ISSN 2347 - 3983

Volume 8. No. 5, May 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter12852020.pdf

https://doi.org/10.30534/ijeter/2020/12852020

Implementation of E-Commerce Security Methods and Tools

Saparova Gauhar Ajiniyazovna[1],Tashmatova Shakhnoza Sabirovna[2], Qurbonova Kabira Erkinovna[3], Elmurodov Temurmalik Dilshod ugli[4]

[1]Tashkent University of Information Technologies of Nukus branch named after Muhammad al-Khwarizmi, Uzbekistan,Karakalpakstan, gasaparova@mail.ru

[2]Tashkent State Technical University named after Islam Karimov, Uzbekistan, shaxnoza.tashmatova@tdtu.uz

[3]Tashkent State Technical University named after Islam Karimov, Uzbekistan, kabira.qurbonova@tdtu.uz

[4]Tashkent State Technical University named after Islam Karimov, Uzbekistan, temurmalikelmuradov@yandex.ru

ABSTARCT

In this paper a data protection method that allows to increase the secrecy of the transfer of confidential information during electronic trading operations via the Internet and the mechanism of ensuring e-commerce security to meet the requirements of business applications related to e-commerce and the secrecy of the signed messages through the use of a hash chameleon are proposed. As well a scheme of integrated e-commerce environment and a method for assessing the security of information resources in integrated e-commerce systems are built up.

Key words:SSL/TLS protocols**,** ICMP packets, Pareto distribution, Chameleon hash, CHAM-SIG,CHAM-VER.

1. INTRODUCTION

Effective development of the modern information society is impossible without the widespread use of information technology. Currently, the basis of systems that ensure the security and defense of the country are computer and telecommunication systems. They implement modern information technology, providing the processing, transmission and storage of large volumes of data. The massive use of computer technology can effectively solve the problem of automating the processing and storage of information. However, this raises a new problem related to ensuring information security of computer systems. Moreover, ensuring information security requires an integrated and systematic approach to its decision.

One of the most promising areas of information technology development is the wide penetration of e-commerce systems in almost all areas of the modern state. E-commerce is one of the most progressive areas of the economy, which, using information technology, is actively used in areas such as electronic payments, government services, procurement and auctions, electronic trading platforms, online stores and online banking.

2. IMPLEMENTATION OF A DATA PROTECTION METHOD IN ELECTRONIC TRADING

Currently, remote banking systems (RBS) for individuals have become an integral part of the services of any bank building a business with private clients. This is due to several factors. Firstly, with the development of high-speed payment services, which no longer require the client to visit a bank branch or office of the organization. Secondly, with the competition between banks and virtual money payment systems, which were the first to occupy a segment in the market for operations through mass service channels. Moreover, the problems of ensuring security and information protection are relevant for all channels of the RB. The basic mechanisms for protecting the services of RBS have been implemented for quite some time.

The most common methods of attacks on remote banking systems:

- malware (Trojans, botnet clients, etc.);
- phishing;
- the use of attacks such as Man-in-the-Middle for fraudulent transactions;
- internal attacks;
- targeted attacks on client sites.

Most often, when conducting a client-bank operation via the Internet, SSL/TLS protocols are used. These protocols enable server authentication and session encryption. They are used everywhere due to the fact that they are implemented in all modern browsers, and allow you to avoid a large number of fairly simple attacks [1]. At the same time, the protocols do not provide protection against compromising the browser or replacing certificates of root certification authorities in client places. To implement such attacks on SSL/TLS protocols, it is necessary to intercept traffic and analyze it, followed by a direct attack. In this case, the absence of one of the components leads to the failure of the attack as a whole.

There is a method of secretly transmitting information in the field of additional information of ICMP packets by blocks of secret text previously encrypted using cryptography methods. Another way to covertly transmit information over an IP network is to covertly transmit information by placing it in the "Identifier" field of the IP datagram header. The methods have a significant drawback **-** the blocks of secret information are directly contained in the packet fields and can be easily extracted, deleted or modified.The implementation of the method is explained as follows (Fig. 1):

form arrays for storing the bit sequence of the carrier message $\{C_i\}$, where $I = 1, 2, \ldots K$;
bit sequence of the information message $\{T_i\}$, where $j = 1, 2, \ldots N$;bit sequence of the marker message $\{\{F_i\}$, where $I = 1, 2, \ldots K$(Fig.1, block 1).

Next, the arrays $\{C\}$ and $\{T\}$ are filled with bit sequences (Fig. 1, blocks 2, 3). Install the counters in the initial state $I = 1$ and $j = 1$ (Fig. 1, block 4). The values C_i and $T_i$are sequentially read from the corresponding arrays and compared (Fig. 1, blocks 5, 6). If the bit values match, then the flag value is F_i. set to “unit” and increase the values of counters i and j per unit (Fig.1, blocks 7, 9, 10).

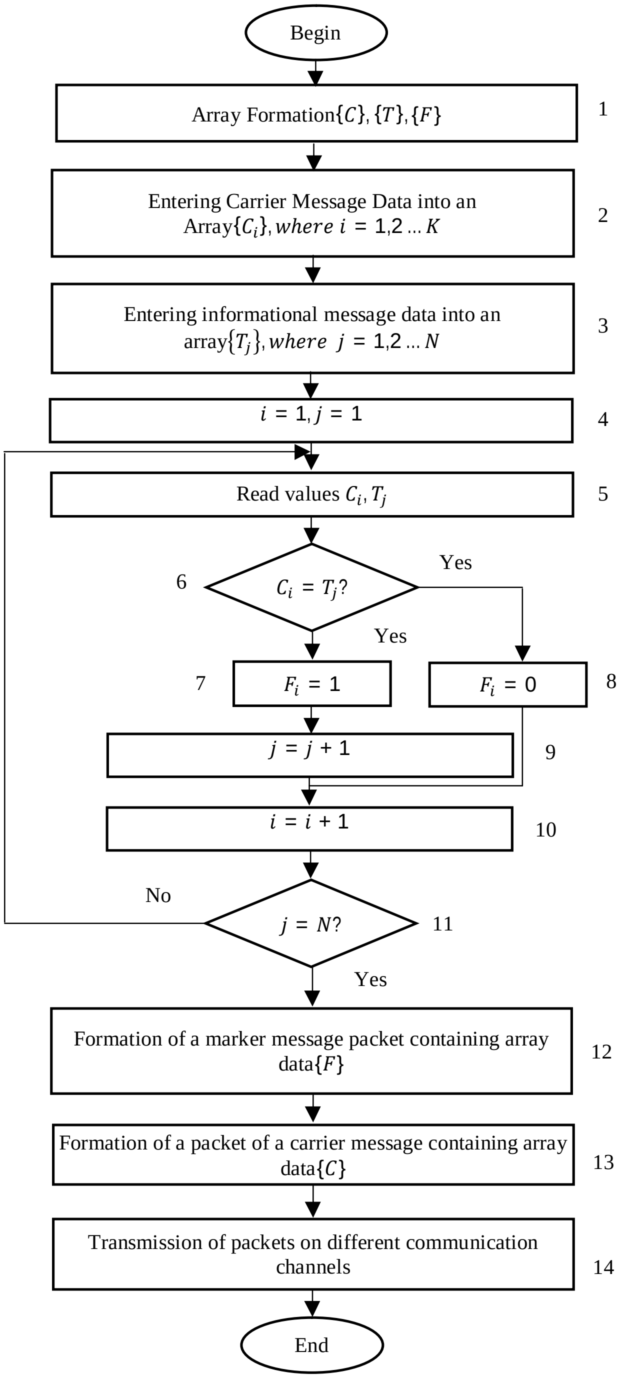
Begin
Array Formation$\{C\}, \{T\}, \{F\}$
1
Entering Carrier Message Data into an Array$\{C_i\}, where\ i = 1,2 \ldots K$
2
Entering informational message data into an array$\{T_j\}, where\ j = 1,2 \ldots N$
3
$i = 1, j = 1$
4
Read values C_i, T_j
5
6
$C_i = T_j?$
Yes
Yes
7
$F_i = 1$
$F_i = 0$
8
$j = j + 1$
9
$i = i + 1$
10
No
$j = N?$
11
Yes
Formation of a marker message packet containing array data$\{F\}$
12
Formation of a packet of a carrier message containing array data$\{C\}$
13
Transmission of packets on different communication channels
14
End

Figure 1: Flowchart of the method of protecting information in electronic trading

If the bit values do not match, then the flag value $F_i$is set to “zero” and only the value of counter i is increased by one (Fig.1, blocks 8, 10). After the entire bit sequence of the message is reflected in the bit sequence of the carrier message (Fig. 1, block 11), a marker message packet containing the data of the array $\{F\}$is formed (Fig. 1, block 12), for which, in the information field network layer packets sequentially write data from the array $\{F\}$.

Next, a packet containing a carrier message is formed (Fig. 1, block 13), for which purpose data from the $\{C\}$ array is sequentially written into the information field of the network layer packet. After that, packets are transmitted over different communication channels (Fig. 1, block 14).

Next, two bits of the information message are compared sequentially with two bits of the carrier message [2]. If the bits are not equal, then zero is written to the marker message sequence array $\{F\}$ and the next two bits of the carrier message are taken for comparison. If the bits are equal, then one is written to the array of marker message sequence $\{F\}$, and for comparison, the next two bits of the information message and the carrier message are taken. After all the bits of the message sequence have been matched with the flag value in the array $\{F\}$, they begin to form a packet of marker messages containing the data of the array.

The algorithm of the process of extracting an informational message from a carrier message using a marker message is shown in Fig.2 and is explained as follows.

Arrays are formed for storing the bit sequence of the carrier message $\{PC_i\}$, where $I = 1,2 \ldots K$, the bit sequence of the marker message $\{PF_i\}$, where $I = 1, 2, \ldots N$and the bit information message sequence $\{PT_j\}$, where $j = 1,2, \ldots N$ (Fig.2, block 1). Then, packets of a carrier message and a marker message are received from different communication channels (Fig.2, blocks 2, 4). The data of these packets are written into the corresponding arrays (Fig.3, blocks 3, 5), the counters are set to the initial state $I = 1$ and $j = 1$ (Fig.3, block 6), and the values PC_i are sequentially read from the corresponding arrays and PF_i (Fig.2, block 7). If the value of the flag PF_i is equal to unity (Fig.2, block 8), then the value of the bit sequence PC_i is written to the cell of the array PT_j (Fig.2, block 9) and the values of the counters i and j are increased j (Fig.1, blocks 10, 11). If the value of the flag PF_i is equal to zero, then only the value of counter i is increased by one (Fig.2, block 11). After all the flag values have been read (Fig.2, block 12), they decide to receive the message (Fig.2, block 13).

To conduct the simulation of the proposed method, it is necessary to determine the initial data and the mathematical apparatus of the model. The main source data will be:

- size of information messages L_{im};
- message carrier size L_{mc};
- probability density of information in informational messages;
- probability density of information in carrier messages.

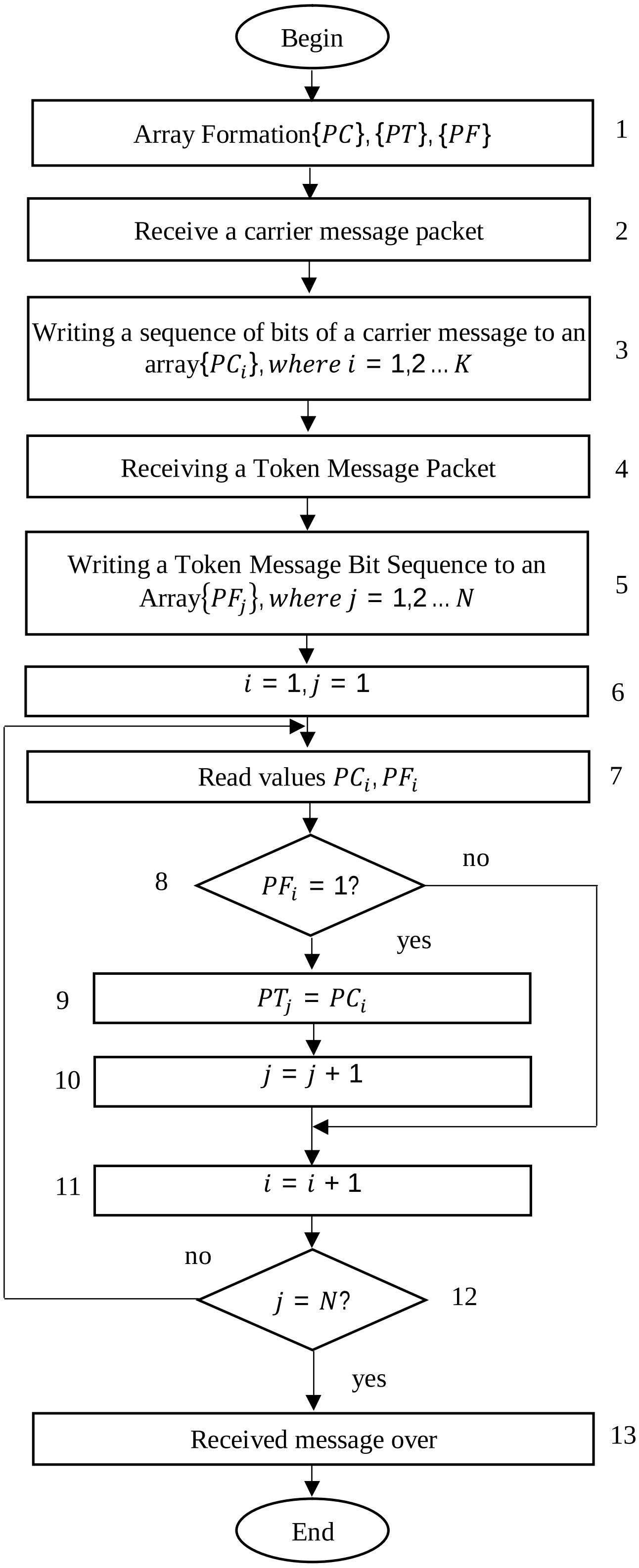
Begin
Array Formation$\{PC\}, \{PT\}, \{PF\}$
1
Receive a carrier message packet
2
Writing a sequence of bits of a carrier message to an array$\{PC_i\}, where\ i = 1,2 \dots K$
3
Receiving a Token Message Packet
4
Writing a Token Message Bit Sequence to an Array$\{PF_j\}, where\ j = 1,2 \dots N$
5
$i = 1, j = 1$
6
Read values PC_i, PF_i
7
8
$PF_i = 1?$
no
yes
9
$PT_j = PC_i$
10
$j = j + 1$
11
$i = i + 1$
no
$j = N?$
12
yes
Received message over
13
End

Figure 2: Algorithm for the process of extracting messages in electronic trading

To simulate the size of the transferred files, typical messages, web pages, the Pareto distribution is often used, which has the following form:

$$w(x) = \frac{\alpha k^{\alpha}}{x^{\alpha+1}};\ \alpha > 0; k < 0; x > 0,$$

α −form parameter;

k −parameter that defines the lower bound for a random variable.

Using a computer, it is possible to generate uniformly distributed random variables y in the range from 0 to 1. In order to model a random variable x with a Pareto probability distribution density, it is necessary to find the functional transformation x = f (x). This can be done based on the expression:

$$w(x = f(y)) = w(y)\left|\frac{dy}{dx}\right|$$

where from

н $= \int w(x)dx = \int \frac{\alpha k^{\alpha}}{x^{\alpha+1}}dx = 1 - \left(\frac{k}{x}\right)^{\alpha}$, at $x > k, \alpha > 0$;

Thus, we obtain the following expression for modeling a random variable with a Pareto probability density distribution:

$$x = \frac{k}{\sqrt[\alpha]{1 - rand}},$$

where

rand is a random number that obeys the uniform distribution law generated on a computer in the range from 0 to 1. Parameter α is associated with the Hurst exponent by the expression

$$\alpha = 3 - 2H.$$

The parameter α is usually calculated on the basis of the maximum likelihood method using the known results of measuring the intensity of real traffic $X = [x_1, x_2, \dots, x_n]$:

$$\alpha = \frac{n - 1}{\sum_{i=1}^{n} logX_i - nlogk},$$

where

$$k = \min_i k$$

In practice, the value of the self-similarity parameter is in the range from 1/2 to 3/2.

Thus, it is possible to simulate the sizes of both carrier messages and information messages. A more important role in the method will be played by the ratio of the size of the carrier message to the information message (LHC/LIC).

It can be seen from the logic of the method that with a small carrier message and a large information message, the algorithm will not converge. Therefore, it is necessary to determine $G_{\text{add}} > (LHC/LIC)$the border at which the size of the carrier message will be sufficient to find the display of the information message in it. Or consider the option of forming a sequence of several carrier messages to transfer information of one message. Since the appearance of the bits "0" and "1" in the messages obeys a uniform law, it can be assumed that the composition of two laws of uniform distribution density specified in the same section will correspond to the Simpson distribution law. However, taking into account the message sizes LHC and LIC, in accordance with the limit theorem, the total law of distribution of random variables will correspond to the normal law.

Thus, the claimed method due to the lack of direct embedding of the message in the carrier message, transmission of the carrier message and the marker packet of the message on different communication channels can increase the secrecy of the transmission of confidential information.

3. IMPLEMENTATION OF AN E-COMMERCE SECURITY MECHANISM BASED ON THE FUNCTIONING OF A HASH CHAMELEON

A mechanism to ensure the properties of inexpressibility and secrecy is a hash chameleon. The combination of EDS(electronic digital signature) and a hash chameleon is called a signature chameleon. A hash chameleon is a hash function with a loophole. That is, a chameleon hash is a hash function that is collision-resistant without knowing the recipient's secret key, and satisfies some special requirements, including non-transmission and secrecy. A hash chameleon can be combined with any EDS algorithm. To authenticate a message, the sender calculates its hash value using a hash chameleon. Then he signs this hash value using an arbitrary basic EDS algorithm [3]. Thus, the requirement of compatibility of the hash chameleon with various EDS algorithms is achieved.

The main properties that provide the use of a hash chameleon in standard EDS protocols are:

- non-interactivity - the ability to verify the signature off-line;
- compatibility - the possibility of coordinated work with standard EDS protocols;
- stability based on solving discrete logarithm or factorization problems depending on the selected basic EDS protocol;
- Reversibility - the ability to convert the chameleon signature to standard;
- non-transferable EDS - the impossibility of proving the validity of the EDS to a third party without the participation of the subscriber;
- secrecy of the message, which consists in the absence of the need to disclose the content of the message to a third party in the course of resolving possible contradictions.

For a clearer understanding of the mechanism of the hash chameleon, the hash chameleon on identifiers (ID) is considered, the scheme of which is shown in Figure 3.

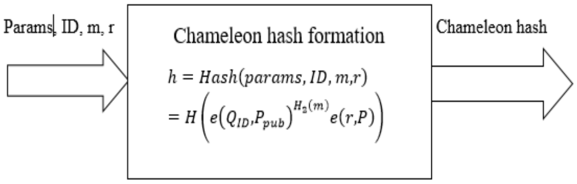
Params, ID, m, r
Chameleon hash formation
$h = Hash(params, ID, m,r)$
$= H\left(e\left(Q_{ID},P_{pub}\right)^{H_2(m)}e(r,P)\right)$
Chameleon hash

Figure 3: Chameleon hash formation pattern

In Fig.3, the following notation is used:

$\langle G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H\rangle$ —-open system parameters.

G_1 —is a cyclic additive group with a generator of the group P;

$q$is the order of P;

$G_2$is a cyclic multiplicative group of order q;

$e: G_1 \times G_2$ —pairing;

$H_1: \{0,1\} \rightarrow G_1$; $H_2: \{0,1\} \rightarrow Z_q$; $H: G_1\{0,1\}^n$ —hashfunctions (n-message length, $Z_q$is an integer ring of order q);

$ID \in \{1,0\}^n$ —recipient identity;

m – message;

Recipient key pair:

$Q_{ID} = H_1(ID) \in G_1, B = sQ_{ID}$ —public and secret keys of the recipient, respectively. The key pair of the third trusted party (TTP):

$P_{pub} = sP$ — public key, s — master key.

The functioning of the hash chameleon on ID can be represented in the form of four algorithms:

- setting system parameters;
- key calculation;
- hashing
- fake formation.

Setting system parameters - params are directly generated.

Key calculation - the algorithm calculates $Q_{ID} = H_1(ID) \in G_1$ and sets information about the loophole $B = sQ_{ID}$.

Hashing - having params = $\langle G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H\rangle$, $ID \in \{1,0\}^n$,random number $r \in G_1$ and m, the subscriber calculates the hash value. The algorithm is always started by the subscriber [4]. As a result of this stage, there are:

$Q_{ID} = H_1(ID) \in G_1$ —public key of the recipient;

$h = Hash(params, ID, m, r) = H\left(e\left(Q_{ID}, P_{pub}\right)^{H_2(m)} e(r, P)\right)$ — is a hash chameleon.

Fake formation - having params, ID information, information about loophole B associated with ID, message m 'and hash value h from message m, the algorithm calculates $r' \in G_1$. The scheme of the fake algorithm is shown in Fig.4.

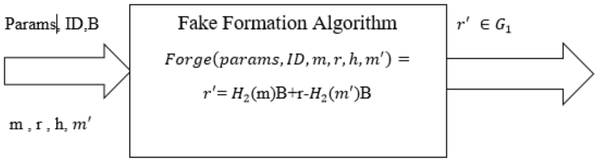

Figure 4: Fake Formation Algorithm Scheme

Identity Chameleon Signature Algorithm

The participants are the subscriber, the recipient and the judge, which is necessary to resolve the conflict between the subscriber and the recipient.

The keys. Subscriber key pair:

VK_s и SK_s — are public and secret keys, respectively. The recipient key pair was defined in the hash chameleon algorithm:

ID — is the subscriber's public key and $B = sQ_{ID}$ —is the secret key, or loophole information.

Generation of a chameleon-signature on the identifier-CHAM-SIG.

The subscriber has: message m, his private key SK_s and ID.

1. A hash chameleon of message m is generated, a random number $r \in G_1$ is selected and calculated:
2. $h = Hash(params, ID, m, r) = H\left(e(Q_{ID}, P_{pub})^{H_2(m)} e(r, P)\right)$.
3. Calculates $sig = SIGN_{SK_s}(hash, ID)$.
4. EDS of message m has the form $SIG(m) = (m, r, sig)$.

Verification of the chameleon signature on the identifier - CHAM-VER

The recipient has: the signature $SIG(m) = (m, r, sig)$,the public key of the subscriber VK_s,information about the loophole (or his private key) $B = sQ_{ID}$.

1.Computes: $h = Hash(params, ID, m, r)$.

2.Verifies signature authenticity:

$$Verify_{SK_s}((hash, ID), sig) = valid$$

The mathematical apparatus of the hash chameleon is based on pairing in the group of points of elliptic curves, due to which the stability of the scheme is based on the classical problem of complexity of solving the discrete logarithm problem in the group of points of an elliptic curve.

The use of a chameleon-signature will satisfy the requirements of the innovative nature of electronic document management systems, namely the non-transferability of electronic digital signatures and the secrecy of the signed message.

4. METHOD FOR ASSESSING THE SECURITY OF INFORMATION RESOURCES IN E-COMMERCE SYSTEMS

To protect against interception and to protect information during a transaction, both symmetric and asymmetric cryptographic algorithms are used [5]. At the same time, additional communication channels other than Internet channels are used: fax, telephone, regular mail, etc.

When considering the possibility of intercepting information of interest, it is impossible not to exclude the “human factor”, therefore, along with software and hardware, it is necessary to use organizational ones that protect information resources, exclude blackmail, control passwords, etc.

An analysis of the sources made it possible to formulate a general scheme of an integrated environment (Fig.5):

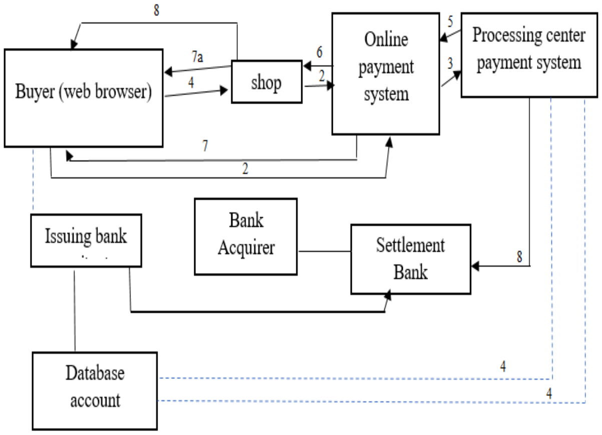

Figure 5: Integrated e-Commerce Integrated Environment Diagram

1. A buyer in an electronic store forms a basket of goods and selects a credit card payment method.
2. Credit card parameters must be transferred to the Internet payment system for further authorization.
3. The Internet payment system transmits an authorization request to the traditional payment system.
4. This step depends on whether the issuing bank maintains an online database of accounts. If there is a database, the processing center transmits an authorization request to the issuing bank (4a) and then, (4b) receives its result.
5. The authorization result is transmitted to the Internet payment system.
6. The store receives an authorization result.
7. The buyer receives the authorization result through the store (7a) or directly from the Internet payment system (7 b).
8. If the authorization result is positive:
   - it stores provides a service, or ships the goods (8a);
   - the processing center transfers to the settlement bank information about the completed transaction (8b). Money from the customer’s account in the issuing bank is transferred through the settlement bank to the store’s account in the acquiring bank.

Recently, numerous methods for processing non-numerical information are widespread, among which the methods of expert evaluations are most famous. Using these methods, the main source of information is an expert in the field of security of corporate Internet systems. The basis for the use of these methods is the decomposition of a complex, difficult to formalize problem into a sequence of simpler subtasks corresponding to a certain type of elementary examinations [6-7]. Evaluation of non-numerical information refers to attributing non-numerical characteristics to quantitative or qualitative values on a selected measurement scale. The determination of risk weights is used to streamline them and determine priority actions to protect information.

One of the solutions is based on the results of mathematical methods of the theory of qualimetric scales, models of linear ordering of alternatives and pairwise comparisons.

Let the risk options for the enterprise network $r_g$be compared in pairs in terms of their significance for ensuring the security of the corporate system by a fixed non-numerical characteristic, and the results of the comparisons be written in the form of a matrix of pairwise comparisons $A = (a_{ts})_{kxk}$in probabilistic calibration.

Belonging of the risks r_g to a fuzzy binary relation of greater importance of one of them over the other according to the considered characteristic $\mu_r: R \times R \to [0,1] \mu_r(r_t, r_s) = P(r_t > r_s)$. $P(r_t > r_s)$is the probability the fact that the risk $r_t$if implemented, leads to more serious consequences than the implementation of the risk r_s. The elements of the matrix of pairwise comparisons in probabilistic calibration satisfy the following relations: $\forall i \forall j; 0 \le a_{il} \le 1;\ a_{ij} + a_{ji} = 1$

To construct a matrix of pairwise comparisons in a probabilistic gauge, a strict linear order qualimetric scale

$S =< H, R_{>.}$ Is subjected to arithmetization.

Suppose, as a result of a pairwise comparison of the risks $r_t$and $r_s$by a fixed non-numerical characteristic, the risk $r_t$to item $h_p$of the strict linear order qualimetric scale $S =< H, R_{>.}$,

where

$$H = (h_0, h_1, h_2, h_3, h_4, h_5, h_6),$$

a pair $(h_i, h_{i+1}) \in R,\ i = 0,1,..,5, h_i, i = 0,1 \dots .6$ –points of the scale S given in Table 1,

$R_{>.}$ Is the strict linear order relation defined on the medium H, and the risk r_s to point $h_p, p \neq q$.

Then the elements of the matrix of pairwise comparisons $A(t, s) = (a_{ts})_{k\times k-}$ in the probability calibration are defined as follows:

$$a_{ij} = \sum_{s=1}^{z} p_s \sum_{g=0}^{s-1} p_q + 0{,}5 \sum_{i=0}^{z} p_i p_q, a_{li} = 1 - a_{ij}$$

where

$p_s(p_q) -$ the probability of assigning to the item $h_p(h_q)$ the scale $S =< H, R_{>.}$numerical value $\frac{s}{z}$;

$s = 0,1, \dots z \langle \frac{q}{z}, q = 0,1, \dots z \rangle$ as a result of scale arithmetic $S =< H, R_{>.}$To the normalized scale of points $SB =< H, R_{\geq} > c$ with a scale carrier $Z = \left\{0, \frac{1}{z}, \frac{2}{z}, \dots, \frac{z-1}{z}, 1\right\}$ and the linear order relation $R_{\geq}$ using a normalized stochastic process with equally probable monotonic trajectories [7-8]. They are sets of points of a rectangular integer lattice $[0, m + 1] \times [0, z]$of size $(m + 2)(z + 1)$

After the approval of weight coefficients $k_{ij} = a_{ij}$ of risks r_g by a fixed non-numerical characteristic, the risks are ordered using the constructed matrix of pairwise comparisons $A = (a_{ts})_{k\times k}$.

The obtained matrix of pairwise comparisons contains the initial data for models of linear ordering of alternatives.

The scale of strict linear order shown in Table 1 quantifies qualitative subjective judgments about the level of risk $r_g$by the fixed characteristic $y_t^{(g)}, t = 1, \dots, p$, described by a non-numerical line.

Table 1: Options scale

Items qualimetric scales h_i	Definition values	Commentary on the meaning of meaning
h_0	The significance of the analyzed risk is practically low.	There is practically no risk
h_2	The significance of the analyzed risk is moderate	Thereis a risk
h_4	Relevanceriskanalysissubstantial	Riskissignificant
h_1, h_3, h_5	Interim estimates between two adjacent judgments	Applyin compromise cases
h_6	Relevance analyzed significant risk - very strong	Biggestrisk

A comparative analysis of linear ordering models allowed us to conclude that it is advisable to use the dominant function model to select the most significant risk [9]. It is focused on processing fuzzy preferences of the decision maker (auditor). When interpreting the elements of the matrix $A = (a_{ts})_{k\times k}$ by the degree of belonging of the compared risks r_i and r_j to the fuzzy preference relation given on the set of considered information security risks of the Internet.

The dominance function$L_R(r_i) = \max_{j\neq i} a_{ji}$ characterizes the significance of the risk r_i. With $L_R(r_i) = 0 -$ there is not a single risk that would lead to more serious consequences than the risk r_i, and with $L_R(r_i) = 1 -$ there is a risk that, compared with the risk r_i,, leads to more serious consequences. Risks are ordered by increasing dominance function. After ordering the risks r_i,, each of them is assigned a numerical value $y_t^{(g)}, t = 1, \dots p$, equal to the minimum risk numberr_i, in the optimal ordering

$$W(g) = \left(W^\wedge(g), W_2(g), W_3(g), \dots, W,(g)\right)$$

In the simplest case, the vector performance criterion

$$W(g) = \left(W_i(g), W_2(g), W_3(g) \dots, W_l(g)\right)$$

coincides with the vector of characteristics

$y^{(g)} = (y_1^{(g)}, y_2^{(g)}, \dots, y_p^{(g)}, y_{p=1}^{(g)}, \dots, y_n^{(g)})$.

In e-commerce systems, conducting a security audit remains open, since today a comprehensive and high-tech solution to this problem has not been fully developed.

5. CONCLUSION

The main results of the work can be represented by the following conclusions:

1. Method of data protection during electronic trading operations hides the data transfer of SSL/TLS protocols due to the lack of direct embedding of the message in the carrier message, transmission of the carrier message and marker message packet in the communication channel were proposed.
2. Given mechanism providing the security of electronic commerce based on the functioning of the hash chameleon allows you to satisfy the requirements of some business applications related to electronic commerce and the secrecy of the signed message due to the presence of systems based on identifiers.
3. A method for assessing the security of information resources in integrated e-commerce systems was proposed and a scheme of an integrated e-commerce environment was constructed.

REFERENCES

1. GulomovSh.R., Abdurakhmanov A.A., Nasrullaev N.B.**Design Method and Monitoring Special Traffic Filtering under Developing** «Electronic Government». International Journal of Emerging Technology & Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal), Volume 5, Issue 1. January, 2015. India. – P.66-73
2. Savateev E. O. **Design of Steganography System Based on the Version 4 Internet Protocol** // IEEE

International Siberian Conference on Control and Communication (SIBCON-2005). Tomsk — pp. 26-49.

3. K. Ruth Ramya, B. Manjula Josephine, K. Durga Praveen, M. BalaMaruthi, Ch.Sai Kumar. **An Efficient and Secured Biometric Authentication for IoT**. International Journal of Emerging Trends in Engineering Research. Volume 7, No. 10 October 2019.
4. Yuanqiao Wen, Chunhui Zhou "**Research on E-Commerce Security Issues**". 2008 International Seminar on Business and Information Management. https://doi.org/10.1109/ISBIM.2008.168
5. N. Chandra Sekhar Reddy, Purna Chandra Rao Vemuri, A. Govardhan. **An Emperical Study on Support Vector Machines for Intrusion Detection**. International Journal of Emerging Trends in Engineering Research. Volume 7, No. 10 October 2019 https://doi.org/10.30534/ijeter/2019/037102019
6. Zhang F., Safavi-Naini R and Susilo W, **ID-based Chameleon hashes from bilinear pairings**. http://eprint.iacr.org/2013/208.
7. HatoonMatbouli,Qigang Gao. (2012). **An Overview on Web Security Threats and Impact to E-Commerce Success**. International Conference on Information Technology and e-Services, 2. https://doi.org/10.1109/ICITeS.2012.6216645
8. P.Prashant. **The role of trust in e-commerce relational exchange: Auni_ed model**. Information & Management,2009, pp. 213-220. https://doi.org/10.1016/j.im.2009.02.003
9. ShaziaYasin, Khalid Haseeb. "**Cryptography Based E-Commerce Security: A Review**". IJCSI-Vol. 9, Issue 2, No 1, March 2012