Mobile Commerce & Security Issues

Jamilu Muhammed Aliyu

Abstract— Being the fact that M-Commerce or Mobile Commerce is a subset and advancement of traditional E-Commerce and E-Business in general; the goal of this paper is to show that security is primarily the most important aspect Information technology, while m-commerce is an advancement of the traditional e-commerce. The paper gathers different information's regarding mobile-commerce and security issues and offered potential solution based on the requirement of online transactions and its potential security threats.

Keywords: E-Commerce, Information Technology, M-Commerce, Mobile Transactions, Security Issues & Solutions,

1 INTRODUCTION

In the past few decades, developments in and extensive implementation of information technology (IT) have prompted fast improvement in e-commerce. This contains automated transaction of traditional commerce (electronic marketing, etc.) and also with the development of new era of transaction model that were impossible without the use of typically implemented technological innovation (Information Technology) [1].

M-commerce is the B2B, B2C or C2C e-commerce which keeps on cell mobile phones, PDA, portable PCs and other wi-fi devices. It brings together the Internet, mobile connections technological innovation and other relevant technological innovation, so customer's on-line routines activities will never be restricted by time and area; hence, it will significantly accomplish customer's life [2]. The innovation of technological wireless communication, and persistent commercial infrastructure guarantee to improve this perspective, secure environment to mobile potential customers, and possibly to remove the difference between the "on-line" and "off-line" worlds [10].

The growing position of m-commerce develops new security, protection and level of privacy challenges mainly because of new technological innovation, novel programs/applications, and improved consistency. With the arrival of 3G also known as third generation mobile networking and communication era with the accelerating popularization of Smartphone's, M-commerce, M-wallet, M-banking, with other mobile transactions is boosting up progress in the global business [3].
Nevertheless, to be able to be effective and successful in m-commerce transactions, security functions must be powerful enough to secure the customer from unlawful violations and to get assurance from him [11].

1.1 Research Area

Mobile commerce is an interesting research area that is literally rise from information technology management and business processing, this work is going to adapt three different kind of research areas mainly IT management which includes security matter and business information systems which are all parts of management information systems. One of the advancement for this kind of research towards an industry is that it brings integrity and user confidentiality,

The research will help in bridging a security gap for mobile transaction as well as mobile computing in general by discussing and comparing best possible solutions.

1.2 Research Objectives

The main objective as well as main goal of this research is to explore, confer, and present some promising potential solutions to mobile commerce security threats. To explore different literatures and brings about security needed and user confidentiality.

2 LITERATURE REVIEW

The most vital subject when it comes to m-commerce is security concern, and how those security concerns is going to be treated accordingly such that more users could be attracted and feel more confident [4]. The steady condition of progress implies that new vulnerabilities will keep on giving open doors for hackers and fraudsters therefore security will keep on being the top concern for portable device and mobile ventures, such as providers of mobile services and developers for mobile applications [5].

M-commerce has a long history of security threats being the fact that it bridges together both traditional e-commerce as well as the wireless communication [6]. Technical limitations of cell phones and remote or wireless communication, business concerns, and legitimate requirements muddle the functional utilization of mobile commerce [7]. It is very unfortunate that the present platform built for mobile communication have failed to claim a complete scale of security measures in terms of integrity of transaction [9]. In the entire context of

- *Jamilu Muhammed Aliyu is currently pursuing PhD degree program in MIS in Kadir Has University, Turkey, PH- +905357278922. E-mail: jamil.aliyu@gmail.com*

transaction life-cycle and procedure of electronic commerce in general, there are 3 core factors that suffer vulnerability when it comes to security threats which arose from mobile terminals, network side, and mobile radio interference. The survey has critically explored diverse ways of bridging a gap in m-commerce transactions threats, thus mostly discussed in terms of WPKI and WAP gateway which diminishes problems in mobile devices [10].

The boundless utilization of cell phones now daily creates tremendous measure of incomes by diminishing time and cash required for different purposes. The quick advancement in portable computing technology not just makes a few open doors for the business and furthermore opens the entryway for doing catastrophes utilizing abuse of innovation. But there are some weaknesses when it comes to technological limitations of mobile platforms which may bind the size of file to be processed, also UI could not be friendly enough to function [11]. The principle preferred standpoint of M-commerce contrasting with E-commerce additionally exists in. Indeed while the utilization of E-commerce is given just when the client is at his/her own home or working environment or in some other area he/she needs to get through the media, for example, Internet, Television. M-commerce simply requires Mobile-telephone. It is noted that m-commerce is getting bigger and more attention than traditional e-commerce [12]. thus both business as well as personal information is required to ignite and conclude generally m-payments data of the clients are found in the endpoint, it is very significant to examine the level of risk of information to be mined dwelling inside such endpoint [13]. In order to be able to transform the mobilecomputing atmosphere very pervasive, it is essential that the communication carrier is feast overboth wired and wireless means [14].

4 METODOLOGY

As indicated by Easterbrook et al. [8], suggested that one of the initial steps while picking a proper research strategy by enlighten the research method. Following such recommendation it has led this research in to the following methodology.Therefore, the research discussed different literally works from the previous scholars and suggest the potential techniques in solving m-commerce security treats through a descriptive researchtechnique.

5 A REVIEW ON THE METHODOLOGY OF SERVICE QUALITY EVALUATION

Evaluative methods of Quality of Service (QoS) perform essential functions in service technology. Assessment or evaluation of the quality of service can determine whether the service system and procedures operates in the appropriate direction, and frequently enhance the quality of the service been offered to customer. The process is the same to m-commerce [15].

5.1 Transaction modes of mobile e-commerce

Based on the features of transactions, mobile e-commerce will be separated into two different processes of business-to-customer (B2C) and person-to-person (P2P). Distinct from area of Internet e-commerce to m-commerce, this section design is not global in m-commerce; the more common section type is depending on the various transaction patterns.

5.2 The security needs of mobile e-commerce

M-commerce security challenges consist of the following concerns: the stability and reliability of transactions, information privacy, data confidentiality and secrecy, acknowledgement of transactions as well as data integrity. Reliability usually means reassured transactions item is real and true. Confidentiality represents the material of the message was not irrelevant to see. It is unquestionable that of the people in the transaction is to make sure that the two factors can never be declined, and engaged within the transactions. While data integrity represents information or data will not be harmful modify in the procedure of transmission, while also the information received by the target is sent by transmitting information and data, at same moment, the sender sent the precision of the information can be passed on through the recipient hands [16].

5.3. Possible components in m-commerce transaction

Transactions of mobile commerce usually consist of several components of networks (multicast server, location database as well as preference database) as shown in the figure below.

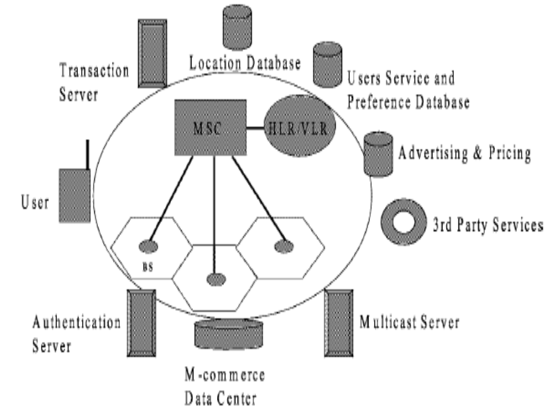
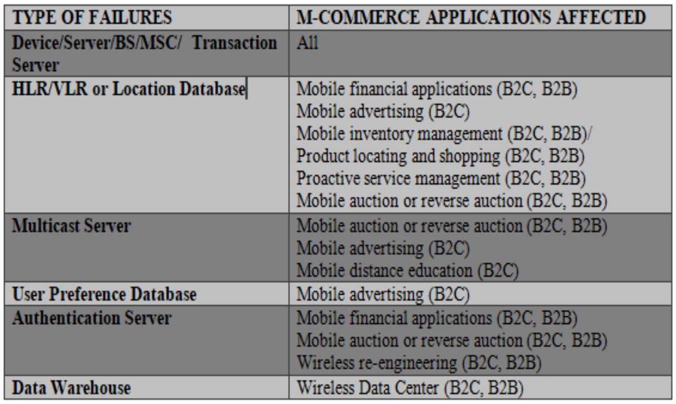


Fig. 1. Components of M-Commerce [17].

TABLE 1
IMPACT OF WIRELESS FAILURE ON M-COMMERCE



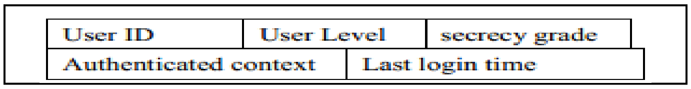
TYPE OF FAILURES	M-COMMERCE APPLICATIONS AFFECTED
Device/Server/BS/MSC/ Transaction Server	All
HLR/VLR or Location Database	Mobile financial applications (B2C, B2B) Mobile advertising (B2C) Mobile inventory management (B2C, B2B)/ Product locating and shopping (B2C, B2B) Proactive service management (B2C, B2B) Mobile auction or reverse auction (B2C, B2B)
Multicast Server	Mobile auction or reverse auction (B2C, B2B) Mobile advertising (B2C) Mobile distance education (B2C)
User Preference Database	Mobile advertising (B2C)
Authentication Server	Mobile financial applications (B2C, B2B) Mobile auction or reverse auction (B2C, B2B) Wireless re-engineering (B2C, B2B)
Data Warehouse	Wireless Data Center (B2C, B2B)

Therefore, various transactions may perhaps demand different kind as well as quantity of the components of network considering (table 1). For instance, mobile online deal or auctions might require multicast, place as well as authentication servers, although advertisement of mobiles could simply make use of LD (Location Database). For that reason, transactions of m-commerce would definitely be affected due to the failures or breakdowns of various components of networks [17].

5.4 Collaborative mobile electronic commerce

Collaborative Mobile electronic Commerce (CMEC) describes as a structure, or business model through working with 3G, some newly means of communication as well as the internet, allowing the organization's up-stream suppliers and raw materials, business organizations, distributors, department of telecommunication, business organizations, the financial division to operate with or interact personally with one another, and allows them to perform business operations without time limitations, in order to accomplish the collaborative business bunch and own value added CMEC has some models of security such as collaborative database layer, wireless network security interface, system application layer, and application layer as well [18].

TABLE 2
LAYOUT OF MOBILE STATION AUTHENTICATED



User ID	User Level	secrecy grade
Authenticated context	Last login time	

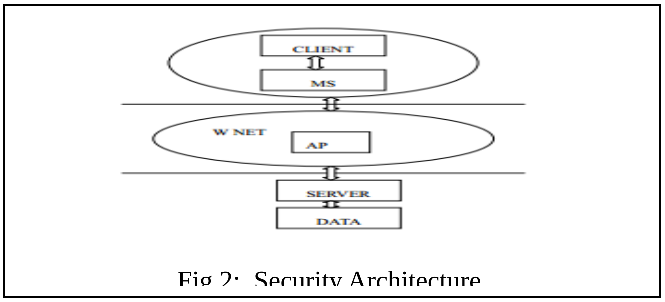


Fig 2: Security Architecture

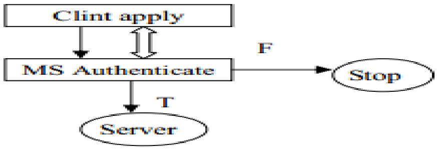


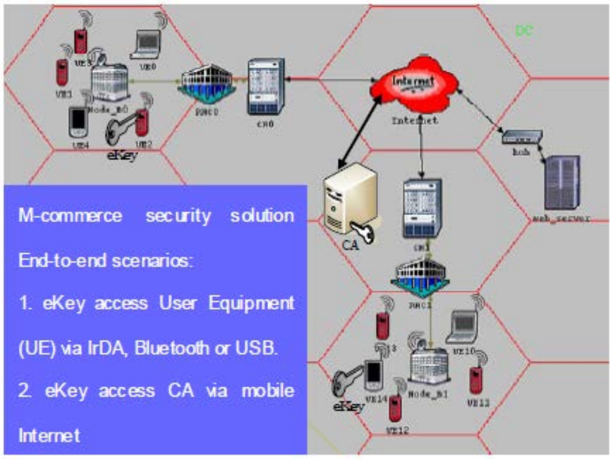
Fig 3: Authentication procedure.

A Wireless Application Protocol (WAP) offers all the fundamental services of a computer-based web-browser but basically to function within the limitations of mobiles, like its lesser view screen. Therefore, users can be connected to Wireless Application Protocol sites: websites published in, and actively transformed to (Wireless Markup Language) WML as well as accessed through the Wireless Application Protocol browser [19].

6 MOBILE COMMERCE SECURITY SOLUTIONS

The present M-commerce has introduced three different kinds of security solutions such as: (software-only, hardware-based and biometrics alternatives). Several financial institutions such as banks, have considered the hardware security encryption, such as digital or electronic key, alternate application software protection and encryption for the customers. But the present M-commerce continue to presumes application protection or software encryption, even the simply written text message of SMS to secure the professional deal of commercial transaction, which is uncomplicated and easier to be mauled by the malware or viruses and cyberpunk (hackers).

The essential factor of M-commerce Security Solution is mainly the location where the encryption key is saved. Generally, encryption key usually saved in the device i.e. mobile device (ME) or the Prospective subscriber Identification Component simply known as Subscriber Identity Module (SIM) [20].



M-commerce security solution

End-to-end scenarios:

1. eKey access User Equipment (UE) via IrDA, Bluetooth or USB.

2. eKey access CA via mobile Internet

Fig 4: Mobile-Commerce Security Solution.

M-commerce security provide an approach for application layer, which utilizes all types of mobile security solutions and services for the benefit of comfort: administration and user identification, also known as(Authority and Key Agreement), Data Integrity (DI), Data Confidentiality (DC), verification information interpretation between e-Key and web server.

A. User confidentiality

Key identification (KID) of permanent user as well as user M-commerce solutions and services are unable to be identified by eavesdropping which obtained by use of short-term and temporary identity (TID) which is allocated by UE via web server. KID is transmitted in clear-text when developing TID [24].

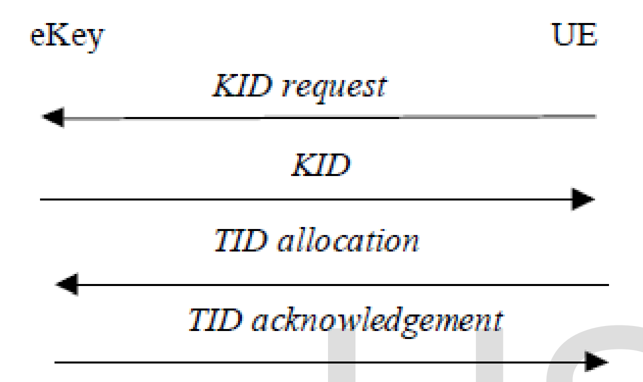


Fig 5: User confidentiality.

B. Mutual authentication

During (AKA) Authentication Key Agreement the UE and server verify one another, therefore they are more consent on cipher reliability i.e. integrity as well as cipher key (CK, IK).these keys are utilized right until their time has ended. Through supposition of reliable server and CA, and reliable hyperlinks or simple links between them, right after AKA that guarantee UE together with server that IK and IK never employed from the first place, security method must be arranged to consider the fact over security, reliability and integrity algorithm as well as criteria [21].

C. Data integrity

Authentication and data integrity of M-commerce origin signaling the data is essential to be provided. Both server and user decide on integrity key with procedure during AKA and security process set-up.

D. Data confidentiality

Both user data and signaling must be secured from snooping. While server alongside user, settle on to check algorithm through AKA and security set-up process.

6.1 Mcommon Solutions

A suitable solution of m-commerce security or mobile e-commerce protection weaknesses is to create the end-to-end security mode, which defends each inadequate link in m-commerce business and transaction approach to make sure that data and information from the transmitting point to the ultimate destination is totally secure [22].

Customer normally takes his/her ID card and credit card to any organization or financial workplaces of bank organization fills up in "Personal mobile transaction Banking Services Application Form" in order to apply for the service and attain digital security system or device as well as authentication code. Pursuing the process mentioned in Customer's Guide, user can set up m-payment (mobile payment) user software on their cell phone via OTA. All the finalized details such as MSISDN, IMSI, IMSI, username, security password, authentication code etc. is saved in background database for long term financial transaction [23].

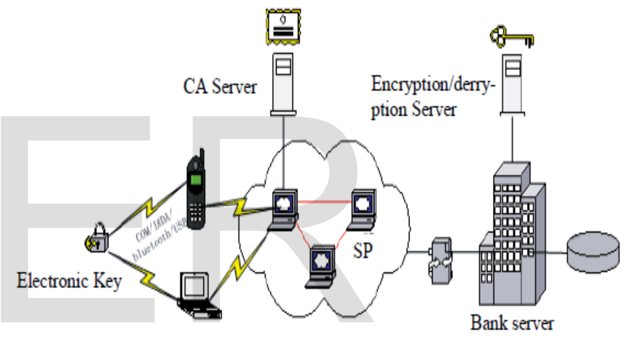


Fig 6: Mobile payment solution.

7 CONCLUSION AND FUTURE WORK

Online business precisely e-commerce is broadly viewed as the purchasing and selling of items over the web, yet any transaction that is executed exclusively through electronic medium can be viewed as web based business (e-commerce). Step by step E-business and M-commerce assuming great job in online retailing advertising and individuals groups utilize this innovation step by step. The combination of both mobile devices with traditional e-commerce made it possible for anywhere and anytime access to an online transactions, Regardless of advantages that gave in online business by smartphones because of communication nature of the remote communication, it is obligated to manage new potential security dangers. Mobile transaction has the most difficult angle which is the information and data transmission as well as providing a security measures in mobile devices for generally m-commerce. Service providers have a frequent and consistent challenge in order to tackle the issue once and for all.

We must consider that, through the advancement mobile network system in the direction of the 3G technological innovation as well as the optimization of mobile delicate atmosphere (the improvement of Wireless Application Protocol as well as the perfection of information technology and description language), the issues of-commerce security will obtain a greater solution. Therefore, mobile commerce simply increased at the moment, which can definitely recognize the desire of providing information anywhere and at any given time, enabling clients not to rely on area boundaries or region limits, therefore by making both person as well as the information flow. Consequently, wireless rate has extra running effects than cable rate. The program and applications of m-commerce will attain a greater advancement in the future especially by implementing a proper method of security for better transactions.

8 References

[1] Thanh, D. V.,"Security Issues in Mobile eCommerce" International Conference on Electronic Commerce and Web Technologies S, and Fan, L, , 467-476, doi: 10.1007/3-540-44463-7_41.

[2] Wang, S, and Fan, L, (2010), "A solution of mobile e-commerce security problems," IEEE comp. society, 20I0 2nd International Conference on Education Technology and Computer (ICETC), ISSN: 978-1-4244-6370-1 pp. 188-189.

[3] Prakash, K., Balachandra, Kumar, C., & Avinash. (2014). Enhancing PKI for mobile commerce security. *2014 International Conference on Science Engineering and Management Research, ICSEMR 2014*, 1–4. https://doi.org/10.1109/ICSEMR.2014.7043635

[4] Rashad, Y and Mahomed, S. (2013). Mobile Commerce and Related Mobile Security Issues. International Conference on Software and Computer Applications. *IPCSIT Volume 9*, *9*, 198–201.

[5] Seeburn, K., (2014), "*Securing Your Mobile Commerce*, ISACA Trust in, and Value from, Information Systems." Journal of Theoretical and Applied Economics.

[6] Ali, S., Farag, W., & Rob, M. A. (2015). Security Measures in Mobile Commerce : Problems and Solutions. *The Fourth International Conference on Electronic Business*, (April). Retrieved from https://www.researchgate.net/publication/221365986 page 1-6.

[7] Siau. K, and Lim. E. P (2001),, *Mobile commerce: Promises, challenges and research agenda Journal of database management,* IDEA group publishing, pp 2-11.

[8] Easterbrook. S, Singer J., Storey. M.-A., and Damian. D., (2008), "*Selecting empirical methods for software engineering research*". In Guide to advanced empirical software engineering pages 285-311. Springer, 2008.

[9] Wushishi. U. J., and Ogundiya. A. O. (2014), *Mobile Commerce and Security Issues,* International Journal of Scientific Research Engineering and Technology, (IJSRET), ISSN 2278 – 0882 Vol 3, Issue 4 pp2-10.

[10] Mirarab. A., and kenari A. R. (2014), *Study of secure m-commerce, challenges and solutions*, ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 2, No.8 , March 2014, ISSN : 2322-5157

[11] IVAN. I., MILODIN. D., and ZAMFIROIU. A., (2014), *Security of M-Commerce transactions*, Journal of Theoretical and Applied Economics.

[12] Niranjanamurthy M et.al (2013), Analysis of E-Commerce and M-Commerce Advantages, Limitations and Security issues: *International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2013*

[13] Cavallari .M. and Tornieri F. (2017), Vulnerabilities of Smartphones Payment Apps: The Relevance in Developing Countries *International Journal of the Academic Business World.*

[14] Prakash. K and Balachandra (2015), Security Issues and Challenges in Mobile Computing and M-Commerce, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015.

[15] Peng L and Lai. L, (2009) "A study on service quality assurance in mobile commerce," IEEE comp. society, 2009 Second International Workshop on Computer Science and Engineering, ISSN: 978-0-7695-3881-5/09, pp. 207-209.

[16] Jiang, H. (2008) "Study on Mobile E-commerce Security Payment System," IEEE comp. society, International Symposium on Electronic Commerce and Security, ISSN: 978-0-7695-3258-5/08, pp.754-755, 2008.

[17] malloy A. D., Varshney, A and Snow, A P.(2002) "Supporting Mobile Commerce Applications Using Dependable Wireless Networks," *Mobile Networks and Applications 7*, 2002 Kluwer Academic Publishers. Manufactured in Netherlands, pp. 255-256

[18] Jing W and Bingwen Q. (2010) "The Security Model Design for Collaborative Mobile E-Commerce Based on Wireless Middleware," IEEE comp. society, 978-1-4244- 7618-3 /10, pp. 1-2.

[19] ZhengLeina, P T. (2012) "New Mobile Commerce Security Solution Based on WPKI," IEEE comp. society, 2012 International Conference on Communication Systems and Network Technologies, ISSN: 978-0-7695-4692-6/12, pp. 486, 2012.

[20] Pan Tiejun, Zheng Leina, Fang Chengbi, Huang Wenji and Fang Leilei, (2008) "M-commerce Security Solution Based on the 3rd Generation Mobile Communication," IEEE comp. society, 2008 International Symposium on Computer Science and Computational Technology, ISSN: 978-0-7695-3498-5/08, pp. 364-365, 2008

[21] He. L, Ning Zhang, Lirong He, Ian Rogers (2013), "Secure M-commerce Transactions: A third Party Signature Based Protocol" IAS 07 Proceedings of the Third International Symposium on Information Assurance and Security. Pages 3-8 IEEE Computer Society, ISBN:0-7695-2876-7

[22] Patro. S. P., Padhy N, and Panigrahi, R. (2017)," Security Issues over E-Commerce and their Solutions" International Journal of Advanced Research in Computer and Communication Engineering ISSN (Online) 2278, Vol. 5, Issue 12, December 2016

[23] Dechao Sun, Tiejun Pan, Zhong WAN, and Haiyan He, "Research of Mobile E-commerce Security Solution based on External Electronic Device," IEEE comp. society, 2010 Sixth International Conference on Semantics, Knowledge and Grids, ISSN: 978-0-7695-4189-1/10, pp. 355-366, 2010.

[24] Malathy, M., Smilee S. J., Samuel , J. N (2016) "Secure Mobile Agent in M-Commerce over Internet " IEEE comp. society, ISSN: 978-1-4673-6725-7/16 pp. 1-5.