ISSN: 0974-5823 Vol. 7 No. 2 February, 2022

*International Journal of Mechanical Engineering*

# A Two-Level Authentication Protocol for Secure M-Commerce Transactions using Encrypted OTP

**Mr. S. Ramana,** *Research Scholar Dept. of Computer Science, Osmania University, Hyderabad, India.*

**S. China Ramu**, *Professor, Dept. of CSE, CBIT (A), Hyderabad, Telangana, India.*

**N. Bhaskar,** *Assistant Professor, Dept. of Computer Science, Bhavan's Vivekananda College, Secunderabad, India.*

**M. V. Ramana Murthy,** Former Professor and Chairman, Computer Science, Dept. of Mathematics, Osmania University. Presently working at MGIT.

**Abstract—**

*Trading is the crucial and defacto factor of the world's economic growth, has a lot of impact on any country's GDP. Trading has remarkably changed its shape from the ancient barter system to the latest mobile commerce because of enhancements in technologies, the Internet, the use of digital currency and human beings livelihood, and in this pandemic situation of CARONA where everyone is focusing on online/digital trading.*

*Because of upgradations in technology usage and a drastic improvisation in hardware front, the entire computational devices and mobile phones have changed their motto of usage, where 90 percent of market users are using palmtops, laptops and smartphones and the human beings lifestyle is also drastically changed where they want everything on a single click through mobile apps irrespective of time and location (anytime from anywhere). The so-called e-commerce is merged with mobile communications, which emerged into mobile commerce.*

*Mobile commerce, also called mobile e-commerce or m-commerce, is defined as all activities related to a potential commercial transaction conducted through communications networks that interface with wireless or mobile devices. Mobile Commerce addresses electronic commerce via mobile devices, where the Consumer is not in physical or eye contact with the goods that are being purchased.*

*The advantages are massive with mobile commerce from the customer's point of view and the manufacturer's point of view. However, there are also many complexities and network security issues involved with this mobile commerce, which doesn't allow many mobile users to opt for m-commerce transactions.*

*Many Cryptographic security algorithms and communication protocols were utilized to build a robust payment system for mobile commerce, but they still need some ifs and buts. This paper provides a "Two-Level Authentication Protocol for secure M-Commerce Transactions using encrypted OTP" using any conventional or public-key cryptosystem algorithm and any one of the Messaging Protocols.*

*The Solution provided in this paper will overcome two major security attacks called "Replay Attack." and "Man in the middle attack."*

**Keywords:** M-Commerce, Cryptography, Authentication, E-Commerce, AMQP, Replay Attack, Man in the Middle Attack.

## I. INTRODUCTION

Mobile commerce represents online transactions using cell phones, tablets pc, and any other handheld devices. These online transactions are due to online shopping or any other cash transactions. Nowadays, everyone uses Google pay, phone pe, and Paytm applications for transactions, and every bank provides a UPI facility[1].

M-commerce accounted for 34.5 percent of all e-commerce sales in 2017. M-commerce has the most significant impact on the small scale industry to large scale industries. Using this m-commerce, bill payment for utilities became very easy. Even though there are so many advantages, we have to concentrate on the security issues of m-commerce[2].

## II. WIRELESS SECURITY

### *A. Public-key cryptography*

Public key cryptography (PKC) is employed to exchange a personal key or symmetric key utilizing a certificate, and there, in any case, the transmission is encrypted using the transferred key. Small key size of 40 bits is employed due to power restriction. Here WIM(Wireless Identity Module)is a component of the WAP Architecture to store private data securely (Keys pairs, Certificates, PINs) within mobile devices which can be a tamper-proof component[3,4,5]. In practice, a WIM is implemented by employing an open-end credit. WAP 1. x technology uses Wireless terminology (WML).

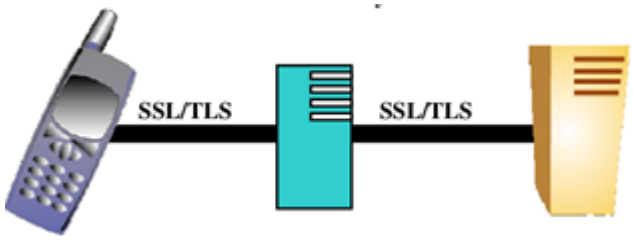


*Figure 1: WAP gap model.*

Because all I.P.-based technology requires end-to-end security, WAP2.0 utilizes TLS (Transport Layer Security) instead of WTLS to address the security vulnerabilities of WAP Gateway[6,7]. PKI stands for Public Key Infrastructure enabling protocol that offers security parameters like confidentiality and authentication via methods such as DSC and PKC. DSC stands for Digital signature certificate, PKC stands for public-key certificates. Encryption is provided by cryptographic techniques such as RSA, RC4, 3DES, and SHA-1[8]. For the first time, Wireless PKI (WPKI) has been issued. The WAP proxy model is shown in Figure 2.

### *A. Public Key Infrastructure*

PKI systems and WTLS are the essential components of the mobile security system. These both put together are also called mobile security. WTLS must be converted into SSL in the WAP system, an Internet standard at the WAP gateway. PKI will give fast services for mobile commerce applications by providing digital signature certificates and public-key certificates. These features will provide confidentiality and secured authentications for m-commerce applications[9,11].

PKI uses Certificate Authority (C.A.), Registration Authority (R.A.), and Certificate Holders, Verification Authority (V.A., Clients, and Repositories to provide secured transactions. WPKI is an enhanced version of traditional PKI for the wireless environment. "WPKI encompasses the necessary cryptographic technology and a set of security management standards that are widely recognized and accepted for meeting the security needs of M-Commerce" [18]. The architecture of WPKI is shown in figure 3.

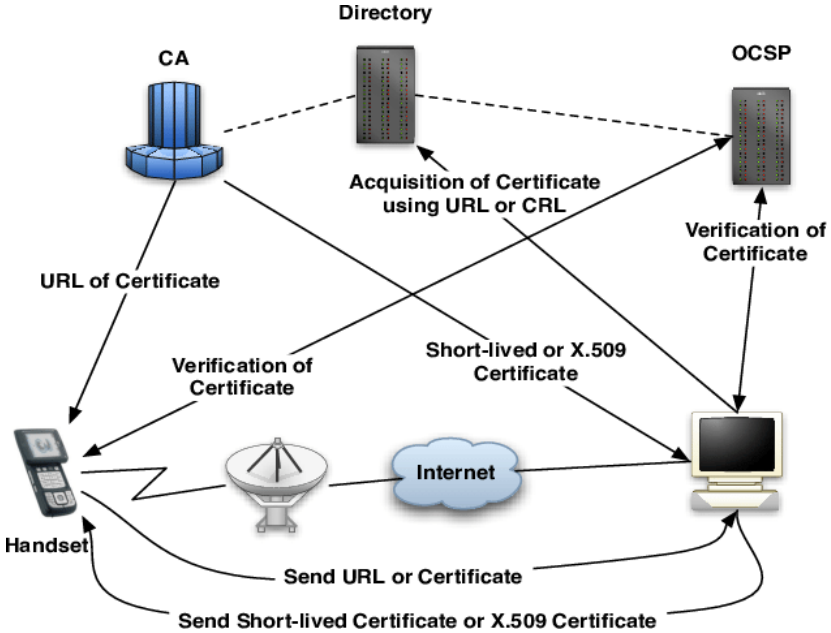


*Figure 2: Architecture of wireless PKI*

## II. AMQP PROTOCOL

Cryptography is converting standard clear English into unintelligible writing and vice versa. It is a method of storing and transmitting data in a format that can only be read and processed by authorized people. The AMQP is a message-oriented middleware application layer protocol accessible to each user. AMQP stands for Advanced Message Queuing Protocol. Message orientation, queuing, routing (including point-to-point and publish-and-subscribe), dependability, and security are all crucial aspects of the Advanced Message Queuing Protocol (AMQP) (i.e., messaging middleware). The main objective of AMQP protocols is to give level 2 security for banking transactions. AMQP includes definitions for both networking and message broker application functionality. AMQP is

an application layer protocol that specifies the operations of routing and storing messages with message brokers and a set of rules for networks. Two servers may interact using an encoding schema and many processes, independent of the technology utilized. AMQP's overall aim is to allow messages to flow via broker services across TCP/IP connections. Because AMQP is a binary protocol, everything transmitted through it is binary data; it's called a compact protocol. A binary protocol prevents unnecessary data from being sent across the wire. [14].

*A. The Advanced Message Queuing Model*

The following figure shows the AMQ model along with itscore components.

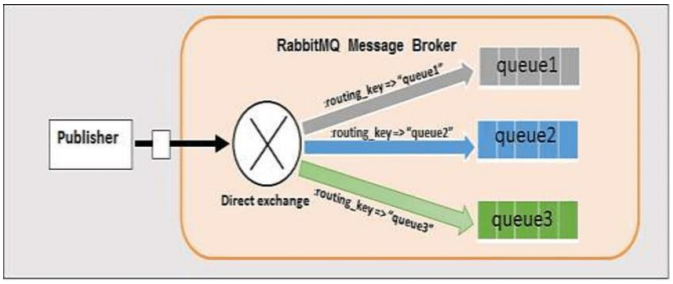


*Figure 3: AMQP Model*

Typically, a message is sent to exchange by a single client known as the producer. The message copies are then distributed to queues according to the rules specified by the exchange type and routing key supplied in the message. The message is eventually consumed by a subscriber[16].

A queue serves as a buffer or a temporary storage area for messages consumed later. Several characteristics may be specified during the establishment of a queue. It may be set as durable, auto-delete, or exclusive, indicating that it can only be utilized by one connection and that this queue will be destroyed when that connection ends. Beginner's guide to RabbitMQ Exchanges, routing keys, and bindings help you understand the many types of exchanges, bindings, and routing keys, as well as when and how to use them. It may be marked as durable to guarantee that it survives a broker restart or auto-delete to ensure that it is automatically deleted after the last queue has been unbound[15].

A queue serves as a buffer or a temporary storage area for messages consumed later. Several characteristics may be specified during the establishment of a queue. It may be set as durable, auto-delete, or exclusive, indicating that it can only be utilized by one connection and that this queue will be destroyed when that connection ends.

## III. RELATED WORK

We'll go through a few different payment mechanisms in thissection.

C→ CustomerM→ Merchant

I→ Issuer, i.e., client's bank

A→ Acquire, i.e., merchant's bank

There are four parties involved in these payment protocols in general. The payment gateway (P.G.) provides both issuer and acquirer services, acting as an interface between them and between client and merchant for clearing purposes.

The following are their high-level procedure steps:

A. *SET protocol*

SET protocol stands for *Secure Electronic Transaction Protocols* is a mechanism for securing electronic transactions. The SET protocol consists of two request/response messages, is a well-known credit card payment mechanism. Public key certificates are needed for all parties that use the SET payment mechanism. Payment initiation, purchase order authorization, capture payment, and card inquiry phase are the five transaction stages in the SET protocol implementation [17,18].

*B. iKP protocols*

iKP stands for *Internet Key Protocol*. The iKP protocols are based on public-key cryptography and vary in terms of the number of parties who own their public key pairs, represented by the protocol names: 1KP, 2KP, and 3KP. The larger the number of parties who possess public-key pairs, the higher the degree of security. Customer, merchant, and payment gateway (acquirer) are among the iKP's involved parties [19,20].

*C. The anonymous payment mechanism developed by C.Tellez J. et al.*

Tellez J. et al. [10] presented client-centric anonymous payment methods that use a digital signature technique with message recovery utilizing self-certified public keys. The five stakeholders involved are client, merchant, acquirer, IssuerIssuer, and payment gateway. The merchant registration and payment protocols are two sub-protocols of this payment protocol.

*D. The mobile payment protocol developed by D.Kungpisdan et al.*

S. Kungpisdan et al. [21] developed a secure account-based mobile payment system based on symmetric key operations requiring less computation from all parties involved. The following five parties are engaged in this protocol: client, merchant, IssuerIssuer, acquirer, and payment gateway. The protocol developed by Kungpisdan S. [22]et al. comprises two sub-protocols: merchant registration protocol and payment protocol. The customer must first register with the business by executing the merchant registration protocol before making a payment—the client and the merchant exchange a set of secret keys Xi after completing the registration procedure. A secret Key Yi is exchanged between the customer and the IssuerIssuer, and a secret Key Zj is shared between the merchant and the payment gateway.

## IV. PROPOSED SOLUTION

This paper, The Proposed Architecture, consists of Four Entities:

1. Customer: He wants to purchase the products in online mode and make a secure payment digitally.
2. Merchant/Supplier: The warehouse or digital platform provides the customer's required goods to be purchased.
3. Verification Centre: It is a trusted third party responsible for the financial Transactions between the other three entities (Customer, Merchant/Supplier, and Bank).

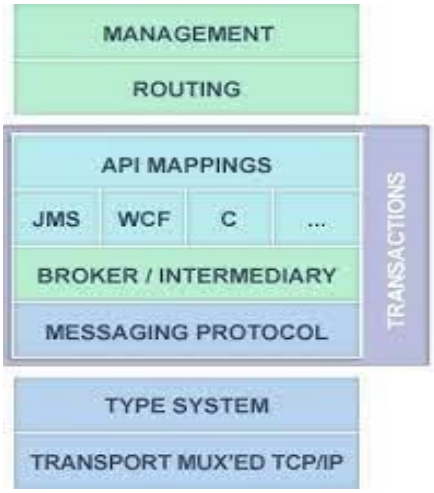


*Figure 4: Architecture of AMQP Model*

*4.* Bank: It is responsible for holding the accounts of customers and Merchant/Suppliers and doing credit/debit operations on their accounts.

The generalized model works as follows: The Consumer and the Bank will share a secret value used at the second level of authentication for payment processing.

**Step 1:** The consumer access the supplier app for purchasing the goods from the respective supplier on his/her mobile, palmtop, or any handheld device.

Level – 1 of Two-Level Authentication Protocol For Secure M-Commerce Transactions using AMQP Protocol.

**Step 2:** The Consumer enters the login credentials, which are encrypted at the consumer side using any conventional cryptographic algorithms. (First Level of the Authentication protocol for verifying the Consumer Identity, i.e., Authentication)

**Step 3:** The Encrypted message is transferred to the supplier application server through AMQP protocol, wherein the transmitted credentials are decrypted and verified with theregistered Consumer.

**Step 4:** If the entered credentials by the Consumer are found correct, then the next phase of selecting and buying the goods is started by the Consumer.

**Step 5:** After completing the selection of products, the Consumer goes for the payment method to choose his type of payment method from one of the payment options provided by the supplier.

**Step 6:** We provide the next level of the proposed two-levelauthentication protocol for secure M-Commerce Transactions using AMQP Protocol for the paymentprocessing using encrypted OTP.

Level – 2 of Two-Level Authentication Protocol For SecureM-Commerce Transactions using AMQP Protocol starts step 7.

**Step 7.:** At the second level, The Consumer receives an Encrypted OTP from the verification center. The Consumer enters the successfully decrypted OTP and completes the transaction by sending all the credentials to the verification center.

**Step 8:** The transmitted data is now transferred to the concerned bank through AMQP protocol, decrypting the credentials, debiting the amount from the respective account, and confirming to the Consumer and supplier.

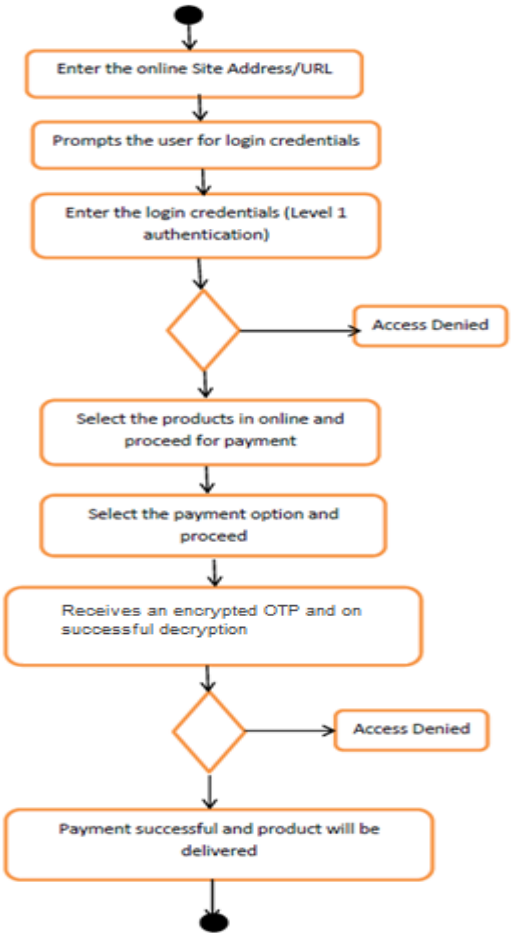


*Fig 4: Flow chart of the Proposed Model*

The flow of our proposed algorithm is explained in figure 4. It will give two-level security for digital transactions.

## V. CONCLUSION

The Payments module aspect in Mobile Commerce applications is an important issue that needs further investigation to develop secured and authenticated transactions. Many existing Conventional and Public key / Private Key encryption algorithms can perform encryption and decryption. At level two, by using encrypted OTP, it is established that we can achieve a greater level of security to overcome the security attacks such as "Replay Attack.", "Man in the middle attack." and many such.

Further, it is observed that the generalized proposed (A Two-Level Authentication Protocol for Secure M-Commerce Transactions using Encrypted OTP ) model will be verified across all the parameters and should be customized to some particular parameters in a specific context.

**REFERENCES**


[1] Ganley, M.J. (2000), ―Elliptical Curve Cryptography‖, Zaxus White Paper, 1-9.

[2] Goldman, Jeff, ―Wireless Security and M-Commerce‖, The Feature, March 8, 2001, <http://www.thefeature.com/article?articleid=9862>

[3] Harrison, A. (2000), ―Motorola, Certicom Ink Elliptic Crypto Deal‖, Computerworld, May 22.

[4] "How the French are Succeeding with M-commerce", Wireless Developer Network,

[5] Juul, Niels C., and Jorgensen, N. (2001), ―WAP may stumble over the Gateway‖ http://webhotel.ruc.dk/ncjuul/papers/wap.pdf.

[6] Pietro, Robert D., and Luigi V. Mancini, ―Security and Privacy Issues of Handheld and Wearable Devices‖, Communication of the ACM, September 2003, Vol. 46(9), 75-79.

[7] "PKI Moves Forward Across the Globe", Wireless Developer Network, <http://www.wirelessdevnet.com/channels/wap/features/m commerce3.html>

[8] Vainio, J.T. (2000), ―Bluetooth Security", <http://www.niksula.cs.hut.fi/~jiitv/bluesec.html>

[9] Vanstone, S.A. (2003), ―Next-generation security for wireless: elliptic curve cryptography‖, pp 412- 415,

http://www.compseconline.com/hottopics/hottopic20_8/ Next.pdf

[10] Tellez J. & Sierra J, "Anonymous Payment in a Client-Centric Model for Digital Ecosystem", IEEE DEST, 2007, pp. 422 - 427.

[11] Weimerskirch, A., Parr C., and Shantz, S.C., (2001), Proc. of the 6 Australian Conf. on Information Security and Privacy, July 11 -13, Sidney.

[12] Woodbury, A.D., Bailey, D.V., and Paar, C. (2000 ), ―Elliptic Curve Cryptography

[13] Smart Card without Coprocessors‖, Proc. of the 4 Smart Card Research and Advanced Applications Conf., September 20-22, pp.1-20.

[14] "Visualization for Data Analytics and Data Science", International Journal of

Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162,

Vol.5, Issue 3, page no.586 -594,

March-2018, Available :http://www.jetir.org/papers/JETIR1803362.pdf

[15] I. Ahmad and K. Pothuganti, "Smart Field Monitoring using ToxTrac: A Cyber-Physical System Approach in Agriculture," 2020 International Conference on Smart Electronics and Communication (ICOSEC), 2020, pp. 723-727, doi: 10.1109/ICOSEC49089.2020.9215282.

[16] R Alugubelli, "DATA MINING AND ANALYTICS FRAMEWORK FOR HEALTHCARE", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.534-546, February 2018, Available at

:http://www.ijcrt.org/papers/IJCRT1134096.pdf

[17] Bellare, M., Garay, J., Hauser, R., Herzberg, A., St einer, M., Tsudik, G., Van Herreweghe, E., and Waidner, M, "Design, Implementation, and Deployment of the iKP Secure Electronic Payment System", IEEE Journal of Selected Areas in Communications, 2000, pp. 611 -627.

[18] C. Wang & H-f. Leung, ―A Private and Efficient Mobile Payment Protocol‖, London: Springer-Verlag, LNAI, 2005, pp.1030- 1035. http://www.setco.org/set_specifications.html

[19] Jun Liu, Jianxin Liao, Xiaomin Zhu, ―A System Model and protocol for Mobile Payment‖, Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'05), 2005

[20] Krueger, M, The future of M-Payments–business options and policy issues, Seville. Spain, 2001.

[21] Kungpisdan, S., Srinivasan, B., and Phu Dung, L, ―Lightweight Mobile Credit-Card Payment Protocol‖, Berlin Heidelberg: Springer –Verlag, 2003a, pp. 295-308

[22] Kungpisdan S., Srinivasan B., and Phu Dung Le, ―A Secure Account-based Mobile Payment Protocol‖, Proceedings of the International Conference on Information Technology: Coding and Computing, Vol. 1, Las Vegas, USA, 2004a, pp. 35-39