Sher, M. (2015). A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electronic Commerce Research, 16(1), 113–139.
33. D. A. Ortiz-Yepes, "Areviewof technical approaches to realizing near-field communication mobile payments," IEEE Security and Privacy, vol. 14, no. 4, pp. 54–62, 2016.
34. P. Subpratatsavee and P. Kuacharoen, "Internet banking transaction authentication using one-time mobile password and QR code," Advanced Science Letters, vol. 21, no. 10, pp. 3189–3193, 2015.
35. B. Zhang, K. Ren, G. Xing, X. Fu, and C.Wang, "SBVLC: secure barcode-based visible light communication for smartphones," in Proceedings of the 33rd IEEE Conference on Computer Communications (IEEE INFOCOM '14), pp. 2661–2669, Toronto, Canada, May 2014.
36. H. Suryotrisongko, Sugiharsono, and B. 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, vol. 65, pp. 906–912, 2012.
37. P. De and J. Eliasson, “An assessment of QR code as a user interface enabler for mobile payment apps on smartphones,” in Proceedings of the 7th International Conference on HCI (IndiaHCI ’15), pp. 81–84, Guwahati, India, December 2015.
38. Terán, Luis, Celine Horst, B. Fausto Valencia, and Priscila Rodriguez. "Public electronic payments: A case study of the electronic cash system in Ecuador." In a democracy & eGovernment (ICEDEG), 2016 Third International Conference on, pp. 65-70. IEEE, 2016.
39. ChitraKiran, N., Bhuvan Teja, Suchira Suresh, B. Krishna, S. M. Akarsh, and Jerrin Yomas. "A biometric-based payment system by using payee and payer module." In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on, pp. 2252-2256. IEEE, 2017.
40. J. Kang; D. Nyang, "A Privacy-Preserving Mobile Payment System for Mass Transit," in IEEE Transactions on Intelligent Transportation Systems, Vol.PP, No.99, pp.1-14, 2017
41. J.-H. Yang and P.-Y. Lin, “A mobile payment mechanism with anonymity for cloud computing,” J. Syst. Softw., vol. 116, pp. 69–74, Jun. 2016.
42. Kang, Baoyuan, and Danhui Xu. "Secure electronic cash scheme with anonymity revocation." Mobile Information Systems, 2016 (2016).
43. Fan, Chun-I., Wei-Zhe Sun, and Hoi-Tung Hau. "Date attachable offline electronic cash scheme." The Scientific World Journal 2014 (2014).
44. Kiran, Chitra N., and G. Narendra Kumar. "Implication of secure micropayment system using process-oriented structural design by hash chaining in a mobile network." International Journal of Computer Science Issues (IJCSI) 9, no. 1 (2012): 329.

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020

45. Kiran, N. Chitra, and G. Narendra Kumar. "Reliable OSPM schema for the secure transaction using a mobile agent in micropayment system." In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on, pp. 1-6. IEEE, 2013.
46. Jianming Zhu; Ninghong Wang; JianFeng Ma, "A micro-payment scheme for multiple-vendor in m-commerce," E-Commerce Technology for Dynamic E-Business, 2004. IEEE International Conference on , vol., no., pp.202,208, 15-15 Sept. 2004.
47. Solat, Siamak. "Security of electronic payment systems: A comprehensive survey." arXiv preprint arXiv:1701.04556 (20
48. L.CHARLIENE KARUNYA, P.HARINI, S.ISWARYA, A.JERLIN. "EMERGENCY ALERT SECURITY SYSTEM FOR HUMANS." International Journal of Communication and Computer Technologies 7 (2019), 6-10. doi:10.31838/ijccts/07.SP01.02
49. Georgiev, D. Remarks on the number of tubulin dimers per neuron and implications for Hameroff-Penrose Orch OR (2009) NeuroQuantology, 7 (4), pp. 677-679.
50. Klapproth, F. Single-modality memory mixing in temporal generalization: An effect due to instructional ambiguity (2009) NeuroQuantology, 7 (1), pp. 85-94.

DOI: 10.37200/IJPR/V24I4/PR201056
Received: 22 Oct 2019 | Revised: 13 Sep 2019 | Accepted: 15 Jan 2020