Journal of Al-Qadisiyah for Computer Science and Mathematics Vol. 14(3) 2022 , pp Comp. 88–111

Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

STRUCTURAL DESIGN OF SECURE E-COMMERCE WEBSITES EMPLOYING MULTI-AGENT SYSTEM

Farah Tawfiq Abdul Hussien [a*], Abdul Monem S. Rahma[b], Hala Bahjat Abdul Wahab[a]

a: Faculty of Computer Science, University of Technology, Baghdad, 100001, Iraq .*Email: Farah.T.Alhilo@uotechnology.edu.iq*, b: Department of Computer Science Al-Maarif University College Anbar, Iraq , *monem.rahma@ uoa.edu.iq, hala.b.abdulwahab@ uotechnology.edu.iq*

ARTICLE INFO

Article history:
Received: 30/05/2022
Rrevised form: 01/07/2022
Accepted : 05/07/2022
Available online: 13 /08/2022

Keywords:

Software Agent,

Lightweight AES,

E-commerce security,

E-bank system

ABSTRACT

The vast growth in electronic trading and monetary transactions results to increase the importance of E-commerce applications rapidly. In order to accomplish the fully functioning, reliable, scalable, secure, efficient and user-friendly E-commerce applications, sufficient system analysis and design processes are important. Shopping over the internet requires offering secure payment method.

Providing security for each individual online consumer at the same time (particularly for large websites) is a time-consuming effort that can result in a variety of issues, including response delays, customer orders being lost, and system freeze or crash, all of which impair system performance.
This work seeks to present a new multi-agent system prototype structure that solves the challenge of security while avoiding issues that might degrade system performance. By creating integrated system taking into account the three parties the e-commerce, the e-bank and the customer, the main concentration is to create an archeticture that helps in decreasing the website traffic and supportng the security with effective performance. To simulate the real systems a recommendation system is created based on the customer behaviors to increase system performance in helping the customers to find their favorite products and solve problems like cold start, sparsity of user-item matrix, scalability, and changes in user interest.
This is done by creating a commercial environment (e-commerce and e-bank websites) and a software agent that is installed on the client's device to handle the purchase and ciphering procedures without the need for the consumer to intervene. The security process involve preprocessing phase followed by a modified lightweight AES employing chaotic tent map to generate encryption key.

MSC..

https://doi.org/ 10.29304/jqcm.2022.14.3.996

∗Corresponding author

Email addresses:

Communicated by ‘sub etitor’

1. Introduction

Currently, the e-commerce technologies are critical in supplying a diverse range of products and services [1]. Because of the services provided by these systems, the number of clients working with these systems is quickly expanding [2], [3]. As a result, the volume of data transferred via the internet has risen [4], [5]. Some of this information is deemed critical, particularly payment information, which may be vulnerable to various forms of assaults [6]. As a result, ensuring security for e-commerce websites has become a necessary aspect in order to win clients' trust [7], [8]. Another issue arises here, namely, providing security for each online customer may be a difficult task (especially for large commercial websites), which may reduce performance and slow the system's response time, resulting in financial problems due to customers' dissatisfaction with the website's service quality [9], [10]. Different techniques to securing e-commerce systems may be used, one of which is encryption. The software agents developed a new trends of communication. They improved the effectiveness and efficiency in various ways in the market processes [11]. The agent technology established and development from the existing physical market towards the virtual markets. They will have dramatic competition effects by fast transfer of information through new technology [12]. The software agents play the role of mediators for the tasks of selecting products and merchants. In general the software agents work as a vehicle between the E-Commerce and the business [13]. The security of E-Commerce means the cybersecurity ideas that allow for an online secure electronic transactions. The security of E-Commerce lets people to purchase and sell services and products over the Internet with a framework which provides security for all the involved parties[14]. For several reasons the security of the e-Commerce site is critical, espicially protecting the sensitive data and the privacy of the customers on a website, protection of the finances of an online business, stopping fraud and financial scams, and defending the reputation of an e-shop as a safe place to conduct transactions [15]. Data mining has been proposed for use in an intelligent e-commerce system in a number of research [16] [17]. An e-commerce system based on a web application and data mining might benefit from agent technology to speed up the process. Some of the drawbacks of e-commerce web applications: Security, Lack of privacy, People fear to operate in a paperless and faceless electronic world, Legal issues, Insufficient telecommunication bandwidth, No one can buy during site crash (deadlock). The main contributions of this paper are :

1. Providing a software agent that is installed on the customer's device to create a secure environment. Without meddling with the consumer, this agent is in charge of buying and security control.
2. Creating an effective recommender system that addresses the aforementioned issues and may be used in an e-commerce site to improve the recommending process. This is accomplished by relying on consumer behavior as well as statistical methodologies that leverage real-time customer trends to ensure that the RS lists that will be recommended to clients are as accurate as possible.
3. Increase confusion and diffusion and increase system randomness by employing several preprocessing techniques
4. Provide additional protection for the password by applying hash function (bcrypt) to make harder for an intruder to determine the encryption key.
5. Achieve the balancing between level of security (complexity) and encryption time (speed) in order to avoid system deadlock and support system performance.
6. Automate all the processes and transactions among the three entities of the system, the clients , the e-commerce website and the e-bank website.

The rest structure of this paper as follow: section two explain the related works, section three describes the proposed system, section four explains the customer device sides, section five the software agent details, section six the e-banck side section seven explains the experimental results and section eight presents conclusions.

2. Related Works

Rregarding employing agent system for e-commerce system several studies are achived some them are:

- The core concept of this study [18] is to hire a completely certified broker who can intelligently detect the buyer's demands based on standard factors that are provided to help solve the challenge of discovering interesting things. The suggested framework intends to provide meaningful replies to meaningful requests, as well as to supply relevant things to individuals who need them, when they need them, and in a way that is in their best interests.
- A framework for the employment of software agent technologies was provided in this study [19]. The usage of an agent controller paradigm will provide the e-marketplace more reliability and scalability. Multiple vendors may be registered in the framework, while buyers can fulfill their needs by utilizing a mobile purchasing agent to communicate their needs to the e-marketplace. Furthermore, the framework was tailored to meet the needs of buyers and sellers in e-business transactions.

- This study [18] proposes a personalized e-shopping system that use agent technology to improve the automation and efficiency of e-commerce shopping processes. Agent for e-commerce establishes connectivity on an anytime-anywhere-any-device basis in order to deliver the precise items requested by customers while maximizing transaction cost and scalability. The client agent communicates with the controller agent, which is in charge of all agent data. The item information is sent from the controller agent to the client agent, who then selects products and adds them to the shopping cart.
- (4) Using a negotiation procedure, this article [19] built a fuzzy-logic based multi-agent e-commerce system capable of negotiating a mutually advantageous arrangement for the supplier and buyer. It made use of fuzzy logic to let people express their preferences for a product using ambiguous phrases like low, medium, and high. The system assesses offers using a fuzzy utility function, then feeds utility scores to a fuzzy inference engine, which calculates the next counter offer.
- The study [20] proposed an agent-oriented approach for verifying that security objectives and security validation criteria are met at various phases of the created system lifetime. Furthermore, the system must give mapping for the security list of risks in order to determine whether any of the dangers on the list may be used to enhance the system. The meta-agents automatically create a security checklist to regulate the operations of the client agent.
- A paper by [21] proposed a multi-agent e-commerce system based on block chain technology in another research. The agent technology in an e-commerce system was introduced first, followed by an explanation of the hidden threats. The second step is to present the information transaction and executive structure. Finally, we'll look at the verification method node in the agent transaction process.
- Paper number [22] proposed a security prototype for multi-agent systems. It provided a practical way to ensure that security and design criteria were linked with system duties throughout the development process. In addition, assaults and threats were classified. In addition to the vulnerabilities at the agent level, several threats were examined, such as corrupted mobile agents attacking the chief system host, phony agents, and insecure communication across platforms. Changing the conveying information, message injection, and intrusion detection to agents can be used to deal with agent authentication, fraudulent messages, and altering agents' interactions.
- Another research [23] identified the most common vulnerabilities that might occur in multi-agent systems that handle e-commerce applications. The study's main assumptions are that security measures should optimize and enhance the many security solutions used in the use of e-commerce to prevent identity theft, access to private data, and access control, among other things.

3. The Main Description of The Proposed System

This paper aims to build a prototype model that represents the e-commerce environment. Figure 1 represent the block digram for a scenario and the sequences of the operations of the proposed system environmet.

It consists of several entities which are employed to provide a typical environment to achieve the activities that are performed in a real e-commerce system, they are :

- **Web sites:** there are two websites one is for the e-commerce and the other is for the e-bank. These websites are important to perform the actual sequence of operations that are occure when a shopping process is done by any customer.
- **The suggested software agent:** this software is responsible of managing the purchasing and the encryption operations that will be done during the customer's shopping and payment processes. It is responsible of providing a secure environmnet for these processes between the three parts of the environment, the customer, the e-commerce system and the e-bank system.
- **The suggested encrypion system:** Which include preprocessing operations (padding , shuffling and zigzag), encryption key generation using chaotic tent map , bcrypt hashing function and the encryption algorithm (lightweigt AES).
- **Databases:** The system consists of two databases. The first one is for the e-commerce system which consistes tables about the products, the orderes, the customers, the payments and other details. The second is for th e-bank system that consists of tables about the customers and thier accounts, balance, payment methods and other details. The use case diagrams 2 and 3 describe the behavior of each actor in this environment.

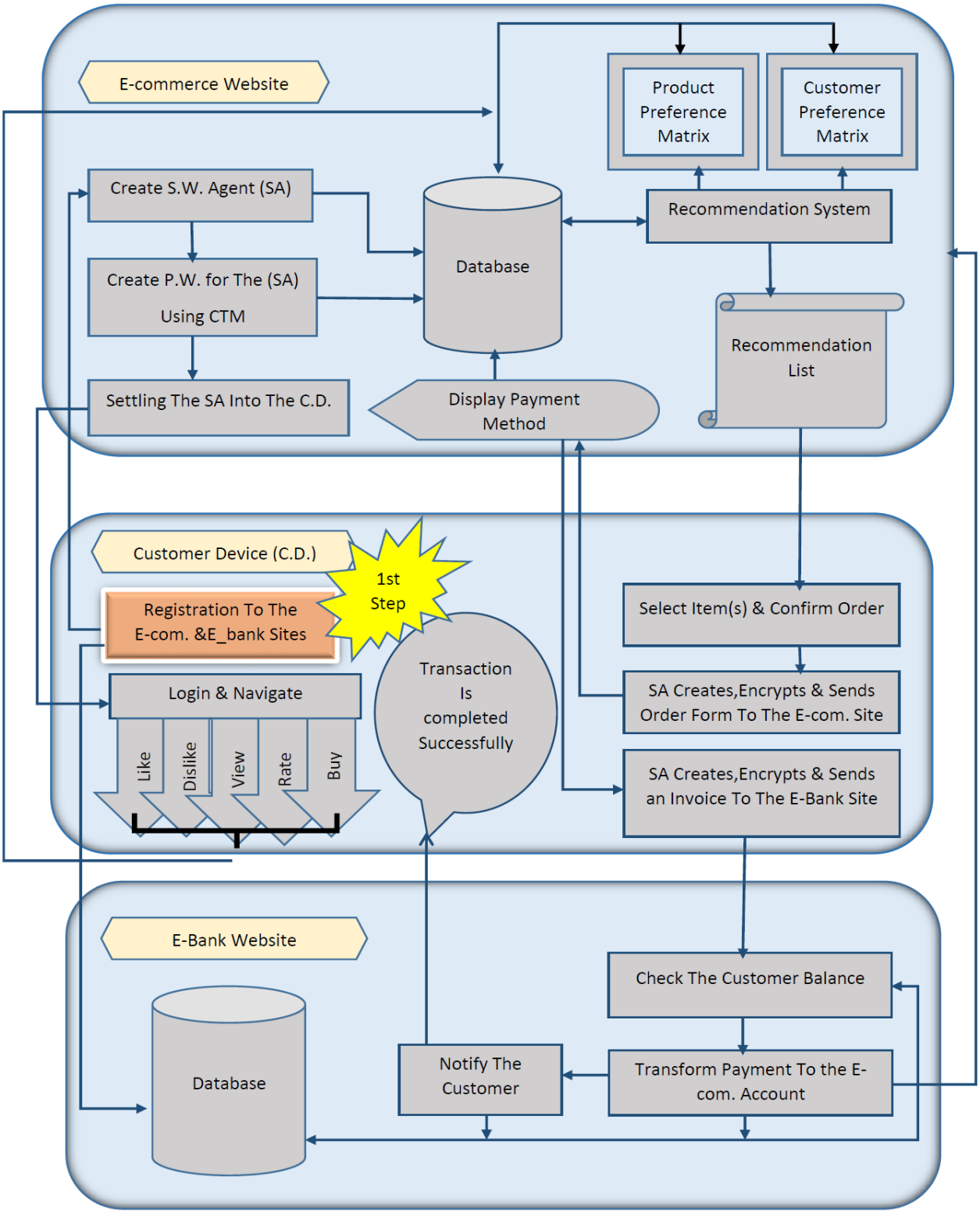

Fig. 1- The block Diagram of The Proposed System

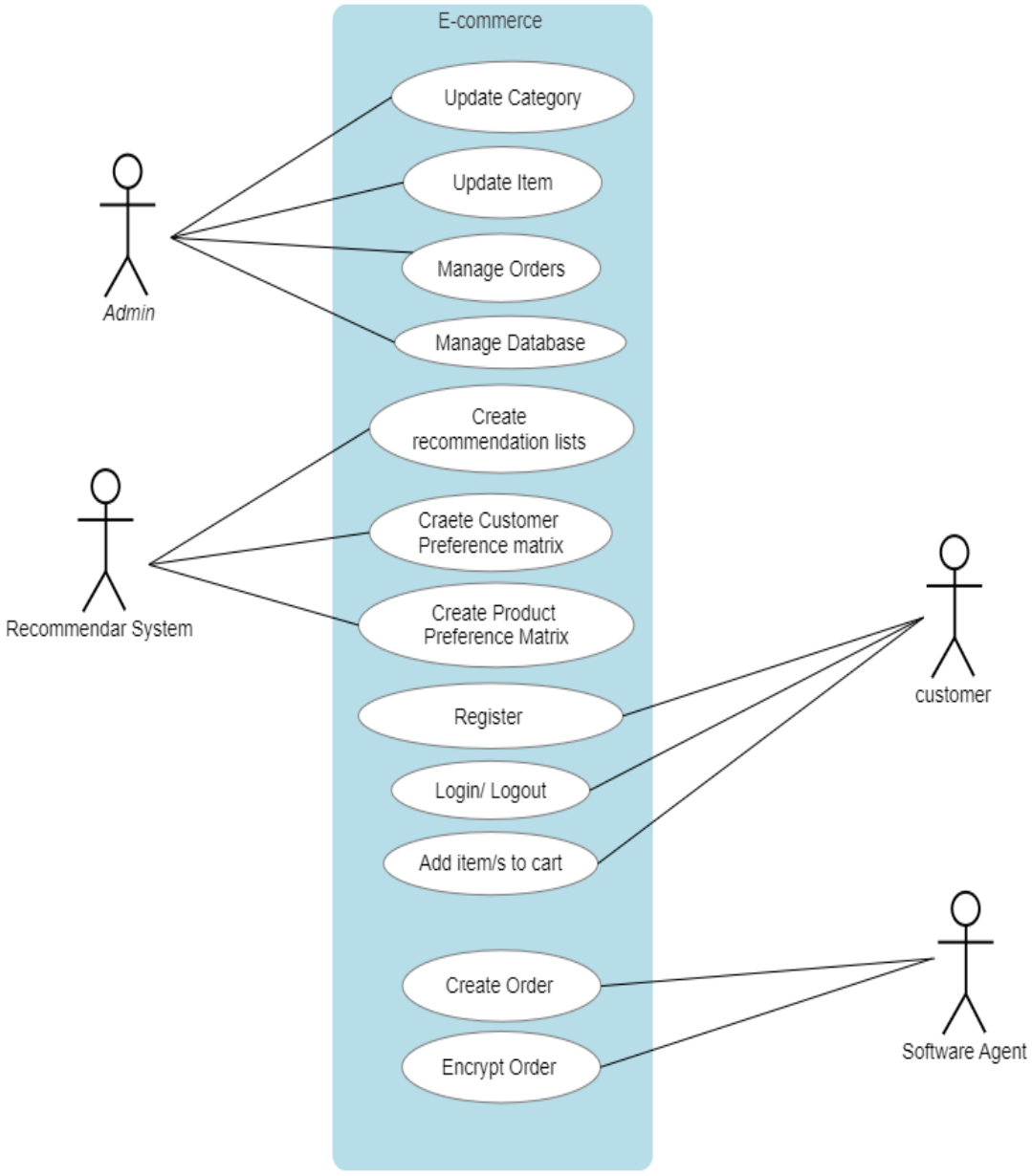

Figure 2. Use Case Diagram of the Actors Roles In the E-commerce System

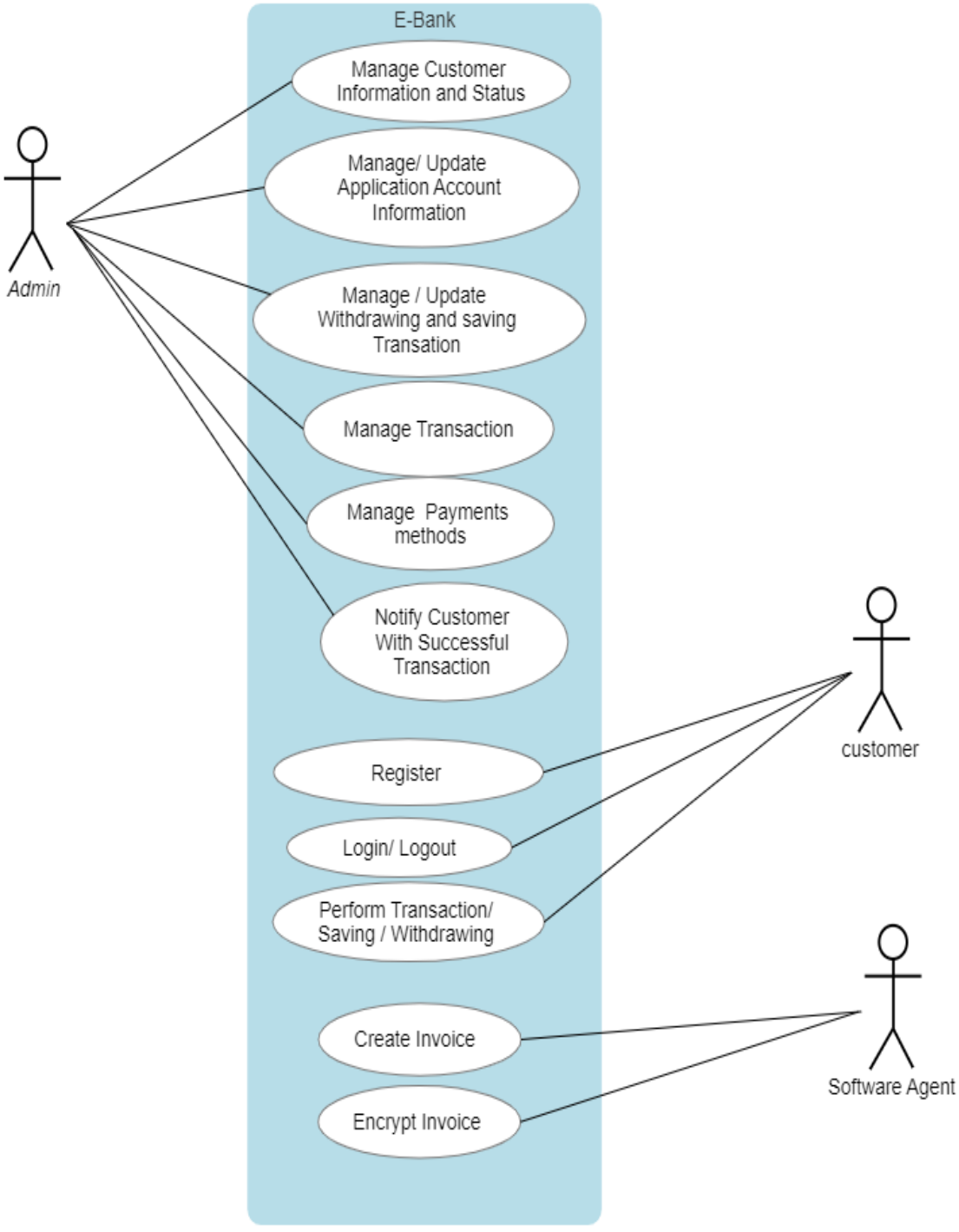

Figure 3 Use Case Diagram of the Actors Roles In the E-Bank System

This prototype approach protects the three elements of the e-commerce environment, lowers system server overload, improves system speed, and secures transactions. Additionally, all of the customers' identities will be validated using agent Id, which includes the following objects and processes:

- *Order*: It's a record form that the agent generates. It contains the following data, which reflects the client's purchase information: Client-Id, Agent-Id, Product-Id, Quantity, Address, Date, and Time are all examples of identifiers.

- *Payment method*: there are five methods of payments credit card, debit card, PayPal, bank transfer and cash on delivery. For all payment methods an invoice will be generated and encrypted by the software agent except cash on delivery.
- *Preprocess*: it contains a sequence of operations to ensure increasing randomness, confusion and diffusion which are performed before the encryption process, these processes involve:
    - Padding: adding additional dummy character to the hashed information.
    - Shuffling: the information will be shuffled using Fisher Yates algorithm.
    - Zigzag: Rearrange the order information depending on certain pattern.
- Encrypt using Lightweight AES algorithm: after preparing the order information and payment information in preprocessing step the encryption process will take place using the proposed lightweight AES algorithm.
- Transfer the order information to the e-commerce website.
- Transfer payment information to the e-bank system.
- Transfer the money to the website account.

The agent is divided into two parts: the first is in charge of handling client requests and orders by converting them into a special form that can be submitted to the website at any time, and the second is in charge of preventing orders from being discarded due to website server overload during peak hours. The suggested system's second component is in charge of safeguarding communication between clients, the commercial website, and the e-banking system. The major purpose is to create an integrated system that considers all three parties in the commercial process and treats the system as a case study to research and demonstrate the gaps that indicate the system's shortcomings, as well as to find solutions for and from these gaps. These flaws include time waste, stalemate, and an insecure communication route, all of which reduce clients' trust in the e-commerce system. This is accomplished by installing an agent application on a client's device, causing each client to visit and purchase from a certain commercial website that allows the customer's identity to be verified. This is accomplished by supplying each client with an encryption algorithm offered by the commercial website.

4. The Customer Device Side

As shown in figure1 that the first step which motivates the complete process starts by the customer. First of all the customer should has an account in the e-commerce system to be able to buy from it and an account at the e-bank system to be able to pay the invoice amount. At registeration step an acount will be created for the customer at the e-bank system and the e-commerce system. For the e-commerce system each registration phase is associated with generating a software agent (SA) for that customer. This SA will be responsible of the purchase and security management between the customer and the e-commerce system, and securing the payment process through the e-bank system. The SA will be settled into the customer device. The customer behavior inside the e-commerce system will help the recommendation system to predict a recommendation list according to the customer's preferences. The customer's behavior involve (like, dislike, view, rate, buy) which will be discussed later. When the customer adds item(s) to his cart, the website will display the order details to be confirmed by the customer. At this point the SA will create and encrypt an order form to be sent and saved at the e-commerce's database system. Then the e-commerce website will display a dialogue box represents the allowed payment methods (five methods as mentioned earlier). The customer will choose payment method. For all methods except for the cash on delivery, SA will create and encrypt a payment bill contain the payment details to be sent to the e-bank system. At the e-bank site the payment invoice is decrypted retrieve the customer information depending on the agent Id and check the customer balance. If there is enough money in the customer's account the e-bank will transform the invoice amount to the e-commerce account then informing the customer that the transaction is completed successfully.

5. The Software Agent

When a consumer registers on the e-commerce site, a SA is created and delivered to the customer's device to be settled. The SA design, architecture, and activities will be discussed in depth in the next section.

5.1. The Software Agent Structure and Activities

The important requirement to maintain security for transferred data via the internet, particularly payment information, is a major concern. Providing security for each individual consumer that visits the e-commerce site places a significant demand on the network and the e-commerce server, perhaps causing a system crash. This

research proposes an agent prototype structure that is responsible for two tasks: purchasing and security management, in order to mitigate and avoid such harm. The process consists the following steps:

- For each client with an account, there will be an agent who is already installed on his device. The e-commerce generates this agent, which is configured to handle two tasks: buy and security.
- For each order, the agent will create an order form that provides the purchase data in the form of an invoice.
- This invoice is encrypted before being submitted to the e-commerce site to secure the customer's information from tampering or theft.
- To minimize time, the encryption operation is carried out utilizing the lightweight AES algorithm.
- The form is decrypted at the receiver using the agent Id, which relates to the customer information.
- The encryption procedure is carried out without the involvement of the consumer. Without the customer intervening, the encryption key is produced and transmitted to the agent.
- Because the encrypting process is maintained by just one party (the e-commerce site), symmetric encryption is utilized. The agent in charge of encryption is produced and supported with the password without the involvement of the consumer. The sequence of operations of the software agent actions inside the client device is represented in Figure 4.

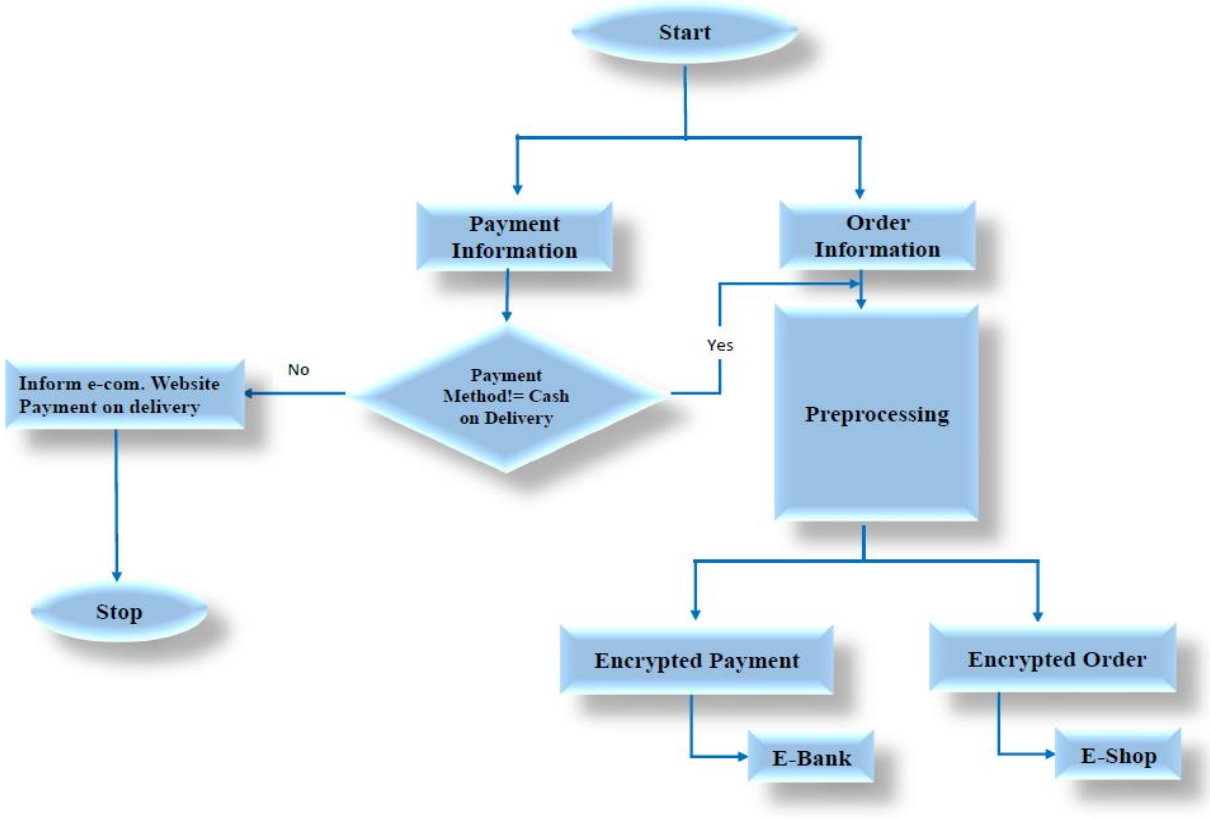

Fig. 4- The sequence of processes (preprocessing and encryption) performed by the software agent

Fig. 5 and Fig. 6 represent a block diagrams that describes the sequence of the activities of the software agent inside the consumer device.

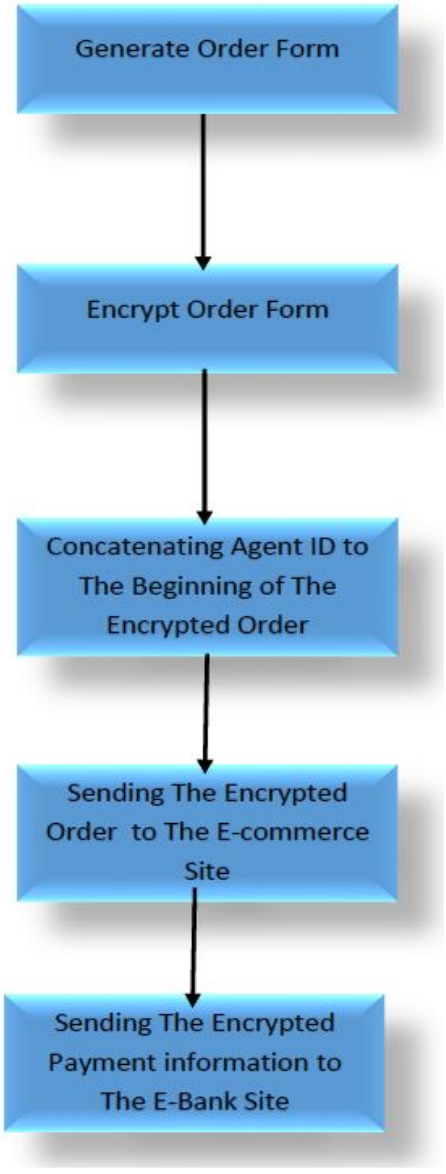

Fig. 5- The Software Agent encrypting an order for purchasing a product

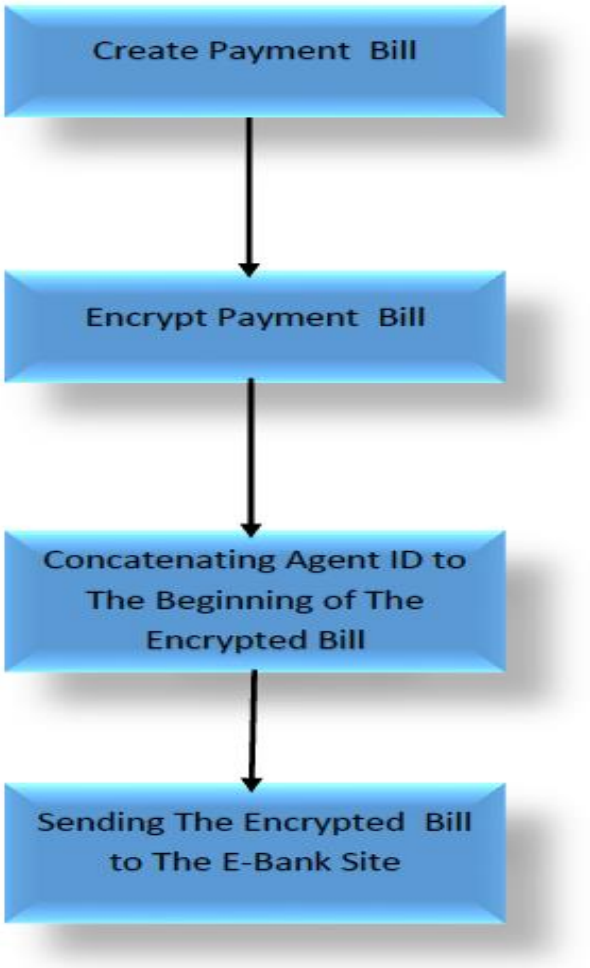

Fig. 6- The Software Agent creating and encrypting a payment bill for buying a product

5.2.The Software Agent Environment

When creating an agent, the initial step should always be to clearly define the task environment. The task environment refers to the performance, environment, actuators, and sensors (PEAS). The PEAS description for the proposed system is shown in Tab.1.

Table.1: PEAS description of the proposed software agent

Agent type	Performance measure	Environment	Actuators	Sensors
Client Agent	Security	Customer PC	Agent Activation	Customer log in
	Reduce time consuming		Recognize the URL	Add item to cart
	Increase no. of served order per (unit of time)		Generate order form	Confirm payment
	Prevent deadlock		Encrypt order	e-shop confirm reception
			Sending packet	

Increase reliability (prevent loosing of orders)	Stop

5.3.Order Form Generation and Encryption

This action can be defined by the next steps:

- A customer visits an e-commerce website.
- An item is selected to be purchased.

The agent converts the chosen product into a unique form. This is referred to as a Record Form, and it contains information such as User ID, Agent ID, Product ID, Quantity, Address, and Time. All of these procedures are carried out without the involvement of the customer. They are carried out under the management of the e-commerce website through the use of an agent on the client's device, which is built using software that is configured to obey specific regulations. An agent is installed on a client's device to handle the purchasing process and offer security without requiring interaction from the consumer. The data transfer handling between the customer's device and the e-commerce website is the responsibility of this agent. This implies that the agent creates and encrypts the record form before sending it to the commercial website. To offer the needed security, these operations are supervised and carried out under the agent's supervision and in accordance with the e-commerce site's regulations. The suggested encryption algorithm is used to carry out the encryption procedure. It is used to send and encrypt purchase and payment information in order to prevent intruders from tampering with the data during transmission.

Because of its secrecy, complexity, strength, and performance, the AES algorithm is commonly employed to encrypt data transmission. It, on the other hand, has difficulty with large computations. Reducing these computations takes a long time, but it improves speed and security without compromising algorithm efficiency. The conventional algorithm has been modified, which will be discussed in the coming sections, but first, certain basic tasks must be completed before the encryption process can begin. Figures 7 and 8 depict encryption and decoding.

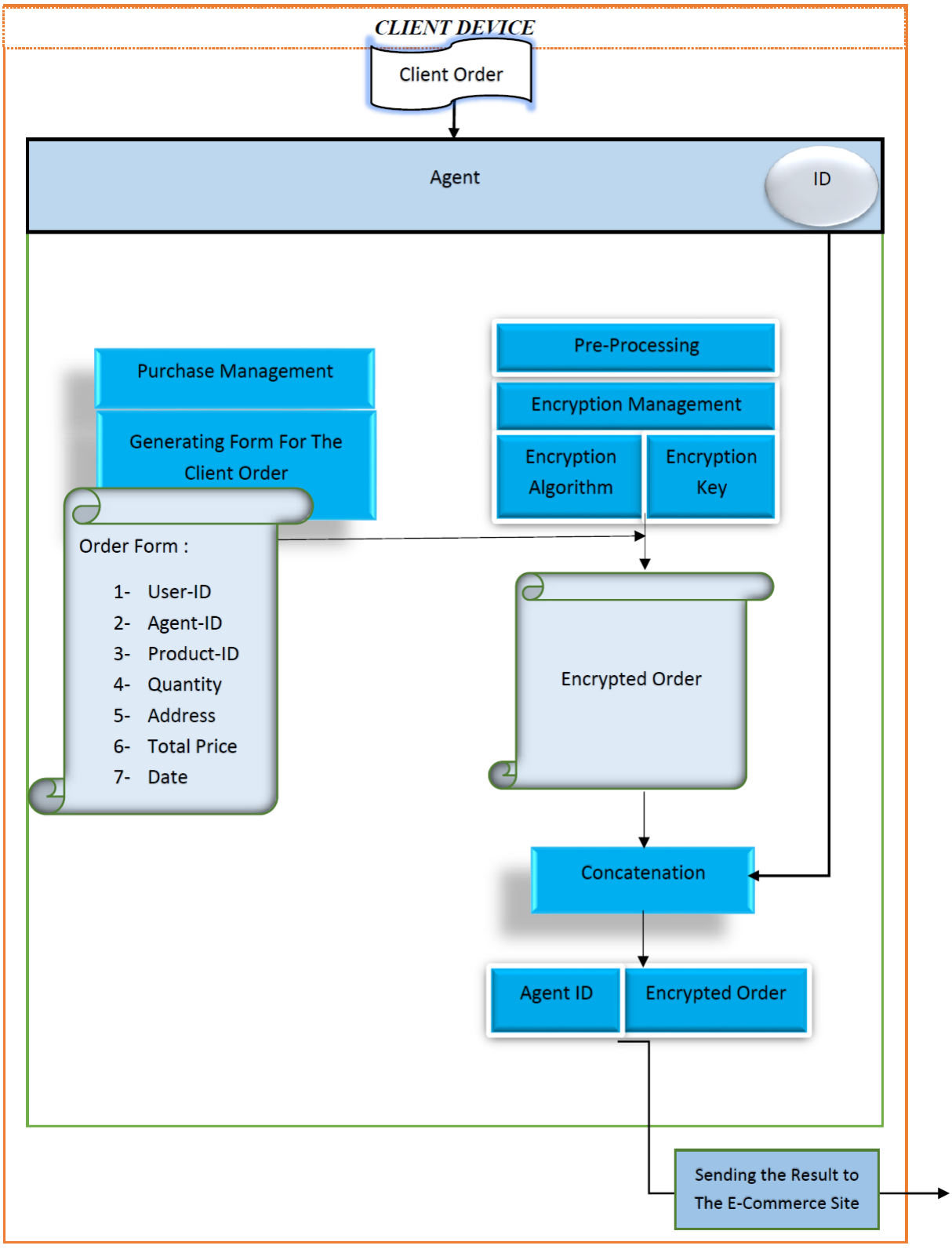

Fig. 7- Order Form generation by the software agent

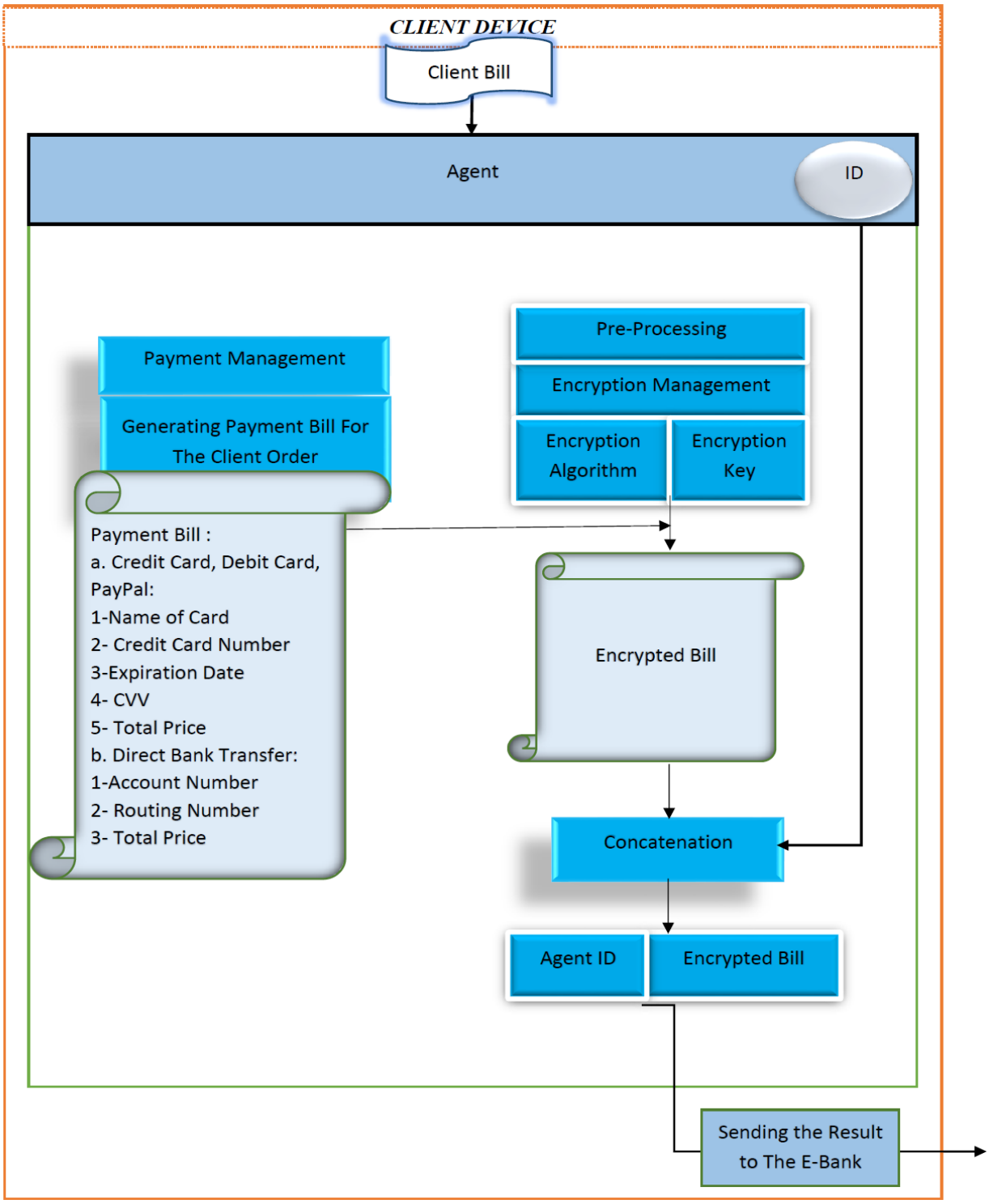

Fig. 8- Invoice generation by the software agent

6.The E-bank System

At the e-bank system, the encrypted payment invoice is received and decrypted to check the details of it. First of all ensure that the customer has an account in the bank then checking the balance of the account, is it enough to make the transaction. If yes then transfer the money to the e-commerce site account and notify the customer that the transaction is completed successfully. Figure 9 represents the sequence of processes that are performed at the e-bank system after receiving an encrypted invoice

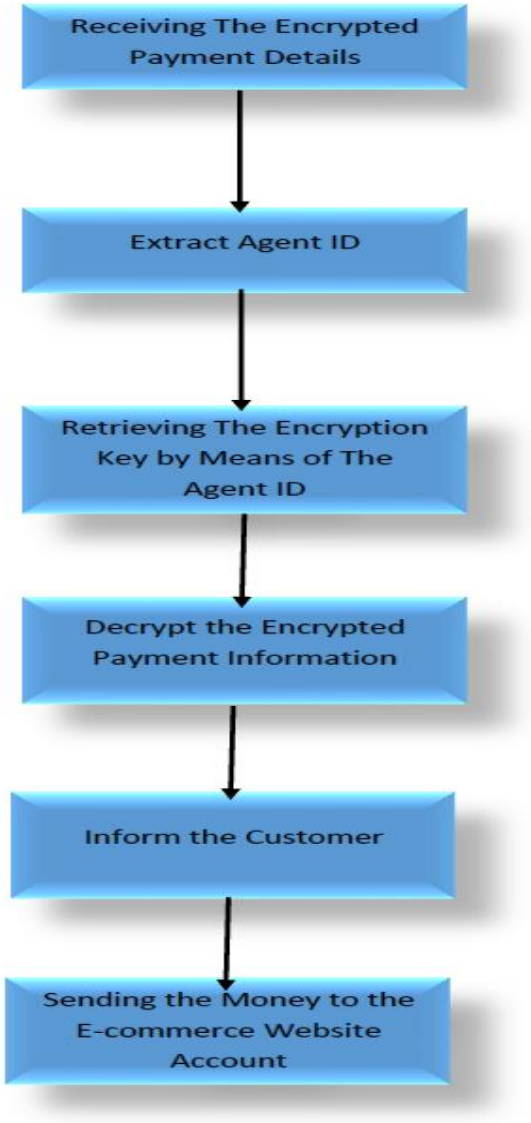

Fig. 9- Invoice encryption and decryption

7. EVALUATION OF THE PROPOSED ENCRYPTION ALGORITHM

Experimental results are used to prove the modified algorithm performance. These criteria involve the NIST test, encryption and decryption time, memory usage on file encryption, and file decryption. The files were encrypted to analyze the performance of the modified AES algorithm. During the experiments, different sizes of text files were tested for ten trials to get the average encryption time and CPU usage of the standard AES and modified AES.

7.1. NIST TEST SUITE

NIST is the most widely used test for utilizing encryption algorithms. These tests provided randomness measures for the encrypted test resulting from both standard AES and the lightweight algorithm. The results are shown in Table 2 below.

TABLE.2: NIST TEST SUITE COMPARISON BETWEEN STANDARD AES AND MODIFIED AES

Test no.	Statistical Test Name	The standard AES		The Light weight AES	
		P-value	Status	P-value	Status
1	Approximate Entropy	0.272	Pass	0.621	Pass
2	Block Frequency	0.050	Pass	0.498	Pass
3	Cumulative Sums	0.876	Pass	0.756	Pass
4	FFT	0.662	Pass	0.810	Pass
5	Frequency	0.433	Pass	0.671	Pass
6	Linear complexity	0.513	Pass	0.802	Pass
7	Longest Run	0.179	Pass	0.375	Pass
8	Non Overlapping Template	0.827	Pass	0.744	Pass
9	Overlapping Template	0.127	Pass	0.400	Pass
10	Random Excursions	0.361	Pass	0.559	Pass

11	Random Excursions Variant	0.311	Fail	0.339	Pass
12	Rank	0	Fail	0.745	Pass
13	Runs	0.132	Pass	0.623	Pass
14	Serial	0	Fail	0.843	Pass
15	Universal	0.069	Pass	0.376	Pass

As shown in the results, the new method has produced more randomness than the standard AES.

7.2 ENCRYPTION AND DECRYPTION

Encryption and decryption time analysis is an important feature for measuring the encryption algorithm performance. Different file sizes are used to measure the execution time for both the encryption and decryption steps and then compared with the standard AES. The results in Table 3 and Figures 10 and 11 show that the new algorithm is faster. The main goal of this dissertation is to provide a faster encryption algorithm for encrypting and decrypting data that will be transformed over the internet.

TABLE.3: ANALYZING THE ENCRYPTION AND DECRYPTION PHASES OF LIGHTWEIGHT AES

File size	**Standard AES**		**Light weight AES**	
	Encryption	Decryption	Encryption	Decryption
10000KB	4726	5530	1260	2810
20000KB	5387	6328	2098	3260
30000KB	6100	7649	3798	4090
40000KB	7742	8624	4690	5140
50000KB	8211	9743	6030	6450

On average the encryption time of lightweight AES is less than the standard AES by 2858 milliseconds while the decryption process is less by 3225 milliseconds.

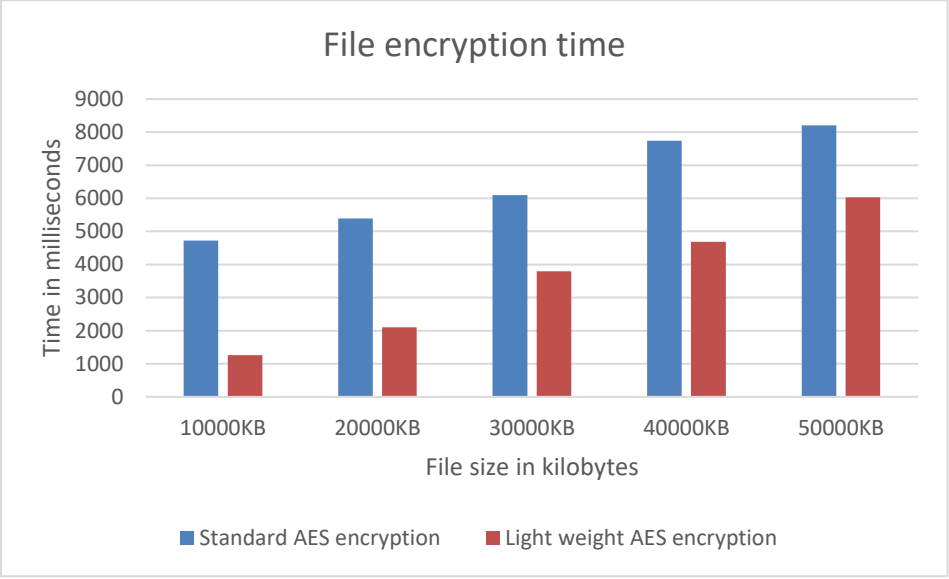

FIG. 10- THE ENCRYPTION TIME FOR DIFFERENT FILE SIZES

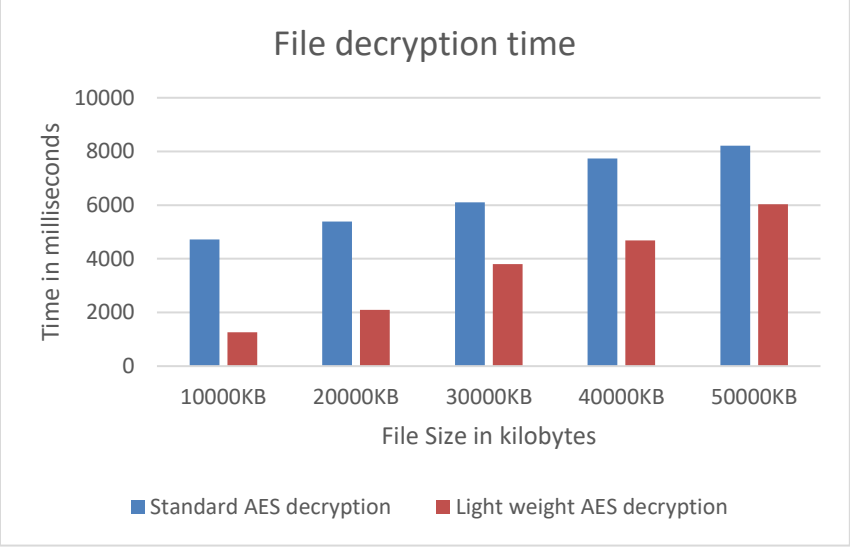

FIG. 11- THE DECRYPTION TIME FOR DIFFERENT FILE SIZES

7.3. MEMORY SPACE UTILIZATION

Analyzing CPU memory using different file sizes shows that the lightweight AES uses less memory than the standard AES during the encryption process. The analysis of memory usage is shown in Figure 12 and table 4.

TABLE.4: MEMORY UTILIZATION FOR ENCRYPTING FILES OF DIFFERENT SIZES

CPU utilization for different file size					
File size	10000KB	20000KB	30000KB	40000KB	50000KB
AES	4232445	4709445	5497823	5434024	6008559

Light weight AES	3188566	3466432	3800123	4255876	4733201

The CPU utilization is increased in the modified AES by 1297620 as average to the standard AES.

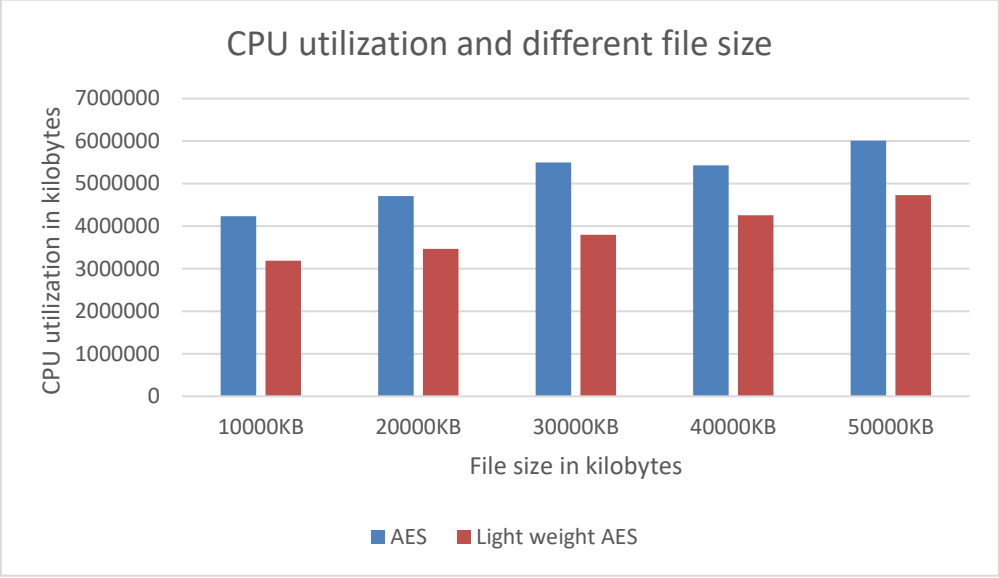

FIG. 12- MEMORY UTILIZATION OF THE ENCRYPTION PROCESS FOR DIFFERENT FILE SIZES

In addition, the memory space that is used during the decryption process in lightweight AES is less than that used by the standard AES. This is shown in Figure 13 and Table 5 The previous results showed that the lightweight AES is better at utilizing CPUs than the standard AES.

TABLE.5: MEMORY UTILIZATION FOR DECRYPTING FILES OF DIFFERENT SIZES

CPU utilization and different file size					
File size	10000KB	20000KB	30000KB	40000KB	50000KB
AES	4499130	4991030	5610998	5849331	6214445
Light weight AES	3911033	4188970	4456991	5076798	5223344

It is obvious that the CPU utilization is increased in the modified AES by 961560 as average to the standard AES.

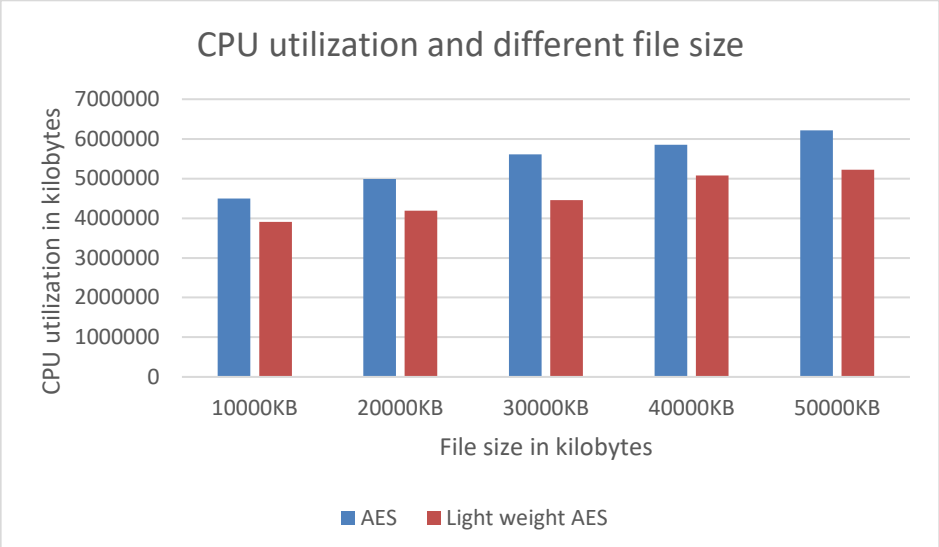

FIG.13- MEMORY UTILIZATION OF THE DECRYPTION PROCESS FOR DIFFERENT FILE SIZES

7.4. AVALANCHE EFFECT

The avalanche effect is a feature of encryption algorithms in which a change in one bit of plaintext causes several bits of the ciphertext to change. The avalanche effect is computed as follow:

$$\text{Avalanche effect} = \frac{No.of\ bits\ flipped\ in\ the\ ciher\ text}{No.of\ bits\ in\ the\ cipher\ text} \quad \ldots\ldots\ldots 1$$

Table 4.5 shows the result of the avalanche effect of the standard and the modified AES. The tests have carried out by altering one bit of plaintext, either the last, first, or middle bit. Although, the avalanche effect of an encryption technique is dependent not only on the complexity of the algorithm but also on the key and plaintext, the modified AES created a stronger avalanche effect than the conventional AES, based on the results. The security level of the method is improved by a high avalanche effect. The results of the avalanche test results comparison between the standard and the modified AES are shown in table 6.

TABLE.6: AVALANCHE EFFECT RESULT

Plaintext	The ciphertext (AES)	%	The ciphertext (Modified -AES)	%
1110001111111111	**2jhlfv483jhsd4khgsja7op349f93jsv**	**46.67**	**158c023be5d70c50545f3d61607a860c**	**59.83**
0110001111111111	**a8hfry49cfbrjvfdsivgresd39586fjd**	**61**	**1771755582db80b309fc0457ab25d380**	**76**
0110001111111111	**nvhdyr053ufjlgjfhe7g4y560yokghdg**	**48.93**	**82db80b2aa8b0cbfd7b466d309fc0457**	**60.59**
0110001111111110	**vdk3islpea98dmxl2tmnz8usuw92ort1**	**60**	**4b4a6e0642692a02802699fee75d0f25**	**77**
1000111123456789	**jdkfli83bc7wux038d7fhhfy7e383292**	**43.01**	**8cdb801eb884a4f793ddb42b6a937897**	**54.62**
0000111123456789	**sa89dgew6tfrejhddfgg093jfuryewid**	**57**	**f7f37dc2e2b9d7cbf4870c90b20b4e70**	**69**

A1B2DDE3245BC6F9	3mvbeu8eu3fnvkfjrue83w22bmto9utu	42.51	4a247aed6aa93193890ef3478285ceb5	53.78
A1B2DDE3245BC6F8	ikv48etyos9234mncc4dclffgnbbgtr4	55	9557144b4a6e06e75d0f251fb253e980	67
98766612345678900	jd83la9dg3uc3ty9o3iqwf5mnp781lsn	40.81	ffb27b9f9e74b0781b90d2c06f51f213	59.10
98766612345678911	kg93i6vhas2qr492kdjfyur8ekfnehdu	66	91d1b68274db79ebb83bda50876854f	75
amjvtrhcpsjhgawl	dje21fp9woj63polmeerfsaaa234399	41.55	c4383d7fbead6f2691b5cc94ebd6efb6	60.80
amjvtrhcqsjhgawl	gh34lk8cmn94ls39gasjh2dkv45uv786	58	9bb1c42692a02802699fead619c975fd	77
abxhskhlerabzskp	1n53sakffe324lkj287mnbzxlsepwqit	50.68	09bcce44b4a6e06e75d0f25828acf496	66.04
abxhskhlirabzskp	rtiyu2349idjsndjgjb09244kaodlkwo	69	e5d70c5050dc4e81be0d9daa545f3d61	85

The avalanche test of the modified AES is increased as average by 14.328 to the standard AES as shown in table 5.

8. Conclusions

The vast volume of data transferred over the internet has necessitated a significant need to secure data, particularly sensitive and financial data, against theft and manipulation. Encryption is one of the most significant and widely used ways for protecting data from theft, but encryption algorithms face a number of challenges, including the time necessary for encryption, which is critical for data carried over the internet.

The suggested agent demonstrated that producing an agent for each client to manage purchase and security tasks is effective in increasing system security and performance, as well as alleviating the problem of system crash, which was the primary purpose of this study. In addition, the network load has grown, resulting in an increase in the number of transactions and clients serviced. As a result, achieve optimal system performance to assure consumer happiness, leading to repeat visits to the same e-commerce website. Agent characteristics are used in a secure e-commerce multi-agent system to ensure high security, high performance, and consumer happiness.

Acknowledgements

The authors would like to thank University of Technology in Bagdad, Iraq, for their cooperation with this study.

References

[1] F. T. A. Hussien, A. M. S. Rahma and H. B. A. Wahab, "Design and implement a new secure prototype structure of e-commerce system," *International Journal of Electrical and Computer Engineering* , vol. 12, no. 1, pp. 560–571 , 2022.

[2] F. T. A. Hussien, A. M. S. Rahma and H. B. A. Wahab, "A secure E-commerce Environment using Multi-agent System," *Intelligent Automation & Soft Computing* , vol. 34, no. 1, pp. 499–514 , 2022.

[3] Asia Ali Al-Karkhi, "Task recovery in self-organized multi-agent systems for distributed domains," *Ph.D. dissertation*, University of Essex, England, 2018.

[4] A.A. Mayyadah, "Providing security for nfc-based payment systems using a management authentication server, "*in 4th International Conference on Information Management (ICIM)*, *IEEE , Oxford, UK,* pp.184-187, 2018.

[5] N.A. Mohd and Z.F. Zaba, "Review of usability and security evaluation model of e-commerce website," *Procedia Computer Science*, vol.161, pp. 1199-1205, 2019.

[6] M.A. Hussain "A study of information security in e- commerce applications," *International Journal of Computer Engineering Science (IJCES)*, vol.3, no. 3, pp.1-9, 2013.

[7] R. Canlas, "Capturing security mechanisms applied to e-commerce :an analysis of transaction security," *International Journal of Security and its Applications* , vol.15, no. 2, pp. 1-10, 2021.

[8] S. Shawon, M. Rahman and R. Luckey, "E-commerce systems security for small businesses," *International Journal of Network Security & Its Applications,* vol. 5, no. 2, pp. 193-210, 2013.

[9] I. AA. Abdul-Jabbar and S. M. Kadhim, " Copyright protection service for mobile images," *Engineering & Technology Journal*, vol. 34, no. 4, pp. 444-450, 2016.

[10] X. Hao, S. Xiao-Hong and Y. Dian**,** "Multi-agent system for e-commerce security transaction with block chain technology, "*IEEE International Symposium in Sensing and Instrumentation in IoT Era ISSI*, Shanghai, China, pp.123-134, 2018.

[11] Y. Huang, J. Debnath, M. Iorga, A. Kumar and B. Xie, "CSAT: a user-interactive cyber security architecture tool based on nist-compliance security controls for risk management, " *IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, USA, pp. 707-697, 2019.

[12] M.I. ALadan.," E-commerce security challenges: a taxonomy," *Journal of Economics, Business and Management,* vol. 4, no.10 pp. 589-593, 2016.

[13] P.D. Shah and R.S. Bichkar, "Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure, " *Engineering Science and Technology, an International Journal,* vol. 24, no.3,pp. 782-794, 2021.

[14] S. Ehikioya and E. Guillemot, "A critical assessment of the design issues in e-commerce systems development," *Engineering Reports*, vol.2, no. 3, pp. 1-24, 2020.

[15] P. Palpunavam, H Foon, T. S. Ono and C.C. Teo, "E-commerce security and identity integrity: the future of virtual shopping," *Journal of Computational and Theoretical Nanoscience*, vol. 23, no. 8, pp. 7849-7852, 2017.

[16] Tarek Helmy, " COLLABORATIVE MULTI-AGENT-BASED E-COMMERCE FRAMEWORK," International Journal of Computers, Systems and Signals, Vol. 8, No 1, pp. 3-12,2007.

[17] Faiz Al-Shrouf1, Aiman Turani2, and Khalil Al-Shqeerat, " Software Agents for E-Commerce Data Workflow Management," J.M. Zain et al. (Eds.): ICSECS 2011, Part II, CCIS 180, pp. 96–106, 2011.

[18] Sougata Khatua*1, Zhang Yuheng 2, Arijit Das 3 and N.Ch.S.N. Iyengar, " A MULTI AGENT BASED E-SHOPPING SYSTEM,", Journal of Global Research in Computer Science , Volume 2, No. 4, pp. 44-54, 2011.

[19] Bala M. Balachandran and Masoud Mohammadian, "DEVELOPMENT OF A FUZZY-BASED MULTI-AGENT SYSTEM FOR E-COMMERCE SETTINGS ," Procedia Computer Science 60 (2015) 593 – 602.

[20] Y. Hedin and E. Moradian, "Security in multi-agent systems," Procedia Computer Science, vol. 60, pp. 1604 – 1612, 2015.

[21] A. G. Briones, P. Chamoso and A. Barriuso," Review of the main security problems with multi –agent systems used in e-commerce application," Advances in Distributed Computing and Artificial Intelligence Journal, vol. 5, no. 3, pp. 55 – 61, 2016.

[22] M.P. Gupta and A. Dubey, "E-commerce study of privacy, trust and security from consumer's perspective," International Journal of Computer Science and Mobile Computing, vol. 5, no. 6, pp. 224-232, 2016.

[23] N. Cooharojananone, K. Akasarakul, T. Wongkhamdi, P. Pruetthiwongwanich and K. Atcha, "The study of the local community products (otop) website characteristics toward buyer decision using eye tracking," IEEE 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, pp. 411-416, 2018.