# An Improved Framework of the Internet Open Trading Protocol in E-Commerce Security System

Gulfishan Firdose Ahmed
Assistant Professor
MANIT, Bhopal (M.P) INDIA

Raju Barskar
Student of M Tech (CSE)
MANIT, Bhopal (M.P) INDIA

## ABSTRACT
The Internet Open Trading Protocol (IOTP) is an electronic commerce protocol being developed by the Internet Engineering Task Force. IOTP aims at providing an interoperable framework for electronic commerce (e-commerce) over the Internet. IOTP is expected to evolve into one of the central building blocks for the developing of next generation e-commerce on the Internet. The success of electronic commerce depends upon effective electronic payment systems. There are many security mechanisms specific to different payment systems. Each payment system defines its own messages and has its own security requirements. Yet one of the major concerns in the internet is interoperability. One way to achieve this is to define a higher level of abstraction, that is, a common electronic payment framework specifying a set of protocols that can be used with any payment system. we introduce a rights insertion, rights verification and rights transfer phase for IOTP. Although many payment systems already implement their own security mechanisms, there still may be a need for additional security mechanisms at the framework level. Finally a number of solutions have been proposed based on the problem and discussed on the prospect of electronic payment system. This is the philosophy of a payment framework proposal, IOTP, described in this paper. It would help to increase the efficiency of electronic payment systems.

## Keywords
Internet Open Trading Protocol, payment handler, Electronic payment framework, security issues.

## 1. INTRODUCTION
The need for electronic payment technologies is to respond to fundamental changes in socio-economic trends. The payment system is the infrastructure which comprised of institutions, instruments, rules, procedures, standards, and technical, established to affect the transfer of monetary value between all the parties. An efficient payment system reduces the cost of exchanging goods and services, and is indispensable to the functioning of the inter-bank, money, and capital markets. The internet open trading protocol (IOTP [1]) is an electronic payment framework for internet commerce whose purpose is to ensure interoperability among different payment system. As of the time of this writing (April 2000,) it is still under development ([1] is an internet draft, i.e., a working document that expires after six months). The IETF working ground that is responsible has the same name (IOTP WG) and belongs to the IETF applications area. The Internet Open Trading Protocol

(IOTP) was developed within the Internet Engineering Task Force (IETF3) consortium, and it provides a standard framework for payment operations for Internet commerce. It is independent of any specific payment system. IOTP provides the data structures and communication protocols for payment transactions: purchase, refund, authentication, deposit, and other protocols that occur in electronic commerce (Burdett, 1999).An IOTP participant can perform one or several trading roles: consumer, merchant, payment handler, delivery handler, merchant, customer care provider. For example, a merchant can be a merchant customer care provider at the same time. The protocol describes the content, format and sequences of e-commerce messages that pass among the participants [12].

IOTP defines rigid roles for commerce actors including Consumer, Merchant, Payment Handler and Delivery Handler, and supports only two-party transactions. IOTP illustrates the current design ethic in electronic markets. IOTP is payment system-independent. That means that any electronic payment system (e.g., SET, DigiCash) can be used within the framework. Each payment system defines certain specific message flows. The underlying payment system-specific parts of the protocol are contained in a set of payment scheme supplements of the IOTP specification. IOTP message are well-format XML (Extensible Markup Language [2] document. A predefined set of IOTP message defines a trading exchange (e.g., offer, payment, delivery, and authentication). IOTP transactions are built of one or more trading exchange. Transactions can be of different types, such as purchase, refund, or authentication. The Internet Open Trading Protocol (IOTP) is defined as an interoperable framework for Internet commerce. It is optimized for the case where the buyer and the merchant do not have a prior acquaintance. IOTP is payment system independent. It can encapsulate and support payment systems such as SET, Mondex, secure channel card payment, Geldkarte etc.

Fig.1. shows the general structure of an IOTP message. It consists of several blocks. Each message has a transaction reference block (Trans Ref Block) that identifies an IOTP transaction. A transaction (e.g., purchases, authentication, withdrawal, deposit) has globally unique transaction identifier (Trans ID). It includes one or more message from a predefined set, and all messages belonging to the same transaction have the same Trans ID. Additionally, each message has its own identifier (Msg ID) that is unique within the transaction. A message contains one or more trading blocks, for example, authentication request/response. Optionally, it can contain a signature block (also a trading block). A signature block carrier digital signatures of trading blocks or trading components and, optionally, the certificates of the public keys for signature verification. Finally, a trading block consists of a set of predefined trading components

(e.g., authentication request/response, payment scheme, payment receipt.

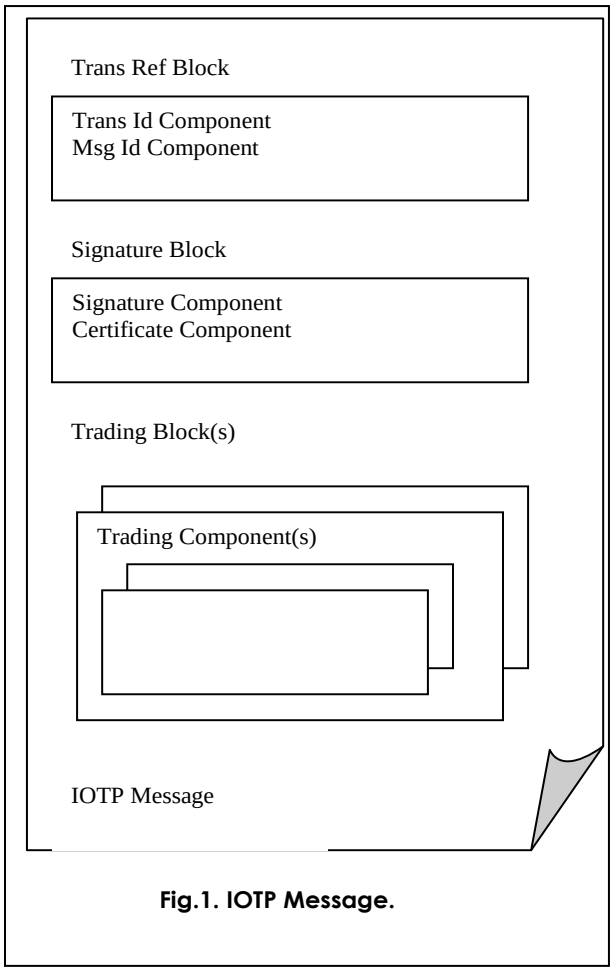


**Fig.1. IOTP Message.**

## 2. SECURITY ISSUE

Security is the main concern of any new technology. Since the present century is the century of information and data, every technology which is working with, they are in exposure of data theft, stealing, and fraud. Three basic building blocks of security mechanisms are used:

**2.1 Encryption**: provides confidentiality, authentication and integrity. Digital signatures: provide authentication, integrity protection and non-repudiation.

**2.2 Checksums/hash algorithms**: provide integrity and can authentication. It Most payment system that can be used within the IOTP framework already has their own security concepts. Nevertheless, there are some security issues that are covered by IOTP to provide optional additional protection. If it is necessary to consider payment security from an IOTP perspective, this should be included in the payment protocol supplement that describes how IOTP supports that payment protocol. IOTP participants can authenticate each other through an authentication exchange. Authentication can be performed at any point in the protocol. It simply suspends the current IOTP transaction. For example, a consumer may want to authenticate the payment handler after receiving an offer response from the merchant and before sending the payment request to the payment handler (see also the next section). The authentication protocol is outside the scope of IOTP. If the authentication transaction is successful, the original IOTP transaction is resumed; otherwise it is canceled. The authentication transaction can be linked to the original IOTP transaction by means of a related to component containing the IOTP transaction identifier (Trans ID) [3, 4].

Data integrity and non repudiation of origin can be achieved by means of digital signatures. For example, a payment handler may want to provide a non repudiation proof of the completion status of a payment. If a payment response is signed, then the consumer can later use the record of the payment to prove that it occurred. In addition, it is possible to use digital signatures to bind together the records contained in a response message of each trading exchange in a transaction. For example, IOTP can bind together an offer and a payment, as is shown in the example below. A signature component consists of the following elements:

- Digest Elements containing digests of one or more trading blocks or trading components in one or more IOTP messages (from the same IOTP transaction);
- Manifest Element including the originator, the recipients, the signature algorithm, all concatenated with the Digest elements;
- Value representing the signature of the Manifest Element.

Optionally, the originator's certificate can be included in the certificate various Trading Roles using a secure channel, such as SSL or TLS. Use of a secure channel within IOTP is optional.

## 3. AN EXAMPLE WITH DIGITAL SIGNATURE

Issuers can make use of all the fraud prevention mechanism available in the market, such as public key crypto-systems and digital signatures. During payment, at least one digital signatures must be created to verify the process. Digital signatures can be used both to assure integrity of the data and the identity of the originator. On the other hand, privacy can be assured by avoiding from revealing any of the identification of a consumer in the payment mechanism. A simple IOTP purchase transaction (Fig.2) consists of an offer exchange and a payment exchange. In the offer exchange a consumer selects the items he wants to purchase from, say, a merchant's Web page. The consumer fills out a Web form and sends it to the merchant. The part is the scope of IOTP. The merchant can now send a list of payment instruments he accepts in the form of a trading protocol options (TPO) block containing a brand list component. The consumer selects a payment brand (e.g., Visa), a payment protocol (e.g., SET), a Currency (e.g., USD), and an amount from the brand list component. He sends his choice to the merchant in a TPO Selection block containing a brand selection component.
In this case the integrity of brand selection component is not guaranteed. Their modification can only cause denial of service if the underlying payment protocol is secure against message modification, duplication, and swapping attacks [5, 6].

On the basis of the information in the web from and the selection payment options, the merchant creates an offer, signs it, and sends it to the consumer. In other word, the merchant creates an IOTP message containing.

- A trans Ref Block with a new trans ID;

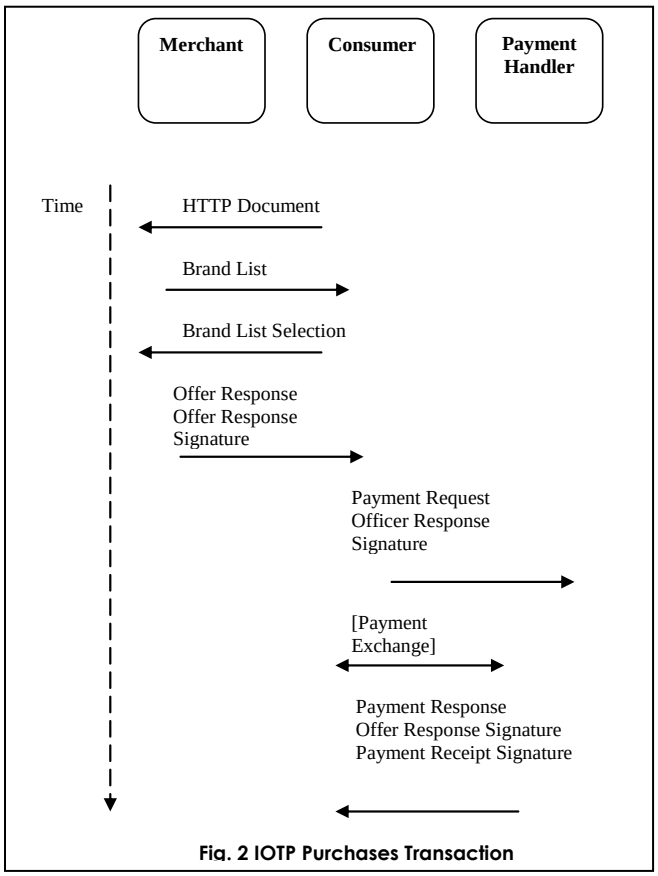


**Fig. 2 IOTP Purchases Transaction**

- An offer response trading block consisting of the trading components describing the offer (e.g., consumer, merchant, payment handler, order, payment).

A signature blocks containing an offer response signature component and the merchant's certificate in a certificate component**.** The Internet Open Trading Protocol (IOTP) is not a separate payment system [11, 15]. Indeed, it is a common electronic payment framework in attempt to ensure interoperability among different payment systems.

The payment component includes a reference to the brand list component. The consumer can now check the information form the merchant and decide whether he wishes to continue with the trade. If he does, he creates a payment request to be sent to the payment handler. A customer and a merchant should register with the payment service provider to participate in the electronic payment system. The payment gateway, run by the payment service provider, connects the public network to inter-bank clearing network, so that the customer is associated with its bank (referred to as issuer bank) and the merchant is associated with its bank (referred to as acquirer bank).

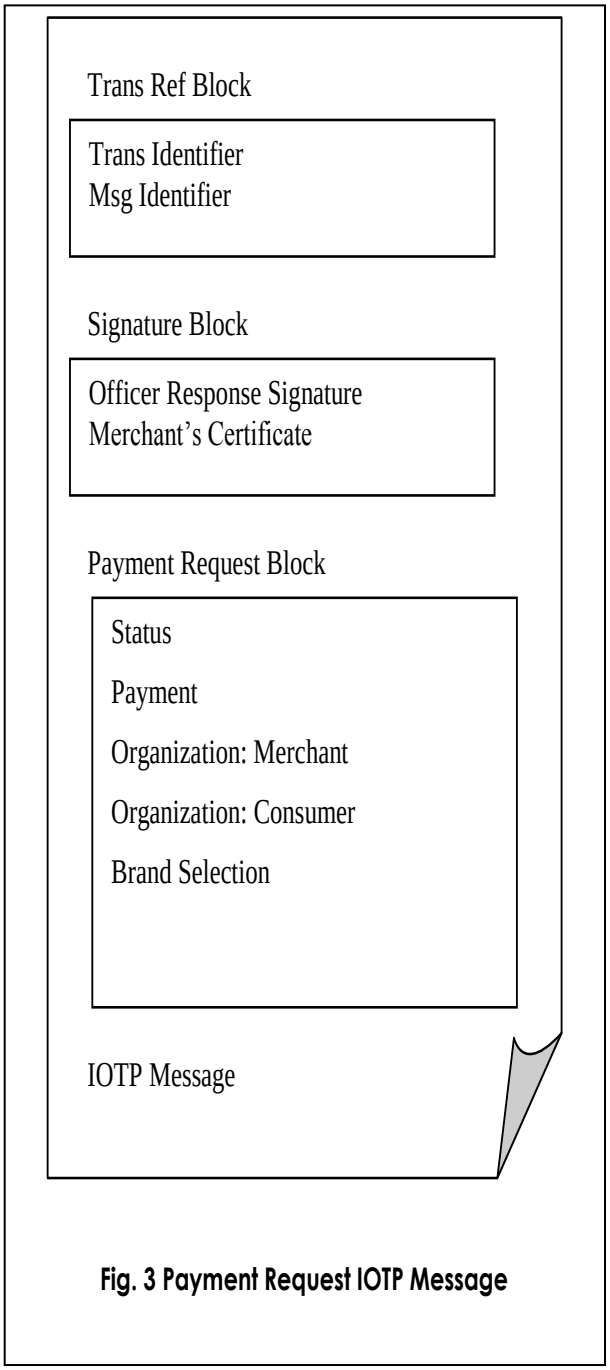


**Fig. 3 Payment Request IOTP Message**

Fig. 3 shows an example of an IOTP message carrying a payment request trading block. It contains the following trading components:

- Status: status information about the success or failure of the trade, copied from the offer response block;
- Payment: also copied from the offer response block;
- Organization: the merchant's identifying information, copied from the TPO blocks;
- Organization: the consumer's identifying information, copied from the TPO block;
- Brand Selection: copied from the TPO selection block (defines payment brand, payment protocol, currency, and amount).

The offer response signature previously generated by the merchant is copied to the signature block. This signature

serves as proof to the payment handler that the merchant agrees with the payment [7, 8, 9].

After the payment request message, one or more payment exchange message can be exchanged between the consumer and the payment handler. This type of message serves to carry the underlying payment-protocol-specific data (e.g., SET). Finally, if everything has gone well, the payment handler sends a payment response message containing a payment response block and a signature block to the consumer. The payment response block contains a payment receipt components, which includes a reference to the payment component form the previous message [10]. Optionally, it may contain an underlying payment-system-specific payment receipt. The signature component can optionally contain the offer response signature and a payment receipt signature. The payment receipt signature includes the digest elements of the following components:

- The Trans ID component of this IOTP message;
- The Trans Ref Block of this IOTP message;
- The Offer Response Signature Component;
- The Payment Receipt Component;
- The Status Component;
- The Brand Selection Component.

# 4. CONCLUSION

E-commerce is undergoing huge growth in terms of the volume of goods and services that are being traded on-line. The growth of e-commerce is dependent, among other factors, on the existence of Secure, user-friendly and cost-effective payment system. Handling payment is a costly process that has been a central part of bank business for the past century. However, it is now being transformed by technology developments, and in particular, the internet. The importance of the payment function lies in the fact that it could encourage convergence between sectors with disparate objectives, since payment systems are the common denominator of all e-commerce transaction. Conceptually, the alternative means of payment available for e-commerce may be classified as either electronic money (e-money), or electronic access products. E-payment systems are becoming central to e-commerce as companies look for ways to serve customers faster and at lower cost. Emerging innovations in the payment for goods and services in electronic commerce promise to offer a wide range of new business opportunities. The current state of online electronic payment is in many ways reminiscent of the medieval ages. The transaction of e-commerce through the payment protocol required a framework to exist the actual payment transaction via internet open trading protocol now this paper we discussed the open trading protocol of internet using security in payment transaction. One of the main reasons is that the virtual environment is a place where the principles of good faith and practice as well as those of trust are not well established making thus consumers reluctant in using electronic payment mechanisms. The current legal framework applicable to electronic payment provides only to an extent protection to consumers. A new framework for digital rights management in the context of the Internet Open Trading Protocol (IOTP) for electronic commerce applications and services was developed. In this framework we used fingerprinting as a tool for content based identification that characterizes the digital content based on its representation such as feature or signals and matches the result to an entry in a database. This paper analysis the problems faced by the customers and offers suggestions for improving the payment systems.

# 5. REFERENCES

[1] ITU-T Recommendation X.200, Information Technology - Open Systems Interaction - Basic Reference Model, July 1994.

[2] World Wide Web Consortium XML Working Group "Extensible Markup Language (XML) 1.0," W3C Recommendation, Feb. 1998,

[3] W3C, http://www.w3.org/TR/REC-xml.

[4] Ouyang, C., Kristensen L. M., and Billington, J. An improved architectural specification of Internet Open Trading Protocol. In Proceedings of 3rd Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools, 119--137. DAIMI PB-554, University of Aarhus, ISSN 0105-8517, 2001.

[5] Raju barskar and Gulfishan Firdose Ahmed *"E-Commerce Payment System Security in Banking Technology: A Review*" In proceeding of International Conference on Next Generation Communication and Computing System (ICNGC2S-10), ISBN: 978-93-81068-00-7, pp-276-279, December-2010, Chandigarh, India.

[6] Papa, M., Bremer, O., Hale, J., and Shenoi, S. Formal analysis of e-commerce protocols. IEICE Transactions on Information and Systems, E84-D(10): 1313--1323, 2001.

[7] D. Burdett. Internet Open Trading Protocol - IOTP. RFC 2801. IETF Trade Working Group, April 2000.

[8] Davidson, K., and Y.Kawatsura, "Digital Signatures fro the v 1.0 IOTP, Internet Engineering Task Force, Internet Draft <draft-ietf-trade-iotp-v1.0-protocol-05.txt>, Nov, 1999.

[9] S.H. Kwok, K.C. Wong, K.F. Tsang, S.C. Cheung, K.Y. Tam, Digital rights management in Internet open trading protocol (IOTP), Proceedings of the International Conference on Electronic Commerce (ICEC 2000), August 2000, pp. 179– 185.

[10] Abhijit Chaudhury, Jean-Pierre Kuilboer (2003): e-Business and e-commerce Infrastructure: Technologies Supporting the e-Business Initiative, McGraw-Hill Irwin, First Edition.

[11] Sandholm, T. and Lesser, V. *Issues in Automated Negotiation and Electronic Commerce:Extending the Contract Net Framework*, First International Conference on Multiagent Systems (ICMAS95). 1995. San Francisco: AAAI Press and MIT Press. pp. 328-335.

[12] Ghosh, A., K., (1998) 'E-Commerce Security: Weak Links, Best Defences', John Wiley &Sons, Inc.

[13] Kwok, S.H., S.C. Cheung, K.C. Wong, K.F. Tsang, S.M. Lui and K.Y. Tam, 2002. Integration of digital rights management into the Internet Open Trading Protocol. Decision Support Systems, 34: pp.413-425.

[14] Internet Open Trading Protocol-IOTP Version 1.0,http://www.ietf.org/internet-drafts/draft-ietf-tradeiotp-v1.0-protocol-07.txt.

[15] Vesna Hassler: Security Fundamentals for E-commerce, Artech House, 2001.