Enhanced the Security of Electronic-Commerce (E-Commerce)

Noura H.Ajam
University of Babylon-Business Administration Collage
nhzijam@yahoo.com

Abstract-

Electronic-commerce (e-commerce) is a very active field of Internet research. A very important aspect of E-commerce is its security. Because of the variety of e-commerce applications, many security policies, protocols and techniques are involved in the deployment of the security. Applications of the E-commerce are demonstrated here. This paper presents a suggested approach to enhance security in e-commerce. The new approach uses two algorithms which is blowfish and MD5. Combining these two algorithms provides high quality encryption, and makes it stronger against any kind of intruding.

KeyWords: Electronic-commerce(E-commerce), security, Blowfish, MD5, hybrid.

الخلاصة

التجارة الإلكترونية (التجارة الإلكترونية) هو احد المجالات الهامة من بحوث الانترنت. وهناك جانب مهم جدا من التجارة الإلكترونية هو أمنها. بسبب مجموعة متنوعة من تطبيقات التجارة الإلكترونية، تشارك العديد من السياسات الأمنية والبروتوكولات والتقنيات في تطوير الأمن والحماية لهذه التطبيقات. البعض من تطبيقات التجارة الالكترونية موضحة في هذه الدراسة. يعرض البحث طريقة مقترحة لتعزيز الأمن في مجال التجارة الإلكترونية. تستخدم الطريقة الجديدة اثنين من الخوارزميات التي هي Blowfish– و MD5. الجمع بين هذه الخوارزميات يوفر جودة عالية من التشفير، ويجعلها أقوى ضد أي نوع من التطفل.

1- Introduction

Electronic commerce (E-commerce) is buying and selling of goods and services across the internet (Nada Al-Slamy, 2008). The main advantages of these new trading methods are its rapidity and the two teams of the trading process can make the contract easily and in short given period of time.(Ashraf Abdel-Kraim Abu-Ein *et al.*, 2012) .As business transaction move to electronic marketplace, most interactions will occur between strangers, due to billions of internet users and the fact that most of them do not share a common security domain. In order to conduct secure transaction, a sufficient level of mutual trust must be established. E-commerce successes largely depend on gaining and maintain the trust and confidence of visitors. There have been several different technologies to deal with security in e-commerce. Encryption algorithms are the most effective security technology today (Gurjeevan Singh *et al.*, 2012). Many research papers have been discussed e-commerce security, and presented threats to e-commerce. These threats come from an actual attacker (obtaining credit card, bank account information; user name and password) or technological failure (poorly written program code or network not configured properly).

These threats or vulnerabilities make e- commerce insecure and nontrusted by people or organizations so as result, a robust and efficient security method are required. In this paper we have been used a hybrid of encryption technology which are blowfish and MD5 algorithms because these two algorithms have not been cracked yet.

2- E-commerce Applications:

Various applications of e-commerce are continually affecting trends and prospects for business over the Internet including:

- E-banking.
- E-shopping and order tracking.
- Shopping cart software.
- E-tickets.
- Domestic and international payment system.
- Online publishing/online retailing.
- E-tailing.

3- Security and E-commerce

In the cyberspace, both the client and the vendor experience issues in demonstrating their personality to one another with certainty, especially during a first transaction. How does the buyer safely transmit sensitive information to the seller? How does the seller realize that this is a legitimate purchase request? How do both parties realize that an evil third party has not duplicated and/or changed the transaction information? These questions and others, describe the issue effecting commercial transactions over the internet, or any public network.

Public Key Infrastructure (PKI) refers to the notion that the most ideal approach to create a system of secure interchanges over networks is to make an infrastructure that will help public key encryption. The PKI would make an environment where any Internet client could "carry" certificates around that distinguish them in a variety of ways. Authentication of parties could get to be very cheap and simple. Some e-commerce proponents recommend that creation of a consistent and powerful PKI would have enormous implication for speeding the development of ecommerce.

E-commerce software packages should also work with secure electronic transfer (SET) or secure socket layer (SSL) technologies for encryption of data transmissions.SSL protocols, which took into consideration the transmission of encrypted data over the Internet by running over the traditional TCP/IP protocols.

It is clear that e-commerce will revolutionize businesses, and customers will be offered new and exciting services. As E-commerce businesses are growing, more secure technologies are being developed and improved every day. The current internet security policies and technologies fail to meet the needs of end user. The success or failure of E-commerce operations hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product and the security of data transmissions and storage. Any business that wants to have a competitive edge in today's global marketplace should adopt a comprehensive security policy in consultation with partners, suppliers, and distributors that will provide safe environment for the coming proliferation of E-commerce. (Nada Al-Slamy, 2008).

Customer (clients) need to be sure that:-

1- They are communicating with the correct server.
2- What they send is delivered unmodified.
3- They can prove that they sent the message.
4- Only the intended receiver can read the message.
5- Delivering is guaranteed.

On the other side, vendors (severer) need to be sure that:-

1- They are communicating with the right client
2- The content of the received message is correct.
3- The identity of the author is unmistakable.
4- Only the author could have written the message.
5- They acknowledge receipt of the message.

All of the concerns listed above can be resolved using some combination of cryptographic method, and certificates methods. (William Stallings, 2003; Ashraf Abdel Karim Abu-Ein *et al.*, 2012).

The types of risks involved are shown in fig3, as results from inadequate security system are:

1- Bugs or miss-configuration problems in the web server that can cause the theft of confidential documents.
2- Risks on the Browsers' side i.e. breach of user's privacy, damage of user's system, crash the browser etc.
3- Interception of data sent from browser to sever or vice versa.

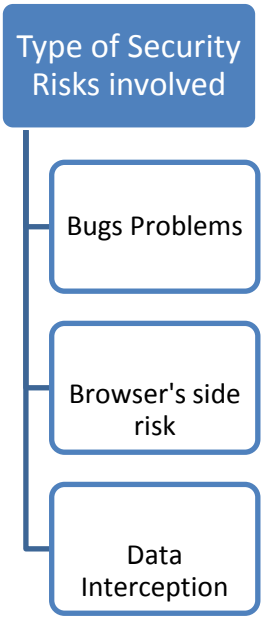

Fig3: Type of Security Risks

4- E-commerce security issues:

Any system has to meet some requirement:

1- **Confidentiality**: This requirement prevents unauthorized disclosure of information. It can be done by means of symmetric encryption algorithms such as DES, AES, and blowfish.

2- **Integrity**: This requirement ensures that information is protected from unauthorized alterations, unintentional modifications, or change. Message Authentication Code is used to do this.
3- **Availability**: This requirement ensures that information and critical services are available when need to meet business requirements. It requires many security techniques and involves several aspects of information security, For example, the intrusion detection and prevention, disaster recovery, and so on.
4- **Non-repudiation**: This requirement assures that a specific action occurred. It comprises of non-repudiation of origin, non-repudiation of submission, non-repudiation of receipt, and non-repudiation of delivery. Digital signature is an approach to guarantee this
5- **Fairness**: This requirement ensures that situations like payment without delivery, or delivery without payment, do not happen. Fairness is tightly related to non-repudiation.(QIN Zhiguang et al., 2004).

5- Material and methods:

Some e-commerce software like Avactis shopping cart,CS Cart, and Xcart use blowfish algorithm to encrypt credit card, cardholder information, payment data or password (Bruce Schneier website). Since blowfish is now considered to be insecure for many applications, so it becomes very important to augment this algorithm by adding new levels of security to make it applicable and can be depending on any common communication channel.(Afaf M.Ali Al-Neaimi et al.,2011) In this paper we have used a combination of two algorithms which are blowfish and MD5 to give more complex and make it stronger against any kind of intruding. The remainder of this paper is organized as follows: section 5.1 gives an overview of Blowfish algorithm. Section 5.2 gives an overview of MD5 algorithm. Section 5.3 describes the design and implementation of the new approach (MD5-blowfish algorithm). Finally, our conclusion are described in section 6.

5.1- Blowfish algorithm:

Blowfish is a Symmetric block cipher that can be used as a replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms (Bruce Schneier, 1994). Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two Parts: a key- expansion part and a data- encryption part.

- Key- expansion converts a key of at most 448 bits into several arrays totaling 4168 bytes.
- Data encryption occurs via a 16 –round Feistel network. Each round consists of a key dependent Permutation, and a data –dependent substitution. All operations are XORs and additions on 32 bit words.

Diagram shown in Figure (1) shows the action of Blowfish. Where Blowfish has 16 rounds, the input is a 64 –bit data element, divided into two 32 bit halves: XL, XR.

Then, for i = 1 to 16:
XL = XL XOR Pi
XR = F (XL) XOR XR
Swap XL and XR

After the sixteenth round, swap XL and XR again to undo the last swap.
Then, XR = XR XOR P17 and XL = XL XOR P18.
Finally, recombine XL and XR to get the cipher text (Bruce Schneier, 1994).
F-function splits the 32 bit input into four eight-bit quarters, and uses the quarters as input to the s-boxes. The outputs are added modulo 32 and XORed to produce the final 32-bit output. Since Blowfish is a Feistel network, it can be inverted simply by XORing P17 and P18 to the cipher text block, then using the P-entries in reverse order.
The advantages of the algorithm are fast, high efficiency. It is widely used in encryption of large amount of data. The disadvantage is that the key is easily intercepted when it is transmitted on the network. That will pose a threat to information security. Therefore the security of key transmission needs to be granted.

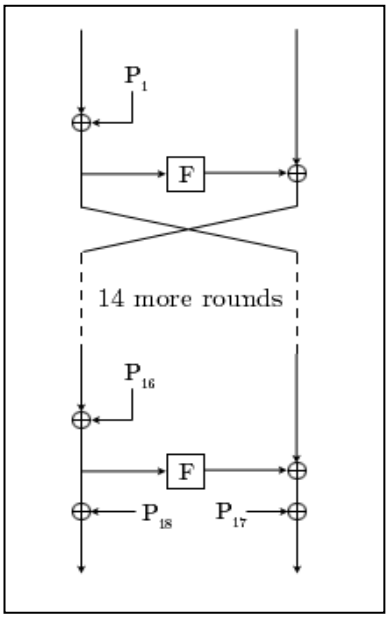

Figure (1). The diagram of Blowfish each round action

5.2-MD5 algorithm:

MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. MD5 has been employed in a wide variety of security applications. MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit little endian integers); the message is padded so that its length is divisible by 512. MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D. These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation (Rivest, 1992).

The disadvantage of the algorithm is collision attack. Which could be hash(M1) = hash(M2).

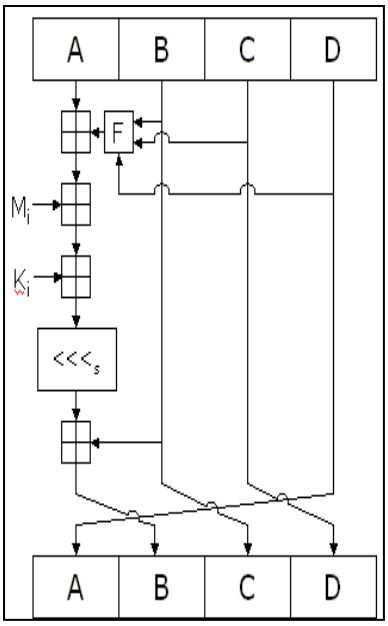

Fig2: The diagram of Elementary MD5 Operation (single step)

5.3-Design hybrid MD5-blowfish algorithm:

In this section we discuses our proposed approach, merging and modifying from MD5 and Blowfish encryption schemes, which can enhance security in e-commerce. The hybrid MD5-blowfish algorithm is developed to overcome the weakness from symmetric block cryptography and hash function schemes as explained above. The process of which is described in fig 4. This algorithm consists of three modules: an initial key –encryption module, an MD5 key expansion module, a blowfish data- encryption module. The initial key is passed into the MD5 key-encryption module and then key expansion module to get the updated encrypted key for the blowfish message –encryption module. (Zhu Wang et.al., 2011).

5.3.1 –Hybrid Encryption Algorithm and Modules:

- **MD5 key Encryption Module**

The key selected by the user for the whole system is transferred to MD5 key encryption module so that the initial key is encrypted by MD5. The input user (private) key may have any length, but the output is fixed with 128 bits long. The reason is that MD5 has no requirement on the input plaintext size, whereas most encryption algorithm such as AES and DES require that the key size be multiple of block size. So it is more convenient for users to select keys.

- **Key expansion Module**

The encrypted key K´ produced by MD5 key encryption module is passed to the key expansion module for further complexity. In this module, the encrypted key H (k) is appended to the user key K. If the total length is no more than 448 Bytes, K || H(K) will be sent to blowfish message encryption module. Otherwise, only the first 448 bytes will be sent over to ensure correct operations. In addition, it also complicates the whole encryption process for further complexity, i.e., security.

- **Blowfish Message Encryption Module**

The algorithm is exactly the same as the Blowfish algorithm except that the key is replaced by the encrypted key from the Key Expansion Module.

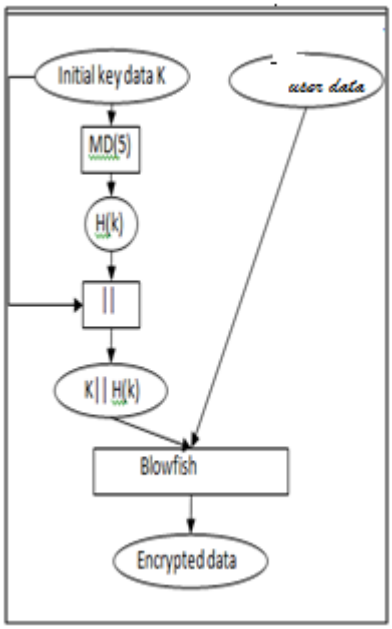

Fig4.The diagram of hybrid MD5-blowfish algorithm

5.3.2-Application of Hybrid MD5-Blowfish Encryption in E-commerce:

For security issues existing in e-commerce website, hybrid encryption technology is used to improve. From fig 4. We can see that the user will enter his information (password) encrypted by blowfish algorithm, in addition to the selected key by user encrypted by MD5 hash function. In this way, we make the registration more complex, this make the user's transaction over net become safe.

6- Conclusion

In conclusion the e-commerce industry faces a challenging future in terms of the security risks it must avert. With increasing technical knowledge, and its widespread availability on the internet, criminals are becoming more and more sophisticated in the deceptions and attacks they can perform. By using hybrid encryption technology, it can provide more reliable and efficient security for e-commerce systems. In this paper we used Hybrid MD5-Blowfish algorithm to enhance the security and improve the encryption performance over existing MD5 and Blowfish algorithm by merging them. The mixture strategy helps increase the algorithm complexity but no cost for implementation.

7- References

Afaf M.Ali Al-Neaimi, Rehab F.Hassan, (2011), New Approach for Modifying Blowfish Algorithm Using 4-States keys,IJCSNS,Vol. 19,pp. 22-25.

Ashraf Abdel Karim Abu-Ein,Hazem Hatamleh,Ahmed A.M.Sharadqeh,Asad Mahmou (2012), E-commerce: Security and Applications, AJAS, ISSN 1546-9239,PP.1868

Bruce Schneier,(1994) , Applied Cryptography, John Wiley@Sons, NewYork.

Bruce Schneier, (1994), Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993) Springer-Verlag, pp.191- 204

Gurjeevan Singh, Ashwani Kumar, K. S. Sandha ,(2012),A Study of New Trends in Blowfish Algorithms, International Journal of Engineering Research and Applications (IJERA), Vol.1, pp.321

Nada M. A. Al-Slamy, (2008), E-commerce Security, IJCSNS, Vol. 8, pp. 340-341.

QIN Zhiguang, LUO Xucheng, GAO Rong, (2004), A survey of e-commerce security, Journal of Electronic Science and Technology of China, Vol.2, p.p. 174.

Rivest, R., (1992), The MD5 Message- Digest Algorithm.

William Stallings, (2003), Cryptography and Network Security, Prentice Hall, 3rd edition.

Zhu Wang, Josh Graharm, Noura Ajam and Hai Jiang,(2011), Design and Optimization of Hybrid MD5-Blowfish Encryption on GPUs, International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA),

Zhenlong Li, Wenping Guo ,Xiaoming Zhao,(2009), Study on the application layer security in E-Commerce websites, WISA'09, ISBN 978-952-5726-00-8,p.p. 120-123.