Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 3915 - 3921
Received 25 April 2021; Accepted 08 May 2021.

Enhancing Security in M-Commerce Transactions

Kaneez Fathima[1], Dr. Savadam Balaji[2]

Research Scholar, KoneruLakshmaiah Education Foundation, Hyderabad[1]
Professor, KoneruLakshmaiah Education Foundation, Hyderabad[2]
fatima.baig06@gmail.com[1], balajis@klh.edu.in[2]

Abstract

M-Commerce is an evolving aspect of e-commerce that should meet the critical requirements of high security and single sign on, including minimalism and manageability. These features can draw ordinary individuals to make use of more M-Commerce. Because there are certain vulnerabilities and wireless communication risks in trade transactions, it is particularly important to examine mobile e-commerce transaction systems in the payment process. In order to satisfy customer requirements, payment protection threats must be avoided in M-commerce by introducing a specific improved security solution in the M-commerce systems. In this paper an architecture is suggested and tested for secure M-transactions with the increased security level of user and service provider authentication. In terms of quality, usability and protection, this proposed architecture must be understood by evaluating its execution time, performance and security.

Keywords: www, M-Commerce, Cryptography, biometrics, critical requirements, vulnerabilities*;*

1. Introduction

Trade, on a wide scale, buys and sells goods. The system is comprised of economic, social , cultural, legal and technical structures operating in any region. Trading of products / services using computer networks is e-commerce or electronic commerce. Technologies such as M-commerce, Internet marketing, inventory systems, online transaction management, electronic data interchange (EDI), electronic transfer of funds, and automated data collection systems are appealing to electronic commerce. The World Wide Web (WWW) and also other tools, such as e-mail, are used for modern e-commerce. The first online shopping system was demonstrated in 1979 by Michael Aldrich. Many individuals trust that biometric frameworks can identify liveness in biometric tests [2].

Application of Digital Technologies to Agriculture is an innovative idea focusing on the enhancement of agricultural development in rural areas [3].It is essential to build security solutions by adopting a Security Framework for any organization to find solutions for majority of vulnerabilities and flaws [4]. Secure data transmission is the fundamental need for the users of internet community [6]. Mobile Commerce is a growing E-Commerce domain where consumers can use a mobile and wireless network to communicate with service providers, deploy a mobile gadget for data recovery and deal with dispensing. The sophisticated version of e-commerce activities carried out using mobile phones or PDAs is defined by M-commerce, which enables the consumer to carry out future transactions through a wireless telecommunication network (Khasawneh 2009; MuhibUllah et al 2012). Although there are also a host of parallels between e-commerce and M-commerce, they also have firm differences. Under such a condition, transforming the information from the transmitter to the receiver requires more security.[7].

Although there are also a host of parallels between e-commerce and M-commerce, they also have firm differences.

2. Existing System

Differences such as internet access are a permanent must in e-commerce, but there are no such constraints in the course of M-commerce; video conferencing is done by M-commerce where it is beyond the realm of e-commerce; energy is an important factor in e-commerce, while in M-commerce it is not vital.

Issues and Challenges in M-Commerce

M-commerce has emerged as a promising technology in which consumers have the flexibility to connect with service providers for data / service request, reclamation and transaction functions using a mobile device with a cellular network. It is unfortunate, however, that mobile devices submit themselves unwittingly to the unscrupulous hands of hackers by allowing them illicit access to corporate networks, paving the way for the injection into these networks of viruses and other dangerous software (Fengling Han et al 2012). In addition, M-commerce is plagued by many mobile computing security vulnerabilities that are detailed below:

1. Computer and data theft / loss: Data stored on the computer can easily be physically accessed by unauthorised individuals if the device is lost or stolen.
2. Clone: Setting up a cell phone chip in a way that changes the ESN.
3. Hijacking: Dominate, imitating one of them, the contact session between two individuals.
4. Malware: malicious code in the form of a virus , worm or other malware for the execution of illegal tasks.
5. Phishing: Monitoring and pressuring a victim to disclose sensitive confidential information or download malware.
6. Wireless link vulnerabilities: It is possible to obtain hidden data sent through many different insecure wireless networks.

From the air by ambushers, causing considerable harm to the handheld gadget and causing the networks through which the handheld unit is connected to untold problems.

Challenges and Techniques

The primary problem facing the M-commerce system is the identification and authentication of users to conduct secure M-shopping. Recent years have seen a growing awareness of the need to improve information security [9]. The human characteristic has to be distinctive and unswerving for the purpose of defining a particular person. The study showed that validation of fingerprints is the most fruitful approach for other biometrics. Protection technologies, as opposed to parallel expression, face and iris detection techniques, are known to be more reliable and cost-effective. In the M-commerce method, M-payment is another obstacle faced by server authentication. For server authentication, there is a need for a specific process to submit the PIN securely through a network. Distributed PIN double encryption is one of the reliable server authentication techniques that provide M-commerce with a secure level. In this work to accomplish secure M-commerce transactions, the following issues were considered and implemented:

Develop an efficient reversible data hiding technique to keep user information protected in the WAP (wireless application protocol) gateway when transmitting user data. Implement an effective biometric framework based on fingerprints for safe user authentication. Study and use the best algorithm by comparing different algorithms (AES, RC4, DES, 3DES) for encryption and decryption. Build a special PIN distribution architecture (authentication and external server) with two servers. Develop and formulate a unique sequence table to transform the user's PIN number before encryption into a stable unique sequence. Using the double encryption paradigm in the architecture to increase the security level.

Challenges and Techniques

The primary problem facing the M-commerce system is the identification and authentication of users to conduct secure M-shopping. Recent years have seen a growing awareness of the need to improve information security [9]. The human characteristic has to be distinctive and unswerving for the purpose of defining a particular person. The study showed that validation of fingerprints is the most fruitful approach for other biometrics. Protection technologies, as opposed to parallel expression, face and iris detection techniques, are known to be more reliable and cost-effective. In the M-commerce method, M-payment is another obstacle faced by server authentication. For server authentication, there is a need for a specific process to submit the PIN securely through a network. Distributed PIN double encryption is one of the reliable server authentication techniques that provide M-commerce with a secure level. In this work to accomplish secure M-commerce transactions, the following issues were considered and implemented:

Develop an efficient reversible data hiding technique to keep user information protected in the WAP (wireless application protocol) gateway when transmitting user data. Implement an effective biometric framework based on fingerprints for safe user authentication. Study and use the best algorithm by comparing different algorithms (AES, RC4, DES, 3DES) for encryption and decryption. Build a special PIN distribution architecture (authentication and external server) with two servers. Develop and formulate a unique sequence table to transform the user's PIN number before encryption into a stable unique sequence. Using the double encryption paradigm in the architecture to increase the security level.

3. Proposed System

Cryptographic Techniques

Only in the framework containing said characteristics above can trustful M-commerce transactions be made. We have performed fingerprint matching in two steps: i) point-wise match and ii) trim false matches with arithmetical constraints [1]. The assistance of techniques such as cryptography in M-commerce transactions is taken into account to achieve such characteristics. There are two types of cryptographic techniques:

- Symmetric key cryptographic techniques (RC4, DES, 3DES, AES)
- Asymmetric key cryptographic techniques (RSA, DSA, HECC)

As symmetric algorithms are compared to asymmetric algorithms, the former is the easiest algorithm compared to the latter. The simplicity of the symmetric algorithm is because both encryption and decryption use only one key; therefore, compared to asymmetric algorithms, it processes the data quickly (Lalit Singh &Bharti 2012). In addition, as shown in Figure 1, symmetric cryptographic methods can be categorised into two.

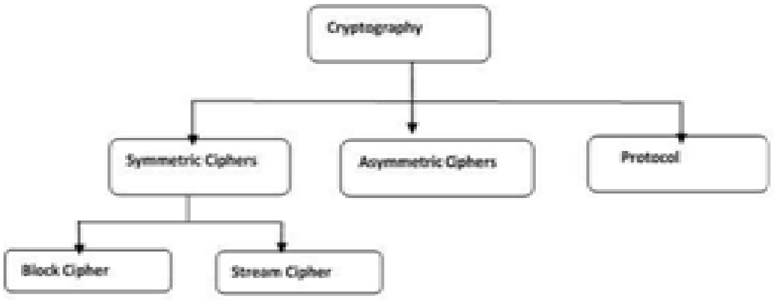

Fig. 1 Cryptographic Techniques

The block cypher divides the text into moderately large blocks and independently encrypts each block. Each block's encryption depends, at most, on one of the previous blocks, and each block uses the same key. But in stream cypher, the text is divided into small blocks and each block's encoding depends on several previous blocks, and a different key is created for each block, and block cyphers normally need more memory as they operate on larger pieces of data and have often been carried over from previous blocks. As they operate faster by taking just a few bits at a time that lets them consume little energy and memory, a stream cypher is commonly used as a preferred method for mobile devices. This feature will assist in saving the mobile's battery life. So, Stream cyphers fulfil the requirements of low H / W complexity, high throughput multimedia applications. RPM and TLA processing provide final results which are undoubtedly visible for health practitioner reviews for pre and post or even during surgical activities [10].

3.1 Use of pin techniques in existing system

However, due to its portability and compatibility, cell phones are more common; it pointedly has security threats to end-users. That is because mobile devices tend to be more personal, not like desktop stations, which have more personal user details, and are often stored in an unsafe way. Every year, countless numbers of handheld mobile devices are lost (Stephanie 2010). If attackers mimic the real users, the key problem with the missing devices is the lack of identity authentication.

The user is only authenticated in this system after receiving the service request, then the client side is requested by the server side to capture personal biometrics such as fingerprint , iris, photo, etc. After the verification is done on the server side, which provides a stable M-banking mechanism, the client side may perform a transaction. Both server and customer can protect their rights and interests in the case of any M-banking quarrels due to internet hacking or mobile theft for M-banking. The only downside of the component is that there is no discussion / use at the transmission stage of any stable encryption method algorithm.

For M-commerce transactions (SugataSanyal et al 1997), the Safe Electronic Transaction (SET) approach has been used. It is an open protocol specification built over the internet for credit card transactions. This technique has several drawbacks, such as a problem with the management of limited resources, and sniffing can be used to target the wireless network. When the external device is cracked, the whole PIN can be obtained.

3.2 Proposed and improved pin distribution technique in M-Commerce

When it offers anonymity, protection and honesty, M-commerce transactions can be widely performed by ordinary individuals via mobile phones. Only by overcoming the risks associated with trade transactions via wireless links and evaluating the weakness of the M-commerce transaction systems can these characteristics be allowed. It can be done by improving the gateway security solution.

Through the WAP gate, which has been done in this work by using distributed pin technology and double encryption model, it is important to submit the user pin number and payment information in a protective way. The Figure shows the full flow diagram of the proposed Improved Pin Distribution Techniques in the M-Commerce method.

4. Conclusion

To satisfy the customer completely during the transaction, improved protection is required. Therefore, in the service supplier authentication side of M-commerce systems, the distributed PIN is used. In addition , it uses a ground-breaking mobile protection framework and strategy. It can be accomplished through an increasingly secure WAP gateway that uses double encryption models. The handling of verification using a distributed PIN system also facilitates enhanced protection and reliability. Although all of these innovations have been applied separately, using all of these together would improve the security of M-Commerce to a greater degree. The use of distributed PIN for verification and merchant authentication purposes, with all the limitations of mobile devices, makes communication highly efficient and provides enormous security, guaranteeing the customer that the transaction is carried out with the right person. Different authentication schemes with the combination of PIN and Biometric technologies on the user and server side of the architecture have been carried out and tested in mobile environments for the successful and safe use of M-commerce transactions.

5. Reference

[1] Sahithi, S., Anirudh, A., Swaroop, B., Ruth Ramya, K. Biometric security for cloud data using fingerprint and palm print 2019 International Journal of Innovative Technology and Exploring Engineering863383432https://www.scopus.com/inward/record.url?eid=2s2.085069451595&partnerID=40&md5=6a4102e306106fd16731338b23028bd9

[2] Tarannum, A., Rahman, M.D. Multi-modal biometric system using Iris, Face and fingerprint images for high-security application 2019 International Journal of Recent Technology and Engineering 76314320 https://www.scopus.com/inward/record.url?eid=2-s2.085067962719&partnerID=40&md5=b1b1c2acd0ee967c767d7a35cad52cbc

[3] Puvvada, N., Prasad Babu, M.S.Semantic web based banana expert system 2018 International Journal of Mechanical and Production Engineering Research and Development 833643713 https://www.scopus.com/inward/record.url?eid=2-s2.085062992172&partnerID=40&md5=3579f6c1ea568fcc5ab66dc77cdd7dd1

[4] Veerapanenic, S.S., Raja Sekhar, K. A systematic study of asset management using hybrid cyber security maturity model 2019 International Journal of Recent Technology and Engineering 76678683https://www.scopus.com/inward/record.url?eid=2s2.085065160274&partnerID=40&md5=ab47677f05cff6ca9f2834f94c41ac1e

[5] Aparna, Puvvadi; Kishore, PolurieVenkata Vijay Biometric-based efficient medical image watermarking in E-healthcare application IET IMAGE PROCESSING FEB 28 2019 13 3 421 428 10.1049/iet-ipr.2018.52886

[6] Sahu, Aditya Kumar; Swain, Gandharba Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis INTERNATIONAL JOURNAL OF ELECTRONIC SECURITY AND DIGITAL FORENSICS 2019 114458476 10.1504/IJESDF.2019.102567

[7] Biometric-based efficient medical image watermarking in E-healthcare application Aparna, P; Kishore, PVV IET IMAGE PROCESSING FEB 28 2019 10.1049/iet-ipr.2018.528864

[8] Adaptive PVD Steganography Using Horizontal, Vertical, and Diagonal Edges in Six-Pixel Blocks Pradhan, A; Sekhar, KR; Swain, G SECURITY AND COMMUNICATION NETWORKS 2017 10.1155/2017/19246184

[9] A Dependency analysis for Information Security and Risk Management Krishna, BC; Subrahmanyam, K; Kim, THE INTERNATIONAL JOURNAL OF SECURITY AND ITS APPLICATIONS AUG 2015 10.14257/ijsia.2015.9.8.17

[10] Bangare, Sunil L.; Pradeepini, G.; Patil, Shrishailappa: a new computational technique for precise medical imaging INTERNATIONAL JOURNAL OF BIOMEDICAL ENGINEERING AND TECHNOLOGY 2018 27 1-2 76 85

[11]Yang, X.S., 2012, September. “Flower pollination algorithm for global optimization.” In International conference on unconventional computing and natural computation” (pp. 240-249). Springer, Berlin, Heidelberg.

[12] Jena, S. R., Lavanya, D. R., &Gadde, S. S. (2017). “Minimization of execution time over cloud computing environment using fuzzy technique.” Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 18)

[13] Phanikumar, V., &Satyanarayana, K. V. V. (2017). “Advanced data sharing and group scheduling procedure for dynamic resource allocation of cloud computing”.Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 6), 396-409.

[14] Rathod, S. B., & Reddy, V. K. (2017). “Dynamic framework for secure VM migration over cloud computing”. Journal of Information Processing Systems, 13(3), 476-490.Doi:10.3745/JIPS.01.0015

[15] Krishna, P.V., . “Honey bee behaviour inspired load balancing of tasks in cloud computing environments”. Applied Soft Computing”, 13(5), pp.2292-2303.

[16] Jena, S. R., Lavanya, D. R., &Gadde, S. S. (2017). “Minimization of execution time over cloud computing environment using fuzzy technique.” Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 18) Retrieved from www.scopus.com

[17] Siva NageswaraRao, G., &Srinivasu, S. V. N. (2017). “Hybrid approach for task scheduling in heterogeneous cloud based systems”. Journal of Advanced Research in Dynamical and Control Systems

[18] Raghav, rs; amudhavel, j; dhavachelvan,P, “Enhanced artificial bee colony optimization for solving economic load dispatch” iioab journal 2017 1994238 Potluri, S., &Rao, K. S. (2017).

[19] SirishaPotluri,KattaSubbaRao ,”Quality of service based task scheduling algorithms in cloud computing”. International Journal of Electrical and Computer Engineering, 7(2), Vol. 7, No. 2, April 2017, pp. 1088~1095.

[20] Praveen, SP; Rao, KT; Janakiramaiah, B “Effective Allocation of Resources and Task Scheduling in Cloud Environment using Social Group Optimization” Arabian journal for science and engineering AUG 2018 10.1007/s13369- 017-2926

[21] Lavanya, K; Reddy, LSS; Reddy, BE, “Distributed Based Serial RegressionMultiple Imputation for High Dimensional Multivariate Data in Multicore Environment of Cloud”international journal of ambient computing and intelligence apr-jun 2019 10.4018/IJACI.20190401051

[22] Dey, NS; Gunasekhar, T “A Comprehensive Survey of Load Balancing Strategies Using Hadoop Queue Scheduling and Virtual Machine Migration”, IEEE ACCESS 2019 10.1109/ACCESS.2019.2927076A

[23] Babu, K.R., Samuel, P, “Enhanced bee colony algorithm for efficient load balancing and scheduling in cloud”. In: Innovations in Bio-Inspired Computing and Applications, pp. 67–78. Springer,New York (2016).

[24] Nagesh P, Srinivasu N, Ranganadh N” Optimal vmplacement using particle swaroptimization”, et al. International Journal of Scientific and Technology Research (2020)

[25] Akhila B, Srinivasu N, Varalakshmi A, et al. “Energy efficient scheduling of virtual machines

in cloud data center",International Journal of Recent Technology and Engineering (2019)

[26] A Seenu, M R Narasingarao, U S SPadmajyothi, International Journal of Advance Research in Computer Science, 2014, "A System for Personal Information Management Using an Efficient Multidimesional Fuzzy Search".

[27] GaikwadKiran P, Dr. C M Sheela Rani, International Journal of Scientific & Technology Research, 2020, "Regression Model with Modified Linear Discriminant Analysis Features for Bimodel Emotion Recognition".

[28] Mr.PrashantMininathMane, Dr. C M Sheela Rani, IJPAM, 2018, "Triple Data Encryption Algorithm based Multiple Authority Access Control in Cloud System Using Optional Threshold".

[29] D V Manasa, M R NarasingaRao, A S Lalitha, International Journal of Applied Engineering and Research, 2014, "Analyzing the Services and Privacy Conflict Resolutions of Shared Data in OSNs".

[30] SwathiKarkarlapudi, M R NarasingaRao, International Journal of Science and Advanced Technology, 2011, "A Novel Facial Recognition Model Using an Artificial Neural Networks"

[31] SunandaNalajala, KanekarAkhil, VenkatSai, DivyenduShekhar, Praveen Tumuluru, 2019, "Light Weight Secure Data Sharing Scheme for Mobile Cloud Computing".

[32]Senthil Kumar AvinashiMalleswaran, BhaskarakraoKasireddi, Dec, 2019, IJSTR, "An efficient Task Scheduling Method in Cloud Computing Envirnoment Using Fire Fly Crow Search Algorithm (FF-CSA)".

[33] Dr V Krishna Reddy, G NarasimhaRaju, K Lakshmi, N Vamsi, 2019, IJAST, "An Advanced Keyword Attacks over Encrypted Data in Cloud".

[34] B Tirapathi Reddy, ChBhuvaneshChava, T Susanth Kumar, V GopiKalayan, Nov, 2019, IJAST, "Security Key Provided for Group data Sharing in Cloud Computing"

[35] P Raja Sekhar Reddy, K Ravindranadh, 2019, IJITEE, "An Exploration on Privacy Concerned Secured Data Sharing Techniques in Cloud"